CHAPTER 5

EFFICIENT NODE COOPERATION AND SECURITY IN MANET USING CLOSENESS TECHNIQUE

5.1 INTRODUCTION

A MANET does not wait on any eternal infrastructure. In description, all networking utilities nodes for routing and mobility management. Mobility management is accessed in a self-organizing manner. On the other hand, it is rigid to support cooperativeness among the nodes for their own restricted resources that require to be conserved. These scrupulous nodes which are also termed as selfish nodes decline to help other nodes in forwarding packets owing to the anxiety of saving resource. Several researches design a new method that aims at attaining confidentiality of the location for an efficient communication. The privacy appears from the mobile network and users expand the control over disclosure of their locations.

Bu et al (2011) designed, combined continuous user authentication and intrusion detection in high security mobile ad hoc networks using Value Iteration Algorithm (VIA) to provide security to MANET. But the value iteration-based solution for computing the Gittins Index only works for a MANET with a small number of nodes and states. For a large network with a variety of nodes, the value iteration based solution becomes computationally intractable and is inefficient in providing security to nodes. Another method proposed by Dong et al (2011), On-Demand Multicast Routing Protocol (ODMRP) using a High-Throughput metric (ODMRP-HT) is capable in
providing high throughput but the efficiency in improving security in terms of quality is lower.

In this work, a closeness mechanism accepted from the assumption of small-world event or also termed as degrees of separation to persuade cooperativeness among nodes in a trusted node’s community is proposed. The research work also provides some general idea on establishing a better security on the trusted MANET community by adapting security features of trust. The simulation of the proposed Efficient Node Cooperation and Security (ENCS) in MANET work is done for varying topology, node size, attack type and intensity with different pause time settings. The ENCS provide efficient node cooperation, clustering and performing closeness technique with large number of nodes. In addition, ENCS supports better security in MANET and outperforms well even when the numbers of malicious node are high. The performance evaluations are carried over in terms of packet transmission efficiency, average information leakage, average cost and security level compared with an existing VIA and ODMRP-HT.

5.2 VULNERABILITIES OF THE MOBILE AD HOC NETWORKS

MANET is infrastructure less network as defined before. Due to its structural characteristics, the mobile ad hoc networks are more vulnerable than the traditional wired networks. Security is a difficult task to preserve the packet in the MANET than in the wired network. The lists of various vulnerabilities that survive in the MANET are elaborated below.

5.2.1 Lack of Secure Boundaries

The sense of this vulnerability is self-evident. The vulnerability occurs due to unclear secure boundary seen in the MANET. The boundaries
in the MANET network are compared with the plain line of protection in the traditional wired network. This vulnerability originates from the character of the mobile ad hoc network like freedom to attach, detach and travel inside the network.

In the wired network, intruders get physical access to the network medium, or even travel through several lines of protection such as firewall and gateway before inflicting malicious behavior to the destinations. But, in the MANET, there is no need for an intruder to obtain the physical access to stay in the network.

Once the attacker is in the radio range of nodes in the MANET, it interacts with those nodes in its radio range and thus joins the network automatically. As a result, the MANET is unable to offer secure boundary to protect the network from some energetic dangerous network accesses.

Lack of secure boundaries builds the MANET vulnerable to the attacks. The MANET undergoes all-weather attacks. The weather attacks force any node in the radio range of any node in the network at any time and aim to any other node in the network. The security of the MANET is affected more badly as there are various attacks endanger the network and make it even harder for the nodes in the network to defend against the attacks. The attacks generally consist of passive listening, active interrupting, data interfering, message repeat, and message corruption, denial of service and leakage of secret information.

5.2.2 Threats from Jeopardize Nodes Inside the Network

The previous subsection argues that the vulnerability due to lack of clear secure boundaries in the MANET leads to several link attacks. These link attacks lay their importance on the links between the nodes, and attempts
to execute some malicious behaviors to make damage to the links. But, there are some other attacks that intend to increase the power over the nodes by some unrighteous means and then use the jeopardized nodes to perform additional malicious actions. This susceptibility is viewed as the threats that come from the jeopardized nodes inside the network.

Since mobile nodes are self-directed units that connect or disconnect the network with freedom, it is difficult for the nodes to execute some successful rules to maintain the feasible malicious activities from all the nodes it interact with. Because of the behavioral diversity of different nodes the transmission of packets is further difficult. Additionally, due to mobility nature of the ad hoc network, a cooperated node often modifies its attack goal and makes malicious activities to various nodes in the network.

Thus, it is very complex to follow the malicious activity executed by a jeopardized node particularly in a large scale MANET. Therefore, threats from jeopardized nodes inside the network are extreme and highly dangerous than the attacks from outside the network. The inside attacks are much complex to perceive as they come from the jeopardized nodes, which behave well before they are endangered.

A good example of inside attack threats comes from the possible Byzantine failures attacked in the routing protocol for the MANET. Byzantine failure occurs when a set of nodes are suspected in the network. The efficient node cooperation between the nodes in the ENCS is such a way that the inaccurate and malicious activity is straightforwardly detected.

Because of the cooperation among these suspected nodes, the execution of malicious activities are highly detected. The cooperated nodes apparently perform healthily. In addition, the cooperated node essentially utilizes the defects and variation in the routing protocol to gradually demolish
the routing fabric of the network. The suspected node promotes new routing information that holds missing link, gives false link state information, or even floods other nodes with routing traffic. Because the suspected nodes are not easily recognized, their malicious activities are prone to be unobserved by other nodes. Therefore, Byzantine failure is very harmful to the MANET without node cooperation.

The above descriptions show that the threats from jeopardize nodes inside the MANET needs additional attention. Additionally, the trust on mobile nodes and infrastructure of any node in the network is undesirable even if it performs well before it is compromised.

5.2.3 Lack of Centralized Management Facility

MANET is an autonomous network without a centralized piece of management equipment such as a server. The unavailability of central piece of organization leads to some vulnerable problems.

First of all, the non-existence of centralized management equipment creates the detection of attacks a very hard problem as it is not simple to observe the traffic in a highly energetic and large scale MANET. It is quite frequent in the MANET that benign failures, such as path breakages, broadcast harms and packets dropping occur regularly. As a result, malicious failures are more complex to detect, particularly when adversaries alter their attack outline and their attack destination in various periods of time.

For each of the losses, as it can only monitor the failure that happens in it, this short-time examination cannot make a believable conclusion that the breakdown is caused by an attacker. But, quite simple to examine from a system point of view that the attacker has performed such a large quantity of misbehaviors that is securely conclude that all of the failures
caused by this attacker should be malicious failure instead of benign failure. From this example, it can be concluded that lack of centralized management machinery causes various problems when the attacks in the ad hoc network is detected.

Secondly, absence of centralized management equipment blocks the trust administration for the nodes in the MANET. In MANET, all the nodes are needed to cooperate in the network process, as no Security Association (SA2) is understood for all the network nodes. Thus, it is not helpful to make an a priori classification, and as a result, the common attempt of establishing a line of resistance, which differentiates nodes as trusted and non-trusted, cannot be attained in the mobile ad hoc network.

Thirdly, some algorithms in the MANET depend on the cooperative participation of all nodes and the infrastructure. The lack of centralized management and decision making in MANET directs to decentralize, so the attacker make use of this vulnerability and present some attacks to crack the cooperative algorithm proposed by Guan et al (2012).

In one word, the lack of centralized management equipment reasons susceptibility that controls numerous features of operations in the MANET. An efficient technique is required to deal with the lack of centralized management problems.

5.2.4 Restricted Power Supply

Due to the mobility of nodes in the MANET, it is frequent that the nodes in the MANET depend on battery for the purpose of power supply method. While the nodes in the wired network do not depend on the power supply trouble as they receive electric power supply from the channels, which usually indicate that their power supply should be roughly unlimited. The
nodes in the MANET necessitate considering the controlled battery power, which leads to several issues.

The primary difficulty caused by the restricted power supply is Denial-of-Service attacks proposed by Shu et al (2010). Since the attacker identifies that the destination node is battery-restricted, either it endlessly sends extra packets to the destination and requests it routing individuals extra packets, or it makes the destination to be fascinated in some manner of time-consuming calculations. By these, the battery power of the target node is consumed by these worthless tasks, and thus, the destination node is out of service to all the kind service needs as it has run out of power.

Additionally, a node in the MANET performs in a selfish way when it discovers that there is only restricted power supply. The selfishness reasons some troubles when there is a requirement for this node to cooperate with other nodes to hold some functions in the network. The difficulty in power restriction is considered in ENCS with the operational behavior of clustering neighboring nodes in monitoring node all time to observe the abnormal behavior in the network traffic for the entire cluster.

But, an important precondition for ENCS technique is that every node in the cluster is prepared to take their task in monitoring node and supply to all other nodes in a period of time interval. There are some nodes that perform selfishly and unlike to cooperate in the monitoring node selection process. The selection process becomes a failure on the presence of too many selfish nodes.

Furthermore, not all the selfish nodes are malicious nodes. Some nodes meet restricted power supply problem and thus behave in a selfish manner. The selfish behavior is tolerable but there are some other nodes that purposely broadcast it, runs out of battery power and so do not desire to
cooperate with other nodes in some cooperative operation. But essentially, this node still has sufficient battery power to carry the cooperative operation. In a word, selfish behaviors should not be observed as malicious behaviors, but necessitate knowing if the selfishness is really caused by the restricted battery power, or by the intended non-cooperation. ENCS is planned in a way to affect DoS attack by eliminating selfish nodes.

5.2.5 Scalability

At last, the scalability problem is addressed in the list of vulnerabilities in MANET. Unlike the traditional wired network the scale is normally predefined when it is intended and the scale of the ad hoc network remains varying all the time. Because of the mobility of the nodes in the MANET, it barely calculates the number of nodes. As a result, the protocols and services that are functional to the MANET such as routing protocol and key management service are well-matched to the constantly varying scale of the MANET, ranging from decades of nodes to hundreds of nodes, or even thousands of nodes.

From the above discussion, it is concluded that the MANET is insecure by its nature. There is no such obvious line of resistance because of the freedom for the nodes to connect, disconnect and travel inside the network. Some of the nodes are compromised by the attacker and thus, make some malicious activities that are inflexible to detect. Lack of centralized equipment causes some troubles when there is requirement to have such a centralized administrator.

Restricted power supply leads to some selfish problems and incessantly varying scale of the network set higher needs to the scalability of the protocols and services in the MANET. As a result, compared with the wired network, the MANET needs more healthy security scheme to ensure the
security of it. In the next section, ENCS elaborates the security solutions to security related problems and improves the security environment in the ad hoc network.

A MANET comprises of self-directed mobile nodes that are liberated to roam subjectively with no central controller for instance router to establish the communication paths. Each node in the mobile ad hoc network relies on each other so as to promote packets. This sort of MANET needs mobile nodes to contain good collaboration with each other to make certain that the commenced data communication process is a success. On the other hand, it is not simple to support cooperation as there are existing nodes with selfish behavior in the network.

The selfish behaviors on nodes are forced to protect their own partial resources for example battery energy, time and bandwidth in MANET. These nodes are very calculative as they use other nodes possessions for their broadcasts but hesitate to split their resources to assist other nodes processes. This phenomenon is common because there is no middle controller or essential authority in MANET.

In a wireless network, a communication range of node will frequently not face the whole network, so end-to-end transmission might require routing information during some nodes. So, ad hoc networks are termed as multi-hop networks, where a bound is a straight link among two nodes. In an ad hoc network, nodes are referred to as routers or terminals. Since ad hoc network is an environment without infrastructure, the co-operation among the routers is worst.

Since they are independent of each other, the problem might arise in the routing framework. The nodes are also being misbehaved. These types of nodes are referred to as selfish nodes, when selfish nodes in the network
increases, then lifespan of the network will automatically decrease. The main solution to address these problems is secure routing.

Even though, the node’s precision to remain its resources at fine performance for its individual data communication operation, where that type of activities will carry no good to the successful of MANET operation. For a particular node to drive or accept packets, the assistance of every connecting node is very vital. If all nodes in a distinct MANET environment perform selfishly, the outcome of such problem will guide to zero throughput.

In MANET, environments which rely seriously on nodes contribution, the reality of selfish nodes would involve the triumphant of a packet communication. Since the trouble is processed by the authoritative internal nodes, even with the consumption of the best cryptographic method will not resolve the problem. Thus, there is a requirement to propose a resolution that could promote the cooperation among nodes. MANET is typically self-organized networks and transitional nodes broadcast the uninterrupted communication. To attain this, each node depends on its neighbor to pass the packet to the target. In fact, most of preceding revises on MANET has absolutely unspecified that nodes are supportive.

As such, the concern of node cooperation becomes very imperative in MANET. Nevertheless, cooperation is made harder to implement in MANET than in communications based networks owing to numerous reasons. At initial stage, nodes can subjectively connect or depart the network. Second, recognition of naughtiness and consequent separation of a misbehaved node has to effort in a dispersed method owing to lack of central control.

Finally, user precise requirements or approach should not be overlooked. Some users observe their power resource as being restricted by battery life, and consequently they may not believe disposed to transmit track
for other users. As such, a user's performance will blow the system performance determined by his relevance needs or substantial constraints. This study presents a technique to diminish the trouble of containing selfish nodes in MANET known as closeness mechanism that is agreed from the premise of event to promote cooperativeness among nodes in a trusted environment.

5.3 ACHIEVING COOPERATION AMONG NODES

Cooperation among nodes in MANET is inflexible to be completed owing to the existence of self-centered nodes that do not desire to place their restricted resources like battery power, CPU and bandwidth at risks. It vigorously concerns them in a packet transmission operation. For instance, a selfish node merely crash packets that are anticipated to be thrower to other nodes as serving forwarding those packets disgraces its resource. The occurrence is obligatory in closeness technique since each node has its individual right to do so as there is no essential organizer in MANET environment to inform each node about the process of cooperation. Consequently, a network operation is paralyzed as MANET relies deeply on intermediary nodes to promote packets till end of process. Nevertheless, the cooperation between nodes in MANET is confident with the utilization of appropriate mechanism.

Closeness technique from diminutive world event diminishes the selfish node’s trouble effectively in MANET. The elimination of selfish nodes avoids the DoS attacks, a limitation, which was designed by Shu et al (2010). The closeness technique is processed by generating common trust between nodes before they enter the network path. The common trust among nodes is fashioned by enclosing physical associations in advance which are recognized along with the relationships prepared by a particular mobile node’s in the network. Closeness technique presented a mobility replica depending on the
association of mobile devices approved by individuals into the network. It represented the behavior of the nodes in the network by moving in groups that present a structure of relationships, therefore, capable to forecast the association pattern of nodes based on the decisions carried out by the trust values.

The same notion is processed in this closeness mechanism whereby the construction of relationships among nodes is done based on the communications made by the users who institute common trust with each other. All the nodes’ relationship uniqueness will then be processed by individual nodes to create initial trust. Nodes that have been surrounded in the closeness mechanism are extremely cooperative with each other owing to the primary trust element that has been formed in advance.

By adapting ENCS mechanism, nodes are permitted to promote packets simply amongst trusted nodes in the group. As for that, nodes are not be able to assist other unidentified nodes that are not in the nodes trusted list as they are surrounded in the ENCS mechanism policy. The nodes are punished for being selfish owing to the opposition to cooperate with other nodes which are not in the similar group of nodes, but owing to they are appreciative to pursue the rules of the group nodes they are belong to, they are tagged as behave badly and therefore will not be punished. The careful forwarding activities such as transmit packets only among nodes are not only capable to avoid them from being punished but also set aside nodes’ resources.

5.4 ENHANCING SECURITY OVER MANET

The closeness mechanism, though afforded a secure proposal for nodes to transmit with the organization of primary trust, is still facing some security threats particularly in managing compromised nodes. It is feasible for
the neighboring nodes in the trusted list to be cooperated as there are many new security attacks. The security method by adapting features on every node symbolizes all nodes in the network with the evidence properties in the relevant nodes relationships organization process to produce a trusted MANET community. To accomplish security in MANET, numerous features are utilized. The security features are classified into two major categories namely performance metrics evaluation and quantitative trust value.

In performance metrics evaluation group, the effectiveness of chosen features utilized are accessed by employing definite metrics such as route detection time, routing traffic, routing overhead and number of data packets distributed. When a source node needs to promote packet to its destination, it requests its neighboring nodes to propose their feature’s attribute number for inspection. If the neighboring nodes handle to present an attribute number that accomplishes the source node’s constraint, the attribute number will be implanted in the packet format and the node is decided to promote the packet to other neighboring nodes earlier than attaining the vital destination. The effectiveness of packet forwarding process based on selected features are measured based on secure transmission from the source to destination in a less interval of time.

5.5 EFFICIENT NODE COOPERATION AND SECURITY IN MANET USING CLOSENESS TECHNIQUE

The ENCS work is efficiently designed for enhancing cooperatives of the nodes and secure communication over MANET by adapting the closeness technique. The ENCS method for node cooperation and security using closeness technique in MANET comprises of three operations.

Figure 5.1 illustrates the process involved in ENCS using closeness technique. The first process is evaluating the cooperativeness range of the
nodes in the network. The second process is attaining the process of node cooperativeness in the network. The third process is to enhance the security of the nodes in the network.

The initial process in evaluating the cooperativeness of each node in the MANET is done based on the behavior and activities of the node done while the communication is taking place between the nodes in MANET. The monitoring of the behavior of nodes is carried out based on the cooperativeness of the nodes assumed. The weightage of the cooperativeness of each node is computed based on the spatial events occurring at different aspects of communication. The second process is to attain the cooperatives of the nodes in the mobile ad hoc network.

The third process describes about closeness technique that are able to motivate more cooperation between the nodes in a MANET environment. The closeness technique is adopted from the theory of diminutive world occurrence with six degrees of linkage. The process of recommending trust is carried on until each person attains the utmost level of the sixth degree of linkage.
Figure 5.1 shows that a clustering process is presented based on reputation and ranking system in an ad hoc network. The reputation system is enabled to allow nodes to construct informed choices regarding which nodes to assist with or prohibit from the network. To enhance the cooperativeness of the nodes, self organization of nodes is done harmoniously. For secure communication, the network is clustered using the Closeness technique, which diminishes selfish nodes.
communication, closeness technique is presented to improve the security and cooperation of nodes in the network.

The expansion number of nodes is high, since the ENCS mechanism processes a unidirectional trust association as an alternative of bidirectional association. A unidirectional association reveals that a distinct node merely trust any node that it would similar to the situation of containing the entrusted nodes in the network. For instance, node A authenticate node B in a unidirectional method devoid of containing node B’s approval. In unidirectional idea, this is measured as one preliminary trust association where as for bidirectional thought; node B must authenticates node A in return, only then one primary trust association is measured and created. The described notions can be further processed as shown in Figure 5.2 and Figure 5.3.

Figure 5.2 show a unidirectional association to node B. The node does not surround trust to node A in return to generate a trusted association. Trusted relationship among the nodes is measured since, node A’s right to authenticate either node it needs devoid of having to be trusted in return.
On the other hand, Figure 5.3 shows a bidirectional association needs of nodes A and B to authenticate each other so as to generate one trusted connection.

The idea of the ENCS mechanism is the recommendation of nodes around the network. The trusted value ranges in closeness technique increase the nodes cooperativeness of a trusted society. In security characteristic, even though the work does not affect any vital authority, the security is conserved in such a way that any two nodes are desired to contain a trusted value range before they launch a trust association with each other. The situation of closeness technique comes with the statement that all trusted nodes will not contain any disobedient property at all, because all involving nodes contain 100 percent reliability with each other.

5.5.1 Algorithmic Flow of ENCS Mechanism

Efficient node cooperation and security in MANET are found for varying topology, node size, attack type and intensity with different pause time settings. The ENCS mechanism algorithmic steps are shown below

**Input:** Nodes, N₁, N₂, N₃,…,Nₙ, Threshold Value t, Reputation Table RT

**Step 1.** Start

**Step 2.** Identify best t(Nₙ) node in MANET

**Step 3.** For each packet data,

**Step 4.** Check selfish nodes from Nₙ nodes

// Reputation System

**Step 5.** For each Nₙ

**Step 6.** Assign a rank R(Nₙ) based on RT(Nₙ)

**Step 7.** Group the nodes Nₙ based on t(Nₙ), R

**Step 8.** Choose the cluster head CHᵢ
Step 9.   End for
//Closeness Mechanism
Step 10.   For each node identify the weight $W_i$
Step 11.    Cooperative node formation $C_i$
Step 12.   End for
Step 13.   For inspection
Step 14.   Utilize feature’s attribute number $AN_i$ for validation
Step 15.    Security feature selection (FS)
Step 16.    Form a secure channel
Step 17.   End for
Step 18.   End for
Step 19.   End

Output: Secure Node Cooperation in MANET

The above algorithm describes the reputation mechanism on the nodes $N_1$, $N_2$, $N_3$,....,$N_n$ in MANET with threshold value $t$. The reputation system assigns the rank to the nodes based on most visited node i.e., the cooperation provides nodes. The selfish nodes are removed as on the checking process performed in the system. The similar numbers obtained in the ranking are grouped together in MANET. The grouped nodes based on rank are chosen as a cluster head $CH_i$.

The closeness mechanism in mobile ad hoc network forms a cooperative nodes $C_i$ by removing the selfish behavior nodes. The set of nodes $N_1$, $N_2$,...., $N_n$ identify the weight age for the cooperativeness of node formation. The inspections are performed on packet flow based on feature attribute number and validated by selecting the particular features to form a secure channel. The closeness mechanism developed an effective cooperativeness and secure channel in MANET.
5.6 PERFORMANCE EVALUATION

The node cooperativeness estimation and security using closeness technique are efficiently done through evaluating the cooperative rater. To estimate the performance of efficient node cooperation and security in MANET, simulations are run on a Linux machine having a P4-3.4GHz processor with 2GB of memory. ENCS efficient node cooperation and security in MANET implemented in NS-2 environment. The simulation area extents 900x900 m², in which nodes move from a random starting point to a random destination, with speeds of 3, 6, 9 m/s and a pause time of 3 to 5 seconds. At first, the nodes cooperativeness is identified based on the behavior and activities of the nodes in the network environment using closeness technique, after evaluating the cooperativeness value, the nodes are reorganized in a same way.

Then the node clustering is done based on the directional trust range values of the neighboring nodes. Since the node clustering is performed based on weightage of cooperativeness scheme, the clustering process is an efficient one. Then, the communication among the nodes is also being good compared to an existing secure key model framework. The performance of the efficient node cooperation and security in MANET is measured in terms of, average information leakage, packet transmission efficiency, security level and average cost.

Average information leakage rate during transmission of packets is defined as the data exposed and is compared with existing model proposed by Bu et al (2011). The level of cooperation extended by the node towards the MANET functions removes the misbehavior of selfish nodes increasing the security level. Node cooperativeness means that a node must not behave selfish in mobility model. This behavior speeds up the movement of nodes inside the network enhancing security. The security level is defined as the
amount of security given for the fulfillment of an obligation using closeness mechanism (i.e.) the information flow from the source to destination in mobile ad hoc network system. It is measured in terms of percentage (%). The security method by adapting features on every node symbolizes all nodes in the network with the evidence properties.

Packet transmission efficiency is defined as the method of network data transmission, in which small blocks of data, or packets, are transmitted over a channel in mobile ad hoc network using the closeness mechanism. Transmission of standardized packets of data over transmission lines rapidly with high-speed switching enhancing the transmission time taken compared with ODMRP-HT designed by Dong et al (2011). Average cost denotes the number of packet transmission between the source and destination.

5.7 RESULTS AND DISCUSSION

ENCS method shows how a secure communication is done based on the closeness technique for node cooperativeness range. Bu et al (2011) proved that the existing structural results for combined continuous user authentication and intrusion detection in high security mobile ad hoc networks provides Value Iteration Algorithm (VIA) security to MANET. But the value iteration-based solution for computing the Gittins Index only works for a MANET with a small number of nodes and a small number of states and observation states. For a large network with a variety of nodes, the value iteration based solution become computationally intractable. The ENCS provides efficient node cooperation, clustering and performing closeness technique with large number of nodes.

In addition, ENCS supports better security in MANET and outperforms well even when the numbers of malicious node are high. The
efficiency of ENCS is compared with the existing ODMRP protocol using a High-Throughput metric as ODMRP-HT designed by Dong et al (2011). Even though ODMRP-HT provides high throughput, the efficiency in providing security in terms of quality is lower. The results describe the performance of the efficient node cooperation and security in MANET.

5.7.1 Average Information Leakage

Average information leakage is defined as the rate of revealing information during broadcasting or extraction of information by the adversary. Average information leakage is avoided to a certain level by performing clustering formation bonding the nodes tightly causing less leakage of information. VIA provides less information leakage for a network but faces computational complexity in executing large number of nodes.

Figure 5.4 describes the tabulation for average information leakage. The results also show that the average cost and the average information leakage decrease when the number of available nodes in the network increases from 0 to 100. The reason is that there are more nodes that are selected for authentication and interruption detection, so suspected and low-energy nodes are avoided. Figure 5.4 shows that information leakage remains stable for the first four probabilities and decreases when the system becomes more secure in ENCS. The reason for this is that the ENCS avoid choosing the selfish nodes through closeness technique. When the closeness probability further increases, the average information leakage decreases.
Table 5.1 Average Information Leakage

<table>
<thead>
<tr>
<th>Total Number of Nodes</th>
<th>Average Information Leakage (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VIA</td>
</tr>
<tr>
<td>20</td>
<td>8.06</td>
</tr>
<tr>
<td>40</td>
<td>44.15</td>
</tr>
<tr>
<td>60</td>
<td>11.18</td>
</tr>
<tr>
<td>80</td>
<td>12.55</td>
</tr>
<tr>
<td>100</td>
<td>36.25</td>
</tr>
<tr>
<td>120</td>
<td>20.46</td>
</tr>
<tr>
<td>140</td>
<td>23.91</td>
</tr>
<tr>
<td>160</td>
<td>28.54</td>
</tr>
<tr>
<td>180</td>
<td>34.21</td>
</tr>
</tbody>
</table>

Figure 5.4 Average Information Leakage

5.7.2 Packet Transmission Efficiency

The packet transmission efficiency is measured based on the time required to process the incoming packets from source to destination. Packet
Transmission Efficiency (PTE) measure the performance of packet delivery using the closeness technique, defined by Equation (5.1)

\[
PTE = \frac{DPT_{\text{noattack}} - DPT_{\text{attack}}}{DPT_{\text{noattack}}}
\] (5.1)

DPT indicates the Data Packet Transmission. DPT\text{attack} and DPT\text{noattack} represent DPT when the network is under attack and not under attack, respectively. Thus, data packet transmission efficiency captures the cost (number of data packet transmissions) per data packet received.

Compared to the existing ODMRP-HT, the ENCS consumes less time to transmit the packet. Since the ENCS presented closeness technique, the trust value of the neighboring nodes are estimated. Based on the trust values, the packets are passed to the nearest nodes in the network.

Figure 5.5 describes the packet transmission efficiency required to broadcast the packets from source to destination in a specified time. The results of the efficient node cooperation and security in MANET are compared with an existing ODMRP-HT (ODMRP protocol with high throughput). ENCS provides better data transmission efficiency with the given number of packets for about 10-15% compared to ODMRP-HT. As source node promotes packet to its destination as per the request of neighboring nodes features attribute number based on inspection.
### Table 5.2 Data Transmission Efficiency

<table>
<thead>
<tr>
<th>Number of Attackers</th>
<th>Cost per received Packet (pkts)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ODMRP-HT</td>
</tr>
<tr>
<td>1</td>
<td>2.61</td>
</tr>
<tr>
<td>2</td>
<td>2.59</td>
</tr>
<tr>
<td>3</td>
<td>2.56</td>
</tr>
<tr>
<td>4</td>
<td>2.49</td>
</tr>
<tr>
<td>5</td>
<td>2.46</td>
</tr>
<tr>
<td>6</td>
<td>2.43</td>
</tr>
<tr>
<td>7</td>
<td>2.37</td>
</tr>
<tr>
<td>8</td>
<td>2.34</td>
</tr>
<tr>
<td>9</td>
<td>2.31</td>
</tr>
</tbody>
</table>

**Figure 5.5 Data Transmission Efficiency**
5.7.3 Security Level

ENCS facilitates high security on estimating the neighboring node trust values. Based on the trust values, the levels of security are recognized. Quantitative trust value inspected using the features attribute number aids in identifying the threats and the security levels which is computed using the Equation (5.2).

\[
\text{Security level} = \frac{\text{Quantitative trust value}_{\text{Feature attribute}}}{\text{Neighboring node trust value}}
\]  

(5.2)

ENCS is compared with the value iteration algorithm in structural results for combined continuous user authentication and intrusion detection in high security MANET proposed by Bu et al (2011). Figure 5.6 is depicted for both VIA and ENCS.

<table>
<thead>
<tr>
<th>Number of Nodes</th>
<th>Security (%)</th>
<th>VIA</th>
<th>ENCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>40</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>42</td>
<td>61</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>46</td>
<td>67</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>49</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>54</td>
<td>74</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>58</td>
<td>78</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>62</td>
<td>81</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>68</td>
<td>86</td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>74</td>
<td>91</td>
<td></td>
</tr>
</tbody>
</table>
Figure 5.6 illustrates the security level, compared to existing VIA, the ENCS has high level of security and the variance is 15-25% high. Since the ENCS supports security by estimating the neighboring node trust values leads to identification of security levels.

5.7.4 Average Cost

Average cost is defined as the number of packets transmitted per unit time. Existing VIA results in high cost since the other sensors make decision based on out-of-date Gittins indices. ENCS aims at increasing the average cost of transmitting data packets.

Figure 5.7 describes the average cost for the given number of nodes. Since the nodes in the reputation table makes better decisions with complete information, the average costs for packet transmission is increased. The results show that the average cost from the value iteration algorithm is less about 10-15% compared to ENCS.
### Table 5.4 Average Cost

<table>
<thead>
<tr>
<th>Number of Nodes</th>
<th>Average Cost (kbps)</th>
<th>VIA</th>
<th>ENCS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>4.23</td>
<td>5.02</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>4.45</td>
<td>5.12</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>4.67</td>
<td>5.24</td>
</tr>
<tr>
<td>30</td>
<td></td>
<td>4.79</td>
<td>5.35</td>
</tr>
<tr>
<td>40</td>
<td></td>
<td>4.87</td>
<td>5.47</td>
</tr>
<tr>
<td>50</td>
<td></td>
<td>5.05</td>
<td>5.56</td>
</tr>
<tr>
<td>60</td>
<td></td>
<td>5.17</td>
<td>5.69</td>
</tr>
<tr>
<td>70</td>
<td></td>
<td>5.23</td>
<td>5.78</td>
</tr>
<tr>
<td>80</td>
<td></td>
<td>5.31</td>
<td>5.84</td>
</tr>
<tr>
<td>90</td>
<td></td>
<td>5.45</td>
<td>5.94</td>
</tr>
</tbody>
</table>

![Average Cost Graph](image)

**Figure 5.7 Average Cost**

At last, the experimental evaluation concludes that the efficient node cooperation and security in MANET proficiently provide a communication framework among the nodes in the network in a secure manner by evaluating the nodes cooperativeness range.
5.8 SUMMARY

ENCS mechanism overcomes the bottleneck of selfish nodes in MANET by creating initial authentication among nodes through node cooperation. The ENCS mechanism is capable of providing high security by avoiding the misbehavior nodes from replacing the security associations with unidentified nodes. Security associations are only replaced with nodes in trusted community, improving the security inside group of trusted nodes. Security associations presented the realization of features in every node inside the group. The selections of security features are done based on the validation of common usage of nodes in the specified network. Experimental results showed that the ENCS mechanism outperforms in terms of packet transmission efficiency, average information leakage, average cost and security level in the range of 15-25% high compared to the existing VIA and ODMRP-HT.