# MAC Issues in Mobile Ad-hoc Network

Khushbu
Phd Scholar, Madhav University Sirohi
Rajasthan-307026, India

R. K. Bathla, PhD
Professor, Madhav University Sirohi
Rajasthan-307026, India

## ABSTRACT
Medium access control is a Protocol. It's arrangement of tenets or proccess to proficient utilization of shared medium, for example, remote, by various client. There are many of Issues of MANET( Mobile AD-Hoc Network) with MAC Layer. MAC layer is a lower sub layer of data-link layer. MAC layer is concerned with per link communication. Impact in MAC layer is the Major Issues in remote Transmission. It enables a few hub in system to share the medium utilizing the channel get to control components. Specially appointed remote systems present more noteworthy difficulties than framework remote systems at the MAC layer. so nonappearance of a unified controller. Macintosh conventions classes into two general classifications of conflict free and dispute based MAC conventions. MANETs have their unique constraints and characteristics. Macintosh conventions embody rule for efficient access to remote shared medium assume basic job in the conclusive and reasonable sharing of rare remote data transmission. The idea of the remote channel brings new issues like time shifting channel, area subordinate transporter detecting, and blasted blunders. Medium access control (MAC) conventions are a functioning point in nowadays, which organize the efficient utilization of the restricted shared remote asset. Be that as it may, in these remote systems, the restricted remote range, time-shifting spread qualities, appropriated numerous entrance control, low unpredictability, and vitality requirements together force significant challenges for MAC convention configuration to give dependable remote correspondences high information rates.

## Keywords
MANET, AD-HOC, Data link layer, MAC Layer, Wireless Transmission

## 1. INTRODUCTION
Wi-Fi cell advert-hoc systems are portrayed as systems with no physical associations. In these systems there is no fixed topology due to the portability of hubs, impedance, multipath engendering and course misfortune. along these lines a dynamic directing convention is required for these systems to trademark appropriately. Many Routing conventions have been developed for achieving this test. Versatile Ad hoc arrange comprises of hubs that must speak with one another without depending on any framework or pre-characterized chain of command. Medium access control (MAC) conventions give a way to hubs to get to the remote medium productively and impact allowed to the best of their capacity. Macintosh give an intend to hubs to get to the remote medium proficiently and impact allowed to the best of their capacity MAC Layer is Concern with per-link Communication. While routing Protocol deal with end-to-end communication [1]. medium access control (MAC) protocols is an active topic in these days, which arrange the efficient utilization of the restricted shared remote asset. Be that as it may, in these remote systems, the restricted remote range, time-differing engendering qualities, conveyed different access control, low unpredictability, and vitality limitations together force significant challenges for MAC convention configuration to give solid remote correspondences high information rates. [2] In the MAC layer, the open shared channel forces a considerable measure of difficulties for medium access control structure. MAC layer offer two class of services those class name is DCF and PCF. In flexible uncommonly named frameworks, obstruct occurs with obliged resources. Blockage occurs on shared frameworks when different customers fight for access to comparable resources (information exchange limit, pads, and lines). Blockage in adaptable improvised frameworks prompts transmission delays and distributes causes wastage of time and essentialness for recovery. Blockage control alludes to the system instrument and strategies used to control clog and keep the heap underneath the systems limit. Blockage dealing with can be partitioned into clog recuperation i.e. reestablish the working condition of the system when request surpasses limit and blockage evasion i.e. foresee clog and maintain a strategic distance from it with the goal that blockage never happens. It is pledged to error correction of anomalies transpire in the physical layer, framing, physical addressing, and resolving conflicts occurring in number of nodes to access the channel.

## 2. RELATED WORK
Here we take content from previous literature surveys and study of history.

**Krishna Gorantala** gave their contribution in the research on "Routing Protocols in Mobile Ad-hoc Networks" In this paper he find a route to a destination on demand, whenever communication is needed. Considering the bandwidth, throughput and packet loss, in both DSDV and AODV routing protocols, DSDV is best suited for only smaller networks and AODV is suited for general Ad-hoc networks in June 15, 2006.

**Basu dev shivahare**, **Charu wahi and Shalini Shivahare** gave their contribution in the field of research on" Routing Protocols in Mobile Ad-hoc Networks" published in international journal of emerging Technology and advanced engineering , march 2012.

**Sourabh Gupta & Girish Tiwari** gave their contribution in the field of "Challenges to MAC Layer in Mobile Ad-Hoc Networks & its Routing Protocols" they broadly discuss the above mentioned challenges at Network layer and MAC LAYER in mobile ad-hoc networks.

**S. Gopalakrishnan & P. Mohan Kumar** gave their contribution in the field of Analysis of Malicious Node Detection in MANET In their research paper "Performance Analysis of Malicious Node Detection and Elimination Using Clustering Approach on MANET" They include different aspects of cluster based malicious node detection methodology is proposed to detect and remove the malicious nodes.

**Muhammad Arshad Ali & Yasir Sarwar** gave their contribution in the field of security aspects in MANET In their research paper "Security Issues regarding MANET: Challenges and Solutions" they included different aspects of security in MANET and also implement some of the solutions security threats within MANET with respect to MANET network.

**Meenakshi Patel and Sanjay Sharma** gave their contribution in the field of malicious attacks. In their research paper "Detection of malicious attacks in MANET: behavioral approach " they included various types of attacks including black hole attack, gray hole attack, flooding etc. author introduced a new concept to categorize the nodes based on their behavior.

**Latha Tamilselvan, Dr. V. Sankaranarayana** has suggested the thought for aversion of various sorts of assaults on MANET. They Proposed an answer that is an improvement of the fundamental AODV directing convention, which will have the capacity to evade dark openings to diminish the likelihood is proposed to take a delay and check the reaction from all the neighboring hubs to locate a protected course.

**Hongqiang Zhal, Jianfeng Wang, Xiang Chen and Yuguang Fang** give there contribution for finding MAC challenges and solutions. In their research paper "Medium access control in mobile ad hoc networks: challenges and solutions" We first identify the challenges that are facing MAC in MANETs. Then we discuss the proposed MAC schemes according to their design goals, focusing on some critical design issues, and tradeoffs.

## 3. PROPOSAL FOR AD-HOC NETWORK ALGORITHM

Well ordered process for tackle issue of Ad Hoc Network

Step 1: sources 'S' check the number of available neighbor node .

Step 2: Select the path by Mobile agent to move towards the destination 'D' from source node S.

Step3: Now the mobile agent detect that congestion occurs between 'A to G' nodes due to earlier high data rates node A to Z forwarding more traffic into low data rate node F.

Step 4: Now the source check the number of available neighbor node (H or G) and clones the Mobile Agent to that neighbor, M1 & M2.

Step 5: The M1 moves towards the destination 'D' and node 'H' in a hop-by-hop manner in the path P1 and M2 in P2 respectively. Then the M1 calculate the data rates of that path P1 and similarly M2 calculates the data rate of P2.

P1 data rate = Size of Data / Channel delay

(E node)

P2 data rate = Size of Data / Channel delay

(G node)

Step 6: Presently source chooses way utilizing most elevated information rates of P2(S-B-D-F-G-H) and send information through the comparing way.

## 4. PROBLEM IN AD-HOC NETWORK

MAC protocol is design in structure so that the restricted transfer speed is used in productive way.

- Bandwidth Efficiency
- Quality of service support
- Mobility of Node
- Synchronization
- Hidden and Expose Terminal problems
- Distributed Nature Lack of Central Coordination

## 5. SOLUTION OF AD-HOC NETWORK

Principally three principle security administrations for MANETs

i. Authentication
ii. Confidentiality
iii. Integrity

**Definition of security services for MANETs**

- Authentication implies remedy personality is known to conveying expert. Verifiable in this definition is the supposition that the genuine creator has taken consideration to avert abuse of its character by unapproved elements and that if fraud has occurred, it is without the plot of the creator. The related idea of ``non-disavowal" suggests that it is infeasible for the implied creator to intrigue in this way.
- Confidentially is easiest way of information security from unauthorized access.
- Integrity means message is unaltered during the communication between two parties. A message has its ``integrity" ensured in the event that it is infeasible for its substance to be changed in travel with no such changes being in a split second clear to the beneficiary.
- When validation is accomplished in MANET then secrecy is simply an issue of encoding calculation on the session by utilizing keys. These security administrations can be given separately or blend, it just relies upon our necessities. Including lot's of problem AD-HOC network have these solution also Hidden Terminal Problem have solution like Request to send and clear to send. Due to the communicate of these message, all neighbor of the sender and beneficiary will be educated that the medium will be occupied, in this way forestalling them for transmitting and maintaining a strategic distance from the Collision.

## 6. PROBLEM OF MAC ISSUES

- PHY layer sit idle in interpreting pointless Packet and last dropping them At Mac Layer.
- Hidden node problem.
- Medium access control

## 7. SOLUTION OF MAC ISSUES

There are many solutions for MAC Issues some are as following.

i. IEEE 802.11 MAC
ii. Four way handshaking
iii. Two way handshaking
iv. Back off algorithm

v. Channel access defer minimization and throughput augmentation can be represented utilizing x-diagram.

vi. Performance measurements, for example, outline overhead, conflict overhead, delay, bundle conveyance proportion, dropped parcels because of crash, throughput and vitality utilization can be examined by handling the follow record utilizing awk content.

vii. Generally, two-way handshaking and four-way handshaking instrument decreases the impact rate. In the two way handshaking signal methodology, a hub transmits the affirmation to the sender hub on getting the information bundle. In the four-way handshaking signal methodology. The improved MAC convention utilizes Ready to Send/Clear to Send (RTS/CTS) procedure to diminish the parcel crash in remote transmissions.

viii. The back-off algorithms also play a vital role in reducing the collision between nodes. Because of various qualities of Mobile specially appointed system security is a functioning examination point in remote way, which is additionally a nontrivial testing to security design.

## 8. MAC LAYER PROTOCOLS FOR AD-HOC NETWORK

Here is much protocol for MAC Layer but some are most categories protocol is as following.

- Contestation Based conventions held Mechanism
- Contestation Based conventions with Scheduling Mechanism
- Contestation Based conventions
- Other

## 9. PREVIOUS MAC PROTOCOL

- Multiple Access with collision avoidance(MACA)
- Power Aware Multi Access Protocol with Signaling (PAMAS)
- Dual busy tone multiple access

**Table1.1: Simulation Parameters**

| NETWORK PARAMETERS | VALUES |
|---|---|
| No. of nodes | 20 |
| Topography area | 1000 m * 800m |
| Connection Type | User datagram protocol |
| Source Traffic | CBR |
| Pay Load | 512 |
| Routing protocol | AODV |
| Simulation Time | 800Sec. |
| No.of active connections | 10 |
| Network Simulator | NS2-2 |

Some important NS2 commands used for the simulation are as follows.

set tcp0 [new Agent/TCP]

Packet delivery ratio: Mathematically, it can be defined as:

PDR= RSize/SSize

RSize: is the sum of data packets received by the each destination and SSize:is the sum of data packets generated by the each source.

Packet Drop (Loss) Ratio: Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination.

Throughput: It is defined as the total number of packets delivered over the total simulation time.

Mathematically, it can be defined as:

Throughput = N/T

Where

N : number of bits received successfully by all destinations

T: is simulation time

Source : Node 1

Destination: Node 20

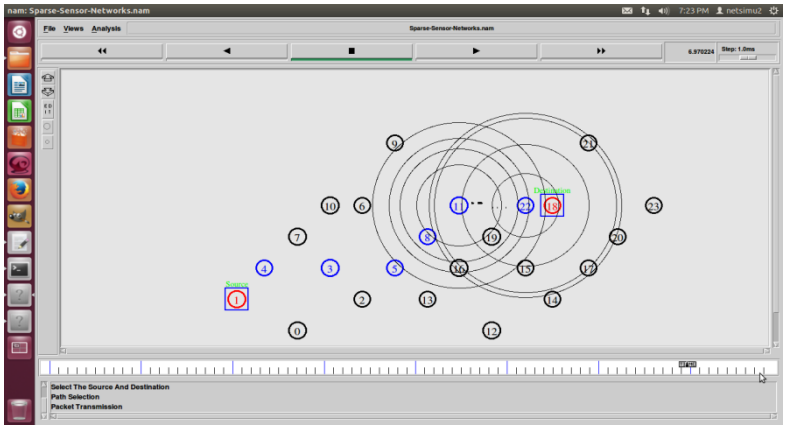



**Figure1.1: NS2-2**

## 10. EXPERIMENTAL RESULTS

Given values of parameters are used to evaluate the performance of network

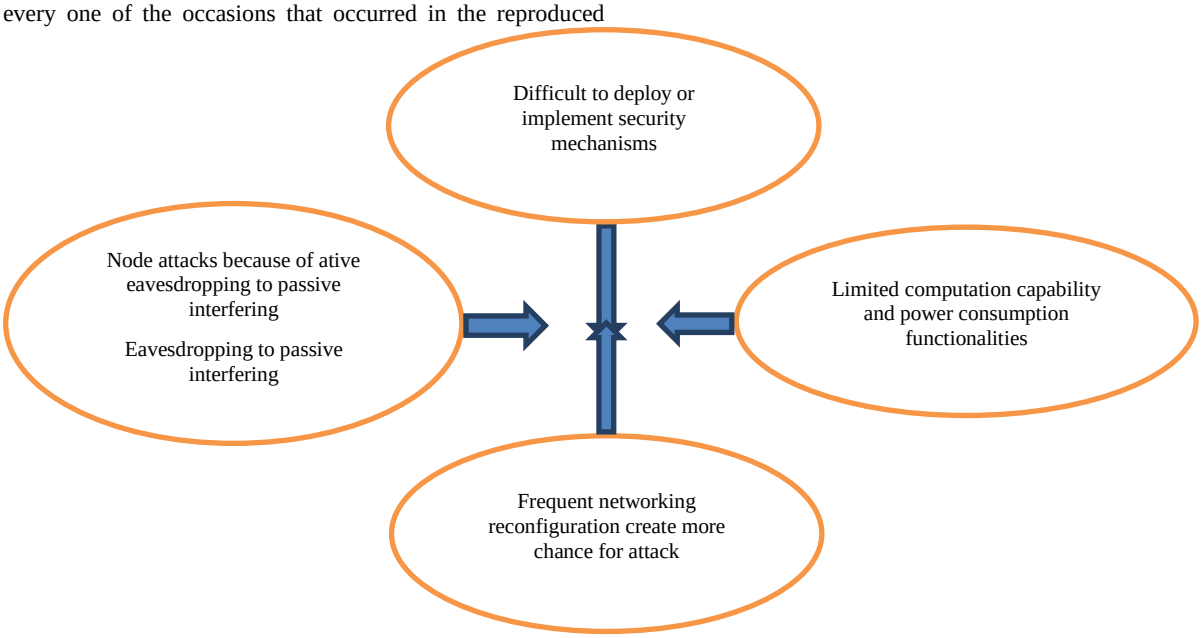
PDR = Total received packets / Total Sent packets

=384590/564905 = 0.68

Throughput = 564905/1000 = 564.90 kbps

At the point when the recreation setup is finished, we run the system test system, which makes two records one is Nam, and othrer is AWK here Nam is imagines and energizes the system. AWK record is a follow document, which catches every one of the occasions that occurred in the reproduced system. To separate the information from the follow record we compose the AWK content. Information got from AWK content is utilized to discover diverse parameters which incorporates bundle (sent,received, dropped) for CBR activity stream. This is utilized to discover PDR, DPR and Throughput, which are utilized to gauge the execution of AODV convention. Second it indicate Throughput = 564905/1000 = 564.90 kbps which is demonstrating great proficiency in bundle sending and reciving.

## 11. CHALLENGES WITH RESPECT TO WIRELESS SECURITY




The general motivation behind research is to:

i. Select non-congested paths or minimize excessive load of a node to its neighbors.

ii. Guarantee proficiency.

iii. Lessen end to end deferral and number of bundle lost by line flood.

iv. Diminish end to end postponement and number of bundle lost by line flood.

v. Improve the overall network performance.

vi. Reduce collision by dynamic channel estimation base route selection.

## 12. ENVIRONMENT OF NETWORK SIMULATION

Calculation based on Simulator-2 (NS-2) with graph notation. The depiction about reproduction condition is as per the following:

Network simulation tool is required to verify the functionalities and performance of networks. NS been designed for the growth of network as well as topology,

protocols, traffic, and etc, and is ready to support simulation for the large-scale network like net. NS difficult for general users to perform network simulation . The network modeling and analysis method should be done manually by users themselves. This circumstance makes it tough to perform reliable network simulation. Framework test framework 2 (NS2) is the delayed consequence of an on-going effort of inventive work that is administrated by researchers at Berkeley. It is a discrete event test framework centered at frameworks organization research. It gives extensive help to reenactment of TCP, coordinating, and multipath tradition. This substance is then used by ns in the midst of the reenactments. The eventual outcome of the reenactments is a yield pursue report that can be used to do data getting ready (learn postponement, throughput et cetera) and to picture the multiplication with a program called Network Animator.

## 13. FUTURE SCOPE AND CONCLUSION

Ad-hoc network has been receiving increasing attention amongst the researches in recent years, as a result of the accessible wireless network and mobile computing hardware bases square measure presently capable of supporting today's demand. All the malevolent nodes within the network can be recognized. it's noted that because the speed will increase, the share of false positive will increase portraying the network behavior. This is often as a result of because the speed will increase, association updates happen, nodes create or serve connections usually. MAC protocols set defined rules to force distributed nodes to access the wireless medium in an order and efficient manner. A large portion of the requirements on the structure of multi-channel MAC conventions for MANETs originate from the inalienable powerlessness of the remote NIC gadgets accessible in the market to send and get information at the same time on different channels. A perfect MAC answer for MANETs would be one that can work on various recurrence channels without wanting to perform channel exchanging. Maybe not long from now, such gadgets will be made accessible to business use requiring little to no effort, yet starting at now, looks into should keep finding an ideal arrangement inside these limitations.

The general reason for Research is to:

i. Select non-clogged routes or to restrict irrational pile of a center to its neighbors.

ii. Guarantee proficiency.

iii. Decrease delay

iv. less number of package lost by line surge.

v. Overhaul the use of advantages.

vi. General framework execution Improve and lessen crash for one of a kind channel estimation base course assurance.

## 14. REFERENCES

[1] Chandra Parkash " AD-HOC wireless Medium Access Protocol "

[2] Dr. Baruch Awerbuch & Amitabh Mishra "Medium Access Control Protocols for Ad-hoc Wireless Network."

[3] Chandra Prankish "Ad-Hoc wireless Media access protocol"

[4] Sunil Kumar, Vineet S. Raghavan "Medium Access Control protocols for ad hoc wireless networks: A survey".

[5] Ajay Chandra V. Gummalla And John O. Limb "Wireless Medium Access Control Protocols"

[6] Ahmed. A. Hadi , Zulkarnain Md. Ali, Yazan Aljeroudi "Improved Selfish Node Detection Algorithm for Mobile Ad Hoc Network".

[7] Alok Dwivedi and Gaurishankar Prajapati "Study of Congestion Control in Multi-Flow in MANET"

[8] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah "curity challenges in mobile ad hoc networks: a survey"layer Designs for Mobile Ad