AN IMPROVED MUTUAL EXCLUSION MAC PROTOCOL FOR MAC LAYER IN MANET TO OVERCOME HIDDEN AND EXPOSED TERMINAL PROBLEM

DRS. HEMALATHA¹, K SREE DIVYA², VENKATAGURUNATHAM NAIDU KOLLU³, SHAIK SHAFI⁴, CHETTIYAR VANI VIVEKANAND⁵, G. VIKRAM⁶, RAMU KUCHIPUDI⁷, PROF. RAJESH PCHINCHEWADI ⁸

¹Professor, Department of Computer Science and Business System, Panimalar Engineering College, Chennai (Tamil Nadu), India. & Post Doctorial Research Fellow, Manipur International University, Imphal, Manipur, India
²Department of Computer Science and Technology, Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh 517325, India.
³Department of Artificial Intelligence and Data Science, Koneru Lakshmaiah Education Foundation, Andhra Pradesh 522302, India.
⁴Department of Electronics and Communication Engineering, B V Raju Institute of Technology, Narsapur, Telangana 502313, India.
⁵Department of Electronics and Communication Engineering, RMK College of Engineering and Technology,
⁶Karunya school of Management, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu 641114, India.
⁷Department of Information Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana 500075, India.
⁸CTO & Dean Innovation, Manipur International University, Imphal, Manipur, India

Email ID pithemalatha@gmail.com¹*, divya.kpn@gmail.com²*, shaikshafi245@gmail.com⁴, vanivivekanand@rmkcet.ac.in⁵, Vikram@karunya.edu⁶, kramupro@gmail.com⁷, Rajesh.cto@miu.edu.in⁸

ABSTRACT

The Hidden and Exposed Terminal problems are the most difficult in Mobile Adhoc Network, because node collisions reduce the performance of the Mobile Adhoc Network. Many protocols were addressed to tackle the issues in hidden and exposed protocols, but none of them were able to provide a permanent solution, and the Hidden Exposed Nodes issues remain in the MANET. This article suggested a novel approach that supports the MAC layer by creating Hidden and Exposed Tables and sending MERT/MER signals. The proposed work, known as the ME-MAC protocol, was implemented with the NS2.34 and the results were compared with the traditional WiMARK protocol, CAD-CW protocol, and CFC-MAC protocol. Furthermore, the proposed work achieved the maximum Packet Delivery Ratio of 60%, less End to End Delay from 0 to 75ms, and higher Throughput.

Keywords: MANET, ME-MAC protocol, MERT/MER, Hidden and Exposed node, MAC layer

1. INTRODUCTION

Due to the intrinsic characteristics of the MANET nodes' ability to move freely, one of the biggest issues in the Mobile Adhoc Network (MANET) remains the Hidden and Exposed terminal dilemma [1]. Figure 1 depicts the transmission range of each node in MANET. A Nodes transmitting packets can reach up to the transmission range, and nodes in the transmission range can receive the packet and retransmit or forward to the next hop. All nodes in the MANET network employ these protocol rules to deliver packets from the source node to the destination node. Each node senses the channel before transmitting the packet; if the channel is free, it begins sending the packet; otherwise, it waits until the channel becomes free, as in CSMS/CD.
For example, in Figure 1.2, nodes want to send a packet to node B, while C nodes want to send a packet to node B. Both nodes detect a free channel and begin transmitting packets to the B node; however, there is a collision at the B node. Both A and C codes could not be aware of each other when transmitting the packet. This is referred to as Hidden nodes. Both the A and C nodes are hidden from each other. According to Figure 1.3, node B wants to send a packet to node A, while node C wants to send a packet to node D. When B and C feel the channel, the channel is free, and both nodes transmit packets to A and D, respectively, where there is a collision. Nodes A and D are exposed in this case.

Several solution classes have been proposed to handle the Hidden and Exposed nodes problem in wireless networks as a result of mobility changes. The major recommended solutions for solving hidden and exposed nodes are launching MAC layer protocols. A group of authors proposed protocols for the Medium Access Layer, such as, WiMARK protocol [2], CAD-CW protocol [3], and CFC-MAC protocol [4], in which each protocol does not achieve all performance parameters and lags on some others.

Another set of research was conducted for changing RTS/CTS signals [5] [6] in corporative and distributed ways, but this research failed when the nodes were mobile. A few studies have been conducted on internal parameters such as clock synchronisation, receiver sensitivity, and SINR value. Adaptive antenna array [7] was the most recent strategy in Antenna centric research, replacing the Omni-based antenna with directional antenna techniques to try to solve the Hidden and Exposed node dilemma. For providing the MAC layer issues solution, recent algorithms [8] of machine learning, deep learning, artificial intelligence, and cluster algorithm were employed. The ultimate solution for the Hidden and Exposed node concerns could not be addressed by any of the methods. Several methods are still being investigated in order to find a solution to the Hidden and Exposed node concerns.

This research article addresses the issue of hidden and exposed nodes by introducing the MAC protocol known as Mutual Exclusion Medium Access protocol (ME-MAC), which forms the Hidden and Exposed table based on the locations of nodes and also uses two signals about packet transmission known as MERT/MER (Mutual Exclusion Request for Transmit /Mutual Exclusion Release). The Venn diagram is used in research to create the Hidden and Exposed nodes table. The article is organised as follows: The related research survey is discussed in Chapter II, followed by the methodology for forming hidden and exposed node tables and MERT/MER signal formatting in Chapter III, simulation work in Results and
discussion in Chapter IV and V, and conclusion and feature in Chapter VI.

2. RELATED SURVEY

The authors of this study, Ketema et al. [9], proposed an Omni-directional and directional antennas-based MAC protocol used in MAC to increase the performance of a wireless sensor network. Incorporating the scheduling method and collision avoidance support for this task, so that unjust channel allocation can be prevented, as well as support for channel wastage in each node. Jenhui et al. [10] introduced a higher throughput achieved MAP protocol for CSMA to support 802.11 and Adhoc networks for concurrent transmission in this study. The time complexity was computed as O (|X| log |X| + |X|M2), where |X| and M signify the number of successful requests, and lastly the simulation results were analysed higher throughput.

The authors Liu Kai and Xing Xiaoqin [6] suggested a unique MAC level protocol with RTS/CTS signal support, reliable ACK, and flexible traffic channel and multi channel selection. This technique eliminates the exposed terminal problem, and the simulation results show that it performs better than the present CAM-MAC protocol. The authors Singh et al. [11] conducted a real time MAC protocol comparative analysis and presented the S-MAC real time protocol, which produced consistent data transfer but increased overhead owing to control packets.

Rajeev Kumar [12], the author of this research, proposed a trustworthy MAC protocol for solving the hidden and exposed node dilemma by providing an addressing technique and a channel access mechanism. Hemant et al. [13] propose a new resource allocation protocol for increasing QoS in MANET TCP/IP in this study. While designing the protocol, the feature of eliminating hidden and exposed nodes was added to improve QoS. The protocol was simulated using V/UHF radios and the performance of TCP/IP was assessed, revealing that only two characteristics improved: data rate and jitter.

The authors Kalfas et al. [2] presented WiMARK, a hybrid technique for eliminating hidden and exposed nodes. All nodes kept a local matrix for gathering other surrounding nodes' current location and making the transmitter transmit or receive with the use of RTs and Status messages. This work has been improved by including a sleep and awake protocol to reduce node energy consumption. The writers of this survey study, Hussien and Mostafa [8], provide a comprehensive survey connected to building a MAC protocol using modern techniques such as machine learning, deep learning, and artificial intelligence. Finally, three features show that machine learning techniques are ideally suited to MAC protocol design.

Mahendrakumar and others [14] In this paper, a nullifying MAC framework for Adaptive Antenna Array was developed to handle MAC layer concerns such as concealed terminal problem, beam problem, and deafness nodes, among others. Simulation was tested with OPNET and MATLAB, yielding limits of 27.22% throughput and 40.46% SNR increase. R. Gudodagi and P. K. [15] the authors of this study devised CAD-CW, a strategy for avoiding collisions utilising contention windows. To avoid collisions, this strategy maintains a contention window in which the highest priority node packets are transmitted first. This technique achieves faster throughput, reduced delay, and lower overhead while consuming the least amount of energy.

Linn and colleagues [4] suggested a technique to reduce heterogeneous collisions using the distributed contention-free cooperative medium access control (CFC-MAC) protocol and the corporative communication system and corporative forwarding mechanism. The simulation determines the corresponding position to study the collision; the findings of the simulation comparison reveal that there is less delay and the collision is minimised. Zhou et al. [16] suggested an Intelligent Multi-hop Low Duty Cycle (IMLDC) Media Access Control (MAC) protocol based on long short-term memory (LSTM) to address the short life cycle issue in UAVS. For optimal mode environment, an LSTM neural network was applied. Real-time simulation only the network life cycle is improved by the LSTM-based IMLDC MAC protocol over existing MAC protocols.

According to the literature review, several protocols were proposed to address the MAC layer hidden and exposed terminal issues, some novel techniques were introduced, distributed channel allocation strategy was also addressed, RTS/CTS signal synchronisation, introduction of various algorithms, Uni directional antennas, adaptive antenna array strategy, and contention window for allocating channels. All of the above methods could not resist the hidden and exposed node issues, and the research work did not address all of the performance in the MAC layer, so more research is needed to find a solution to the hidden and exposed node problem and address all of the performance. This article describes a new technique that is kept in the form of a table to support the issue of hidden
and exposed nodes, as well as two synchronisation signals MERT/MER support for collision avoidance.

3. RESEARCH WORK

This section will cover the proposed Mutual Exclusion MAC protocol's research effort. The protocol's duty is to incorporate in the way of protocols with the MAC layer two values such as hidden and exposed nodes Table and packet synchronisation signals Mutual Exclusion Request Transmit and Mutual Exclusion MERT/MER) signal. This study work use the Venn diagram to generate a mutual exclusion table, and the Venn diagram's functions of union and intersection enable the research to produce the Table.

3.1 Hidden and Exposed nodes Creation

The position of the node in the MANET determines whether it is hidden or exposed. Because of its qualities, MANET nodes are prone to changing location. The hidden and exposed tables are dynamic and will be updated if the location of a beacon signals mobile node changes. Let Set the MANET nodes N= ( n1,n2,n3,....nn} Forming the set of nodes in the same region using Venn Diagram

Venn diagram Region nodes R = {r1,r2,r3,...rn Where every region in Ri has a set of nodes
Ri = { n1,n2,n3,...n}

3.1.1 Algorithm forming the Hidden and Exposed nodes

for( i=1 i<=Maximum region of Ri; i++)
{for(j= i+1 j<= maximum Region of Rj; j++)
{for ( k= j+1 ;k<= Maximum Region Rk ;k++)
 {
Collect the list of nodes in Ri, Rj, Rk using the device location
list of hidden nodes = Apply Ri ∩Rk
Create the difference DRi= Ri−Rj
Create the difference DRk = Rk−Ri
then the DRi and DRl are exposed nodes
}
}

3.1.2 Exposed nodes formation

for( i=1 i<=Maximum region of Ri; i++)
{for(j= i+1 j<= maximum Region of Rj; j++)
{for ( k= j+1 ;k<= Maximum Region Rk ;k++)
 {
Collect the list of nodes in Ri, Rj, Rk , RI using the device location
list of Exposed nodes
create the difference DRi = Ri−Rj
create the difference DRk = Rk−Ri
then the DRi and DRI are exposed nodes
}
}

3.2 Mutual Exclusion Request and Release (MERT/MER) signal

After creating the Hidden and Exposed nodes database for each region, the two signals synchronise the nodes to overcome the hidden and exposed nodes difficulties. Mutual Exclusion Request for Transmit (MERT) and Mutual Exclusion Release (MER) are abbreviations for Mutual Exclusion Request for Transmit (MERT). When a source node wants to send a packet to a destination, a path is chosen based on the routing algorithm. To avoid a collision, the nodes check the Hidden and exposed nodes table and send the MERT signal to all nodes in the table; this MERT is the highest priority signal; other nodes cannot send a packet unless they receive the MER signal. Figures 3.3 and 3.4 demonstrate the MERT and MER formats.

Source ID Sequence Number Hidden node ID State MERT Previous hop node Next hop node

<table>
<thead>
<tr>
<th>Source ID</th>
<th>Sequence Number</th>
<th>Hidden node ID</th>
<th>State MERT</th>
<th>Previous hop node</th>
<th>Next hop node</th>
</tr>
</thead>
</table>

**Figure 3.3 Format of Mutual Exclusion Request**

**Figure 3.4 Format of Mutual Exclusion Release**

Where
Source ID - Indicate the ID number of the Source Node
**Sequence Number** - Generated by the forwarding node to avoid duplication of packet flooding

**Hidden node ID** - Extracted from the source node Hidden and Exposed Node Table.

**State** - Indicate two states which differentiate the signal is Mutual Exclusion Request Transmit or Mutual Exclusion Release.

**Previous hop node** - Indicate the previous node ID initially generated by the source and updated by each intermediate node.

**Next hop node** - Indicate the next node ID initially generated by the source and updated by each intermediate node.

### 3.3. ME-MAC Protocol Workflow

The simulation of NS2.34 was designed in a 500m*500m space during the first stage. The territory is delineated by several small division areas of 50 m*50 m. A region will be formed by the nodes that are located within the region. Similarly, ten zones are defined in the simulation. The node in the region centre generates hidden and revealed region tables, which are then shared with other nodes within the region. In the second stage, the nodes desire to connect with the other node that generates the RREQ signal, as is customary in On Demand protocol route selection.

Once the reliable shortest route is determined, based on the Hidden and Exposed nodes table in the source node, it sends the MERT signal to all the hidden and exposed nodes, which is the highest priority signal; other nodes cannot send any messages to the destination node until they receive the MER signal from the source. This mutual agreement aids in the prevention of Hidden and Exposed node concerns in the MANET. While communicating, the nodes' positions change; the next beacon signal assists in determining the nodes' new location and updating the hidden and exposed node tables, as seen in Figure 3.5.

![Figure 3.5 Workflow for the ME-MAC protocol.](image)

### 4. SIMULATION OF THE RESEARCH

The proposed Mutual Exclusion MAC protocol is implemented using Network Simulator 2.34 with a total of 100 nodes designed in and using the parameters listed in Table 4.1.

MERT/MER signals are two new signals added to the Network Simulator to provide a solution to the Hidden and Exposed Terminal Mutual Exclusion agreement. Every beacon signal in the MANET updated the table of hidden and exposed nodes; when nodes want to connect with other nodes, they check the medium is free and also the Hidden and exposed nodes updated table. If the source node is a Hidden node, the node cannot wait for the medium to become...
free, and the Exposed nodes follow suit. Initially the NS3 is plotted and shows the Collision possibilities with the support of Hidden and Exposed Terminal nodes.

To begin, three nodes are plotted to demonstrate the collision. N1, N2, and N3 are MANET nodes. N1 and N2 desire to interact with the N3, and when both detect that the carrier is free, both N1 and N2 begin sending packets, but a collision occurs at the N3. Two signals are generated in such a scenario. Hidden and revealed signals are used to get an agreement on conveying the packet to its destination.

<table>
<thead>
<tr>
<th>Table 4.1 Network Simulator Parameter Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>S.No</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
</tbody>
</table>

5. RESULTS

The proposed ME-MAC protocol was simulated using NS2.34. Initially, three nodes are established to determine the creation time of the hidden and exposed node tables. The number of nodes is then increased by ten every 20ms, and the time for generating the Hidden and Exposed tables is recorded. There is no difficulty or delay in generating the Hidden and Exposed tables.

5.1 Packet Delivery Ratio

The Packet Delivery Ratio is a ratio that compares the number of packets received from the sender to the number of packets sent, as illustrated in Eq 1. The nodes are initially designated by three integers, which are gradually raised by ten every 20ms. In parallel, the Total Packet for transmission is set to 10 and gradually grows by ten every 20ms. The payload is 10000 bits, and the packet size is 512 bytes with a bandwidth of 512 bytes. The packets sent from the source node and received from the destination nodes are computed to compare performance.

$$PDR = \frac{\text{Packet Received}}{\text{Packet Send}} * 100 \quad \text{Eq}(1)$$

According to Figure 5.1, the WiMARK protocol a maximum of 24% to 37%, the CAD-CW protocol a maximum of 24% to 34%, the CFC-MAC protocol a maximum of 30% to 42%, and the ME-MAC protocol a maximum of 60%.

5.2 Throughput Analysis

The maximum number of packets received from the sender is defined as throughput, which may be determined using the equations Eq2 and 3. The nodes are initially designated by three integers, which are raised gradually by ten every 20ms. In parallel, the Total Packet for transmission is set to 10 and gradually grows by ten every 20ms. The payload is 10000 bits, and the packet size is 512 bytes with a bandwidth of 512 bytes. The packets sent from the source node and received from the destination nodes are compared to the WiMARK, CAD-CW, CFC-MAC, and ME-MAC protocols.

$$\text{Throughput} = \frac{\text{Packet Size}}{\text{Transmission Time}} \quad \text{Eq}(2)$$

$$\text{Transmission Time} = \frac{\text{File size}}{\text{Bandwidth}} \quad \text{Eq}(3)$$

The throughput performance of the WiMARK protocol, CAD-CW protocol, CFC-MAC protocol, and ME-MAC protocol ranges from 1 to 2 based on the simulation value. CAD-CW Protocol have lesser throughputs; CFC-MAC Protocol, and ME-MAC Protocol, have throughput ranges ranging from 1 to 2.

5.3 End to End Delay

End-to-end delay is calculated as the time differences between packets transmit from source and packet arrival at destination using Eq4. The sender side delay is 0ms, but the destination node delay varies, as shown in Figure 5.3 shows a comparison chart of delay between the traditional WiMARK protocol, CAD-CW protocol, CFC-MAC protocol, and ME-MAC protocol.

$$\text{EED} = \text{Packet} * (\text{Difference in delay}) \quad \text{Eq}(4)$$

The simulation value demonstrates that when the number of nodes starts at three, the end-to-end latency is smaller in other protocols such as the WiMARK protocol, the CAD-CW protocol, and the CFC-MAC protocol, but the delay in the ME-MAC protocol is null. Following that, the nodes gradually raise the delay in all other protocols where the ME-MAC protocol latency is appropriate.
due to Hidden and Exposed Table monitoring. When the number of nodes reaches 100, the delay in the a moderate delay ranging from 92ms to 77ms CAD-CW protocol, WiMARK protocol, and CFC-MAC protocol, while the ME-MAC protocol has a delay of 75ms, which is less than the other protocols.

6. CONCLUSION

This research study developed a unique approach that supports the MAC layer by creating Hidden and Exposed Tables and sending MERT/MER signals. The dynamic nature of the Hidden and Exposed tables aids in avoiding node collisions with the use of MERT / MER hand shaking signals. The proposed ME-MAC protocol was implemented with NS2.34 and the results were compared with the traditional WiMARK protocol, CAD-CW protocol, and CFC-MAC protocol. Furthermore, the proposed work achieves the maximum Packet Delivery Ratio of 60%, less End to End Delay from 0 to 75ms, and higher Throughput. In feature this approach can be compared to modern machine learning algorithms such as Deep Learning, Machine learning, Artificial Intelligence algorithms

REFERENCES

[1] Dr. S. Hemalatha, Nileshkumar Patel, Ajay Kumar, Neelsh Kumar Jain, Dr. G. Venkat Narayanan, Manka Manwali, Dr.Harikumar Pallathadka, Prof Rajesh P Chiniewadi (2023)" MANET Hidden and Exposed Terminal - Challenges and Survey " International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 11 Issue: 10s DOI: https://doi.org/10.17762/ijritcc.v11i10s.7593.


Figure 5.1 Throughput Analysis

Figure 5.2 Throughput Analysis
Figure 5.3  End to End Delay