Medium Access Control Algorithms for MANETs

A Project Report

submitted by

S Samantaray
(EE19M011)

in partial fulfillment of the
requirements for the award
of the degree of

MASTER OF TECHNOLOGY

DEPARTMENT OF ELECTRICAL
ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY

MADRAS (June 2021)

THESIS CERTIFICATE

This is to certify that the thesis titled **Survey of MAC solutions for MANETs**, submitted by **S Samantaray**, to the Indian Institute of Technology, Madras, for the award of the degree of **Master of Technology**, is a bonafide record of the research work done by him under our supervision. The contents of this thesis, in full or in parts,have not been submitted to any other Institute or University for the award of any degreeor diploma.

Prof. K Giridhar
Project Guide Professor
Dept. of Electrical Engineering
IIT-Madras, 600 036

Place: Chennai

Date: 24th June 2021

ACKNOWLEDGMENTS

I would like to take this opportunity to thank our Parents & Navy for their support and encouragement without which learning in and becoming a part of such a prestigious institution would not have been possible. I would like to dedicate this work to them.

I am thankful to Dr. K Giridhar for his continual support and invaluable advice throughout the duration of our research. I feel honored and encouraged to have worked under his guidance. Also we are very much thankful to Mr. Venkatesh for his help in the research.

ABSTRACT

MANET stands for Mobile adhoc Network also called as wireless adhoc network or adhoc wireless network that usually has a routable networking environment on top of a Link Layer adhoc network. Studies of adhoc wireless networks are a relatively new field gaining more popularity for various new applications. In these networks, the Medium Access Control (MAC) protocols are responsible for coordinating the access from active nodes. These protocols are of significant importance since the wireless communication channel is inherently prone to errors and unique problems such as the hidden-terminal problem, the exposed-terminal problem, and signal fading effects. Although a lot of research has been conducted on MAC protocols, the various issues involved have mostly been presented in isolation of each other. They consist of a set of static/mobile nodes connected wireless in a self-configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently. Each node behaves as a router as they forward traffic to other specified nodes in the network.

Designing a small scale and a large scale MANET requires efficient MAC protocol to define scheduling/decision rules at various nodes. Further, routing protocol is required to find least hop/optimal route from source node to destination node.

The report covers detailed survey of single channel MAC protocols suitable for small scale MANET with 15-30 nodes in an area of 1 Sq Km and Hybrid channel MAC protocol for large scale MANET with 100 to 200 nodes in an area of 25 sq Kms.

TABLE OF CONTENTS

ACKNOWLEDGMENTS **i**

ABSTRACT **ii**

1 INTRODUCTION **1**

2 CLASSIFICATION OF MANET MAC PROTOCOLS **3**

Basic Classification 3

Survey of Single-channel MAC protocols 6

3 MAC PROTOCOLS FOR SMALL SCALE MANETS **9**

Multiple Access Collision Avoidance 9

IEEE 802.11 MAC Scheme 17

FAMA 20

EMAC 28

4 MAC PROTOCOLS FOR LARGE SCALE MANETS **31**

Tactical Large scale MANET with Link State routing 35

Hybrid MAC Protocol 40

Clustering Techniques 41

5 MARKET SURVEY 42

6 SIMULATION: LARGE SCALE MANET **43**

7 CONCLUSION AND FUTURE SCOPE **43**

CHAPTER 1

Introduction

MANET stands for Mobile adhoc Network also called a wireless adhoc network or adhoc wireless network that usually has a routable networking environment on top of a Link Layer adhoc network.. They consist of a set of mobile nodes connected wireless in a self-configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently. Each node behaves as a router as they forward traffic to other specified nodes in the network.

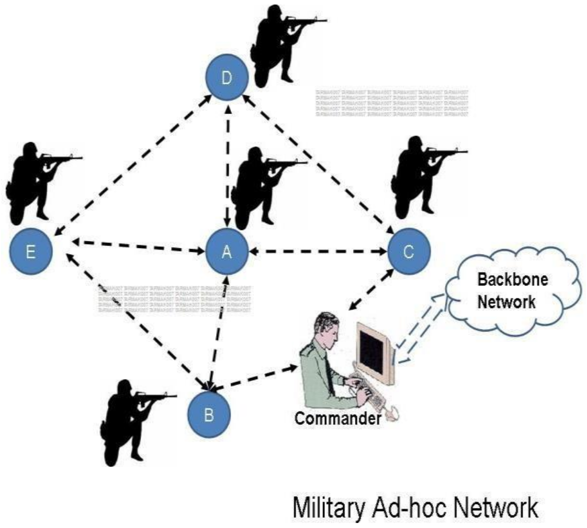


Figure 1.1 Basic Adhoc Network

MANET may operate a standalone fashion or they can be part of larger internet. They form a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes. The main challenge for the MANET is to equip each device to continuously maintain the information required to properly route traffic. MANETs consist of a peer-to-peer, self-forming, self-healing network MANETs circa 2000-2015 typically communicate at radio frequencies (30MHz-5GHz). This can be used in road safety, ranging from sensors for the environment, home, health, disaster rescue operations, air/land/navy defense, weapons, robots, etc.

The main characteristics of MANETs are: the complete lack of centralized control, lack of association among nodes, rapid mobility of hosts, frequent dynamically varying network topology, shared broadcast radio channel, insecure operating environment, physical vulnerability and limited availability of resources, such as CPU processing capacity, memory power, battery power, and bandwidth.

(a). **Dynamic Network Topologies**: The nodes in MANETs are free to move independently in any direction. The network's wireless topology may change frequently and randomly at unpredictable times and primarily consists of bidirectional links.

(b). **Low Bandwidth**: These networks have lower capacity and shorter transmission range than fixed infrastructure networks. The throughput of wireless communication is lesser than wired communication because of the effect of the multiple access, fading, noise, and interference conditions.

(c). **Limited Battery Power**: The nodes or hosts operate on small batteries and other exhaustible means of energy. So, energy conservation is the most important design optimization criteria.

(d). **Decentralized Control**: Due to unreliable links, the working of MANET depends upon cooperation of participating nodes. Thus, implementation of any protocol that involves a centralized authority or administrator becomes difficult.

(e). **Unreliable Communications**: The shared-medium nature and unstable channel quality of wireless links may result in high packet-loss rate and re-routing instability, which is a common phenomenon that leads to throughput drops in multi-hop networks. This implies that the security solution in wireless adhoc networks cannot rely on reliable communication.

(f). **Weak Physical Protection**: MANETs are more prone to physical security threats than fixed-cable nets. Mobile nodes are usually compact, soft and hand-held in nature. Today, portable devices are getting smaller and smaller. They could get damaged or lost or stolen easily and misused by an adversary. The increased possibility of different types of attacks should be carefully considered.

(g). **Scalability**: Due to the limited memory and processing power on mobile devices, the scalability is a key problem when we consider a large network size. Networks of 10,000 or even 100,000 nodes are envisioned, and scalability is one of the major design concerns.

FLOW OF THESIS

The thesis is organized as follows.

1. **Chapter 2** discusses some basic classification of MAC protocols used for MANETs followed by survey of various single channel MAC protocols.

2. **Chapter 3** discusses efficient single channel MAC protocols suitable for small scale MANETs,

3. **Chapter 4** discusses efficient MAC protocols suitable for large scale MANETs, typically of 100-200 nodes in 25 sq km area.

4. **Chapter 5** discusses Market survey of some MANET SDRs available in India & abroad.

5. **Chapter 6** discusses Simulation of Large scale MANET in *NS-3* using Cluster Head as Central Controller.

6. **Chapter 7** gives the conclusion and future work.

CHAPTER 2

CLASSIFICATION OF MANET MAC PROTOCOLS

This chapter briefly discusses some of the basic classification of MAC protocols used for basic MANETs followed by survey of multi-channel MAC protocols.

Basic Classification of MAC Protocols

MAC layer, sometimes also referred to as a sub-layer of the 'Data Link' layer, involves the functions and procedures necessary to transfer data between two or more nodes of the network. It is the responsibility of the MAC layer to perform error correction for anomalies occurring in the physical layer. The layer performs specific activities for framing, physical addressing, and flow and error controls. It is responsible for resolving conflicts among different nodes for channel access. Since the MAC layer has a direct bearing on how reliably and efficiently data can be transmitted between two nodes along the routing path in the network, it affects the Quality of Service (QoS) of the network. The design of a MAC protocol has to address issues caused by mobility of nodes and an unreliable time varying channel.

Various MAC schemes developed for wireless adhoc networks can be classified as shown in **Figure 2.1**. In contention-free schemes (e.g., TDMA, etc), certain assignments are used to avoid contentions. Contention based schemes, on the other hand, are aware of the risk of collisions of transmitted data.

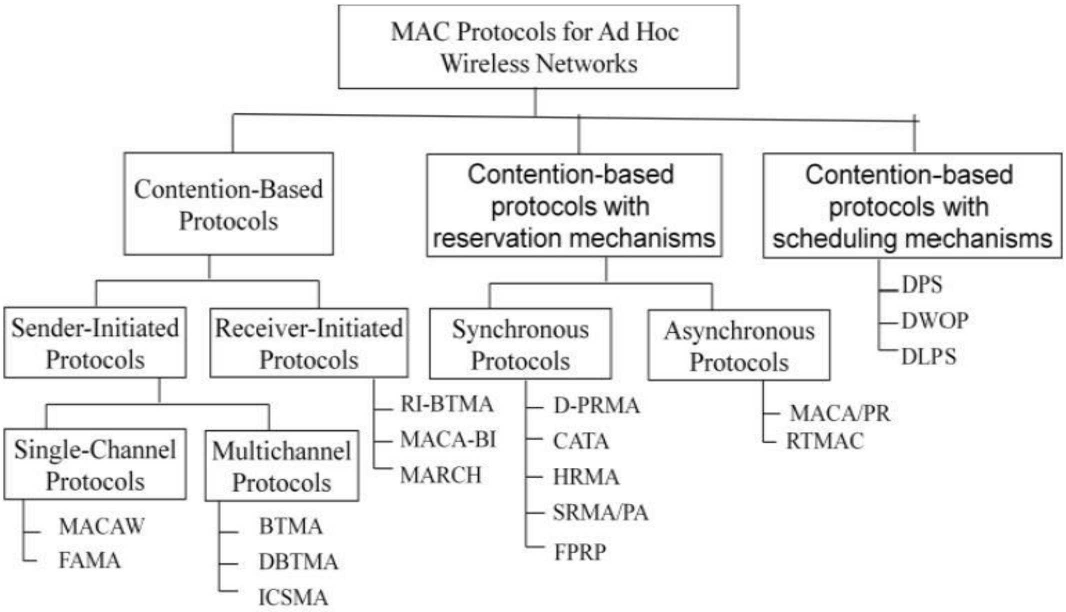

MAC Protocols for Ad Hoc Wireless Networks
Contention-Based Protocols
Contention-based protocols with reservation mechanisms
Contention-based protocols with scheduling mechanisms
Sender-Initiated Protocols
Receiver-Initiated Protocols
Synchronous Protocols
Asynchronous Protocols
DPS
DWOP
DLPS
Single-Channel Protocols
Multichannel Protocols
RI-BTMA
MACA-BI
MARCH
D-PRMA
CATA
HRMA
SRMA/PA
FPRP
MACA/PR
RTMAC
MACAW
FAMA
BTMA
DBTMA
ICSMA

Figure 2.1: Basic MAC Classification

Since contention-free MAC schemes are more applicable to static networks and/or networks with centralized control, we shall focus on contention-based MAC schemes in this survey. We can view this category as a collection of ‘random access’ and ‘dynamic reservation/collision resolution’ protocols.

In Random Access based schemes, such as ALOHA, a node may access the channel as soon as it is ready. Naturally, more than one node may transmit at the same time, causing collisions. ALOHA is more suitable under low system loads with large number of potential senders and it offers relatively low throughput. A variation of ALOHA, termed ‘Slotted ALOHA’, introduces synchronized transmission time-slots similar to TDMA. Nodes can now only transmit at the beginning of any time-slot.

The introduction of time slot doubles the throughput as compared to the pure ALOHA scheme, with the cost of necessary time synchronization. The CSMA-based schemes further reduce the possibility of packet collisions and improve the throughput. In order to solve the hidden and exposed terminal problems in CSMA, researchers have come up with many protocols, which are contention based but involve some forms of Dynamic Reservation/Collision Resolution. Some schemes use the Request-To-Send/Clear-To- Send (RTS/CTS) control packets to prevent collisions, e.g. Multiple Access Collision Avoidance (MACA) and MACA for Wireless LANs (MACAW). Yet others use a combination of carrier sensing and control packets.

The contention-based MAC schemes can also be classified as sender-initiated vs. receiver-initiated, single-channel vs. multiple-channel, power-aware, directional antenna based, unidirectional link based and QoS aware schemes. We briefly discuss these categories in the following. One distinguishing factor for MAC protocols is whether they rely on the sender initiating the data transfer, or the receiver requesting the same. As mentioned above, the dynamic reservation approach involves the setting up of some sort of a reservation prior to data transmission. If a node that wants to send data takes the initiative of setting up this reservation, the protocol is considered to be a ‘sender-initiated protocol’. Most schemes are sender-initiated. In a ‘receiver-initiated protocol’, the receiving node polls a potential transmitting node for data. If the sending node indeed has some data for the receiver, it is allowed to transmit after being polled. The MACA – By Invitation (MACA-BI) and Receiver Initiated Busy Tone Multiple Access (RI-BTMA) are examples of such schemes. As we shall see later, MACA-BI is slightly more efficient in terms of transmit and receive turn around times compared to MACA.

Another classification is based on the number of channels used for data transmission. Single channel protocols set up reservations for transmissions, and subsequently transmit their data using the same channel or frequency. Many MAC schemes use a single channel Multiple channel protocols use more than one channel in order to coordinate connection sessions among the transmitter and IEEE 802.11 MAC Scheme

The IEEE 802.11 specifies two modes of MAC protocol: distributed coordination function (DCF) mode (for adhoc networks) and point coordination function (PCF) mode (for centrally coordinated infrastructure-based networks). The DCF in IEEE 802.11 is based on CSMA with Collision Avoidance (CSMA/CA), which can be seen as a combination of the CSMA and MACA schemes. The protocol uses the RTS-CTS-DATA- ACK sequence for data transmission. Not only does the protocol use physical carrier sensing, it also introduces the novel concept of virtual carrier sensing. This is implemented in the form of a Network Allocation Vector (NAV), which is maintained by every node. The NAV contains a time value that represents the duration up to which the wireless medium is expected to be busy because of transmissions by other nodes. Since every packet contains the duration information for the remainder of the message, every node overhearing a packet continuously updates its own NAV. Time slots are divided into multiple frames and there are several types of inter frame spacing (IFS) slots. In increasing order of length, they are the Short IFS (SIFS), Point Coordination Function IFS (PIFS), DCF IFS (DIFS) and Extended IFS (EIFS). The node waits for the medium to be free for a combination of these different times before it actually transmits. Different types of packets can require the medium to be free for a different number or type of IFS. For instance, in ad hoc mode, if the medium is free after a node has waited for DIFS, it can transmit a queued packet. Otherwise, if the medium is still busy, a backoff timer is initiated.

The initial back-off value of the timer is chosen randomly from between 0 and CW-1 where CW is the width of the contention window, in terms of time-slots. After an unsuccessful transmission attempt, another back-off is performed with a doubled size of CW as decided by binary exponential back-off (BEB) algorithm. Each time the medium is idle after DIFS, the timer is decremented. When the timer expires, the packet is transmitted. After each successful transmission, another random back-off (known as post-back-off) is performed by the transmission-completing node. A control packet such as RTS, CTS or ACK is transmitted after the medium has been free for SIFS. Fig. 4 shows the channel access in IEEE 802.11. IEEE 802.11 DCF is a widely used protocol for wireless LANs. Many of the MAC schemes discussed in this paper are based on it. Some other features of this protocol will be discussed along with such schemes. A. receiver nodes. The FCC mandates that all radios using the ISM band must employ either DSSS or FHSS schemes. Several MAC protocols have been developed for using multiple channels through frequency-hopping techniques, e.g., Hop-Reservation Multiple Access (HRMA) scheme.

Some others use a special control-signal on a separate channel for protecting the actual data that is transmitted on the data channel(s). As mentioned earlier, it becomes important in the context of low power devices, to have energy efficient protocols at all layers of the network model. Much work has already been done for studying and developing appropriate MAC protocols that are also ‘power aware’. Yet another class of

MAC protocols uses ‘directional antennas’.

The advantage of this method is that the signals are transmitted only in one direction. The nodes in other directions are therefore no longer prone to interference or collision effects, and spatial reuse is facilitated. Several MAC schemes have been proposed for ‘unidirectional’ links With the growing popularity of adhoc networks, it is reasonable to expect that users will demand some level of QoS from it, such as end-to-end delay, available bandwidth, probability of packet loss, etc.

However, the lack of centralized control, limited bandwidth channels, node mobility, power or computational constraints and the error-prone nature of the wireless medium make it very difficult to provide effective QoS in adhoc networks Since the MAC layer has a direct bearing on how reliably and efficiently data can be transmitted from one node to the next along the routing path in the network, it affects the Quality of Service (QoS) of the network. Several ‘QoS-aware’MAC schemes have been reported in the literature.

Note that the above categories are not totally independent of each other. In fact, a given MAC protocol may belong to more than one category. For example, Power Aware Medium Access Control with Signaling (PAMAS) is a power-aware protocol that also uses two channels. Similarly; RI-BTMA is a receiver-initiated MAC scheme that uses multiple channels. Several representative MAC schemes for AdHoc Wireless Networks are briefly discussed and summarized in the following two sections. For the sake of convenience in discussion, we have broadly arranged the schemes in ‘Non QoS’ and ‘QoS-Aware’ classes. The non-QoS MAC schemes in Section III have been further divided in the following categories: general, power-aware, multiple channel, directional antenna-based, and unidirectional MAC protocols. Similarly, QoS-aware schemes (in Section IV) have been arranged in a few categories according to their properties. In the process of choosing these MAC schemes, we tended to select those that are more representative in their category. I

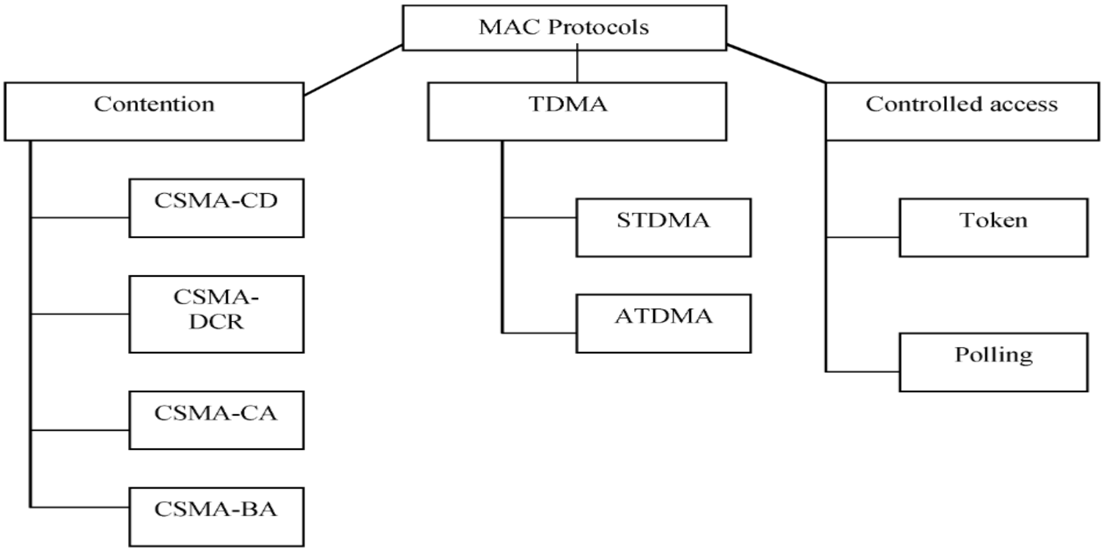


Figure 2.2: Other Classes of MAC protocols

Survey of Single-channel MAC protocols

For accessing the shared wireless medium in adhoc networks, two families of medium access control (MAC) protocols are dominant. The first family is contention-based protocols, typically using Carrier Sense Multiple Access (CSMA) technique. Such MAC protocols use available bandwidth on demand and are very flexible and efficient for low traffic load conditions and small network sizes. When network size increases and network traffic is high, CSMA-based protocols are not able to satisfy QoS requirements, implying that CSMA-based protocols are not scalable.

A second family of MAC protocols for adhoc networks is contention-free protocols, usually based on the Time-Division Multiple Access (TDMA) mechanism. TDMA-based medium access is one of the most common medium access methods where the wireless medium is time-shared by all nodes. Channel bandwidth in the network is divided into time frames, called super frames, with every super frame further partitioned into time slots. Multi-frequency

TDMA (Mf-TDMA) extends the basic TDMA medium access method, which uses only one frequency channel, to multiple channels. Slots in a Mf-TDMA super frame are represented as time-frequency tuples. In TDMA-based protocols each node transmits only during slots allocated to it, avoiding any contention for accessing the shared medium.

Compared to CSMA-based protocols, TDMA-based protocols mitigate internal collisions and thus improve delivered QoS for large-scale networks with high traffic demands. Due to its favorable properties in terms of scalability, TDMA scheduling techniques have gained attention for larger adhoc networks in recent years. However, the reliability and throughput of networks with TDMA access schemes may still be impacted by external interference or the occurrence of exposed/hidden nodes. For the function of slot allocation in TDMA schemes, there are static and dynamic algorithms.

As adhoc networks need to support constant changes in traffic demands and network topology, dynamic scheduling algorithms are known to outperform static scheduling algorithms. There exist two main models for handling dynamic TDMA scheduling: centralized and distributed. Centralized models consist of one or more control nodes that gather information about the network state and make scheduling decisions that are advertised to each node. In distributed models, decision making is done at the node level based on local information on the network without requiring any centralized control; nodes exchange information about slot usage with their neighbors in order to take distributed decisions on slot allocation.

Changes in network topology or traffic patterns result in continuous schedule recalculations and increased control overhead, thus leading to degraded network performance. Moreover, centralized scheduling protocols are not scalable as they incur high control overhead for large-scale wireless networks. In dynamic and large adhoc networks, distributed slot allocation algorithms are preferred to cope with scalability and changes in the network topology. Also, distributed algorithms are more fault- tolerant, as a major problem in centralized algorithms is the existence of a single point of failure; if the central control node fails or disconnects, slot scheduling cannot be executed anymore. In any case, whereas many distributed scheduling protocols are proposed so far, an increase in size and/or density of wireless networks still induces scalability issues for existing protocols. The most common reason for the scalability issues in large-scale adhoc networks is their multi-hop nature, which highly depends on network size and packet forwarding capabilities. Other various classes of MAC protocols are listed in **figure 2.2.**

CHAPTER 3

EFFICIENT MAC PROTOCOLS FOR SMALL SCALE MANETS

Based on literature survey & outcomes from chapter 2, the following MAC protocols are found to be suitable for supporting a small scale MANET. These protocols are based on the categories explained in chapter 2.

Multiple Access Collision Avoidance (MACA)

The MACA protocol was proposed by Karn to overcome the hidden and exposed terminal problems in CSMA family of protocols. MACA uses two short signaling packets, similar to the AppleTalk protocol. In Fig. 3.1, if node A wishes to transmit to node B, it first sends an RTS packet to B, indicating the length of the data transmission that would later follow. If B receives this RTS packet, it returns a CTS packet to A that also contains the expected length of the data to be transmitted. When A receives the CTS, it immediately commences transmission of the actual data to B. The key idea of the MACA scheme is that any neighboring node that overhears an RTS packet has to defer its own transmissions until some time after the associated

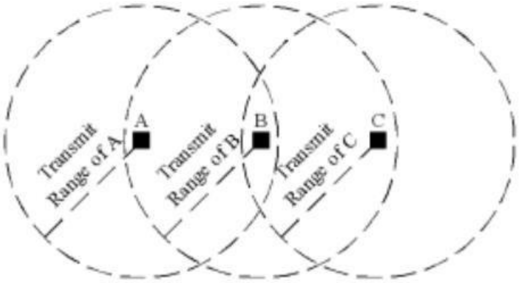


Figure 3.1 Hidden Terminal Problem

CTS packet would have finished, and that any node overhearing a CTS packet would defer for the length of the expected data transmission. In a hidden terminal scenario (see Fig. 3.1) as explained in Section I, C will not hear the RTS sent by A, but it would hear the CTS sent by B. Accordingly, C will defer its transmission during A’s data transmission. Similarly, in the exposed terminal situation, C would hear the RTS sent by

B, but not the CTS sent by A. Therefore C will consider itself free to transmit during B's transmission. It is apparent that this RTS-CTS exchange enables nearby nodes to reduce the collisions at the receiver, not the sender. Collisions can still occur between different RTS packets, though. If two RTS packets collide for any reason, each sending node waits for a randomly chosen interval before trying again.

This process continues until one of the RTS transmissions elicits the desired CTS from the receiver. MACA is effective because RTS and CTS packets are significantly shorter than the actual data packets, and therefore collisions among them are less expensive compared to collisions among the longer data packets. However, the RTS-CTS approach does not always solve the hidden terminal problem completely, and collisions can occur when different nodes send the RTS and the CTS packets.

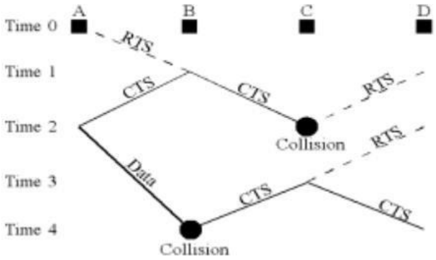


Figure 3.2 Failure of RTS-CTS in solving Hidden Terminal Problem

Let us consider an example with four nodes A, B, C and D in Fig. 3.2. Node A sends an RTS packet to B, and B sends a CTS packet back to A. At C, however, this CTS packet collides with an RTS packet sent by D. Therefore C has no knowledge of the subsequent data transmission from A to B. While the data packet is being transmitted, D sends out another RTS because it did not receive a CTS packet in its first attempt. This time, C replies to D with a CTS packet that collides with the data packet at B. In fact, when hidden terminals are present and the network traffic is high, the performance of MACA degenerates to that of ALOHA. Another weakness of MACA is that it does not provide any acknowledgment of data transmissions at the data link layer. If a transmission fails for any reason, re-transmission has to be initiated by the transport layer.

This can cause significant delays in the transmission of data. In order to overcome some of the weaknesses of MACA, It is also found that MACA for Wireless (MACAW) scheme that uses a five step RTS-CTS-DS-DATA-ACK exchange. MACAW allows much faster error recovery at the data link layer by using the acknowledgment packet (ACK) that is returned from the receiving node to the sending node as soon as data reception is completed. The back-off and fairness issues among active nodes were also investigated. MACAW achieves significantly higher throughput compared to MACA. It however does not fully solve the hidden and exposed terminal problems.

The typical sender-initiated protocols, the sending node needs to switch to receive mode (to get CTS) immediately after transmitting the RTS. Each such exchange of control packets adds to turnaround time, reducing the overall throughput. MACA-BI is a receiver-initiated protocol and it reduces the number of such control packet exchanges. Instead of a sender waiting to gain access to the channel, MACA-BI requires a receiver to request the sender to send the data, by using a ‘Ready-To-Receive’ (RTR) packet instead of the RTS and the CTS packets. Therefore, it is a two-way exchange (RTR- DATA) as against the three-way exchange (RTS-CTS-DATA) of MACA. Since the transmitter cannot send any data before being asked by the receiver, there has to be a traffic prediction algorithm built into the receiver so it can know when to request data from the sender.

The efficiency of this algorithm determines the communication throughput of the system. The algorithm proposed by the authors piggybacks the information regarding packet queue length and data arrival rate at the sender in the data packet. When the receiver receives this data, it is able to predict the backlog in the transmitter and send further RTR packets accordingly. There is a provision for a transmitter to send an RTS packet if its input buffer overflows. In such a case, the system reverts to MACA. The MACA-BI scheme works efficiently in networks with predictable traffic pattern. However, if the traffic is bursty, the performance degrades to that of MACA.

IEEE 802.11 MAC Scheme.

The IEEE 802.11 specifies two modes of MAC protocol: distributed coordination function (DCF) mode (for adhoc networks) and point coordination function (PCF) mode (for centrally coordinated infrastructure-based networks). The DCF in IEEE 802.11 is based on CSMA with Collision Avoidance (CSMA/CA), which can be seen as a combination of the CSMA and MACA schemes. The protocol uses the RTS-CTS-DATA- ACK sequence for data transmission. Not only does the protocol use physical carrier sensing, it also introduces the novel concept of virtual carrier sensing.

This is implemented in the form of a Network Allocation Vector (NAV), which is maintained by every node. The NAV contains a time value that represents the duration up to which the wireless medium is expected to be busy because of transmissions by other nodes. Since every packet contains the duration information for the remainder of the message, every node overhearing a packet continuously updates its own NAV. Time slots are divided into multiple frames and there are several types of inter frame spacing (IFS) slots. In increasing order of length, they are the Short IFS (SIFS), Point Coordination Function IFS (PIFS), DCF IFS (DIFS) and Extended IFS (EIFS). The node waits for the medium to be free for a combination of these different times before it actually transmits. Different types of packets can require the medium to be free for a different number or type of IFS. For instance, in adhoc mode, if the medium is free after a node has waited for DIFS, it can transmit a queued packet. Otherwise, if the medium is still busy, a back-off timer is initiated.

The initial back-off value of the timer is chosen randomly from between 0 and CW-1 where CW is the width of the contention window, in terms of time-slots. After an unsuccessful transmission attempt, another back-off is performed with a doubled size of

CW as decided by binary exponential back-off (BEB) algorithm.

Each time the medium is idle after DIFS, the timer is decremented. When the timer expires, the packet is transmitted. After each successful transmission, another random back-off (known as post-back-off) is performed by the transmission-completing node. A control packet such as RTS, CTS or ACK is transmitted after the medium has been free for SIFS. Fig. 4 shows the channel access in IEEE 802.11. IEEE 802.11 DCF is a widely used protocol for wireless LAN's. Many of the MAC schemes discussed in this paper are based on it. Some other features of this protocol will be discussed along with such schemes.

The typical sender-initiated protocols, the sending node needs to switch to receive mode (to get CTS) immediately after transmitting the RTS. Each such exchange of control packets adds to turnaround time, reducing the overall throughput. MACA-BI is a receiver-initiated protocol and it reduces the number of such control packet exchanges. Instead of a sender waiting to gain access to the channel, MACA-BI requires a receiver to request the sender to send the data, by using a 'Ready-To-Receive' (RTR) packet instead of the RTS and the CTS packets. Therefore, it is a two-way exchange (RTR-DATA) as against the three-way exchange (RTS-CTS-DATA) of MACA.

Since the transmitter cannot send any data before being asked by the receiver, there has to be a traffic prediction algorithm built into the receiver so it can know when to request data from the sender. The efficiency of this algorithm determines the communication throughput of the system. The algorithm proposed by the authors piggybacks the information regarding packet queue length and data arrival rate at the sender in the data packet. When the receiver receives this data, it is able to predict the backlog in the transmitter and send further RTR packets accordingly. There is a provision for a transmitter to send an RTS packet if its input buffer overflows. In such a case, the system reverts to MACA. The MACA-BI scheme works efficiently in networks with predictable traffic pattern. However, if the traffic is bursty, the performance degrades to that of MACA.

Floor Acquisition Multiple Access (FAMA) FAMA is another MACA based scheme that requires every transmitting station to acquire control of the floor (i.e., the wireless channel) before it actually sends any data packet . Unlike MACA or MACAW, FAMA requires that collision avoidance should be performed both at the sender as well as the receiver. In order to 'acquire the floor', the sending node, sends out an RTS using either non-persistent packet sensing (NPS) or non-persistent carrier sensing (NCS). The receiver responds with a CTS packet, which contains the address of the sending node. Any station overhearing this CTS packet knows about the station that has acquired the floor. The CTS packets are repeated long enough for the benefit of any hidden sender that did not register another sending node's RTS.

EMAC.

Protocol Description. EMAC is a wireless medium reservation asynchronous multi-hop wireless networks developed by Texas Instruments and Rice University (USA) in year 2010. It exploits limited routing information at the MAC layer, EMAC enables multiple asynchronous stations along a delivery path to cooperate in their random medium access. In particular, a control frame can travel across a multi-hop path composed of asynchronous nodes, and make synchronized medium reservations for an upcoming data frame transmission. This distributed cooperation at the MAC layer can greatly improve the medium reservation efficiency by reducing intra-flow contentions. EMAC is designed for general multi-hop wireless networks and does not assume clock synchronization. It also supports higher, more varied traffic loads. EMAC introduces synchronized intra-flow coordination across multiple asynchronous hops while still using CSMA/CA to randomly access the wireless medium and to alleviate hidden terminal problems. The simulation results shows that EMAC can significantly improve end-to-end network throughput by reducing intra-flow contention.

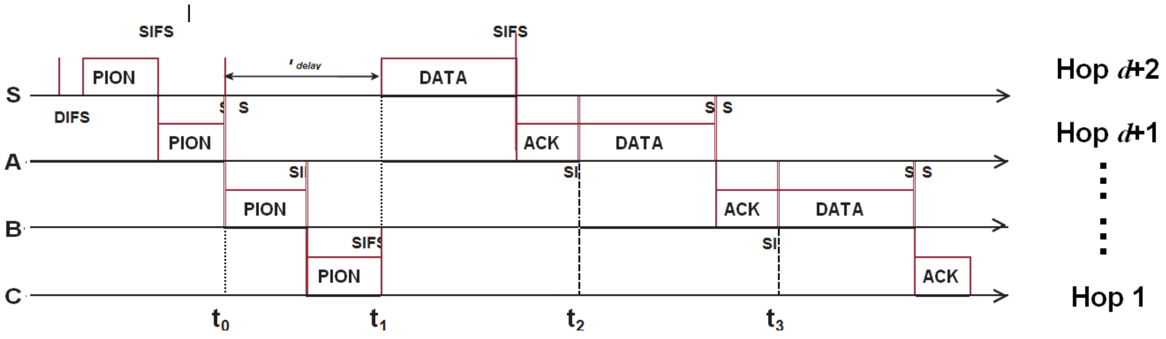


Figure 3.3 Operation of EMAC

Node S here has a data packet to send to some node several hops away. Node S transmits a PION (Pioneer) control frame to the downstream node A, which relays the PION to B. The PION may be relayed again by B if B is not the final destination of the data packet. Similar to an RTS in IEEE 802.11, a PION is used for requesting communication to a downstream node; simultaneously, forwarding the PION is used for confirming the PION receipt from the upstream node, like a CTS in IEEE 802.11.

If S receives the forwarded PION from A, S will then send the data frame to A after a scheduled delay that allows the PION to be further forwarded downstream without interfering with the data transmission. In order to handle asynchronous clocks at distributed nodes and to maximize network throughput, nodes in EMAC calculate and maintains scheduling information such as *Tdelay*, t0, ..., t3 (shown in the figure and described more fully below) in a distributed manner using only their local, un-synchronized clocks.

The transmission of EMAC protocol is as follows:-

(a) **Pioneer (PION) Frame Transmission**:- A PION frame in EMAC contains the necessary information, such as the *Final Destination Address* and *Hop Count*, to allow relaying nodes to forward the PION and reserve the medium for the upcoming data frame over multiple hops across the routing path. EMAC's PION frame also contains a field called *Data Delay Factor*, which controls the delay between reception of a PION and transmission of the corresponding data frame at the originating node. The PION relaying process continues until the final destination is reached, until a dropped PION interrupts the relaying process, or until the current requested transmission schedules conflict with any existing schedule

(b) **Data Transmission**. First, a relaying node must determine the time at which the data frame transmission starts at the hop-0 node along the path. Only after that, a relaying node can further predict when the data will arrive based on the *Data Frame Duration* and the *Hop Count* carried in the corresponding PION. Second, the schedule for data frame transmissions must ensure that data frames do not to collide with the ongoing PION transmissions .In *Figure 3.3*, node S must wait for an extra time period *Tdelay* before starting to transmit the data frame to
A. This delay is necessary, as if S transmits the data frame immediately after receiving the PION from A, the data transmission may collide at A with another PION transmission from a downstream node, such as nodes B or C.

(c) **Scheduling Using Local Clocks**. EMAC also introduces the mechanism of *Transmission Commitment* (TC) at a relaying node to avoid potential scheduling conflicts for correct and efficient medium reservation. A TC is a time segment during which the relaying node will be busy for either receiving or transmitting. A TC is calculated based on a nodes' local clock, which makes it suitable for a network without synchronized clocks. EMAC is intended for higher or more varied traffic loads.

Simulation. The EMAC simulation module is implemented based on the IEEE 802.11 module that is distributed together with ns-2. In the simulations, a *single omni-directional antenna* is used at each node, with radio propagation modeled by the common combined *Free Space* and *Two-Ray Ground reflection model*. Table I shows the key parameters used in our simulations.

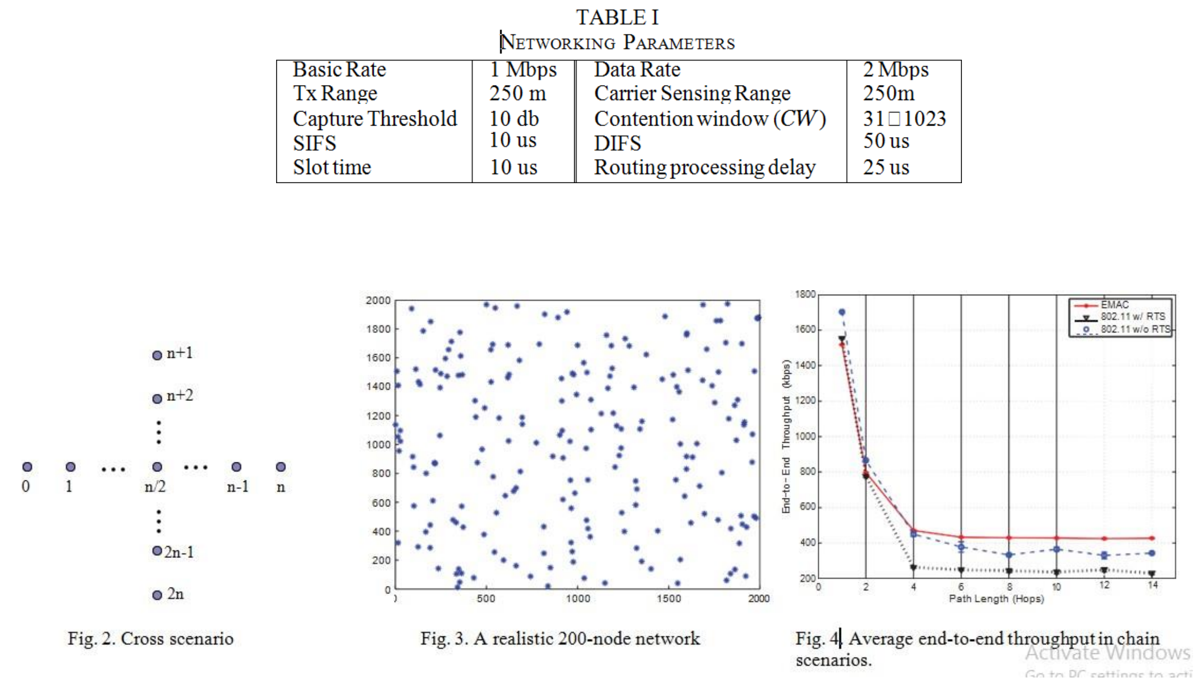


TABLE I
NETWORKING PARAMETERS

Basic Rate	1 Mbps	Data Rate	2 Mbps
Tx Range	250 m	Carrier Sensing Range	250m
Capture Threshold	10 db	Contention window (*CW*)	31□1023
SIFS	10 us	DIFS	50 us
Slot time	10 us	Routing processing delay	25 us

Fig. 2. Cross scenario

Fig. 3. A realistic 200-node network

Fig. 4 Average end-to-end throughput in chain scenarios.

Figure 3.4 Simulation result

In the paper the EMAC Data Delay Factor is set to 2, as it is believed that in most of the cases, simultaneous wireless transmission from 3 hops away will not interfere with a local transmission and reception. In the simulations, traffic loads are generated by constant bit rate (CBR) UDP flows. The UDP packet size is fixed during one simulation. When a data frame is transmitted, the frame includes a 28-byte MAC header (in both EMAC and IEEE 802.11) and a 20-byte IP header, in addition to the UDP payload. The PION frame size is set to 8 bytes larger than a RTS frame (28 bytes, total) to carry the extra information.

In the paper, three basic types of scenarios are considered in simulations, *chain scenarios*, *cross scenarios and realistic scenario*, as illustrated in *Figure 3.4* and *Figure 3.5*, respectively. In a *chain scenario*, nodes are deployed along a *straight line*. Neighboring nodes are *200 meters apart*, which is just within the range of a single wireless transmission hop (250 meters). One CBR flow sends packets from one end of the chain to the other end.

For a *cross scenario*, it is composed of two chains deployed across each other. One node is shared by both chains at their midpoints. Two CBR flows send packets independently, one from the end of each chain to the opposite end of the same chain. Packets of the two flows are generated at the same time and at the same rate to create inter-flow contention in the crossing area.

Also, an example of *realistic scenario* is also considered, shown in Figure 3.5. This scenario has *200 nodes* randomly distributed in a *2000 meters by 2000 meters* square area. 1500 bytes packet size is used for the simulation. Each simulation runs for 10 seconds of simulation time. For each network configuration, the average over 4 runs with random seeds is reported.

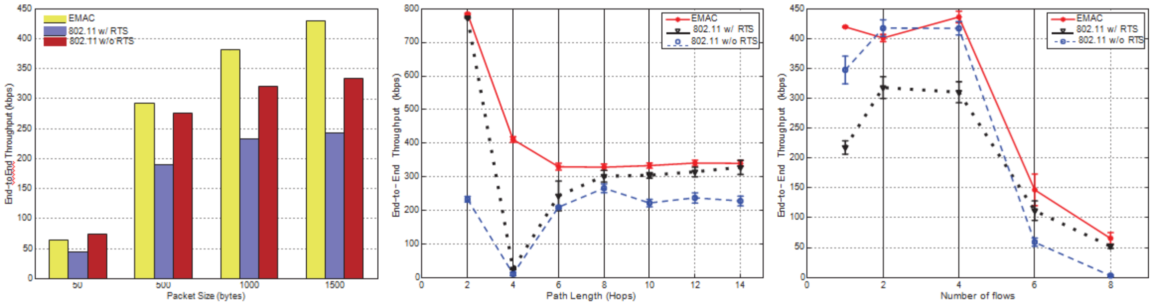


Fig. 6. End-to-end throughput with different packet sizes in the 8-hop chain scenario

Fig. 7. Average end-to-end throughput in the cross scenarios.

Fig. 8 Combined average end-to-end throughput in the realistic scenario.

Figure 3.5: Overview realistic scenari

Evaluations of scenarios is as under mentioned below:-

(a) **Evaluations of chain scenario**. EMAC is evaluated in the chain scenarios, with the length of the chains varied from 1 hop to 14 hops. *Figure 3.5* shows the change in average end-to-end throughput in the chain scenarios with different path lengths when the packet size is 1500 bytes. All three protocols (EMAC, IEEE 802.11 with RTS, and IEEE 802.11 without RTS) decrease significantly in throughput as the path length increases when the path length is smaller than 4 hops, which is because the medium is shared by more links as path length increases. When the path length is 4 hops and more, EMAC shows the best throughput among the three protocols. mechanism over RTS/CTS. In these scenarios, intra-flow contention is the major factor determining the network performance. EMAC's multi-hop delivery capability therefore can be very useful here, since a packet from a node can be delivered multiple hops away before the node begins to send the next packet, significantly reducing the intra- flow contention between one node and its downstream nodes. To show EMAC's performance with different packet sizes, *Figure 3.5* shows the average end-to- end throughput in the 8- hop chain scenario with four different packet sizes. EMAC generally shows its performance advantage over IEEE 802.11 increases as the packet sizes becomes larger, except that IEEE 802.11 without RTS shows the best throughput when the packet size is very small (50 bytes). This is because the overhead of RTS/CTS or PION transmissions cannot be offset by their benefit in preventing hidden terminal transmissions. An interesting observation is that IEEE 802.11 without RTS still has better throughput than does 802.11 with RTS with the large packet sizes, which is against the general belief that RTS/CTS can help improve the MAC efficiency when the packet size is large. This is because in the chain scenario, all the packets are being sent towards the same direction, so that a transmission at a downstream hop may cause the transmission at the immediate upstream hop to fail but not vice versa.

Further, when such a hidden downstream terminal causes some packet drops at the upstream, fewer packets from upstream nodes survive to be received by downstream nodes, limiting the number of further such collisions that can be caused by transmissions from these hidden downstream nodes since they will finally get no packets to send. Therefore, the negative impact of hidden terminals in the chain scenarios is somewhat self-constrained, making IEEE 802.11 with RTS not able to offset the overhead from its RTS and CTS transmissions.

(b) **Evaluations of cross scenario**. EMAC is also evaluated in the cross scenarios with backlogged UDP loads; the path length of the flows is varied from 2 hops to 14 hops. *Figure 3.5* shows the average end-to-end throughput combined from the two flows in cross scenarios with increasing path length when the packet size is 1500 bytes. IEEE 802.11 without RTS performs the worst among the three protocols. This is because both EMAC and IEEE 802.11 with RTS use control frames to avoid the potential data frame transmission collisions caused by hidden terminals in the crossing area. In Figure 3.5, an interesting observation is that when the path length of the flows is 4 hops, IEEE 802.11 receives almost zero throughput. In a 4-hop cross scenario using IEEE 802.11, when the two hop-1 nodes of each flow try to deliver their packets to their next- hop nodes, which are actually the very node at the crossing point, their packets have a very high chance to collide with each other. This problem is becoming worse in that while the two hop nodes wait for each other or wait for the node at the crossing point to resolve their contention, their upstream nodes, the two hop (source) nodes, which can only see clear medium, are still transmitting more packets to them, which further makes the contention at the crossing area worse. The intra-flow contention and inter-flow contention are both very high in the 4-hop cross scenario, driving the throughput of IEEE 802.11 down to a starvation level. For EMAC, however, since a PION frame can be potentially transmitted across multiple hops in one transaction, the source node and the node at the crossing point can coordinate to reduce the severe intra-flow and inter-flow contention; EMAC is thus still be able to have good throughput in this case.

(c) **Evaluations of Realistic scenario**. EMAC is also evaluated in the 200-node realistic random scenario with backlogged UDP loads. Traffic loads in the simulations come from a number of randomly selected 12-hop backlogged UDP flows. shows the change in average combined end-to-end throughput from all flows in the realistic scenario when the packet size is 1500 bytes. IEEE 802.11 without RTS has the worst performance among the three protocols when the number of flows in the network is more than 4 due to its lack of protection against hidden terminals. IEEE 802.11 with RTS, however, has the worst performance among the three protocols when the number of flows in the network is within 4. This is because the use of RTS/CTS frames to protect data frame transmissions against hidden terminals becomes less necessary when inter-flow contention is not severe. Among the three protocols, EMAC generally shows the best performance, regardless of the number of flows.

EMAC is single channel CSMA/CA MAC protocol suitable for small scale. However inside the network it uses synchronized multi-hop medium reservation through a Pioneer (PION) by scheduling frame and distributed schedule resolution algorithm. Simulation results under various scenarios and traffic loads have shown the great potential of EMAC’s PION mechanism over RTS/CTS mechanism in improving throughput in asynchronous multi-hop wireless networks. EMAC improves *throughput over IEEE 802.11 with RTS/CTS by up to 85%*.

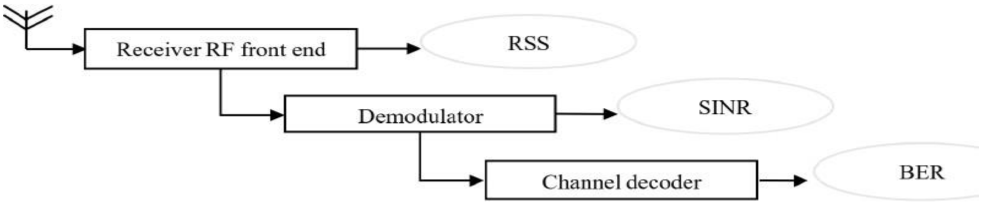
CHAPTER 4

EFFICIENT MAC PROTOCOLS FOR LARGE SCALE MANETS

Based on literature survey & outcomes from chapter 2 & 3, the following MAC protocols are found to be suitable for supporting a large scale MANET.

4.1 Tactical Large scale MANET with Link State routing

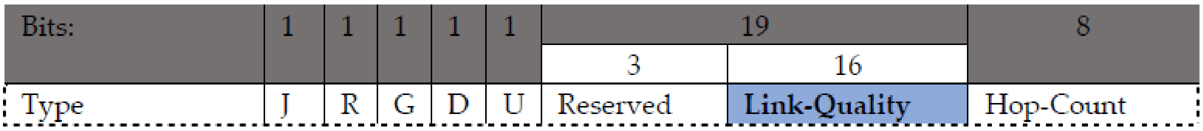
The nature of tactical MANET operations requires more specialized routing & MAC protocols compared to the ones which are used in commercial MANET. Routing decisions in MANETs are usually conditioned on signal-to-interference-plus-noise ratio (SINR) measurements. In order to improve routing decisions for use in highly dynamic tactical MANETs, this solution combines two different metrics to achieve reliable multicast in multi-hop ad hoc networks. The resulting protocol combining received signal strength (RSS) with SINR to make routing decisions is referred to as Link Quality Aware Ad-hoc On-Demand Distance Vector (LQA-AODV) routing. The proposed routing protocol can quickly adapt to dynamic changes in network topology and link quality variations often encountered in tactical field operations. Network connectivity can never be fully guaranteed for any type of wireless technology unless network topology and radio propagation environment are carefully analyzed. One of the design goals of tactical MANETs is to provide robust connectivity at the network edges. Currently, there is a serious shortfall of providing robust connectivity to the lowest-level combat units represented by dismounted troops at the squad and platoon level in order to provide their access to the command information center. Another challenge is that tactical MANETs operate in different types of terrains with very diverse radio propagation conditions. In addition to RSS, the link quality also depends on the level of interference which is quantified by SINR measure. In particular, physical-layer reports can be used to estimate the instantaneous or average link quality over certain time period. Such metrics are attractive, since they are readily available without any additional costs or modification of existing protocols, and they can be used for continuous monitoring of link quality. The key measurements readily available at different stages of the receiver are outlined in Figure 4.1.



<u>Figure 4.1 Key metrics for link quality</u>

A multipath routing protocol utilizing both RSS and SINR metrics is used. The protocol is labeled as Link Quality Aware Ad-hoc On-Demand Distance Vector (LQA-AODV). In other words, designing energy-efficient algorithms that uses SINR to derive the performance (e.g., packet error rate, PER), and RSSI can be used to make decisions about dynamic communication radius when establishing network connectivity.

Due to limited transmission capacity of tactical MANETs, the number of hops for data transmission must be limited. Usually, the maximum number of hops from a sending node is allowed to be at most 4 hops away. Therefore, here need arises to extend AODV protocol to incorporate a hierarchical cluster based routing. Hierarchical MANETs with clusters assign each node to one of the following functions: gateway node (GN), cluster member (CM), and cluster head (CH). The CHs should always be able to reach nodes in other clusters via their respective CHs or via GNs. The CM nodes within the same cluster can communicate either via their CH, or they communicate directly in a peer-to-peer (P2P) manner with possibly up to 2-hops. In proposed protocol, assumption is energy efficient clustering of nodes where CHs are selected to have the largest remaining energy level. In addition, the CHs need to have sufficient connectivity to nearby nodes, so there is a trade-off between CH connectivity and its residual energy. If either the energy level drops below a threshold or the number of known neighbors decreases, a CH rediscovery mechanism is initiated by the current CH to possibly. The RREQ (route request) packet is shown in figure 4.2 & complete route discovery process is shown in figure 4.3.



Bits:	1	1	1	1	1	19		8
						3	16	
Type	J	R	G	D	U	Reserved	Link-Quality	Hop-Count

Figure 4.2: RREQ Packet

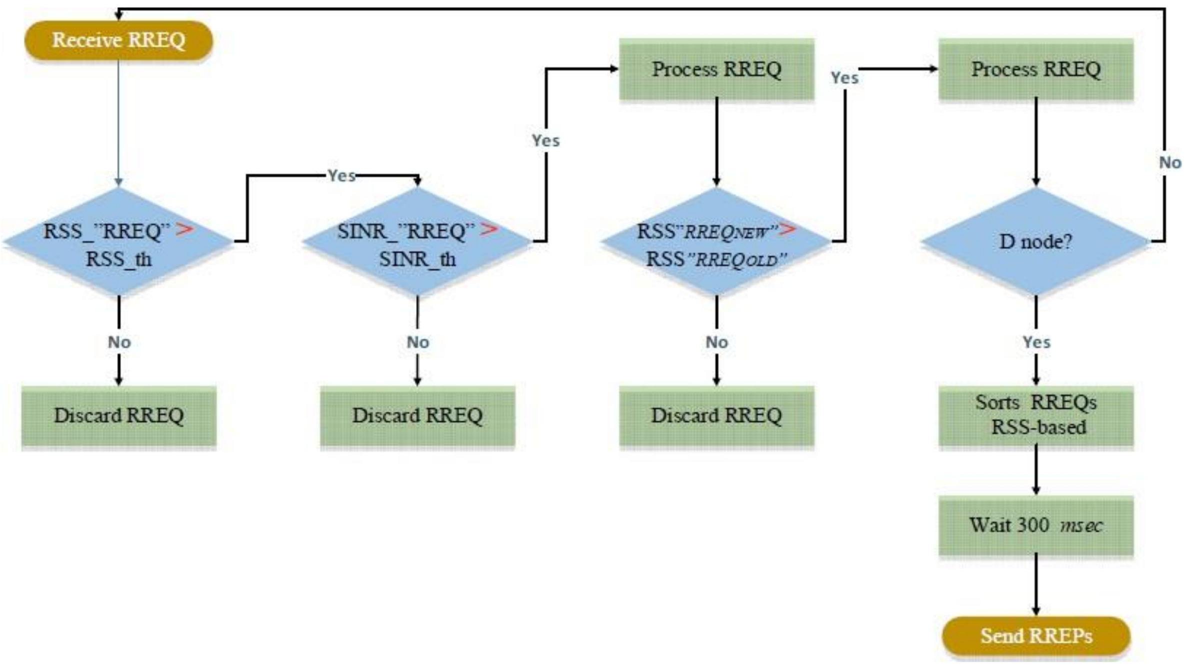


Figure 4.3: Route discovery process

Simulation Environment. All simulations were carried out in NS-2 simulator. The proposed routing protocol is compared with AODV, H-AODV, AOMDV routing protocols with dynamic TDMA as MAC layer protocol. The node density in tactical MANETs changes continuously as the mission evolves. However, the number of nodes in tactical MANETs can research up to several hundred (300) nodes. Typically, the largest traffic volumes flow to small combat units in the front-line including squads, platoon or company formations. The network scalability issue involving as much as 300 nodes is resolved by assuming a 3-level hierarchy network clustering at battalion and company, and then a platoon is formed over the whole tactical MANET. The battalion tactical operations center (TOC) is normally located at rear of tactical operations area where the command post is able to monitor events and assist commanders and subordinate units in mission planning. A unique hierarchical architecture of a tactical MANET comprising different communication links with different maximum ranges is shown in Figure 4.4.

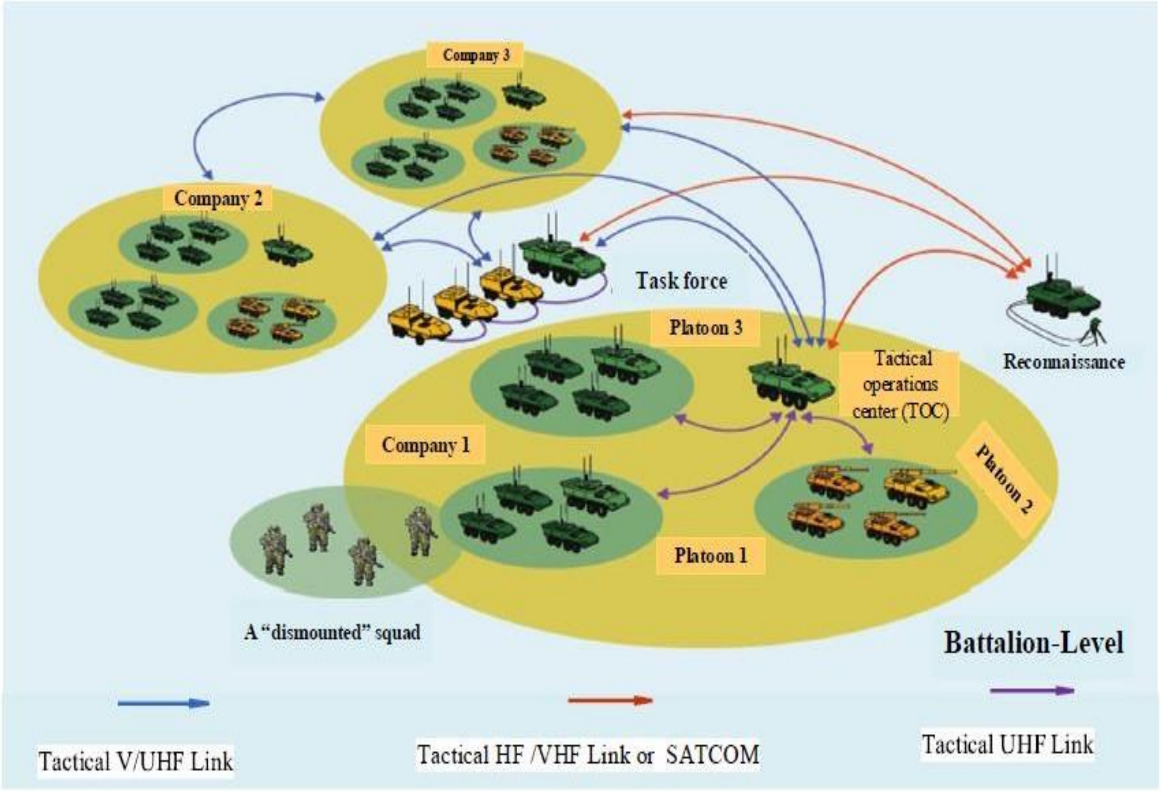
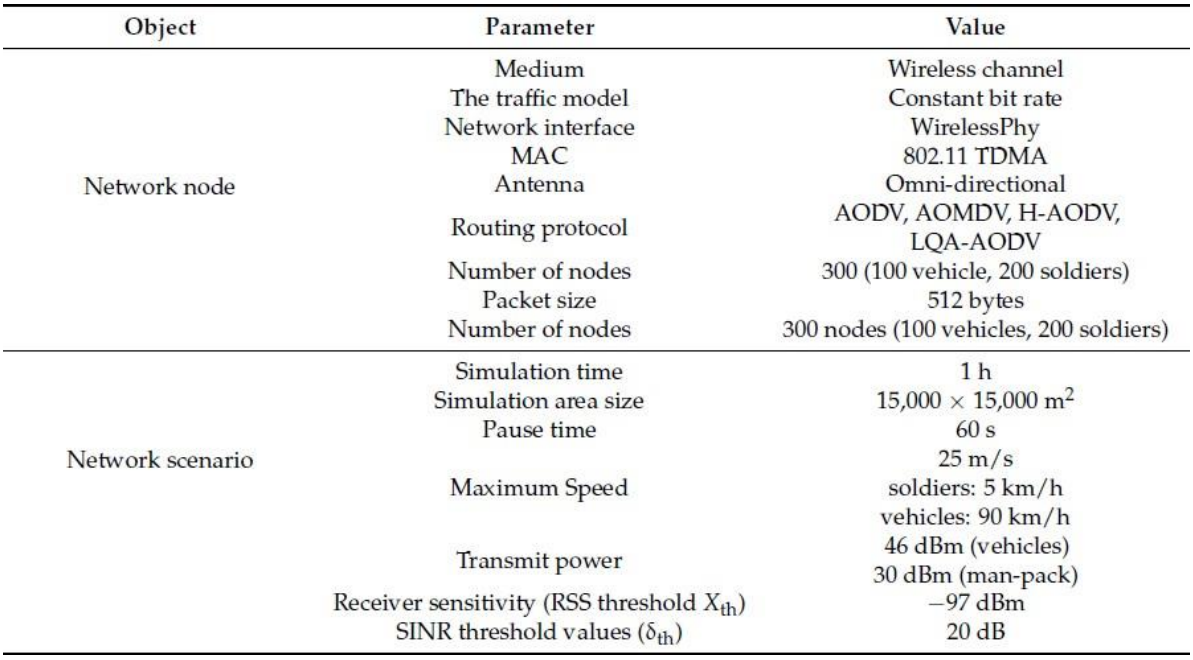


Figure 4.4: Hierarchical Architecture of Tactical MANETs

In tactical MANETs, units and troops often move in tactical formations. The specific position of a unit may have impact on connectivity, however, group mobility is considered. In addition, nodes in tactical MANETs are usually diverging from their initially clustered position. The nodes may move partly in the direction of the leader node, and also partly in their own independent direction when fulfilling the mission objectives. A reference point group mobility (RPGM) model is suitable for such scenarios where a group's individual units and their commander form natural clusters. The simulation parameters are shown in figure 4.5.



Object	Parameter	Value
Network node	Medium	Wireless channel
	The traffic model	Constant bit rate
	Network interface	WirelessPhy
	MAC	802.11 TDMA
	Antenna	Omni-directional
	Routing protocol	AODV, AOMDV, H-AODV, LQA-AODV
	Number of nodes	300 (100 vehicle, 200 soldiers)
	Packet size	512 bytes
	Number of nodes	300 nodes (100 vehicles, 200 soldiers)
Network scenario	Simulation time	1 h
	Simulation area size	15,000 × 15,000 m^2
	Pause time	60 s
	Maximum Speed	25 m/s soldiers: 5 km/h vehicles: 90 km/h
	Transmit power	46 dBm (vehicles) 30 dBm (man-pack)
	Receiver sensitivity (RSS threshold X_{th})	−97 dBm
	SINR threshold values (δ_{th})	20 dB

Figure 4.5: Simulation parameters

NS-2 simulator allows choosing from a large set of available performance metrics. For the simulations: throughout, packet delivery rate (PDR) and end-to-end delay metrics are used to analyze the performance of our proposed protocol, and compare it with other similar protocols. Furthermore, each performance metric is simulated assuming the following 3 key parameters: node speed, and the number of network nodes. The throughput metric is defined as the average number of successfully delivered bits per unit of time. Modern tactical MANETs in digitized battlefield need to support high throughput applications utilizing services such as real-time video. The throughput is affected by the use of heterogeneous network components, and often by jamming and interference. Figure 4.6 & 4.7 compares the average throughput node speed & no. of nodes.

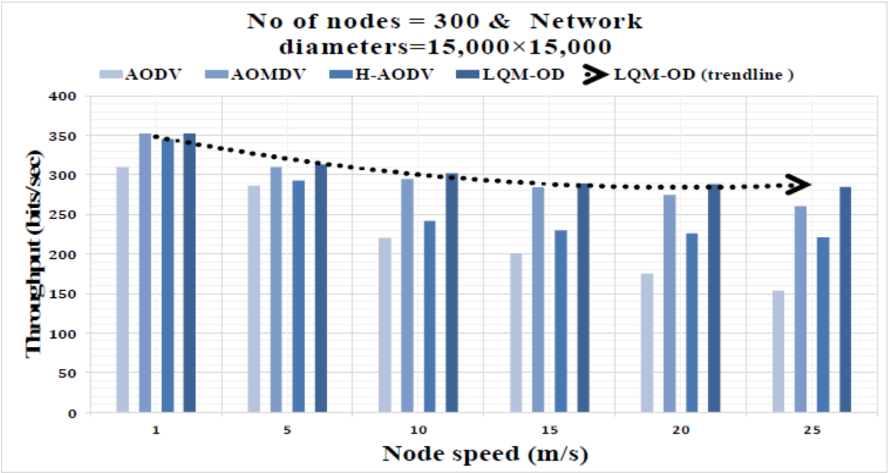


Figure 4.6: Throughput vs Node speed

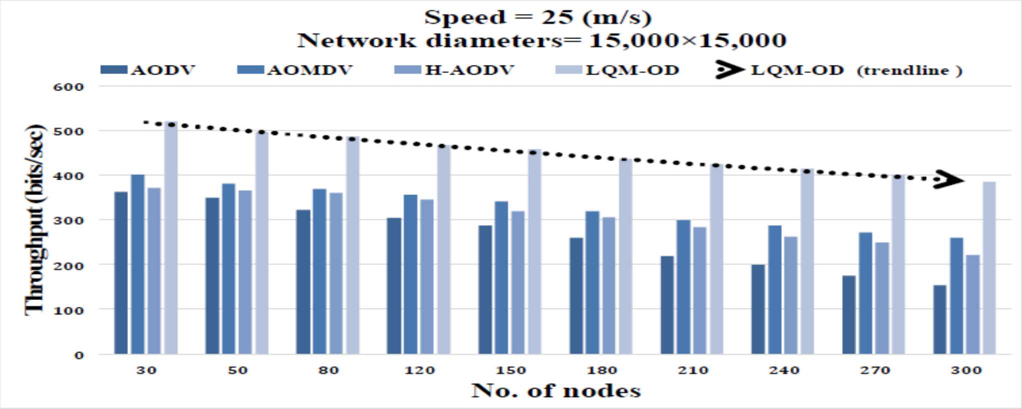
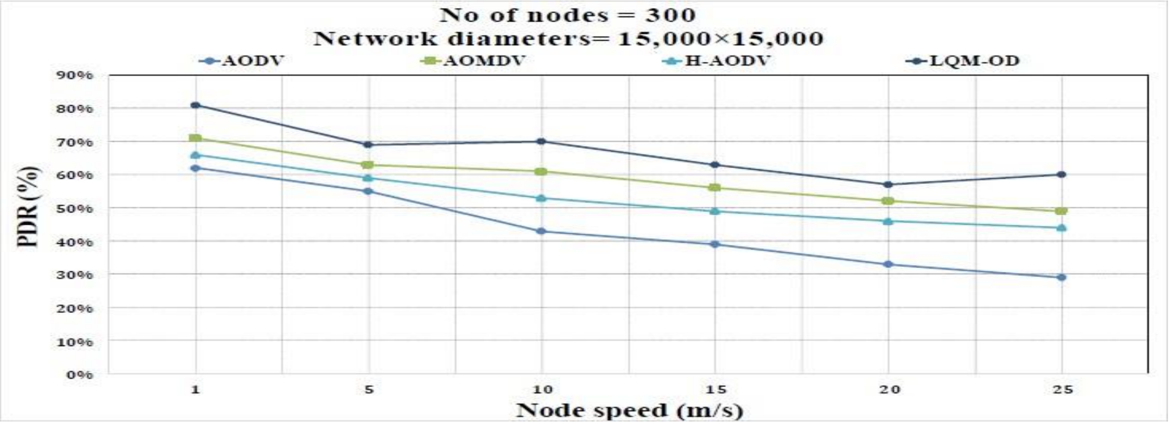


Figure 4.7: Throughput vs Node number

Packet Delivery Ratio (PDR) is a fraction of successfully delivered packets. This metric is often used to estimate link quality small tactical MANETs where network load is a vital QoS constraint to consider. The performance for PDR is evaluated similarly as for the throughput.



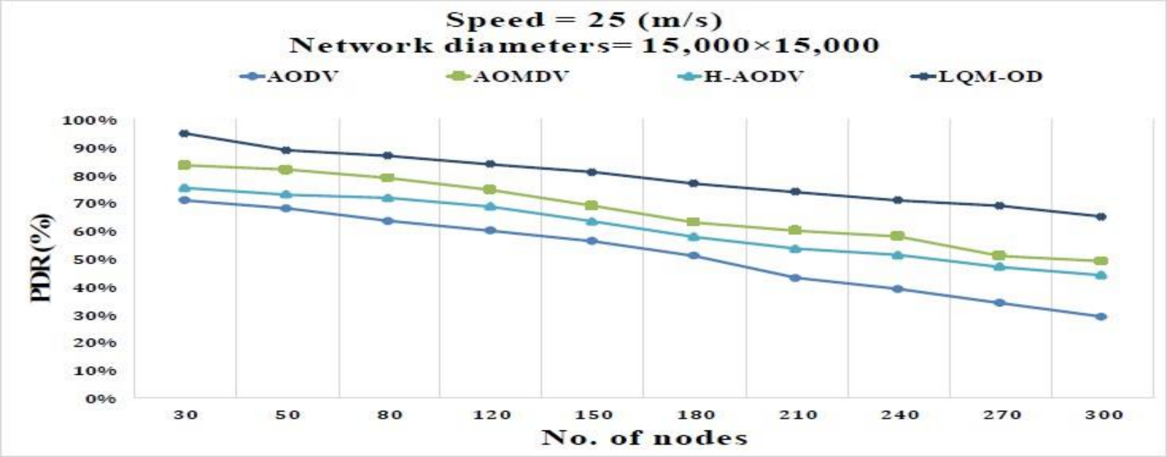


Figure 4.8: PDR comparison

Finally, the end-to-end delay is defined as the time required for the packet to be fully received at the destination. It is another important QoS performance metric often considered in tactical MANETs, especially for time-sensitive and mission-critical applications such as remote drone operations.

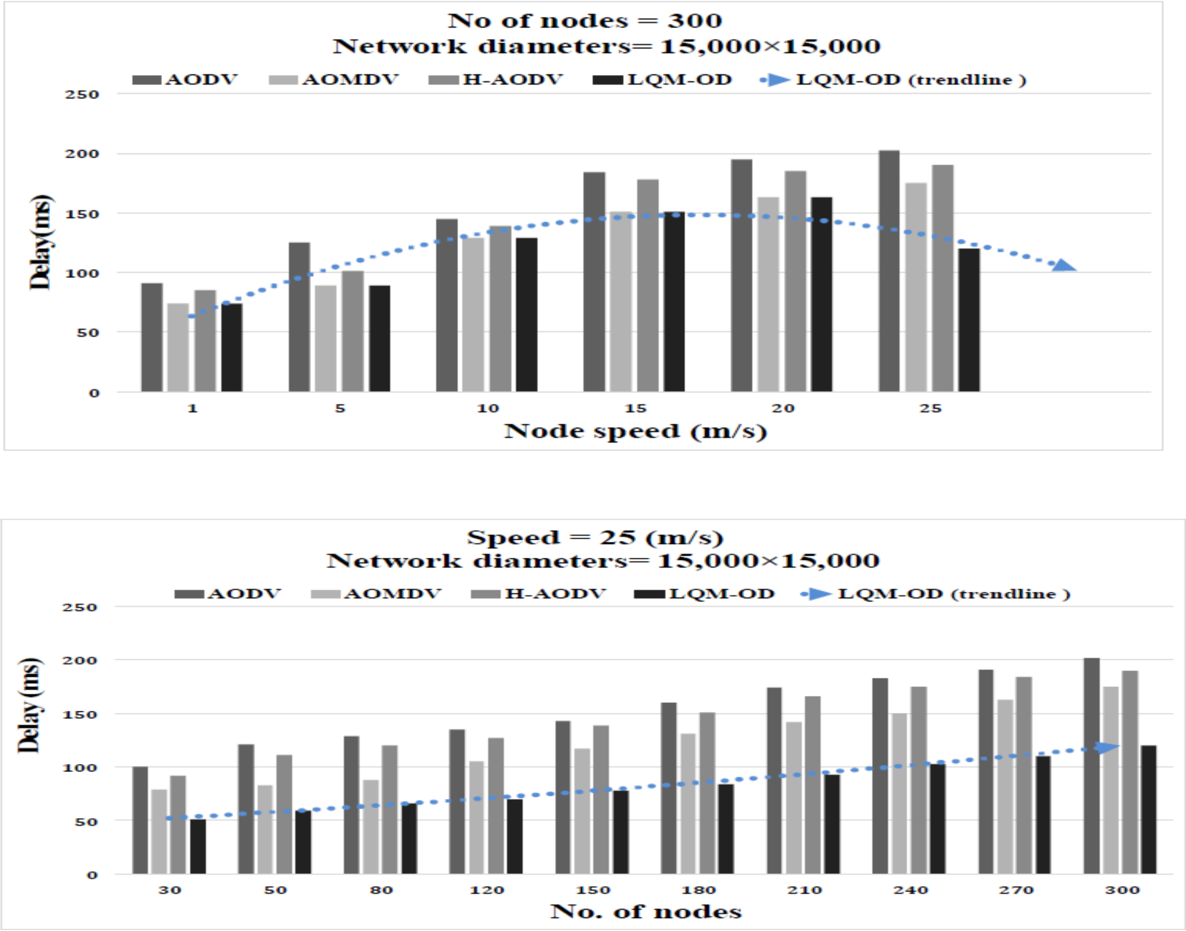


Figure 4.9: End-to-end delay comparison

The technique & protocol mentioned above is suitable for highly dynamic tactical large scale tactical MANETs.

Hybrid MAC protocol

This approach is a hybrid technique which makes use of both CSMA and TDMA based MAC protocol. This protocol exploits CSMA based MAC protocol explained for small scale MANETs for intra-cluster communication and Dynamic TDMA for inter-cluster communication. The frame structure for the same is shown below:-

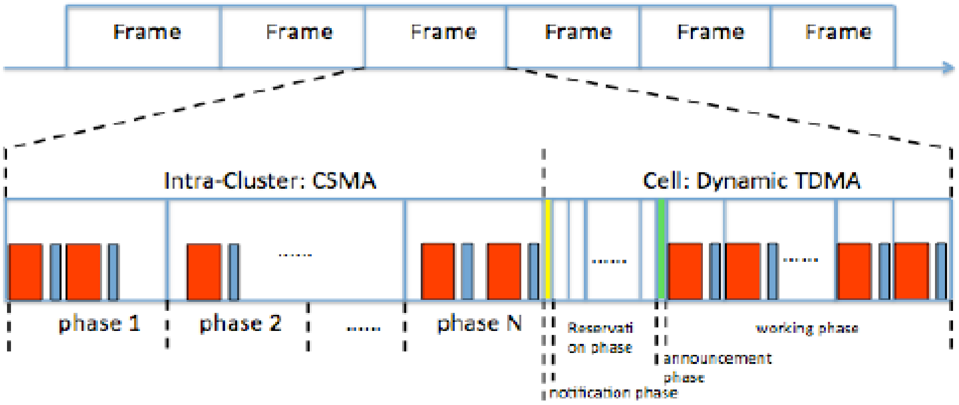


Figure 4.10: Hybrid MAC Protocol

The former is further split into *N* phases, in each of which a part of cluster members send their packets in EMAC manner. The packets are gathered at cluster heads, which are going to be sent in the TDMA period.

Clustering Techniques

The various clustering approaches are tabulated below for large scale MANETs.

APPROACH :1	APPROACH :2	APPROACH :3
➢ Intra-cluster: CM to CM: P2P CM to CM via CH	➢ Intra-cluster: CM to CM : P2P CM to CM via CH	➢ Intra-cluster: CH -Centralized Control (routing & control decisions by cluster head only)
➢ Inter-cluster: CM to GN directly CM to GN via CH	➢ Inter-cluster: CM to GN via CH	➢ Inter-cluster: CH to CH via GN
▪ Slot Decisions at node level ▪ Slot Allocation based on acknowledgment from two hop neighbors ▪ Control slots allocation by CH	▪ Control messages exchange between one hop neighbors only ▪ Less Control Overhead then approach 1	▪ Control , scheduling & routing decisions by CH ▪ Requires continuous scheduling calculation ▪ Increased Control overhead & less scalability ▪ Single point failure if control node fails ▪ Better performance then approach 1 & 2 , but not

		optimal for changing topology & traffic conditions

CHAPTER 5

MARKET SURVEY

An Indian market survey was undertaken to study the technical specifications of SDRs available in market. The details are tabulated below:-

M/s Lekha Wireless Solutions (Mbi)	**M/s Rolta with TCS & Selex**
(i) VHF/UHF range **(ii)** Random topology **(iii)** Nodes – 100 **(iv)** Multi-hop feature **(v)** Rate – 150 kbps to 6 Mbps **(vi)** Range – 1 Sq kms	**(i)** VHF/UHF range **(ii)** Total output power- 5 Watts **(iii)** Rate- 64 Kbps to 2 Mbps **(iv)** Multi-hop feature **(v)** Nodes- 80-120 nodes **(vi)** Area – 5 sq Kms (Final Trials Stage)

CHAPTER 6

SIMULATION OF LARGE SCALE MANET IN NS-3

A large scale MANET was simulated in NS-3 with 100 nodes in an area of 25 Sq. Kms. The Clustering approach used is Cluster head as Central controller, all routing decisions and slot allocations are done by Cluster Head. The MAC protocol used in the simulation is Hybrid MAC protocol with EMAC used for intra-cluster communication and TDMA used for Inter-cluster Communication. The simulation parameters are listed below:-

(1) Nodes – 100 nodes
(2) Area – 5000 * 5000 sq mtrs

(3) No of Cluster – 4

(4) Channel rate – 54 Mbps

(5) Data packet size – 1000 bytes

(6) SIFS – 6 us

(7) MAC protocol – Hybrid

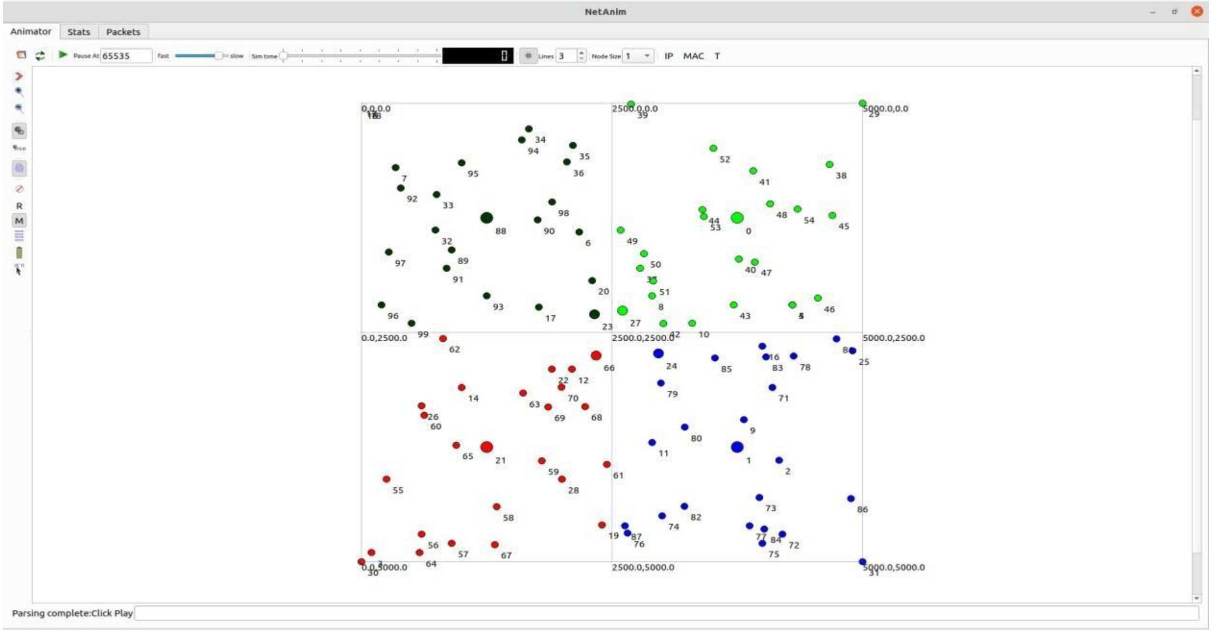
(8) Intra-cluster - 2 hops

(9) Inter-cluster (Next cluster) – 4 hops

(10) Inter-cluster(Diagonal cluster) – 5 hops

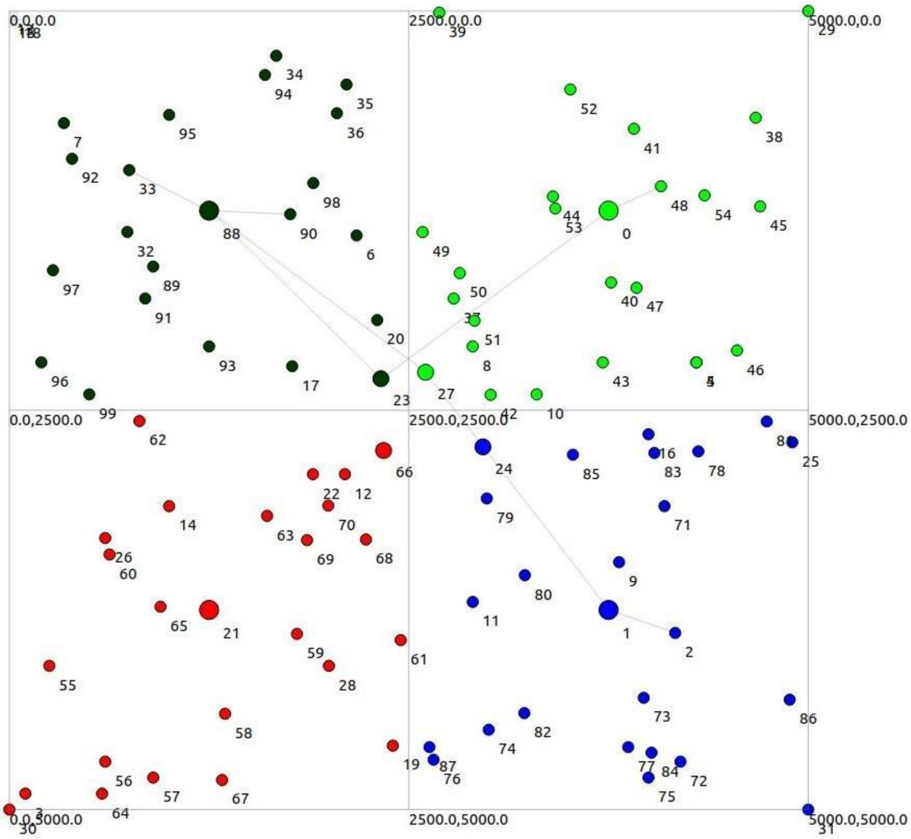
The Simulation steps and results are as shown below: -

(a) The topology scenario simulated is animated in Netanim tool of NS-3 and is shown below: -



Parsing complete:Click Play

(b) The Hoping scenario is shown below: -



(c) The simulation time Vs End to end delay achieved through simulation in GNU plot tool of NS-3 is shown below: -