CHAPTER 5

CROSSLAYER UMPIRING SYSTEM DESIGN

5.1 Cross layer umpiring system

A wireless mobile ad hoc network is a dynamic wireless network with the appointment of supportive nodes with an infrastructure of few networks. Multicasting routing is planned for group communication that supports the distribution of information from a source to all the destinations in a group. Problems in ad hoc networks are scarcity of bandwidth, dynamic topology caused by the mobility of nodes and short lifetime of the nodes due to power constraints. A solution for the above problem is provided, through the proposed cross layer approach.

In a cross layer approach, the medium access control layer functionality and the network layer functionality are performed by a single integrated layer. The basic design philosophy behind the multicast routing part of the architecture establishes and maintains an active multicast tree surrounded by a passive mesh within a wireless mobile ad hoc network. Thus, the multicast backbone is a condensed passive mesh woven around a highly pruned tree. Although tree based and mesh based multicasting techniques have been used separately in the existing multicasting architectures, the novelty in this study is the integration and reengineering of the tree and mesh structures to render them highly energy efficient and robust for real time data multicasting in mobile ad hoc networks. Energy efficiency is achieved by enabling the nodes to switch over to sleep mode frequently and by eliminating most of the redundant data receptions.

In this chapter, two enhancements to the basic operation of the ETUS are proposed. ETUS protect only network layer. The most important objective is to design cross layer umpiring system (CLUS) for improving the security system. The objective of

the research work proposed a new framework in CLUS. In this CLUS framework, the research work has introduced three enhancements that include battery status, link status and normal operations of ETUS such as token status and network operation (i.e.,) (i) detecting (ii) quarantining the malicious nodes and (iii) salvaging. In detection, the misbehaving node is traced and identified. Quarantine procedure envisages marking the offending nodes to ensure they do not participate any further in the network activities. Salvaging operations ensure the alternative path. In this chapter, solutions to the first two issues such as battery status and link status are found. The CLUS, Cross Layer Umpiring System being proposed now, handles all the three functionalities successfully.

Extensive simulation studies using Network Simulator helps the study of the soundness of the proposed solution and proof for the robustness of the system. In this chapter, the research study proposed CLUS (Cross Layer Umpiring System) model is explained. The rest of the chapter is organized as follows: Section 5.2 provides an overview of CLUS, Section 5.3 lists the important assumptions made. Section 5.4 describes the details of implementation of CLUS model. In Sections 5.5 simulation studies are described using QualNet and Section 5.6 provides the concluding remarks.

Battery status and link status mechanism are introduced in the cross layer umpiring system. Two distinct situations are considered namely, disruptions during (i) route reply and (ii) data forwarding phases. In the cross Layer Umpiring System (CLUS) a mechanism to handle each of these two situations has been provided. The disruption during route reply phase is now considered. The loss of route reply packets causes a serious impairment to the performance of routing protocol. This is because route reply packets are obtained only after flooding the entire network with RREQs. (Mekesh Singhal et al. 2006) have proposed and implemented the idea of salvaging route reply (SRR) for on demand routing protocols. This may happen because of either a link failure or a battery shortage. The above reasons are very genuine. The nodes affected with

genuine reason should not book, but may treat it as a separate activity. Hence the false positive is reduced.

In this section, a frame work Cross Layer Umpiring System (CLUS) that provides security for routing and data forwarding operations is proposed. In the proposed system the behavior of each node from source to destination is closely monitored by a set of three umpires. If any misbehavior is noticed, CLUS flag off the guilty node from the circuit. The research study has proposed three enhancements to the basic ETUS namely, Link status, Token status and Battery, these as shown in Figure 5.1.

Protocols have the need for accurate information on the link status between neighboring mobile nodes. Token status is changed in the token status misbehaving nodes. Battery Life status helps the choice of good battery strength nodes. The model with these three enhancements is called CLUS. CLUS using AODV protocol has been implemented.

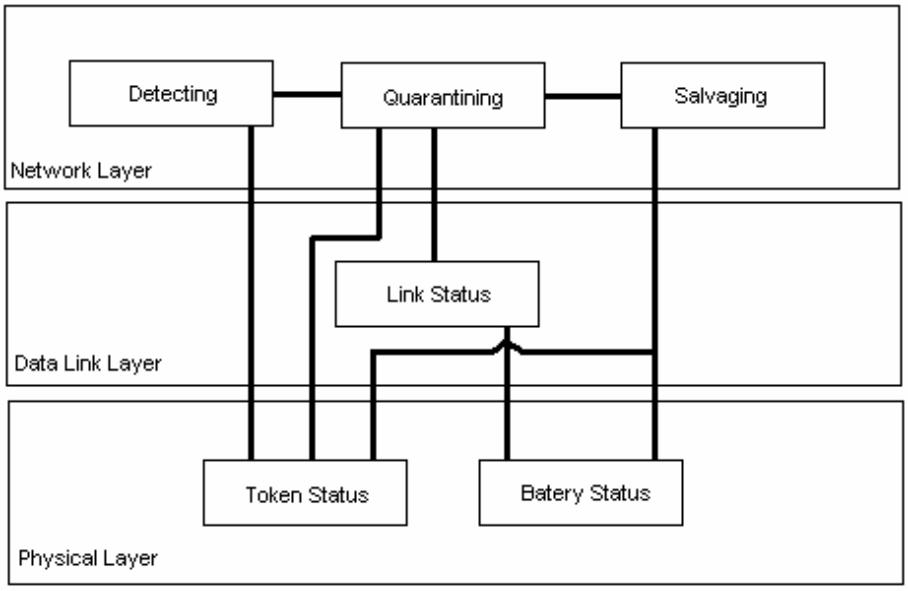

Figure 5.1 Framework of CLUS

5.1.1 CLUS Model

In the Cross Layer Umpiring System (CLUS) a token is issued to each node at its inception which is similar to TBUT and GETUS. The token consists of four fields: NodeID, status, reputation, and battery level. NodeID is assumed to be single and deemed to be beyond manipulation, status is a single bit flag. Initially, the status bit is preset to zero indicating a green flag. Initially the reputation value is zero (i.e.) positive. The token with a green flag and positive reputation is an authorized token issued to each node, which confers the liberty to take part in all network activities.

Each node has to announce its token status bit and reputation value for taking part in any network activity declaring Route Request RREQ. If the token status bit is ‘1’ indicating ‘red flag’ protocol does not allow the node to participate in any network activity. Similarly, if reputation value is ‘1’ indicating ‘negative reputation’ the protocol does not allow the node to participate in any network activity. Like that battery level, more than 50 % alone are allowed to actively participate in the network.

The network layer has two prominent operations namely route identification, and packet forwarding similar to the operations of ETUS. In the forward path, each node during data forwarding monitors the performance of its immediate next node. This way, node A can tell correctly whether node B is forwarding the packet sent by it, by promiscuously hearing node B's transmissions. Similarly, during the reply process RREP, node C can verify whether node B is unicasting the route reply RREP and whether the hop count given by B is correct. Thus, during forwarding path, A is the umpire for node B and node C is the umpire for node B during the reverse path operations.

When a node is found to be selfish with misbehavior say dropping packets, the corresponding umpire immediately sends an M-ERROR message to the source and the status bit of guilty node is set to ‘1’ – red flag using MFlag message and reputation value is set to 1. An additional field next hop, link status and battery status have been

introduced in all routing messages as done in CLUS for accurate correlation of the overhead message. Though, there are several kinds of misbehavior that could be captured by promiscuous hearing, the research work is focusing only selfish actions, dropping packets and not on their transmission.

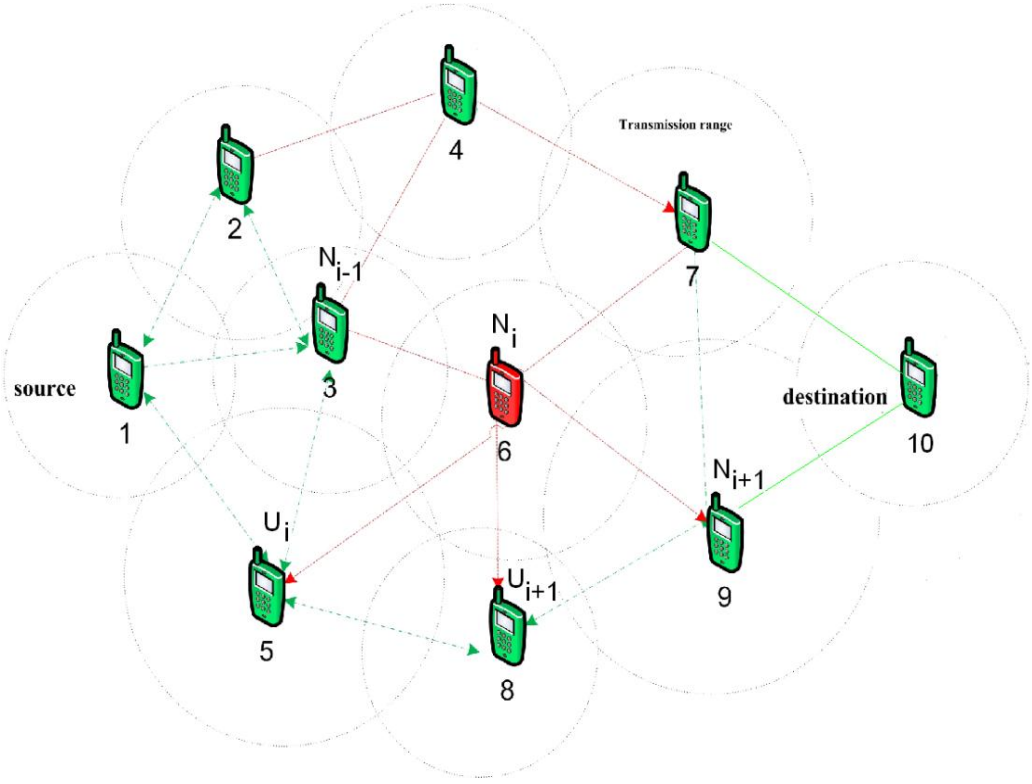

Figure 5.2 CLUS Operations model

To design the safety system is to limit the overhead to the minimum possible, but getting a good development in throughput. Nodes source, Node 1, Node N_{i1}, specified as active path and node N_i node N_m specified as destination paths. Thus there are N_{m+2} nodes in the active path, umpiring node specified as U1, U_2 Ui ,Ui_{+1}, . . U_m and U_{m+1} as shown in Figure 5.2. Umpire Ui is located in the messaging zones of nodes N_i, N_{i1}, Ui_1 and Ui_{+1}. For node $N_{i,}$ the two umpires will be Ui and Ui_{+1}. The third umpire will be N_{i1} in the forward path and N_{i+1} in the reverse path. When N_i is found to be disobedient, say plummeting packets or not forwarding control packets, M- ERROR message is sent to

the source by the umpire node Ui ,Ui_{+1} & N_{i1} in the forward path and N_{i+1} in the reverse path , indicating red flag by MFlag message and then sets the status bit of guilty node N_i to ‘1’and reputation value is set to ‘1’.

The objective of the research study is to design the security system to limit the overhead to as minimum as possible while getting a good improvement in throughput. SCAN system and ETUS with requirements of signatures on the tokens by a minimum of 'k' neighbors, encryption, and periodic renewal of tokens is robust, but at a huge cost of control overhead and energy efficiency.

5.1.2 Route reply phase

CLUS is operational during the route reply phase. The immediate predecessor monitors the performance. If in this phase node N_i misbehaves, and says, announces a wrong sequence number. This is immediately observed by the node N_{i+1} which sets the status bit of N_i to red and starts the RREP salvaging operation. On the other hand, if N_i simply loses the communication link or shortage of battery power with $Ni_{+1,}$ N_i is not booked, they route reply salvaging alone is undertaken.

5.1.3 Data forwarding phase

If node N_i misbehaves during the data forwarding phase i.e. it drops packets, it is observed by nodes N_{i1}, Ui_1, and Ui_{+1}, they send MFlag messages and convict the guilty node, further they unicast messages among themselves to establish an alternative path via N_{i1}, Ui, $Ui_{+1,}$ and$N_{i+1.}$ Self_USS is operational in this segment.

On the other hand, if node N_i goes out of the communication link or shortage of battery power but the umpiring nodes do not receive the hello messages from N_i and simply switch over to an alternative path, thus booking of the innocent node is avoided. Thirdly, umpire Ui may go out of the communication link with Ui_1, $N_{i1,}$ N_i, and $Ui_{+1.}$ In

such a case N_{i1} monitors N_i and N_i monitors N_{i+1} under Self_USS.

5.2 Models and assumptions

In this section, the research work focused on MANET network, security model and the selfish attacks.

5.2.1 Network model

A MANET containing an unhindered number of wireless mobile nodes is considered. For separation between nodes, each node is required to have a unique nonzero identification (ID) number. Assumptions made in the model of Cross Layer Umpiring System (CLUS) are as follows:

1. A MANET where nodes are free to move about or remain at stand still, at their will is assumed.
2. Every node may join or leave the network at any time.
3. Nodes may fail at any time.
4. The source and the destination node are not selfish nodes.
5. Every node in the network has a neighbors list.
6. There is a survival of a bidirectional communication link between any pair of nodes, which is a constraint for most wireless MAC layer protocols including IEEE 802.11 for reliable broadcast.
7. Wireless interfaces support the promiscuous mode of operation. Most of the obtainable IEEE 802.11 based wireless cards helps such promiscuous mode of operations for improvement in the performance of the routing protocol.

The promiscuous mode operation may invite additional communication overhead and energy exploitation to process the transit packets. Energy efficiency is not addressed in this work.

5.2.2 Security Model

MANET is vulnerable to security attacks due to its features of shared radio channel, unconfident open medium, active changing topology and lack of supportive algorithms and centralized monitoring, limited resource availability and physical vulnerability. Attacks on MANET can be classified into two categories namely, active attacks and passive attacks. An active attack effort is meant to destroy or alter data packets and to route messages as a swap in the network. It is harmful to the network security. The passive attack does not interrupt the operation of the network. The focus of the research work is on the passive attack, but the nodes that eavesdrop and record other nodes broadcast are not dealt with the selfish nodes that reject for complete participation in the network routing operations are addressed. The security model proposed by the research work is put into practice on top of the popular AODV routing protocol.

5.3 Simulation Experiments

Simulation studies have been done using QualNet 5. The objective of research work focused on four parameters namely packet delivery ratio, false negatives probability, false positives probability and control overhead when mobility and percentage of malicious nodes vary.

The performance assessment for investigations is based on the simulations of 100 wireless mobile nodes that form a wireless ad hoc network over a square

(1000 X 1000 m) even space. Distributed Coordination Function (DCF) of IEEE 802.11, is a MAC layer protocol used in the simulations. The presentation setting parameters are given in Table 5.1.

Table 5.1 Parameter Setting for CLUS

Property	Values
Simulation Time	600 seconds
Propagation Model	Two rays Ground Reflection
Mobility Model	Random way point
Maximum Speed	0 – 20 m/s
Pause Time	0 seconds
Traffic Type	CBR (UDP)
Payload Size	512 Bytes
Number of Flows	10 / 20 flows
Node Placement	Random
Transmission Range	250 meters
Radio Bandwidth	2 Mbps

Prior to the simulation the research study made an arbitrary selection of a certain portion, ranging from 0 to 40 percent of the network population as malicious nodes. We considered only two attacks namely dropping packets and modifying the hop count. No change was seen in any flow between its source and destination for the life span of a simulation run.

5.3.1 Throughput

In MANET, packet delivery ratio has been accepted as a standard measure of throughput. Packet delivery ratio is the ratio of the numbers of packets received by the destination to the number of packets sent by the sources. Figure 5.3 presents the packet delivery ratios of CLUS with node mobility varying between 0 to 20 m/s.

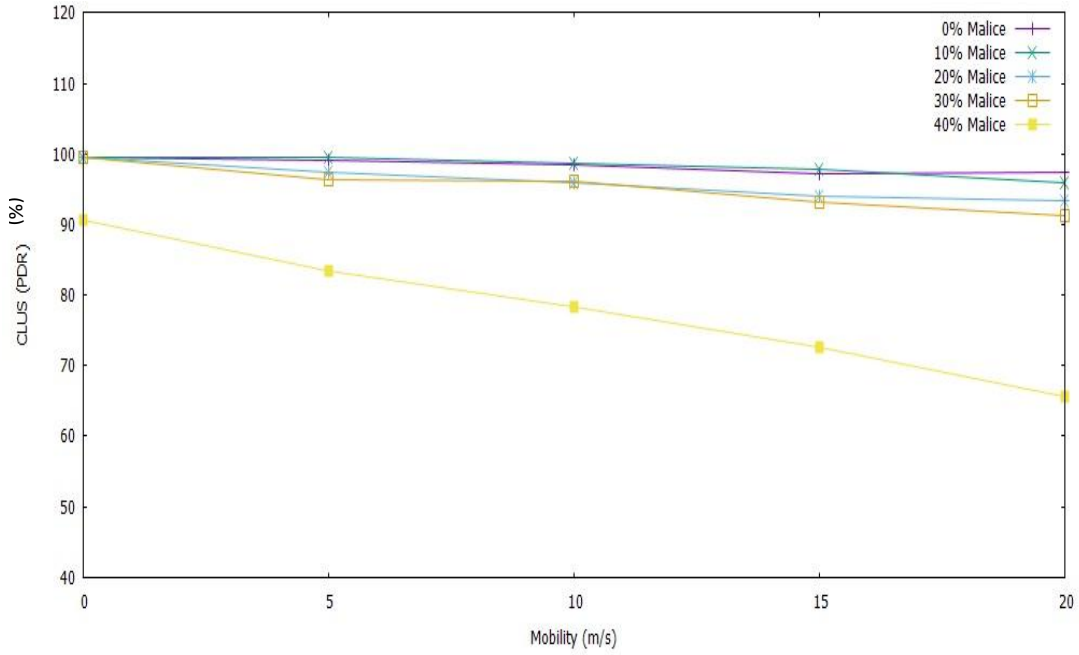

Figure 5.3 Comparison of CLUS throughput with various malicious nodes in percentage

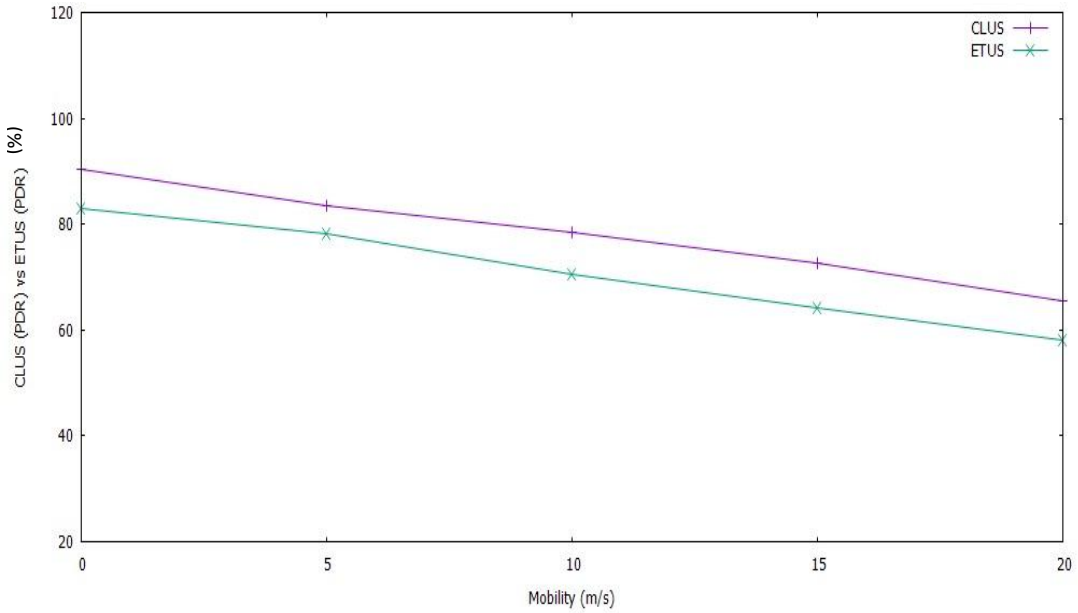

Figure 5.4 Comparison of CLUS and ETUS with 40 % of malicious nodes

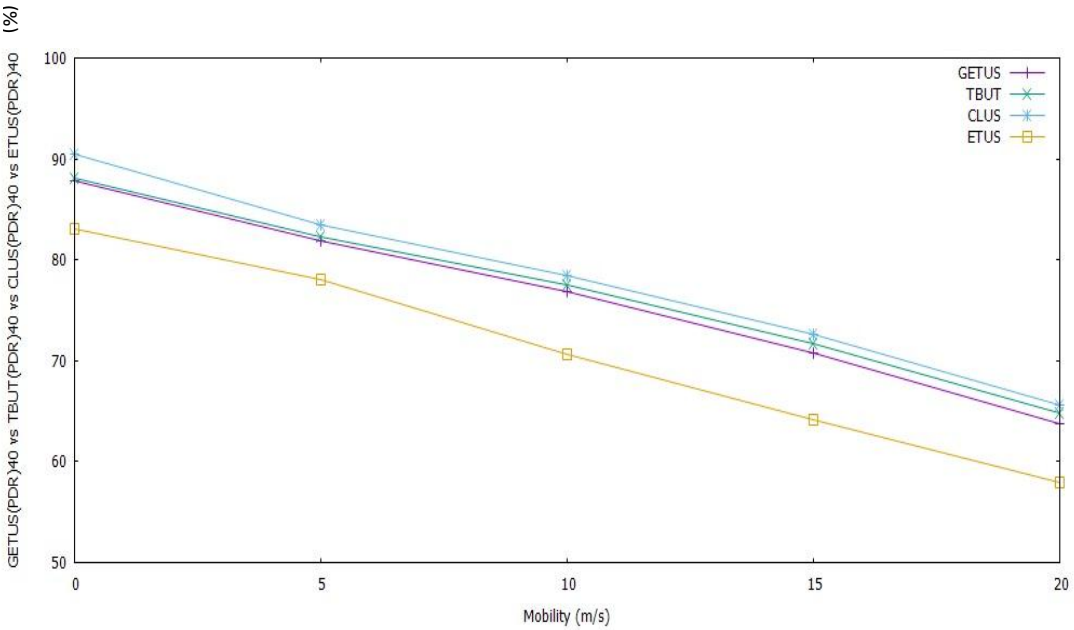

Figure 5.5 Comparison of generic ETUS, TBUT, CLUS and ETUS in the presence of 40 % of malicious nodes

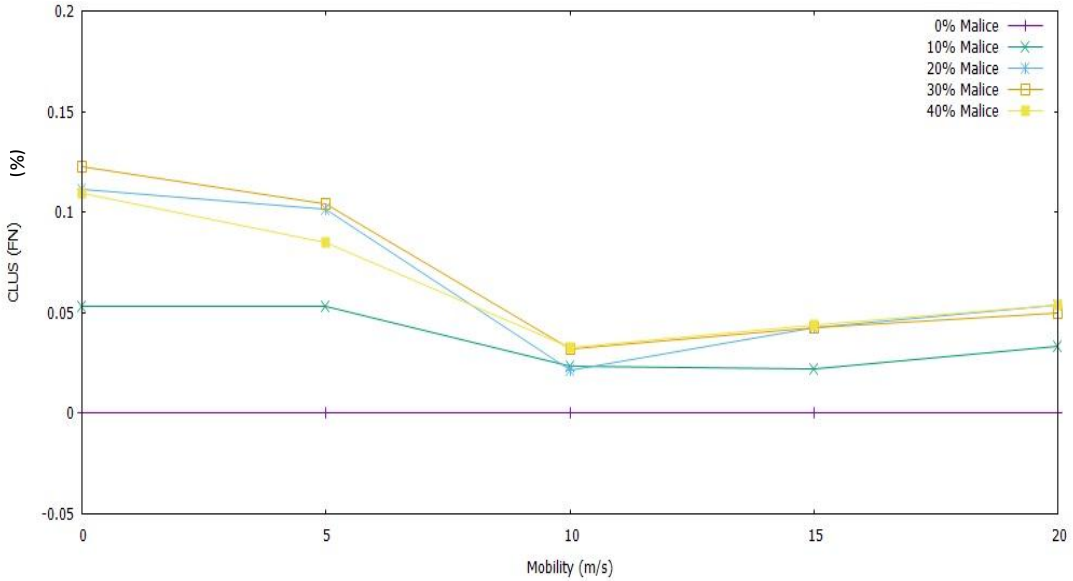

Figure 5.6 False negative, for 40% selfish node with node mobility varying between 0 and 20 m/s

From Figure 5.3, Figure 5.4 and Figure 5.5 the following conclusions can be drawn:

- Packet delivery ratio decreases as mobility and percentage of malicious nodes increase.
- CLUS is found to yield a much higher packet delivery ratio compared to generic ETUS, TBUT and ETUS in the presence of 40% selfish nodes. A higher packet delivery ratio ranging from 2.65 % (CLUS 20 m/s mobility) to 1.22 % is found for TBUT.

5.3.2 Failure to Deduct (False Negatives) Probability

Figure 5.6 details of the failure to deduct probability as a function of mobility and percentage malicious nodes.

False Negatives Probability can be defined as:

$$\text{False Negatives Probability} = \frac{\text{Number of malicious nodes left undetected}}{\text{Total number of malicious nodes}} = \frac{N_{LU}}{T_{MN}} \quad (5.1)$$

The above description requires some explanation. For example, two groups of malicious nodes are left unnoticed. The first group consists of those nodes, which never played a part in the network process, they were probably wandering along the boundaries and never had a chance to participate in the network activity.

The next group of malicious nodes consists of those that played a role as a routing node, but went unnoticed. Obviously, the research work proposed umpiring system is accountable only to the second group. The first group of nodes is similar to reserve players on the sidelines, and obviously, umpires do not show the red flag and march off players in the sidelines.

There has been failure to detect probability computation taking into consideration only those nodes, which took part in the network movement. Similar approach adopted by the pervious study also. The results are the same like SCAN (Hao Yang et al. 2006).

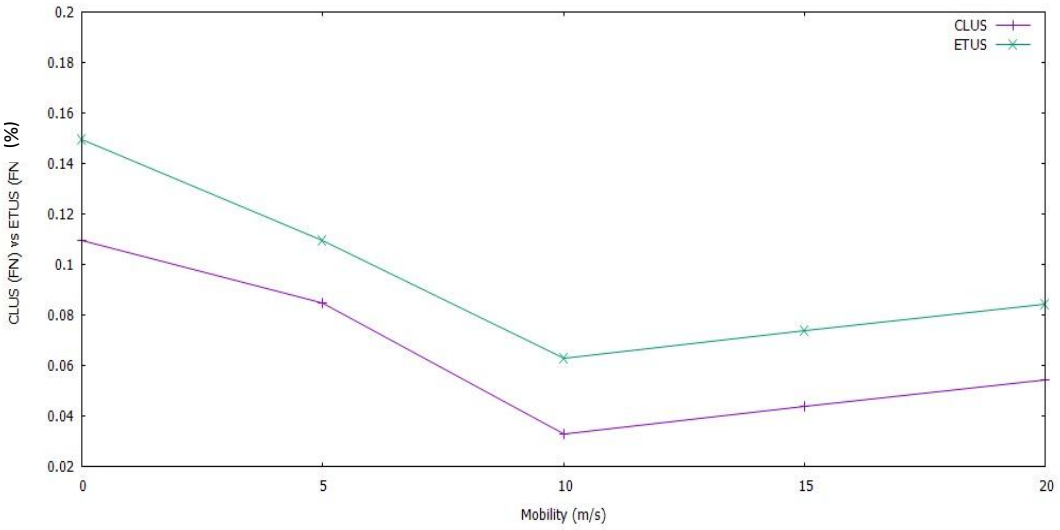

Figure 5.7 False Negatives Comparison of CLUS and ETUS with 40 % of malicious nodes

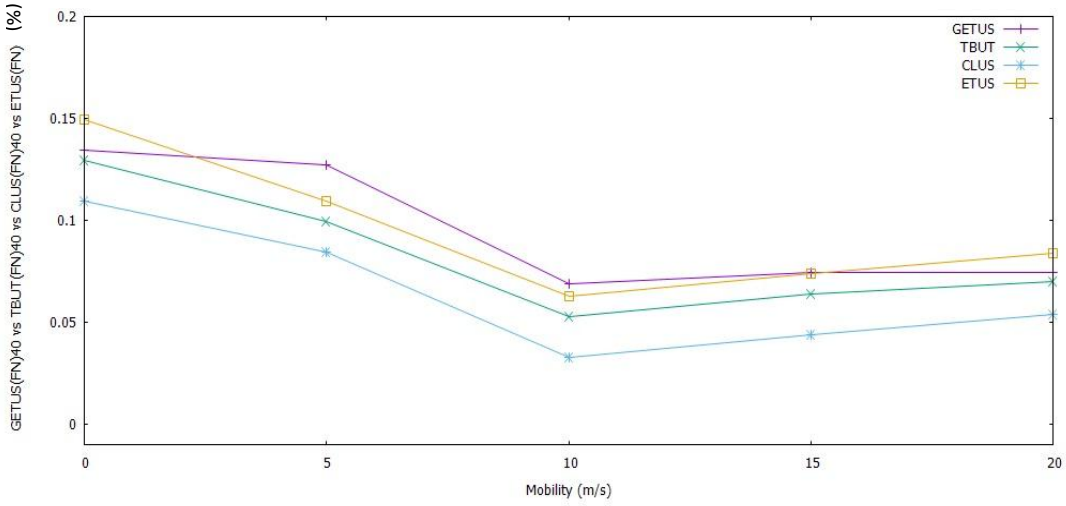

Figure 5.8 False Negatives Comparison of generic ETUS, TBUT, CLUS, and ETUS in the presence of 40 % of malicious nodes

Figure 5.7 and Figure 5.8 present the failure to detect probability as a function of mobility and percentage of selfish nodes of generic ETUS, TBUT, CLUS, and ETUS, respectively. A false negative probability, which is the chance of umpires failure to convict and isolate a selfish node, can be defined as the ratio of the number of selfish nodes left undetected to the total number of selfish nodes.

The failure to detect probability has been calculated by taking into consideration only those nodes that took part in the network activity. Similar approach have been adopted by the pervious study also. From Figure 5.8shows decrease in the false negative probability in CLUS compared to ETUS.

5.3.3 False Accusation (False Positives) Probability

False accusation probability shown in figure 5.9 is the chance of erroneous conviction and isolation of a genuine node by the umpires. In other words, there is likelihood of wrongly booking guiltless nodes. Figure 5.10 presents false accusation probability as a function of the mobility and the percentage of selfish nodes for CLUS and ETUS, respectively. Similar reduced false accusation likelihood is also found at all other combinations of selfish node percentages and mobility values with ETUS. False positive likelihood increases with increasing percentage of selfish nodes and greater mobility are also seen.

An evaluation of false positive probability values between generic ETUS, TBUT, CLUS and ETUS of 40% selfish nodes is shown in Figure 5.11. A slight decrease in probabilities with ETUS is also observed.

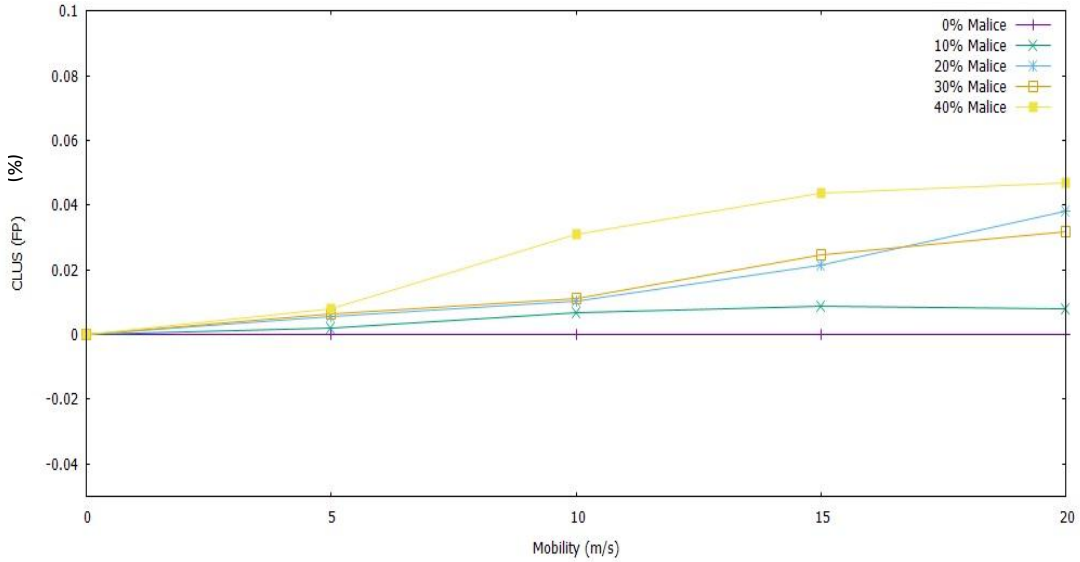

Figure 5.9 Accusation probability as a function of mobility and percentage malicious nodes

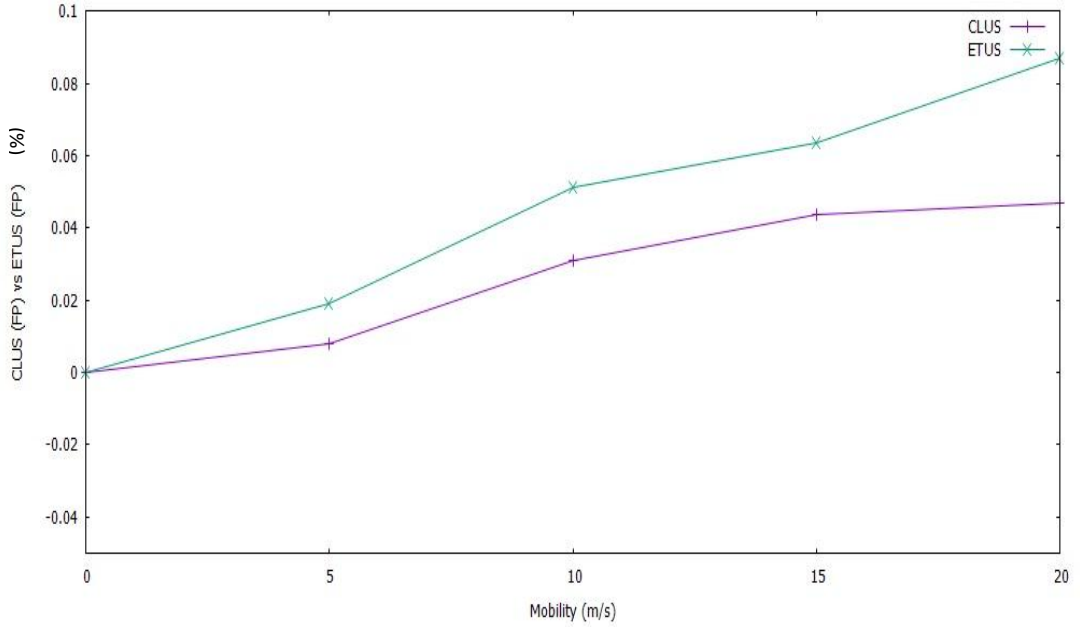

Figure 5.10 False Positives Comparison of CLUS and ETUS with 40 % of malicious nodes

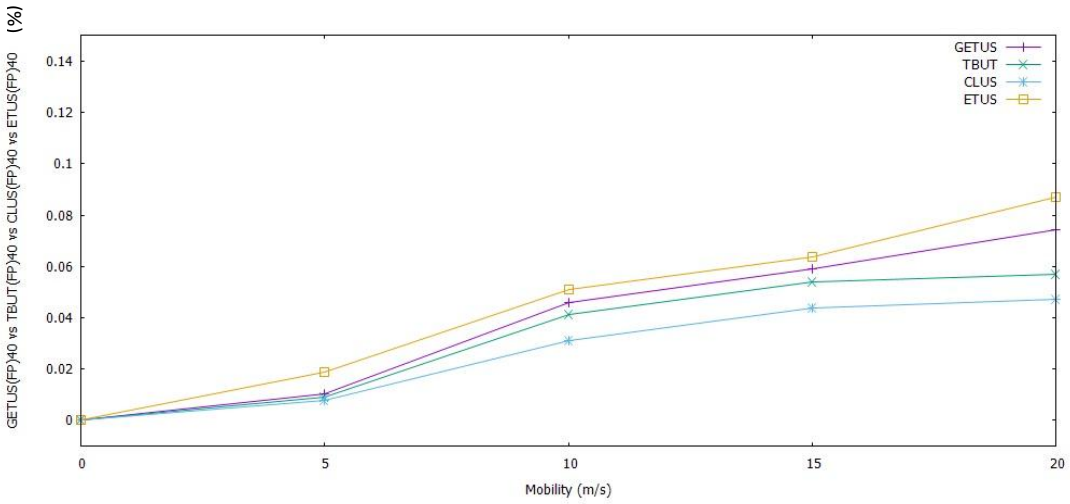

Figure 5.11 False Positives Comparison of generic ETUS, TBUT, CLUS, and ETUS in the presence of 40 % of malicious nodes

5.3.4 Communication Overhead

Communication overhead shows in figure 5.12 can be evaluated on the basis of the number of the broadcast of control messages like RREQ, RREP and RERR in the case of plain AODV and also M_ERROR, umpire, MFlag and neighbor list of messages in the CLUS and ETUS in Figure 5.13. Figure 5.14 shows communication

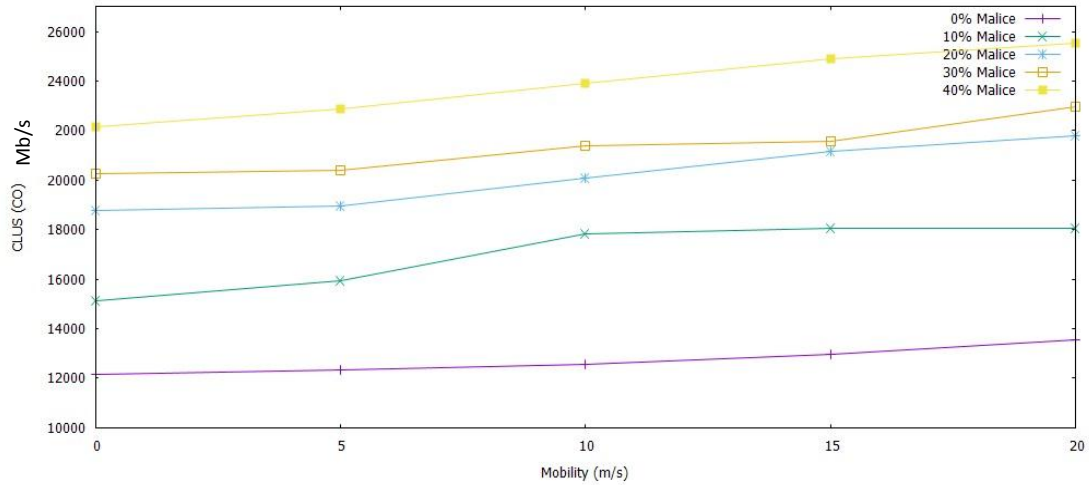

Figure 5.12 Communication overhead Vs. mobility with various percentages of malicious nodes

overhead comparison of generic ETUS, TBUT, CLUS and ETUS in the presence of 40 % of malicious node

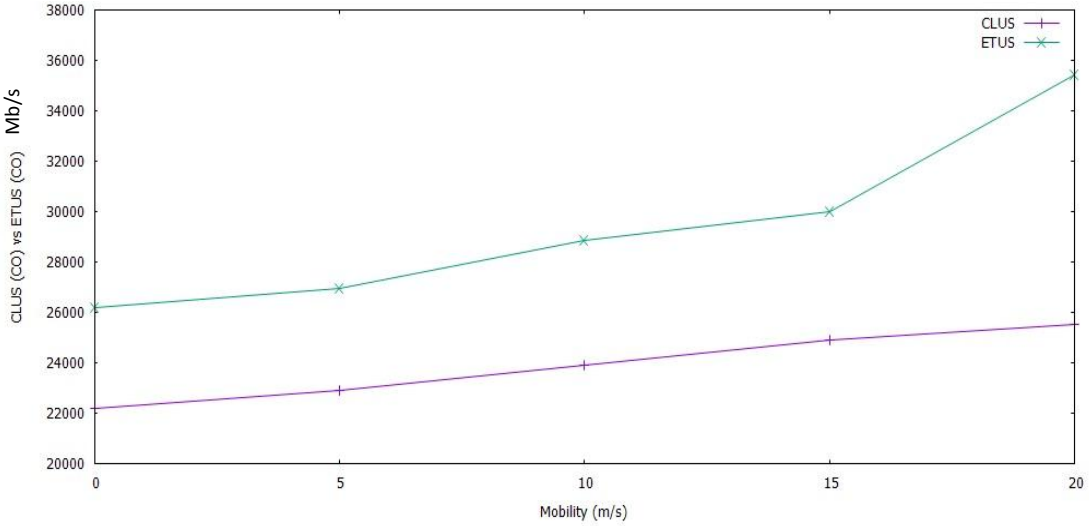

Figure 5.13 Communication overhead Comparison of CLUS and ETUS with 40 % of malicious nodes

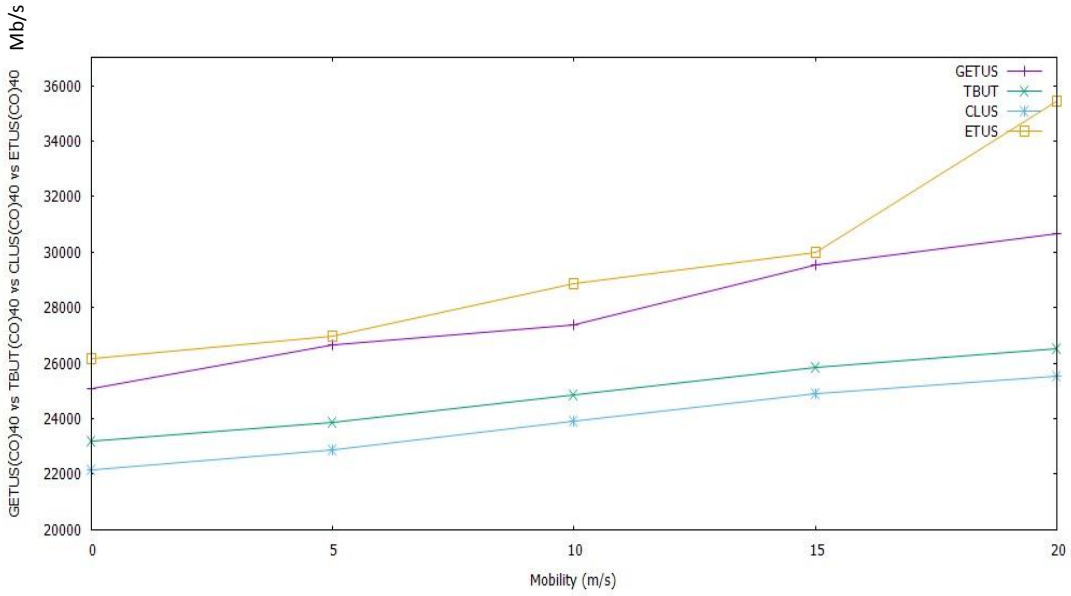

Figure 5.14 Communication overhead Comparison of generic ETUS, TBUT, CLUS and ETUS in the presence of 40 % of malicious nodes

5.4 Summary

In this chapter Cross Layer Umpiring System (CLUS) has been proposed. Simulation studies using QualNet 5.0 evaluate the performance of CLUS have been conducted. The results show that CLUS significantly improves the performance of TBUT and GETS in all metrics namely packet delivery ratio, false positive and false negatives. However, compared to TBUT, communication overhead is increased by 3.84 %. This is understandable since CLUS involves commissioning additional set (m+2) nodes for umpiring as well as link status and battery status. The next chapter discusses the analysis of the three models.