M.Tech (Computer Sys. a

ABSTRACT

In this paper we are going to introduce an ap
enhancement of CSMA/CA MAC protocol for ad hoc
Our proposal is to increase the number of unbloc
causes due to RTS/CTS. According to the timing
CSMA/CA, for reliable communication RTS/CTS are u
nodes by setting their NAV value and are block
communication period. If we can reduce these numb
nodes then they can be used as another communicatio
relay or destination and will increase the network pe
Depending upon their signal power our proposal is
unequal NAV value of the nodes that are lies in tra
detectable and interference zone in ad hoc network. S
time gradually decreases from transmission, dete
interference zone as the signal power of the node
decrease. Mathematically we shows the reduced blo
and variable NAV value of the nodes depending on si
and modify the CSMA/CA MAC timing diagram whic
network performance.

LIST OF FIGURES

TABLE OF CONTENTS

References

CHAPTER 1

- 1.1Wireless Ad Hoc Networks
- 1.2History of Ad Hoc
- 1.3.Self Healing and Self Configuring
- 1.4.Four Important features of Ad Ho
- 1.5.Objectives
- 1.6.Thesis structure

CHAPTER 1

Introduction

Computer Networking is changing our way of lives .The developmen
networking brought about tremendous changes for business , industr
education .Technological advances are making it possible for communi
carry more and faster signals. Mainly a computer network is divided into t

Wired Network
Wireless Network

A computer network, often simply referred to as a network, is a collecti
components and computers interconnected by communication chann
sharing of resources and information. Wired networks provide users
security and the ability to move lots of data very quickly. Wireless netwo
type of computer network that is not connected by cables of any kind. It
which homes, telecommunications networks and enterprise (business
avoid the costly process of introducing cables into a building, or as
between various equipment locations.Wireless telecommunications
generally implemented and administered using a transmission syste
waves.

1.1.WIRELESS AD HOC NETWORK

Ad Hoc is a Latin word meaning “for this”. In general ad hoc word ca
temporary basis, such as temporary oversight of an issue. There may
committee, commission or organization .The study of Ad Hoc network
increasingly popular since in 1990s.

An Ad Hoc network is a group of mobile terminals independent from any
communicating by radio waves ,where each of these terminals offers a
accept a message not addressed to it in order to retransmit it to an
terminal ,which is out of the initial transmitter of this message.

The capacity of terminals to serve as relays is the fundamenta
hoc networks and will be the main topic of this chapter. We will call
capability the capability enabling a message leaving a transmitting term
destination terminal to cross several relays.

IEEE 802.11 is a set of standards for implementing wireless local
(WLAN).Computer communication in the 2.4, 3.6 and 5GHz frequency ban

This kind of network can be used for a specific purpose. In this kind ther
any router or any wireless base station. This network does not rely on a
infrastructure and nodes are mobile.
Besides this, they will send or receive data without any distortion. Since
existing infrastructure all the nodes communicates among themselve
waves, where each nodes offers a relay service and cooperate coordina
node diversity.

These networks introduced a new art of network established and can be
an environment where either the infrastructure is lost or where deploy an
is not very cost effective.

1.2. HISTORY OF AD HOC NETWORKS

ALOHA and CSMA.

2.1) Distance Vector Routing: It is the least cost route between an
the route with the minimum distance.

2.2) ALOHA:

2.3) CSMA:

2.The second generation of Ad Hoc was emerged in 1980s where ad hoc
further enhanced and implemented as a part of SURAN (Surviable A
Networks).This
provides a packet switched network without any infrastructure.T
commercial concepts of ad hoc network was introduced in notebook con
Time the concepts of collection of mobile nodes was proposed at se
conferences.The IEEE 802.11 adopted the term “ad hoc” and the resea
started to deploy the concept in other areas of application.

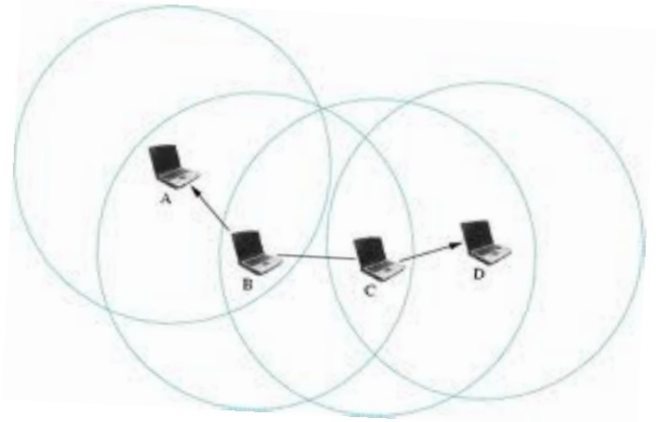


Fig1.Example of a mobile ad hoc network

1.3.SELF CONFIGURING AND SELF HEALING PROCESSESS

Each node identifies the nodes that are available for communications, b
strength, which is mainly related to distance, but is also affected by c
interference. Some nodes may be beyond range, others may be detec
insufficient signal strength for reliable communications .Once the avail
identified, this information
is communicated to other nodes, along with information about the desire

propagation between nodes. As these changes take place, the network configuration and identify new paths from users to destinations. reconfiguration will be repeated over and over as the network changes. N the
same process used in the Internet, where system loading and hardware redirection of a user's data through different routers.

1.4. FOUR IMPORTANT FEATURES OF AD HOC

3.1) **Dynamic Topologies**-Every nodes of a mobile ad hoc network are n They rotate arbitrarily which leads to random changes in topology c network.

3.2) **Variable Throughputs and Limited Bandwidth**-Using wireless connection ,actual communication throughput-after deducting mult access effects,fading,noise,interference etc-is often lower than the transfer rate of the radio interface and in all cases much lower than wired communications.

3.3) **Energy Constraint Function**-The energy conservation will be a vital a for the solutions proposed for the ad hoc network nodes operating i and limited energy sources.

3.4) **Limited Physical Security**-Very easily attackable by intruders by idle listening, identity theft and denial of service.

1.5.OBJECTIVES

In this thesis our proposal is to introduce an approach to enhance C Protocol for wireless Ad Hoc Networks. According to the timing diagram

1.6.THESIS STRUCTURE

The rest of the thesis report is organized as follows. Chapter 2 discus routing protocols in Ad Hoc. Chapter 3 discusses about the transmissio of ad hoc. Chapter 4 consists of how the naming and addressing is d Chapter 5 shows the details about the CSMA/CA Protocol with some bas NAV, RTS/CTS and timing diagram. Chapter 6 discusses some case stu consists of the proposed approach. Chapter 8 shows the analytical s proposed approach with updated timing diagram. Conclusions are draw And finally the last session i.e. Chapter 10 deals with publication and dis the future work.

Chapter 2

Routing Protocols of Ad

- 2.1.Optimised Link State Routing(OL
  - o 2.1.1.Features specific to OLSR
  - o 2.1.2.Benefits
  - o 2.1.3.Messages
- 2.2.Ad Hoc On Demand Distance Vector(AODV)

CHAPTER 2

FOUR IMPORTANT PROTOCOLS OF AD HOC

ROUTING

Since the arrival of ad hoc network concepts ,many propos studied ,simulated and evaluated .The same proposals have led ,specializations to given environments and optimizations .This sect protocols is not intended to provide an in-depth analysis .Our goal is t major classifications of routing algorithms as well as successful solu ,the reader should remember the current growth ,with the miniaturizati ,introduction of terminals with several radio interfaces .

A routing problem in an ad hoc network is the same as in fi

changes are of a much smaller scale than with ad hoc networks.

In the following ,we will go back to traditional hypothesis which are near
for granted by ad hoc protocols designers. We will consider homogeneou
the point of view of their communication capacity as well as their c
storage capacity, using one radiocommunication technology and with t
one communication carrier for the whole network. Even though there
several studies do not use the same hypothesis.

The characteristics in demand by most ad hoc routing algorithm develope

Simplicity: the protocols must generate as little surcharge of manag
possible and must be very simple to develop and deploy:

Self organization: no central control can be admitted in an ad hoc ne
structures necessary for routing management must be created in a distr
resist topology change as much possible;

Scalability : protocols offered must adapt to different ad hoc network siz
different mobility and traffic models.

It is possible to add many more characteristics to the list ,from the reque
service to energy conservation for each mobile device.

4.1 OPTIMISED LINK STATE ROUTING (OLSR)

The **optimized link-state routing protocol (OLSR)** is an IP routing prot
for mobile ad-hoc networks, which can also be used on other wireless ad
OLSR is a proactive link-state routing protocol, which uses *hel*
control (TC) messages to discover and then disseminate link sta
throughout the mobile ad-hoc network. Individual nodes use this topolo
to compute next hop destinations for all nodes in the network using
forwarding paths.

different notion of a link, packets can and do go out the same inter
different approach is needed in order to optimize the flooding proces
messages the OLSR protocol at each node discovers 2-hop neighbour in
performs a distributed election of a set of *multipoint relays* (MPRs). Node
such that there exists a path to each of its 2-hop neighbours via a node
MPR. These MPR nodes then source and forward TC messages that co
selectors. This functioning of MPRs makes OLSR unique from other lin
protocols in a few different ways: The forwarding path for TC messages
among all nodes but varies depending on the source, only a subset of no
state information, not all links of a node are advertised but only those
MPR selections.

Since link-state routing requires the topology database to be synchroni
network, OSPF and IS-IS perform topology flooding using a reliable algo
algorithm is very difficult to design for ad-hoc wireless networks, so
bother with reliability; it simply floods topology data often enough to mak
database does not remain unsynchronized for extended periods of time.

4.1.2.Benefits

Being a proactive protocol, routes to all destinations within the network
maintained before use. Having the routes available within the standard ro
be useful for some systems and network applications as there is no
delay associated with finding a new route.

The routing overhead generated, while generally greater than that of a rea
does not increase with the number of routes being used.

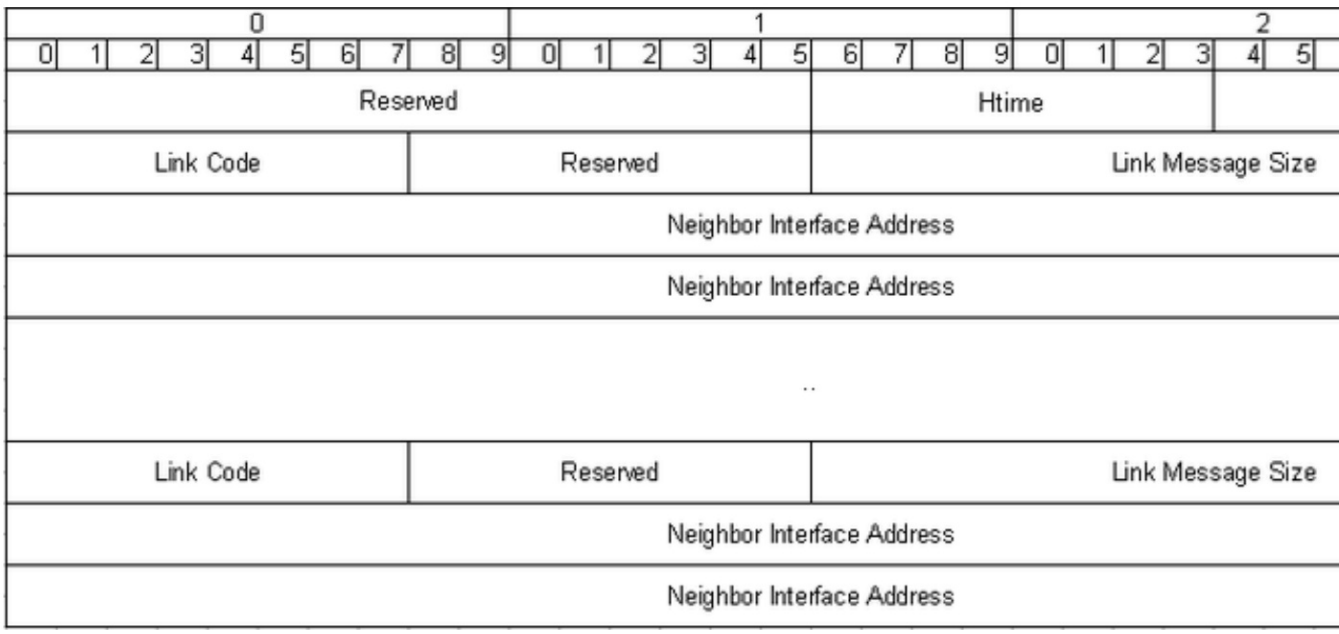
Default and network routes can be injected into the system by HNA mes
for connection to the internet or other networks within the OLSR MANET
routes are something reactive protocols do not currently execute well.

Timeout values and validity information is contained within the messa
information allowing for differing timer values to be used at differing node

4.1.3.Messages

OLSR makes use of "Hello" messages to find its one hop neighbours a
neighbours through their responses. The sender can then select its m
(MPR) based on the one hop node that offers the best routes to the t
Each node has also an MPR selector set, which enumerates nodes that h

Hello



Topology control (TC)

4.2 AD HOC ON DEMAND DISTANCE VECTOR (AODV)

It is a reactive routing protocol, meaning that it establishes a route to a d
on
demand. In contrast, the most common routing protocols of the Interne
meaning
they find routing paths independently of the usage of the paths. AODV i
indicates, a distance-vector routing protocol. AODV avoids the cou
problem of other distance-vector protocols by using sequence num
updates, a technique pioneered by DSDV. AODV is

The routing table memorized in each node is a table where each entry ha
information destination node addresses ,next hop node on the route to t
,sequence number and time of expiration of this entry in the table. E
updated each time the entry is used, deletes routes which have not b
quickly enough. The sequence number is inherent to a destination
possible, when receiving an updated message ,to know if it correspo
recent route than the one stored in the table or not. The algorithm re
recent route and , in the case of equality ,the shortest one.

4.2.1.Properties

a) Reactive or on Demand

b) Descendant of DSDV

c) Uses bi-directional links

d) Route discovery cycle used for route finding

e) Maintenance of active routes

f) Sequence numbers used for loop prevention and as route freshness cr

g) Provides unicast and multicast communication

4.2.2.Technical description

The AODV Routing protocol uses an on-demand approach for finding ro
route is established only when it is required by a source node for tra
packets. It employs destination sequence numbers to identify the most re
major difference between AODV and Dynamic Source Routing (DSR) sten
fact that DSR uses source routing in which a data packet carries the co
be traversed. However, in AODV, the source node and the intermediate n
next-hop information corresponding to each flow for data packet transmi
demand routing protocol, the source node floods the *Route Request*

node updates its path information only if the *DestSeqNum* of the
received is greater than the last *DestSeqNum* stored at the node.

A Route Request carries the *source identifier* (SrcID), the *destination ide*
the *source sequence number* (SrcSeqNum), the *destination*
number (DestSeqNum), the *broadcast identifier* (BcastID), and the *tim*
field. DestSeqNum indicates the freshness of the route that is accepted
When an intermediate node receives a Route Request, it either forwards
Route Reply if it has a valid route to the destination. The validity of
intermediate node is determined by comparing the sequence n
intermediate node with the destination sequence number in the Route R
If a Route Request is received multiple times, which is indicated by the
pair, the duplicate copies are discarded. All intermediate nodes having
the destination, or the destination node itself, are allowed to send Route
to the source. Every intermediate node, while forwarding a Route Requ
previous node address and it's BcastID. A timer is used to delete this
Route Reply is not received before the timer expires. This helps in storing
at the intermediate node as AODV does not employ source routing of
When a node receives a Route Reply packet, information about the previ
which the packet was received is also stored in order to forward the data
next node as the next hop toward the destination.

4.2.3.Advantages and disadvantages

The main advantage of this protocol is that routes are established o
destination sequence numbers are used to find the latest route to the d
connection setup delay is lower. One of the disadvantages of this p
intermediate nodes can lead to inconsistent routes if the source seque
very old and the intermediate nodes have a higher but not the late
sequence number, thereby having stale entries. Also multiple Route Re

4.3. DYNAMIC SOURCE ROUTING (DSR):

As with all reactive protocols ,the DSR protocol uses a process of r
between two network nodes when it is necessary for a specific comm
main characteristic differentiating DSR from the other reactive protocol
routing by the source :the transmitting node of a data packet must kno
intermediate nodes in order to reach its destination .This route is located
headers ,so much so that the intermediate nodes do not need a local rout

Routes that will be discovered on demand are kept for a certain peri
mechanism .As we will see later, different options are available to limit t
route discovery by using these caches .In the DSR protocol ,we find two r
mechanisms: route discovery and route maintenance.

4.3.1.Properties

a) Reactive or On Demand

b) Developed at CMU in 1996

c) Route discovery cycle used for route finding – on Demand

d) Maintenance of active routes

e)No periodic activity of any kind – Hello Messages in AODV

f)Utilizes source routing (entire route is part of the header)

g) Use of caches to store routes

h) Supports unidirectional links - Asymmetric routes are supported

similar to AODV in that it forms a route on-demand when a transmit
requests one. However, it uses source routing instead of relying on the r
each intermediate device.

Determining source routes requires accumulating the address of each d
the source and destination during route discovery. The accumulated pa
is cached by nodes processing the route discovery packets. The learned
to route packets. To accomplish source routing, the routed packets conta
of each device the packet will traverse. This may result in high overhead
or large addresses, like IPv6. To avoid using source routing, DSR optio
flow id option that allows packets to be forwarded on a hop-by-hop basis.

This protocol is truly based on source routing whereby all the routing
maintained (continually updated) at mobile nodes. It has only two major
are Route Discovery and Route Maintenance. Route Reply would only be g
message has reached the intended destination node (route record w
contained in Route Request would be inserted into the Route Reply).

To return the Route Reply, the destination node must have a route to the
the route is in the Destination Node's route cache, the route would be us
the node will reverse the route based on the route record in the Route R
header (this requires that all links are symmetric). In the event of fatal tra
Route Maintenance Phase is initiated whereby the Route Error packets ar
a node. The erroneous hop will be removed from the node's route ca
containing the hop are truncated at that point. Again, the Route Disco
initiated to determine the most viable route.

For information on other similar protocols, see the ad hoc routing protoco

Dynamic source routing protocol (DSR) is an on-demand protocol desig
the bandwidth consumed by control packets in ad hoc wireless networks
the periodic table-update messages required in the table-driven approa
difference between this and the other on-demand routing protocols is th

Reply packet back to the source, which carries the route traversed by the packet received.

Consider a source node that does not have a route to the destination. W packets to be sent to that destination, it initiates a Route Request pack Request is flooded throughout the network. Each node, upon receiving a packet, rebroadcasts the packet to its neighbors if it has not forwar provided that the node is not the destination node and that the packet's ti counter has not been exceeded. Each Route Request carries a seq generated by the source node and the path it has traversed. A node, up Route Request packet, checks the sequence number on the packet befor The packet is forwarded only if it is not a duplicate Route Request. number on the packet is used to prevent loop formations and to transmissions of the same Route Request by an intermediate node t through multiple paths. Thus, all nodes except the destination forward a packet during the route construction phase. A destination node, after rec Route Request packet, replies to the source node through the reverse Request packet had traversed. Nodes can also learn about the neigh traversed by data packets if operated in the promiscuous mode (the mo in which a node can receive the packets that are neither broadcast no itself). This route cache is also used during the route constructior intermediate node receiving a Route Request has a route to the destina route cache, then it replies to the source node by sending a Route Reply route information from the source node to the destination node.

Advantages and disadvantages

This protocol uses a reactive approach which eliminates the need to pe the network with table update messages which are required in a table-dr In a reactive (on-demand) approach such as this, a route is established

reconstruction phase. The connection setup delay is higher than
protocols. Even though the protocol performs well in static an
environments, the performance degrades rapidly with increasing
considerable routing overhead is involved due to the source-routin
employed in DSR. This routing overhead is directly proportional to the pat

4.4.TOPOLOGY BROADCAST BASED ON REVERSE-PA FORWARDING

Topology Broadcast based on Reverse-Path Forwarding (TBRPF) is a
state routing protocol designed for mobile ad-hoc networks, which provi
routing along minimum-hop paths to each destination. Each node
computes a source tree (providing paths to all reachable nodes) ba
topology information stored in its topology table, using a modificatio
algorithm. To minimize overhead, each node reports only *part* of its
neighbours. This is in contrast to other protocols (e.g., STAR) in wh
reports its *entire* source tree to neighbours. TBRPF uses a combination
differential updates to keep all neighbours informed of the reportable pa
tree. Each node also has the option to report additional topology informa
full topology), to provide improved robustness in highly mobile net
performs neighbour discovery using "differential" HELLO messages
only *changes* in the status of neighbours. This results in HELLO mes
much smaller than those of other link- state routing protocols such as OS

4.4.1Assumptions and Terminology

TBRPF requires very few assumptions regarding the network mode
operate in any internet or subnet in which IP hosts are connected thro
or point-to-point links to routers. The current implementation of TBRPF
of IP, similarly to an internet routing protocol such as OSPF. TBRPF ca

nodes u and v to be adjacent (i.e., neighbors) if each node can r
messages from the other. Thus, we map a
physical broadcast link connecting multiple nodes into multiple
bidirectional links. Such a bidirectional link between two nodes u and v
by a pair of links (u,v) and (v,u). Each link has a positive cost that can va
the cost of (u,v) may be different from that of (v,u). Each router u is r
updating and reporting the cost and up/down status of each outgoi
neighbors. TBRPF can also support the broadcast of multiple link costs
for purposes of quality-of-service routing. TBRPF uses a neighbor disc
based on hello packets to establish links to new neighbors and to dete
TBRPF supports both unicast transmissions (e.g., point-to-point or receiv
which a packet reaches only a single neighbor; and broadcast transmissi
single packet is transmitted simultaneously to all neighbors. In particular
an update to be sent either on a common broadcast channel or on one o
channels, depending on the number of neighbors that need to receive the

4.4.2.Link-Level Functions

This section describes the link-level functions of TBRPF, i.e. neighbor dis
reliable link-level transmission of control messages.

4.2.3 Neighbor Discovery

The neighbor discovery protocol detects the following events:

1. A link to a new neighbour is established,
2. The link to an existing neighbour goes down.

Neighbour discovery uses the following three types of control mes
NEIGHBOR, and NEIGHBOR ACK. Every HELLO_INTVL seconds, each no
on the broadcast channel, a HELLO message containing the identity o
receiving a HELLO message from a new neighbour i, a node j res
NEIGHBOR message containing the identity of node j. Finally, upon
NEIGHBOR message, node i sends to node j a NEIGHBOR ACK containing
node i. NEIGHBOR and NEIGHBOR ACK messages also contain the cu

LINKDOWN_INTVL seconds.

2.5.ROUTING SCHEMES

1.UNICAST-This routing scheme delivers a message to a specifi
Scoped-Flood approach maintains unicast routes between the client
servers. This observation leads to another refinement of the approa
delivery phase requests are unicast directly to the closest servers.
provides perfect selectivity in the delivery phase; exactly the desired se
contacted.

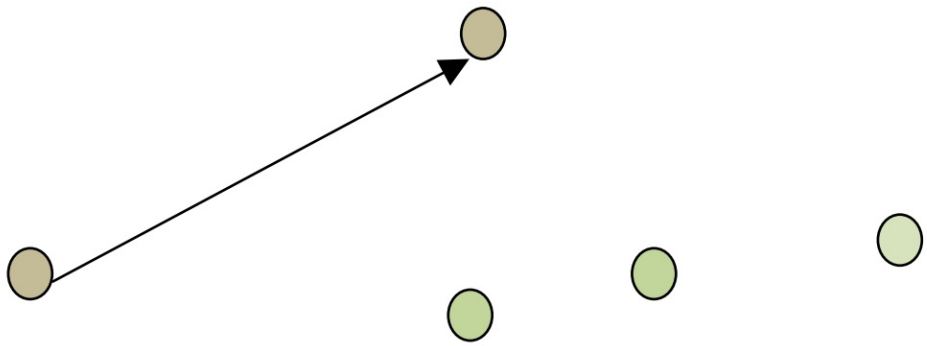
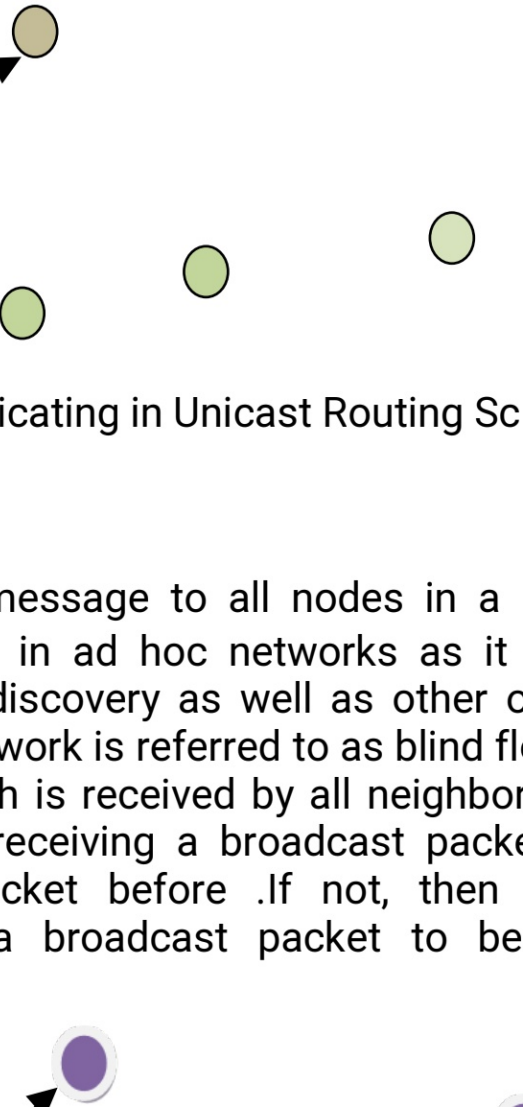


Fig2:Nodes communicating in Unicast Routing Sc

2.BROADCAST-This routing delivers a message to all nodes in a
fundamental operation for communication in ad hoc networks as it
update of network information and route discovery as well as other c
simplest form of broadcast in an ad hoc network is referred to as blind fl
flooding a node transmitted a packet, which is received by all neighbor
are within the transmission range. Upon receiving a broadcast packe
determines if it has transmitted the packet before .If not, then
retransmitted. This process allows for a broadcast packet to be
throughout the ad hoc network.



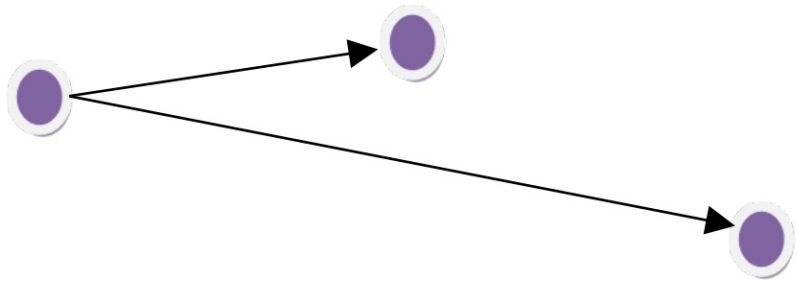


Fig 3: Nodes communicating in Broadcast Routing S

3.MULTICAST-It delivers a message to a group o nodes that hav interest in receiving the message. An approach that uses traditional m to perform
manycast delivery provides an interesting reference. A multicast tree is than flooding and should therefore put significantly less strain on the ne challenge lies in adapting multicast communication to environments wh unlimited and outages/failure are frequent.

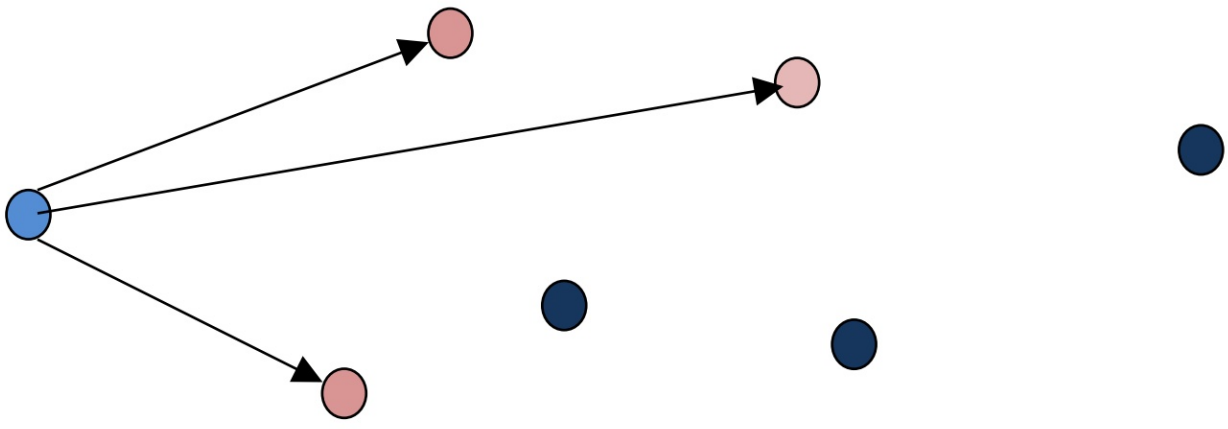


Fig 4:Nodes communicating in Multicast Routing Scheme

4.ANYCAST-It delivers a message to any one out of a group of nodes, t one nearest to the source. It was first introduced to suit of routing protoc networks. In anycast , packet is intended to be delivered to one of the nea hosts, k-anycast ,however is proposed to deliver a packet to any threshol of a set of hosts. Most of the research focused on anycast addressing ,ro

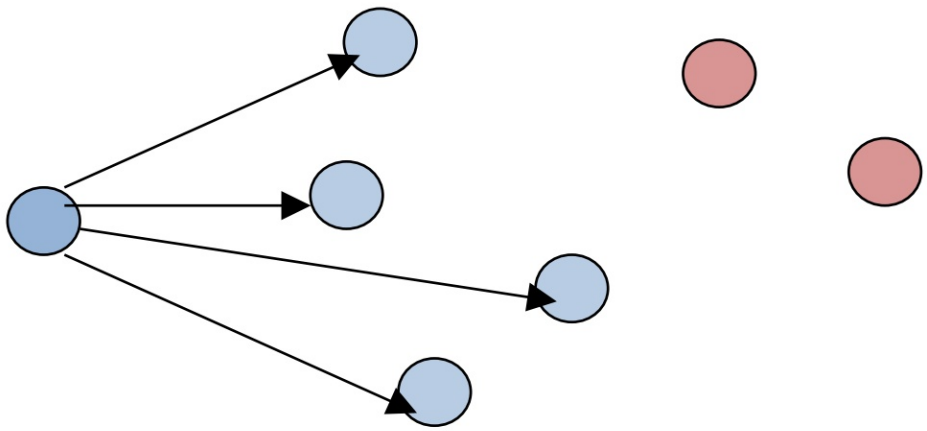


Fig 5:Nodes communicating in Anycast Routing Scheme

Transmission Phenomenon For A Network

- 3.1.Diffraction
- 3.2.Reflection
- 3.3.Diffusion

CHAPTER 3

NETWORKS

A signal transmitted at a given strength has a power density at distar
source that is proportional to the surface of the sphere of radius d c
source; attenuation according to the distance will be an inverse function
square.

In the first place , a certain number of electromagnetic phenomena disrup
signal received when the transmission environment is no longer free sp
important is the shadowing effect produced by obstacles located in the c
between transmitter and receiver. The Earth's atmosphere doesn't h
properties as clear space. The presence of trees, buildings , vehicles a
relief modifies the quality of signal received. The obstacle also disrupt
phenomena as reflection , diffraction and diffusion.

5.1) Diffraction
5.2) Reflection
5.3) Diffusion

4.1.Diffraction:

Diffraction is the bending of a wave around objects or the spreading
through a gap. It is due to any wave's ability to spread in circles or sphe
space. We investigate a new method by which radio waves of GHz ban
UWB, have enough electric field strength to establish ad hoc network
terminals in a room or in a building even deep in the geometrica
improvement of 30 dB at 10 GHz and a high electric field strength almo
of the UWB frequency are reported in this paper with a simple and effe
of an elliptical dielectric column at the end of a finite wall which makes t
shadow of radio waves, e.g. an opening to the next room or to the floor in

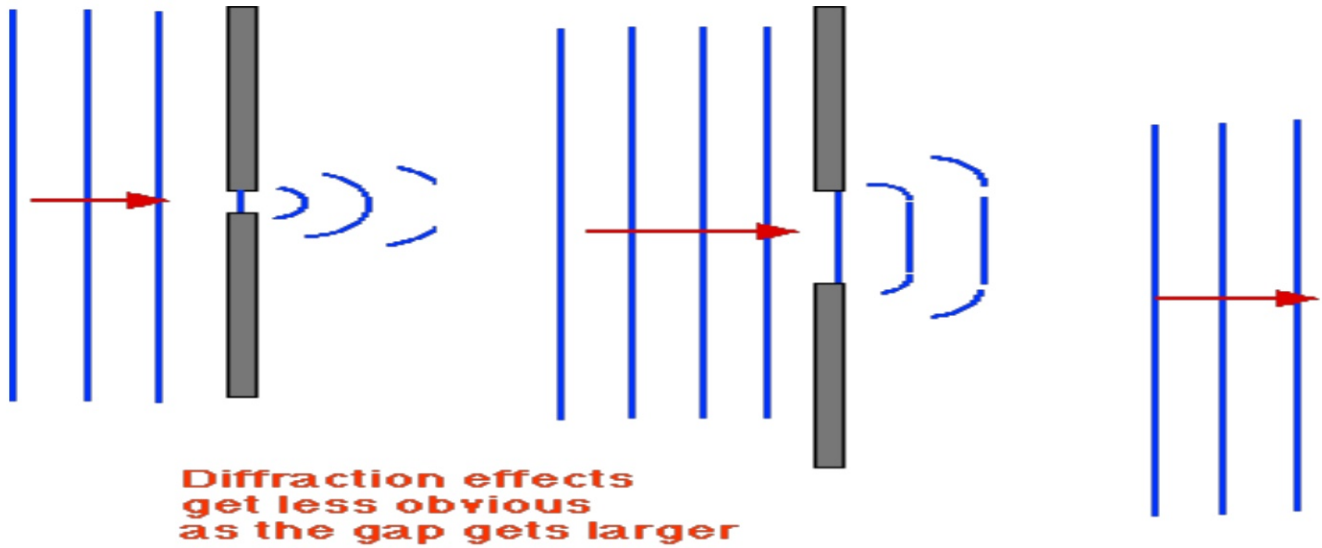


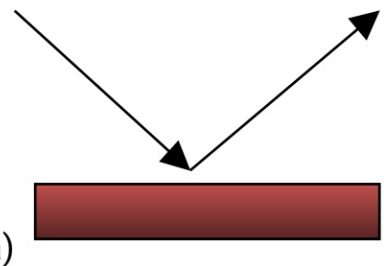
Fig6: Diffraction Transmission Phenomenon

4.2.Reflection

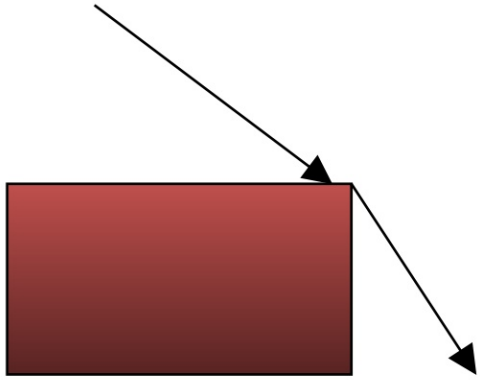
Reflection is the change in direction of a wave front at an between two
so that the wave front returns into the medium from which it originated.

4.3.Diffusion

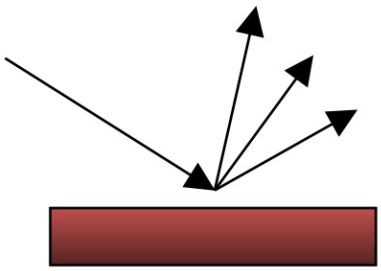
Diffusion is the movement of molecules from a high concentrat
concentration. Many molecules diffuse across cell membranes.



(a)



(b)



(c)

Fig 7:a) A reflection phenomenon ,b) a diffraction phe

and c)a diffusion phenomenon

The different phenomena also generate effects known as multiple path the receiver receives waves from a same transmitter ,but which may different path. These multiple routes have positive effects, such as rece where no direct route exists , but also negative effects , by introducing de greatly disrupt reception, and even cancel it entirely. Finally ,a certain nu phenomena disrupt wireless propagation , induced by the presence electronic equipment or meteorological phenomena.

Chapter 4

Naming and Addressing in

- 4.1.Features of routing in Ad Hoc
- 4.2.Advantages of Ad Hoc
- 4.3.Limitations

NAMING AND ADDRESSING IN AD-HOC NETWO

This short chapter looks at non-standard options for denoting the sende
messages. Traditional Networks such as Fixed Networks, Wireless Ne
Hoc Networks denotes individual nodes by their identity.

As we know ‘Name’ denotes refer to Things. These things sometimes r
data
networks, transactions. Often ,but not always these names are unique w
global, network wide and local. Address is the information needed to fir
such as
IP address ,MAC address. Addresses often hierarchical, because of their
e.g., routing protocols.DNS is used to map between name and addresses
is divided into net id and host id.

4.1.FEATURES OF ROUTING IN AD HOC NETWORKS

To study ad Hoc concepts many proposals have been studied ,simulated
.These same proposals have led to variations ,specializations to give en
optimizations.A routing problem in an ad hoc network is the same as in a

Internet routing is also capable of adapting to dynamics-it is the ma
Internet-but the time scale in which topology changes are made is
internet and a good number of these changes are of much smaller sca
hoc networks.We will consider homogenous nodes,from the point of
communication capacity as well as their calculation and storage capa
radiocoomunication technology and with the help of one communication
whole network. The characteristics in demand by most ad hoc rou
developers are:

and resist topology changes as much as possible.

Scalability protocols offered must adapt to different ad hoc network sizes
Support different mobility and traffic models.

4.2.ADVANTAGES OF AD HOC NETWORKS

Lower getting-started costs . There is no need to install base stations. set up is easy .Well suited to free unlicensed spectrum significant typical auction prices. Ad hoc hypotheses compensate for anomalies not the theory in its unmodified form. Many application software syst underlying database which can be accessed by only a limited number reports. Typically these are available via some sort of menu, and will have designed, pre-programmed and optimized for performance by expert prog

Inherent scalability . Ad Hoc network is based on power control & coope each user contributes to network capacity . In military, ad hoc units are unpredictable situations, when the cooperation between different units The term ad hoc networking typically refers to a system of network combine to form a network requiring little or no planning.

Flexible . These networks are similar to being able to access theIntern different locations. Ad Hoc networks are independent from ce administration. They are self-healing through continuous re-configuration

Ad Hoc networks are widely used in disaster management situation ,w wireless network infrastructure has been damaged .Since ad hoc netw protocol that is adapted to interact with different access points and location ,they don't need any extra deployment.

4.3.LIMITATIONS

While ad hoc networks are typically used where they have the greatest e
advantages, there are some limitations:

• Each node must have full performance
• Throughput is affected by system loading
• Reliability requires a sufficient number of available nodes. Sparse netw
problems
• Large networks can have excessive latency (time delay), which
applications

Some of these limitations also apply to conventional hub-and-spoke base
cannot be addressed by alternate configurations. For example, all networ
by system loading, and networks with few nodes are difficult to justif
solutions.

Chapter 5

Carrier Sense Multiple Acces Collision Avoidance(CSMA/C

- 5.1.Details
- 5.2.IEEE 802.11 RTS/CTS Exchan
- 5.3.Network Allocation Vector(NA
- 5.4.Timing Diagram

CHAPTER 5

CSMA/CA

Introduction

Carrier sense multiple access with collision avoidance (CSMA/CA)
networking, is a wireless network multiple access method in which:

1. a carrier sensing scheme is used.

2. a node wishing to transmit data has to first listen to the channel for a
amount of time to determine whether or not another node is transmitting
within the wireless range. If the channel is sensed "idle," then the node
begin the transmission process. If the channel is sensed as "busy," the
transmission for a random period of time. Once the transmission proce
still possible for the actual transmission of application data to not occur.

5.1.DETAILS

CSMA/CA is a modification of carrier sense multiple access.Collision avo
to improve CSMA performance by not allowing wireless transmissio
another node is transmitting, thus reducing the probability of collision du
a random truncated binary exponential backoff time. The use of collisio
used to improve the performance of CSMA by attempting to divide the w

problems of wireless data communications is that it is not possible
sending, therefore collision detection is not possible

5.2.IEEE 802.11 RTS/CTS EXCHANGE

CSMA/CA can optionally be supplemented by the exchange of a Request
packet sent by the sender S, and a Clear to Send (CTS) packet sent b
receiver R. Thus alerting all nodes within range of the sender, receiver
transmit for the duration of the main transmission. This is known as th
RTS/CTS exchange. Implementation of RTS/CTS helps to solve the
problem that is often found in wireless networking

5.3.NETWORK ALLOCATION VECTOR(NAV)

Network Allocation Vector is a virtual carrier sensing mechanism used
network protocols such as IEEE 802.11 and IEEE 802.16(Wi Max).The
sensing is a logical abstraction which limits the need for physical carrier
air interface in order to save power. The MAC layer frame headers con
field that specifies the transmission time required for the frame in w
medium will be busy.The station on the wireless medium read the duratio
their NAV which is an indicator for a station on how long it must defer f
the medium.

The NAV may be thought of as a counter which count downs to
rate.When the counter is 0,the virtual carrier sense indication is that the
when not 0 this indicates that the medium is busy.

Wireless station are often battery powered,so in order to consume pow
may enter a power saving mode.A station decrements its NAV counter u
0, at which time it is weaken to sense the medium again.

The NAV virtual carrier sensing mechanism is a prominent part of C
protocol used with IEEE 802.11 Wireless LANS

5.4.TIMING DIAGRAM

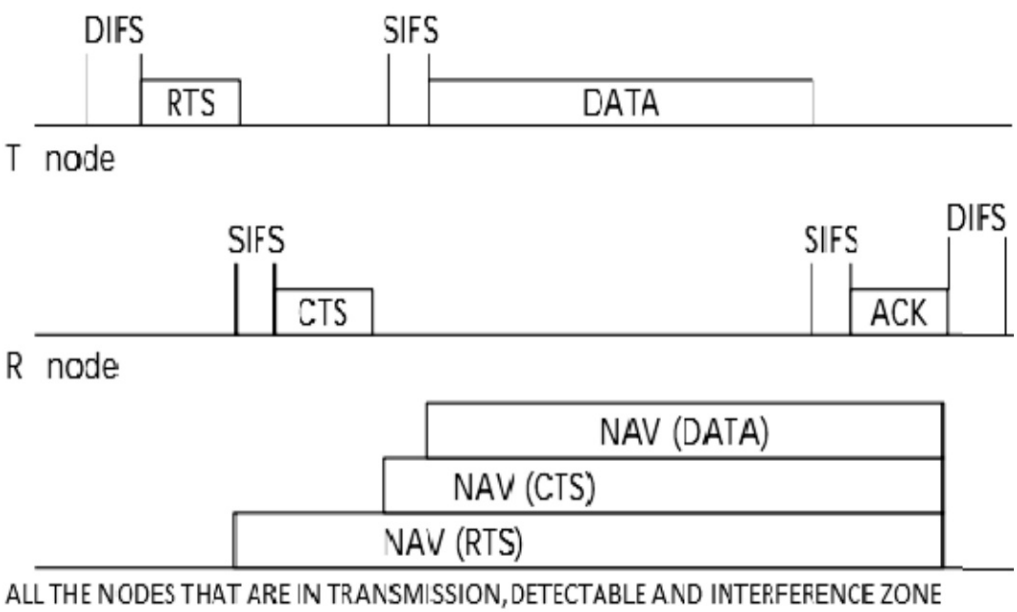


Fig 8: CSMA/CA TIMING DIAGRAM

In the above Fig. we observe that a node want to send some data. For thi
the node wait for some time period randomly. Then it sends RTS (Ready
the nodes which are participating in the transmission. After some tim
nodes send CTS (Clear to send) indicates that they are ready to receive
packet is received without any error the node at the destination respond
(Acknowledgement). If ACK is not received then it is assumed that the
and transmitted again.

Here in the above Fig. 2 shows NAV (RTS) and NAV (CTS) are irrespe
So the nodes which lie in zones of transmission, detectable and interfer
side have same NAV (RTS) and nodes lie in receiver side have same NAV

CHAPTER 6

- Problem Area And Work F

PROBLEM AREA AND WORK PLAN

In paper[2] the interference zone they are not being communic
so there is no need to set the their NAV value. But the inter
cannot be removed fully.

In paper[3] we get the idea to reduce the blockage area usin
Antenna. In this paper a new channel access protocol is p
transmission over cooperative ad hoc networks .The propo
,which aims at minimizing the number of blocked nodes and
improving systems throughput, employs directional anten
source and relay.

Hence in our paper we consider interference zone and i
approach for enhancement of CSMA/CA MAC protocol for ad h
Our proposal is to increase the number of unblocked nodes c
RTS/CTS. According to the timing diagram of CSMA/CA,
communication RTS/CTS are used among nodes by setting the
and are blocked during communication period. If we can r
number of block nodes then they can be used as another com
source, relay or destination and will increase the network perfo
also mathematically reduce blocked area using omnidirectiona

CHAPTER 7

- Case Study

CHAPTER 7

CASE STUDY

The study of Ad Hoc networks creates a drastic change in the fie
communication. A lots of research is going on to success this domain
future.

- "Wireless Ad Hoc and Sensor Networks"-In this book we
definations and concepts of ad hoc networks.

- "Implementation and Performance Analysis of Cooper
Access Control protocol for *CSMA/CA* based Tech
investigate three different MAC protocols based on CSMA/
throughput and channel access delay.

- "Power Saving Mechanism in Clustered Ad-Hoc Networks
the concept that multihop transmission breaks the single h
mobile node to another, into two or more hops, in a m
distances between transmitter and receiver are smaller th
direct transmission, which reduces the transmission power

- "On Reducing Blocking Probability in Cooperative Ad-hoc N
we get the idea of reducing node blockage to improve the p
ad hoc networks.

- "Improved channel access protocol for cooperative ad h

Chapter 8

Proposed Method

- 7.1.Introduction
- 7.2.Proposed Protocol

CHAPTER 7

7.1.INTRODUCTION

Ad Hoc is a kind of network can be used for a specific purpose. In this th
of any router or any wireless base station. This network does not re
existing infrastructure and nodes are mobile. Besides this, they will send
without any distortion. Since there is no pre existing infrastructure
communicates among them using radio waves, where each nodes offers
and cooperate coordination using the node diversity.

These networks introduced a new art of network established and can be
an environment where either the infrastructure is lost or where deploy an
is not very cost effective. The nodes in ad hoc network is surrounded b
they are transmission zone, detectable zone and interference zone. O
antenna is placed at each node. Omni directional antenna covers a rang
to this Omni directional antenna these zones are at certain range having s

At the time of data transmission RTS (Ready to send) is sent by the tra
whether it will be any relay or source. It is received by all nodes which lie
transmission zone, detectable zone and interference zone and set their N
and remain block during the completion of data transmission. After son
CTS (Clear to send) is sent by the receiver node and all other nodes wh
they set their NAV (CTS) value and this receiving time onwards the noc
region are blocked. The signal power is gradually decrease from transm
detectable and interference zone as the distance and power are inversely

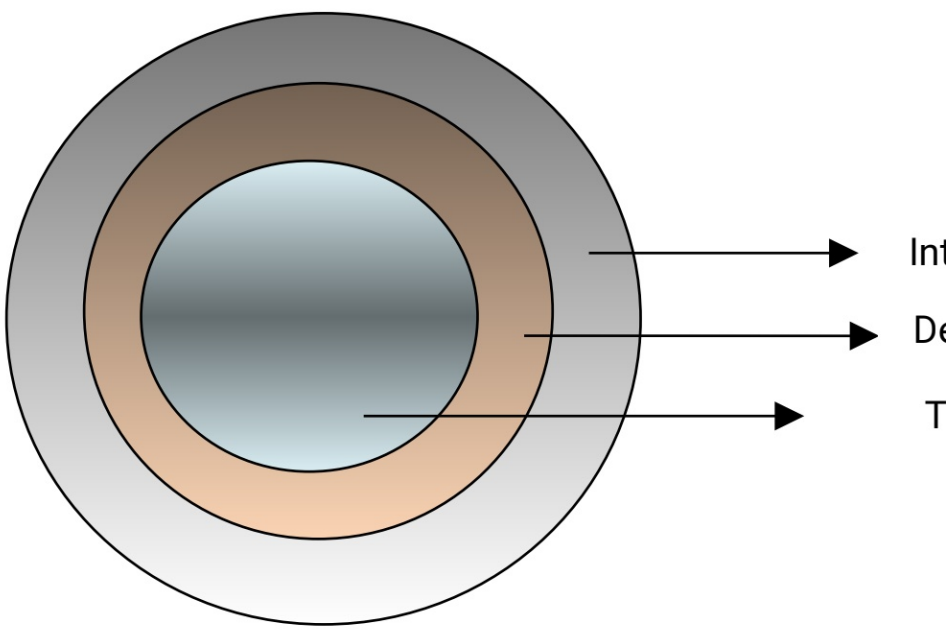


Fig 9:Zones in Ad Hoc

As in Fig 1 all the nodes lies in three zones set same NAV value. But pow
is decreased gradually. Our proposal is to make less time value then orig
and NAV (CTS) value. Similar condition will apply in detectable and tran
That is our proposal the NAV (RTS) and NAV (CTS) time value in transm
greater than detectable zone's NAV (RTS) / NAV (CTS). As well as det
NAV (RTS) / NAV (CTS) than transmission zones (RTS) / NAV (CTS) i.e.
the NAV value. Now in interference zone's node will unblock previous
zone's node and further detectable zone's node will unblock previous t
zone. Which nodes previously unblocked once they are not communic
start communication or used as a relay or destination. Hence the pe
increase.

7.2.PROPOSED PROTOCOL

If we consider the data transmission between source or relay and des
Rs_t is radius of source node to its transmission zone; Rs_d is radius of sou
detectable zone and Rs_i is radius of source node to its interference zone.
the radius of relay node to the transmission zone. Rr_d is the radius of

to Fig.1 it will look like Fig.3.

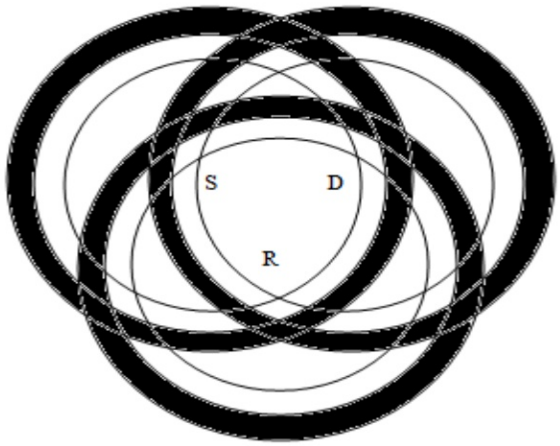


Fig 10 the black colour shows the interference zone of sou
destination

The timing diagram of the above figure is as follows in fig 4.If we wa
proposed protocol we need to segment the NAV (RTS) and NAV (CTS) o
will get the modifications of CSMA/CA as on Fig. 4.

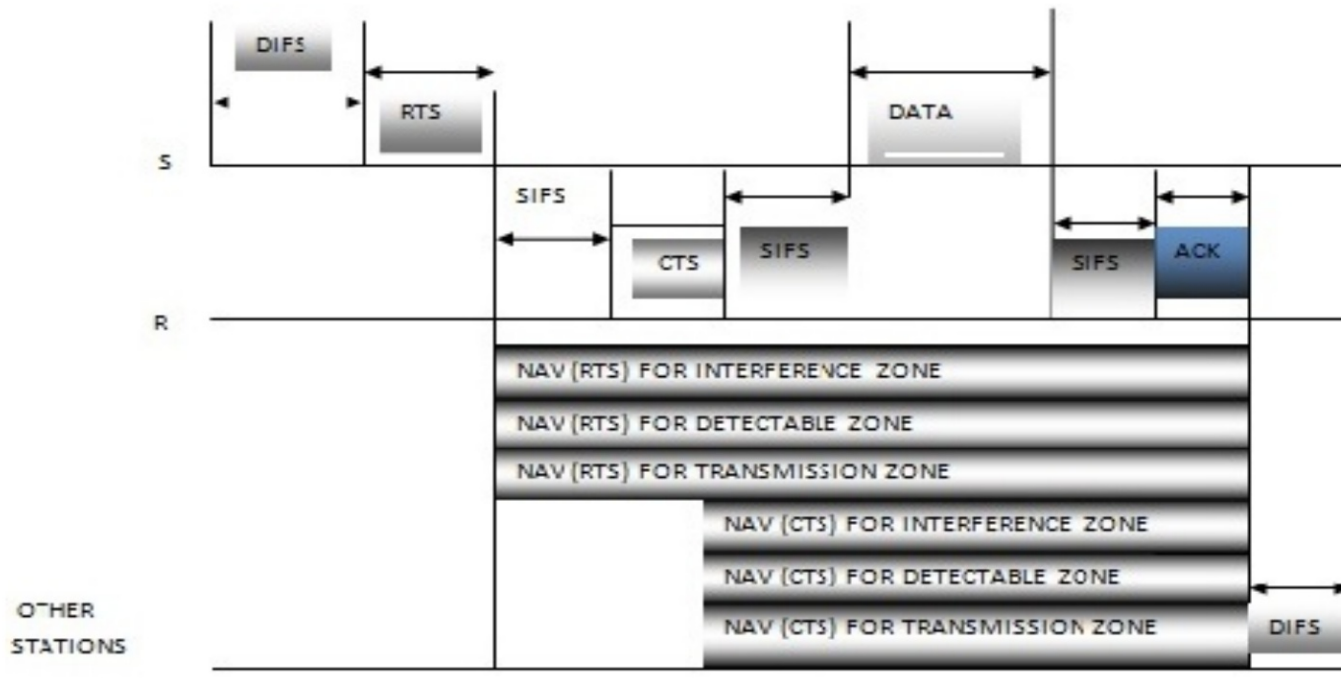


Fig. 11: NAV (RTS) and NAV (CTS) for all zones

NAV (CTS) for destination interference zone.

When we apply our proposed protocol it will again modified and look like
it shows that NAV (RTS) and NAV (CTS) for interference zone is there
zones has less power signal i.e. the nodes in this region will not block d
transmission to some extent.

Chapter 9

Analytical Method

- 8.1.Analytical Representation updated Timing Diagram

METHOD WITH UPDATED TIMING DIAGRAM

In the interference zone they are not being communicate any more so th to set the their NAV[1] value. In interference energy consumption is impo power signal reach to less number of nodes and consumption of energy Energy specification [4] of CSMA/CA MAC protocol is standardized. D distribution of sender and receiver of ad-hoc network interference avera effective so much. Concentrated on the idea of medium access a transmission [6] or retransmission developed a new frequency ban communication.

In the given figure we consider P as source node and Q as destination no

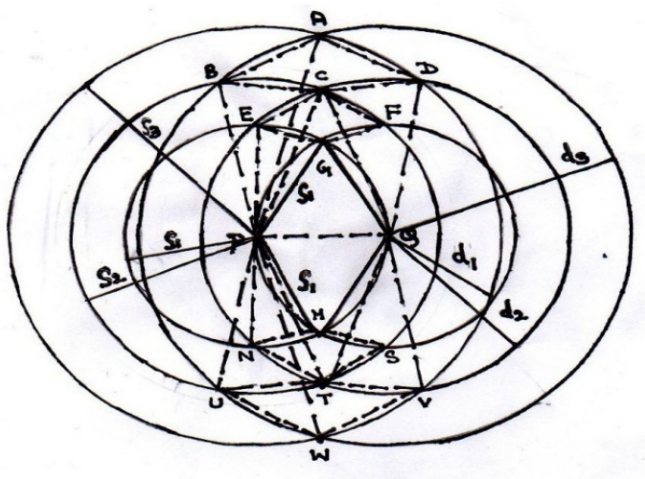


Fig 12: The intersection area of all three zones

The three zones surrounding node P has at distance s_1, s_2, s_3.Similar distance d_1, d_2, d_3. Now According to [2] the area of intersection wh transmits the data is

$$A(L_{max}) = 2d_{max}^2 \cos^{-1}\left(\frac{L_{max}}{2d_{max}}\right) - \frac{1}{L_{max}}\sqrt{4d_{max}^2 - L_{max}^2}$$

Now,
Area of the source interference zone $A_{si}=\pi s_3^2$
Similarly

Where, A_{DT} is the Area of Intersection between source detectable zo
transmission zone. Similarly,

Area of the destination interference zone $A_{di}=\pi d_3^2$
Area of the destination detectable zone $A_{dd}=\pi d_2^2$
Area of the destination transmission zone $A_{dt}=\pi d_1^2$

Now Area of Intersection between destination interference zone a
detectable zone
$AD_{ID} = A_{di} - A_{dd} = \pi (d_3^2 - d_2^2)$
$AD_{DT} = A_{dd} - A_{dt} = \pi (d_2^2 - d_1^2)$

Where, A_{DT} is the Area of Intersection between destination detecta
destination transmission zone.
Now if we remove the Area of intersection then the updated Fig 5 will loo
the area of the blocked region

$A_{BA}= \{(AS_{ID} + AS_{DT}) + (AD_{ID} + AD_{DT})\} - (A(L_{max})$ of outer intersection + inne

Now according to [1] there is area of detectable zone and transmitte
interference zone. In my proposal the NAV value of detectable zone an
zone will not be same as[1] that means only the transmitted the data will
value for RTS and CTS and in detectable zone it will less and in interfere
more less. So we consider variable NAV value for transmission, c
interference zone.
Now let us consider,

Ps_t is the power transmitted by the souce node in transmission zone
Ps_d is the power transmitted by the souce node in detectable zone
Ps_i is the power transmitted by the souce node in interference zone

$Ps_t > Ps_d > Ps_i$

Similarly the $SINR_t > SINR_d > SINR_i$

$SINR_t$ is the signal to noise ratio

So if we set a NAV value for all zones then according to Relation (7)

NAV_t =NAV value

Hence $NAV_t > NAV_d > NAV_i$

Hence the variable NAV values for the blocked area as per Equation 6 updated timing diagram in Fig 7.

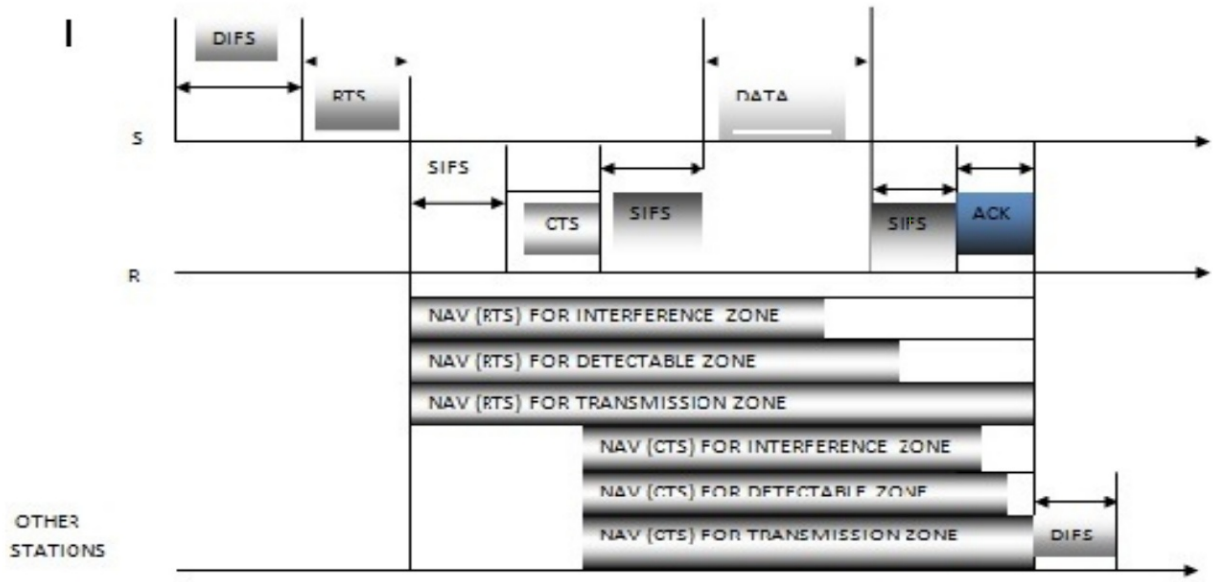


Fig.13: Variable NAV values for three zones

Here, NAV (RTS) is now

a) NAV (RTS) for interference
b) NAV (RTS) for detectable and
c) NAV (RTS) for transmission.

Whereas, NAV (CTS) is now
a) NAV (CTS) for interference zone
b) NAV (CTS) for detectable and
c) NAV (CTS) for transmission zone.

CHAPTER 10

- Conclusion
- Future Work