Proposed Mutual Exclusion MAC Protocol for MANET to Overcome Hidden and Exposed Terminal Problem

S. Hemalatha, Harikumar Pallathadka, Rajesh P Chinchewadi

***Abstract:** Mobile Adhoc Network (MANET) is a kind of wireless transmission network could able to form the communication network without need of any basic infrastructure with all the communication nodes can able to move freely ad communication could be done b forwarding the received packet from one node to another nodes in order to reach until the desired destination node found. One of the major challenges in MANET is nodes can move freely from one region to another region where the possibilities route failure and collision among the node. Especially the of Hidden and exposed node problem is the major challenges in the MANET which could not able to define the permanent solution to resolve the issue. This research article focus on hidden and Exposed terminal problem in MAC layer and proposed the new protocol called the Mutual Exclusion MAC protocol (ME- MAC) which support to solve the Hidden and Exposed Terminal issue in MAC layer.*

***Key words:** MANET, MAC Protocol, Hidden and Exposed Terminal, Mutual Exclusion-MAC Protocol*

I. INTRODUCTION

Several Network evolutions were used to construct the MANET ideology. The Packet Network (PRNET) was invented by the Department of Defense (DoD) in the early 1970s for use in military applications. the Survivable Adaptive Radio Networks (SURAN) programme in the 1980s the PRNET [1] chains. The DARPA [Defense Advanced Research Projects Agency] defined a novel wireless network with architecture that relies on an aerial relay node and has a throughput of 300 kilobits per second while supporting 200 nodes [2]. The PRNET uses a distance vector for routing and an ALOHA and CSMA combination to access the medium. The hierarchical link state routing protocol is used by SURAN. In contrast, infrared communication is used in the 1990s New Version of Development in Adhoc Network based on RF development in a notebook computer.

The Near-term Digital Radio (NTDR) programme planned a self-organized, two-tier Adhoc network using link state routing and clustering routing, which was used by the US army in the middle of the 1990s to obtain Adhoc s. Global Mobile Information System (GloMo) for office environment Ethernet connectivity planned anytime, anywhere, in handheld devices using CSMSCA and TDMA channel access with several routing algorithms The IETF finished the routing protocol for Adhoc networks and created the mobile ad hoc networking (MANET) group. The IEEE 802.11 subcommittee accepted the collision avoidance and Hidden terminal Tolerated Medium Access Protocol. A MAC protocol is used to coordinate and send packets from several nodes in order to reduce collisions. There are numerous MAC protocols available for various uses. For carrier random access, CSMS and MACA are used, whereas TDMA, FDMA, and CDMA are used for channel partitioning. Fragmentation, power-saving mode, association, WEP, scanning, authentication, and other MAC functions are among 802.11's primary functions. The term "hidden terminal problem" refers to a situation in which more than two nodes are sending and receiving packets simultaneously, but they are not in the same transmission range.

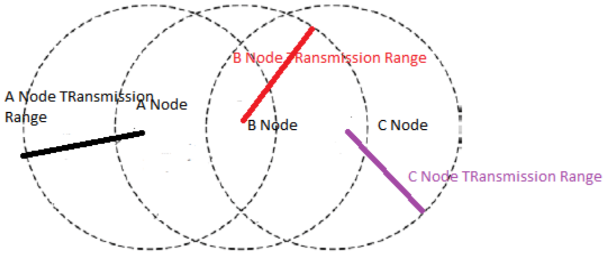
B Node TRansmission Range
A Node TRansmission Range
A Node
B Node
C Node
C Node TRansmission Range

Figure 1.1 Hidden and Exposed Nodes

When node B is inside the range of nodes A and C, it can be shown from Figure 1.1 that A and C nodes are hidden within one another if they attempt to send a packet to it at the same time. As the packet is sent from the B node to the A node, C detects that the signal is busy and is unable to transfer the packet to any other node, such as D, that is not within the same transmission range. B is exposed to the c node in such a circumstance.

II. LITERATURE SURVEY ON RELATED WORK

Using numerous simulation findings and all the literature to serve as a benchmark for the research activity, a brief analysis of terminal problems that are both concealed and exposed has been conducted in this survey.

Manuscript received on 22 June 2022 | Revised Manuscript received on 08 August 2023 | Manuscript Accepted on 15 October 2023 | Manuscript published on 30 October 2023.

*Correspondence Author(s)

Dr. S. Hemalatha*, Professor, Department of Computer Science and Business System, Panimalar Engineering College, Chennai (Tamil Nadu), India.
Post Doctorial Research Fellow, Manipur International University, Imphal, Manipur, India. E-mail: pithemalatha@gmail.com, ORCID ID: 0000-0002-0049-1167

Dr. Harikumar Pallathadka, PhD, DSc Vice Chancellor and Professor, Manipur International University, Imphal, Manipur, India. E-mail: harikumar@miu.edu.in, ORCID ID: 0000-0002-0705-9035

Prof. Rajesh P Chinchewadi, CTO & Dean Innovation, Manipur International University, Imphal, Manipur, India. E-mail: Rajesh.cto@miu.edu.in, ORCID ID: 0009-0001-5891-9605

Caishi Huang and co. [3] Authors presented various receiver power, SINR, interference, and transmission ranges in this paper. This study demonstrated a high RTS/CTS packet transmission rate for a specific DATA broadcast. Integration of transmission power control then takes care of the exposed terminal issue. The writers of Viral V. Kapadia [4][20] present an improved RTS/CTS method that essentially creates jams while consuming the least amount of power. also makes advantage of the omnidirectional aerial, which removes barriers to protocol improvement. Ritu Patidar et al [5] says: For enhancing the functionality of wireless sensor networks, the authors of this study presented the MAC protocol, which is implemented with sensor and directional aerial support. As stated in Lu Wang et alpaper .'s [6]: The authors of this paper proposed the novel Attachment Coding technique as a means of attaching control information to data stream. By preserving a reasonable throughput for fresh data traffic, this coding technique enables the transfer of both data and control. In their paper [7], Khaled H. Almotairi et al. suggested the MMAC -HR as a solution to the exposed terminal problem that results in low channel utilisation. Nodes can find the available medium without using a channel list. According to the comparison findings, this performs better than the DCA in terms of throughput and delay. Adere Ketema, Ramamurthy [8]. The authors of this article suggested a MAC protocol based on omnidirectional and directional antennas that would improve the performance of a wireless sensor network. Kim Ki Hong et al, [9][19]. In this article, the authors conduct research on MAC flaws and analyse the security flaw in the handshaking step, which shows that designing and implementing a light-weight, low-power authentication technique is essential for wireless network. Albert Kai-Sun Wong, Chin-Tau Lea, and Caishi Huang [10] [18] With the use of several proposed protocols, such as contention-based protocols, busy tone signal-based protocols, power-aware protocols, multiple channel-based protocols, etc., the authors of this study resolve the hidden and exposed terminal problems. Rutvij H. Jhaveri, Sudarshan N. Patel, and Viral V. Kapadia, [11] By comparing concealed and exposed terminals in an ad hoc network with control mechanisms like the RTS/CTS mechanism, the authors of this article have found that the transmission rate in the ad hoc study has increased by 1.3 times. Yang C, Chen J, and Sheu S [12][16][17]. Authors of this article examined the R-CA, or dynamic channel interference, which was responsible for channel assignment. Channel assignment improves MANET performance by reducing interference and increasing network throughput. Simple DCF MAC protocol permits parallel transmission, which reduces the exposed terminal problem in IEEE 802.11, according to Liu K, Wong T, Li J, et al [13]. The novel MAC level protocol that gives the new approach Back-off criteria employed by the Virtual Base Station was proposed by Liu Kai* and Xing Xiaoqin [14]. authors. Mounir Hamdi [15], Kaishun Wu, and Lu Wang): The authors of this article developed a virtual jammer system that might stop certain RTS/CTS problems in their tracks.

Table 2.1 Literature Review Summary

S.No	Authors	Invented Mechanism Used
1	Caishi Huang et	RTS/CTS mechanism DATA broadcast.
2	Viral V. Kapadia	RTS/CTS mechanism with omni directional antenna
3	Ms. Ritu Patidar et. al	MAC protocol with antenna support
4	Lu Wang et. al	Attachment Coding technique was suggested attaching control information to data stream.
5	Khaled H. Almotairi et. al	MMAC -HR resolving the exposed terminal problem
6	Ketema Adere, Ramamurthy	Omni directional and directional antennasbased MAC Protocol
7	KiHong Kim et.	MAC light weight low power authentication mechanism
8	. Caishi Huang, Chin-Tau Lea, Albert Kai-Sun Wong	• Contention Based Protocol • Busy Tone Signal Based Protocol • Power Aware Protocol • Multiple Channel Based Protocols Etc
9	Viral V. Kapadia, Sudarshan et .. all	Adhoc network with control schemes like RTS/CTS mechanism
10	Chen J, Sheu S, Yang C	R-CA named for dynamic channel interference which made for channel assignment.
11	Liu K, Wong T, Li J, et al	Simple DCF MAC protocol allows the parallel transmission
12	Liu Kai*, Xing Xiaoqin	Back - off criteria used by the Virtual Base Station
13	Lu Wang, Kaishun Wu,Mounir Hamdi	Virtual jamming that could prevent the various problems of RTS /CTS problem

From the Literature study which is summaries on the Table 2.1 that all the authors proposed the innovative protocol and channels for overcome the limitations in Hidden and Exposed terminal problem, still the hidden and exposed terminal problem could not able to give the finalize in the MANET. More research work is needed to finalize the Hidden and exposed terminal problem with the support of mutual exclusion among the node communication

III. RESEARCH WORK

In order to overcome the Hidden and Exposed terminal problem in the MANET Physical layer challenges there are the several techniques are proposed, but all the proposed method are having the pits and fall on it. In this article proposed the Mutual exclusion Protocol for MAC layer by maintain the hidden and exposed terminal in each node which support to Finding out hidden and exposed terminal in each region. Sample MANET node forming shown in the Figure 3.1 and its Hidden and exposed Terminal nodes shown in the Table 3.1 below. As like the route finding before transmitting the packets the hidden and exposed nodes fining also done parallel which makes the nodes to avoid collision.

A. Mutual Exclusion MAC (ME-MAC) Protocol works as Follows in the Stages.

1. For all the nodes in the MANET form the region
Maintain the hidden and Exposed node table.
2. Generate the beacon signal by collecting the node available position.
3. Upon receiving the node position the nodes which are in the nodes region.

B. Hidden Node Table Creation

```
1.Set = Node { 1 ,2,3,.......N } N is a total number of nodes in a MANET
2. For each node i from 1 to N
        Generate location aware of other node in each $i^{th}$ node transmission range
3. All the node share the nodes which are in the region to its Transmission range nodes.
4. Repeat for ( i=1 to N)
            {
            For (j= i to N)
Hidden node of i =(List of node $i^{th}$ node transmission range ) ∩(List of node in $j^{th}$ transmission range )
           }
```

C. Exposed Node Table Creation

```
1. Set = Node {1,2,3,.......N } N is a total number of nodes in a MANET
2. For each node i from 1 to N
Generate location aware of other node in each $i^{th}$ node transmission range
3. All the node share the nodes which are in the region to its Transmission range nodes.
4. Repeat for ( i=1 to N)
            {
            For (j= i to N)

     Exposed node of i = If i and j are in the same transmission range and List of node $i^{th}$ node transmission range is not equal to List of node in $j^{th}$ transmission range then i is exposed node to j
           }
```

Example of Hidden and Exposed node in following figure 3.1 is shown in the Table 2.2, Totally four region is created for the MANET communication Network. each and every region apply the Mutual exclusion MAC Protocol for finding out hidden and exposed terminal of each region.

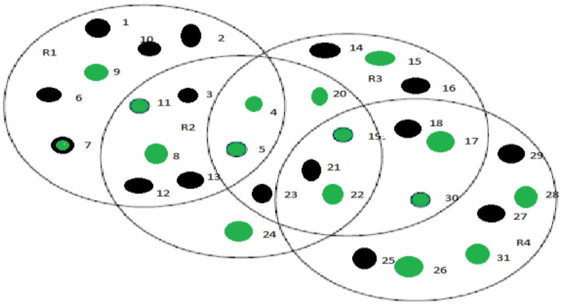

Figure 2.2 MANET Hidden and Exposed Nodes

Table 2.2 Hidden and Exposed Terminal Table

Region	Hidden Terminal	Exposed Terminal
R1	6- 20	11-5-21
R2	3 -14	3-4-14
R3	15 - 2	15-14-25
R4	27-16	22-30-27

IV. CONCLUSION

From this above proposed Mutual exclusion MAC Protocol is designed with the algorithmic stages which support for maintaining the Hidden and Exposed nodes in each nodes in the MANET. This table maintenance support to send the packet to any other node without collision. Every node updating the Hidden and Exposed table in each beacon signal and mutually agreed to send the data to the other node. Certainly if this ME-MAC protocol is implemented with the real time or any simulator support which give tremendous performance comparing with existing MAC protocol.

DECLARATION STATEMENT

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. R. Ramanathan and J. Redi,9 (2002) "A Brief Overview of ad hoc networks: challenges and Directions," IEEE Commun. Mag., vol. 40, no. 5, May. 2002. https://doi.org/10.1109/MCOM.2002.1006968
2. Dr. James A. ,Joseph P. Macker Freebersyser,Advanced Technology Office Defense Advanced Research Projects Agency, " Overview of CBMANET, ITMANET for WAND proposer Day meeting" Feb27, 2007
3. Caishi Huang, Chin-Tau Lea , Albert Kai-Sun Wong (2012)," A joint solution for the hidden and exposed terminal problems in CSMA/CA wireless networks" in ELSEVIER,17 June, 2012. https://doi.org/10.1016/j.comnet.2012.06.008
4. Viral V. Kapadia, Sudarshan N. Patel and Rutvij H. Jhaveri, (2010)" COMPARATIVE STUDY OF HIDDEN NODEPROBLEM AND SOLUTION USING DIFFERENT TECHNIQUES AND PROTOCOLS" JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151- 9617.
5. Ms. Ritu Patidar, Prof. Dinesh Chandra Jain (2012) "Solving the Hidden Terminal problems Using Directional-Antenna Based MAC Protocol for Wireless Adhoc Networks" ijarcsse, Volume 2, Issue 5, May 2012.
6. CaiZ J Lu M, Wang X D. Channel access-based self-organized clustering in ad hoc networks. IEEETransactions on Mobile Computing 2003; 2(2): 102-113. https://doi.org/10.1109/TMC.2003.1217231
7. Khaled H. Almotairi and Xuemin (Sherman) Shen, "Multichannel medium access control for adhoc wireless networks" WIRELESS COMMUNICATIONS AND MOBILE COMPUTING (2011). https://doi.org/10.1002/wcm.1159
8. Ketema Adere, Rammurthy, "Solving the Hidden and Exposed Terminal problems Using Directional-Antenna Based MAC Protocol for Wireless Sensor Networks" 7th International Conference on Wireless and Optical Communication Networks, Colombo (2010). https://doi.org/10.1109/WOCN.2010.5587352
9. Ki Hong Kim, Daejeon, Korea, "Security Attack based on Control Packet Vulnerability in Cooperative Wireless Networks" The Ninth International Conference on Networking and Services 2013.

10. Caishi Huang, Chin-Tau Lea, Albert Kai-Sun Wong," A joint solution for the hidden and exposed terminal problems in CSMA/CA wireless networks" in ELSEVIER,17 June, 2012. https://doi.org/10.1016/j.comnet.2012.06.008
11. Viral V. Kapadia, Sudarshan N. Patel and Rutvij H. Jhaveri, "COMPARATIVE STUDY OF HIDDEN NODEPROBLEM AND SOLUTION USING DIFFERENT TECHNIQUES AND PROTOCOLS" JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151- 9617.
12. Chen J, Sheu S, Yang C. A new multichannel access protocol for IEEE 802.11 ad hoc wireless LANs.Proc IEEE PIMRC 2003. 2003; 2291-2296.
13. Liu K, Wong T, Li J, et al. Performance analysis of UPMA protocol for wireless multihop mobile ad hoc networks. Proc IEEE WCNC 2003. 2003; 971-976.
14. Liu Kai*, Xing Xiaoqin, "A New Exposed-terminal-free MAC Protocol for Multi-hop Wireless Networks" Chinese Journal of Aeronautics 22(2009) 285-292. https://doi.org/10.1016/S1000-9361(08)60101-6
15. Lu Wang, Kaishun Wu,Mounir Hamdi, "Attached-RTS: Eliminating Exposed Terminal Problem in Wireless Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,2012. https://doi.org/10.1109/TPDS.2012.228
16. M. V. Madhuri and Dr. M. V. Sangameswar, "Encryption Technique to Optimize Information Leakage in Multi Cloud Storage Services," International Journal of Engineering and Advanced Technology, vol. 8, no. 6s. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, pp. 1078–1081, Sep. 06, 2019. doi: 10.35940/ijeat.f1002.0886s19. Available: http://dx.doi.org/10.35940/ijeat.F1002.0886S19
17. S. Chandolu, P. S. Naidu, and S. Sindhe, "Secure Energy Trade-off Analysis in Wireless Ad-Hoc Networks using Novel Scalable &amp; Secure Management Procedure," International Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 3. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, pp. 469–473, Sep. 30, 2019. doi: 10.35940/ijrte.a1018.098319. Available: http://dx.doi.org/10.35940/ijrte.A1018.098319
18. A. Chitransh and B. S. Kalyan, "ARM Microcontroller Based Wireless Industrial Automation System," Indian Journal of Microprocessors and Microcontroller, vol. 1, no. 2. Lattice Science Publication (LSP), pp. 8–11, Sep. 10, 2021. doi: 10.54105/ijmm.b1705.091221. Available: http://dx.doi.org/10.54105/ijmm.B1705.091221
19. Dr. A. M. Shamiulla*, "Role of Artificial Intelligence in Cyber Security," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 1. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, pp. 4628–4630, Nov. 30, 2019. doi: 10.35940/ijitee.a6115.119119. Available: http://dx.doi.org/10.35940/ijitee.A6115.119119
20. H. Koli and Prof. M. P. S. Chawla, "Comparative Study of Electric Vehicle Battery Systems with Lithium-Ion and Solid State Batteries," International Journal of Emerging Science and Engineering, vol. 10, no. 10. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, pp. 1–6, Sep. 30, 2022. doi: 10.35940/ijese.i2540.09101022. Available: http://dx.doi.org/10.35940/ijese.I2540.09101022

AUTHORS PROFILE

Dr. S. Hemalatha has completed BE (CSE) and ME (CSE) from Arulmigu Meenakshi Amman college of engineering in the year 2000 and 2004 respectively. Completed PhD from Anna University in the year of 2016. Presently pursuing Post Doctorial Program in Manipur International University under the research area of Mobile Adhoc Security. She has more than 22 years of experience in different engineering colleges. Presently working as a professor and Head in CSBS department at Panimalar institute of technology. She has more contribution in international and national journal , books and patents.

Professor (Dr) Harikumar Pallathadka is a highly accomplished individual in Law and Management, with Post Doctoral Degrees in both fields. With over 300 published research papers in reputable journals, including SCI/Scopus, he showcases his versatility and expertise. He has also published over 300 National and International patents, with around 50 awarded. Prof. Pallathadka is also well known social activist. An experienced administrator and an authority in Constitutional Law and Machine Learning, he currently holds the position of Professor and Vice Chancellor at Manipur International University. His extensive accomplishments and dedication highlight his exceptional abilities.

Prof. Rajesh Chinchewadi has completed BE (Computer Science & Engineering) from University BDT College of Engineering, Davangere, University of Mysore, Of Mysore in the year 1993. Completed EGMP (EMBA) from Indian Institute Of Management, Bangalore. He has more than 25 years of experience in different IT Technology MNCs - Hewelett Packard, Cisco, GE GXS, Startups in senior management positions. Presently working as a professor and Chief Technology Officer & Dean Innovation for Manipur International University, Director, Strategy for Global Investment firm and mentor to startups.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Lattice Science Publication (LSP)/ journal and/ or the editor(s). The Lattice Science Publication (LSP)/ journal and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.