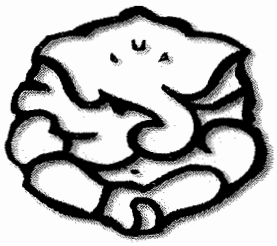
Sri Kadari Lakshmi Narsimha Swamy



8TH SEM CSE/ISE

AD HOC NETWORKS

ASHOK KUMAR K

VIVEKANANDA INSTITUTE OF TECHNOLOGY

Mob: 9742024066

E-MAIL : celestialcluster@gmail.com

Note:

Notes for unit 1, 2, and 7 are prepared by:

RAKESH S

VIVEKANANDA INSTITUTE OF TECHNOLOGY

MOB: 9535052814

I would dedicate my notes to the following students:

VAIBHAV PAI

SANTOSH NAIKAR

SUNIL L V

BHARATH V

SANDEEP R

SANTOSH M

SHASHIDHAR B

SUHAS SRINIVASAN

PRASHANTH

CHIRANTHAN

- **RAKESH S**

Dedicated To:

DEEPIKA N
Sri Venkateshwara College of Engineering, Bangalore

NAYANA M C
Sri Venkateshwara College of Engineering, Bangalore

DEEPIKA C
Global Academy of Technology, Bangalore

MALA B C
BGSIT, Nagamangala, Mandya

SPECIAL THANKS

I would also like to thank some of the students for their valuable feedback on my previous notes.

RAJESH RN, *JVIT, Ramanagaram*
SHWETHA, *DBIT, Bangalore*
JANU KHANDARI, *SKIT, Bangalore*
BIPIN, *JSSATE, Bangalore*
SHILPA, *SRSIT, Bangalore*
LAKSHMI, *SKIT, Bangalore*
MANASA, *JSSATE, Bangalore*
RAMYA, *RNSIT, Bangalore*
BRADLEY, *Mangalore*
SUMANTH, *JSSATE, Bangalore*
APEKSHA, *RNSIT, Bangalore*
SRIKANTH, *Tumkur*
RUKMINI, *Hassan*
KARTHIK RAO, *PESSE, Bangalore*
NISHITHA, *PESCE, Mandya*
SHIVU, *BNMIT, Bangalore*
KARTHIKA, *AMCEC, Bangalore*
BHARATH, *JVIT, Ramanagaram*
JAGANNATH, *BMS Evening College, Bangalore*
HEMANTH, *Shimoga*
NACHAPPA, *JSSATE, Bangalore*
PRADEEP, *DSCE, Bangalore*
DARSHINI, *JVIT, Ramanagaram*
MRUDULA, *GAT, Bangalore*
DEEPAK, *RNSIT, Bangalore*
SUHAS K.M, *Bellary*
JAYPRADEEP, *Sapthagiri College of Engineering, Bangalore*
ASHRITHA ALVA, *NMIT, Bangalore*
SANDEEP PAI, *HKBKCE, Bangalore*
HARISH, *Chikmaglur*
GIRISH, *JVIT, Ramanagaram*

Syllabus

AD HOC WIRELESS NETWORKS

* Introduction
* Issues in Ad Hoc Wireless Networks
* Ad Hoc wireless Internet.

INTRODUCTION

* The principle behind adhoc networking is **multi-hop relaying.**

View of past to present

How msgs were sent ?

» line of shouting men positioned on tall structures or heights. [Adhoc voice communication]

↓

In 1970, ALOHAnet [Invented by Norman Abramson]
It utilised single hop wireless n/w & a multiple access soln for sharing a single channel

↓

Then came, Ethernet [Developed by Robert Metcalfe]
&
PRNET → Packet Radio Network

PRNET used combination of ALOHA & CSMA i.e., Carrier Sense Multiple Access, for access to shared radio channel. PRNET proved feasibility & efficiency of n/w.

↓

Mobile Adhoc Networks (MANET)

↓

In 1994, bluetooth came into existance

↓

piconets & scatternet

Cellular & Ad hoc Wireless Networks

* The figure below shows the representation of different wireless networks.

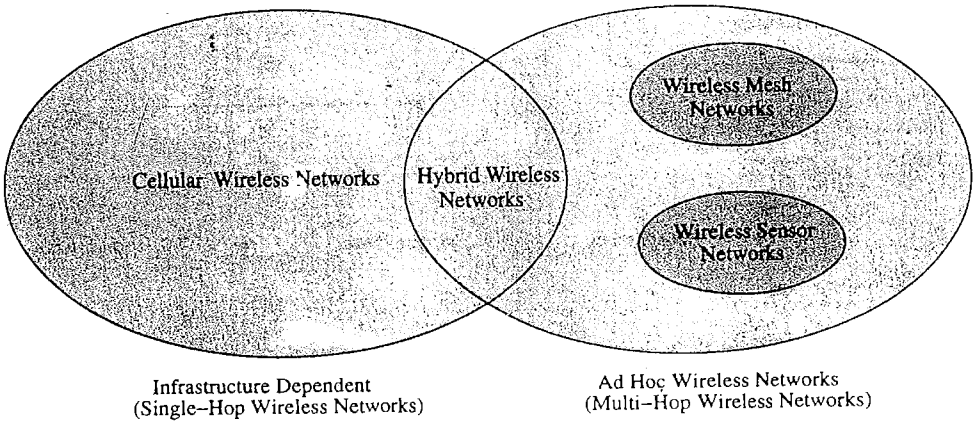
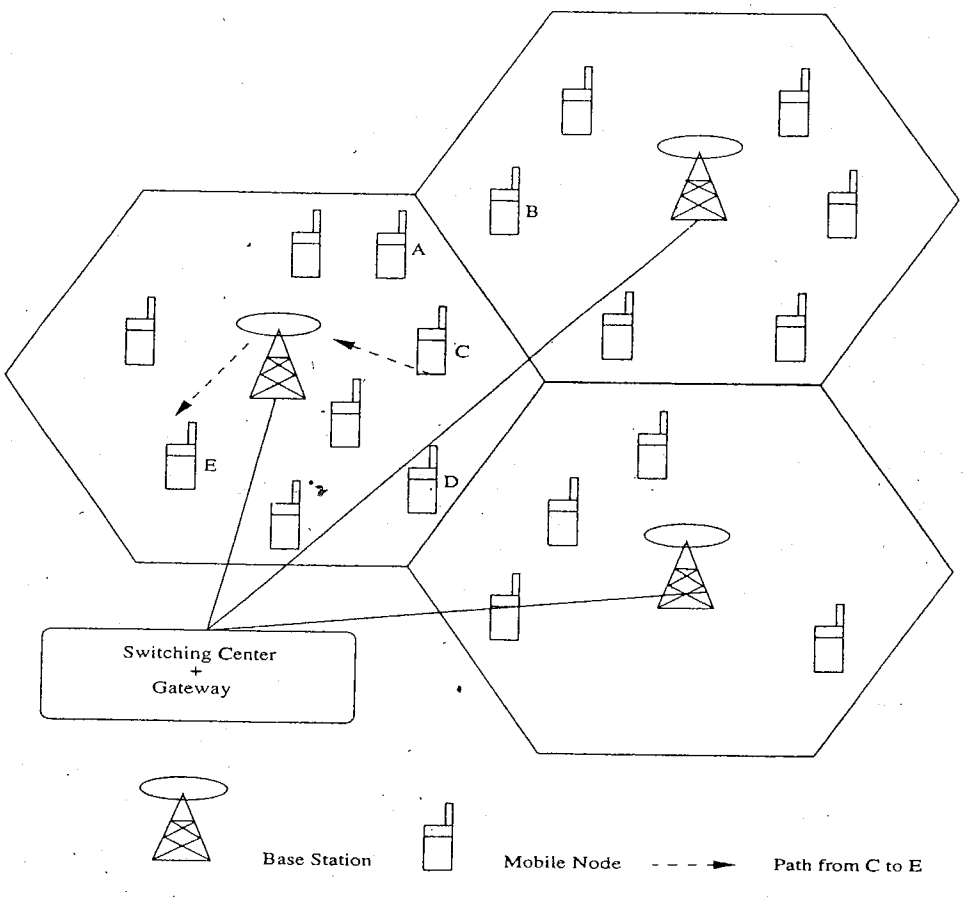


Figure : Cellular and ad hoc wireless networks.

* The current cellular wireless networks are classified as the infrastructure dependent nw. The path setup for a call b/w 2 nodes, say, node C to E, is completed through base station as illustrated in fig below

Figure : A Cellular Network



* Ad hoc wireless networks are defined as a category of wireless n/w that utilize multi-hop radio relaying & are capable of operating without the support of any fixed infrastructure.
* Absence of any central co-ordinator or base station makes the routing complex.
* Adhoc wireless n/w topology for the cellular n/w shown in above fig is illustrated below. The path setup for a call b/w 2 nodes, say, node C to E, is completed through the intermediate mobile node F.
* Eg of adhoc wireless n/w's :- wireless mesh n/w & wireless sensor n/w.

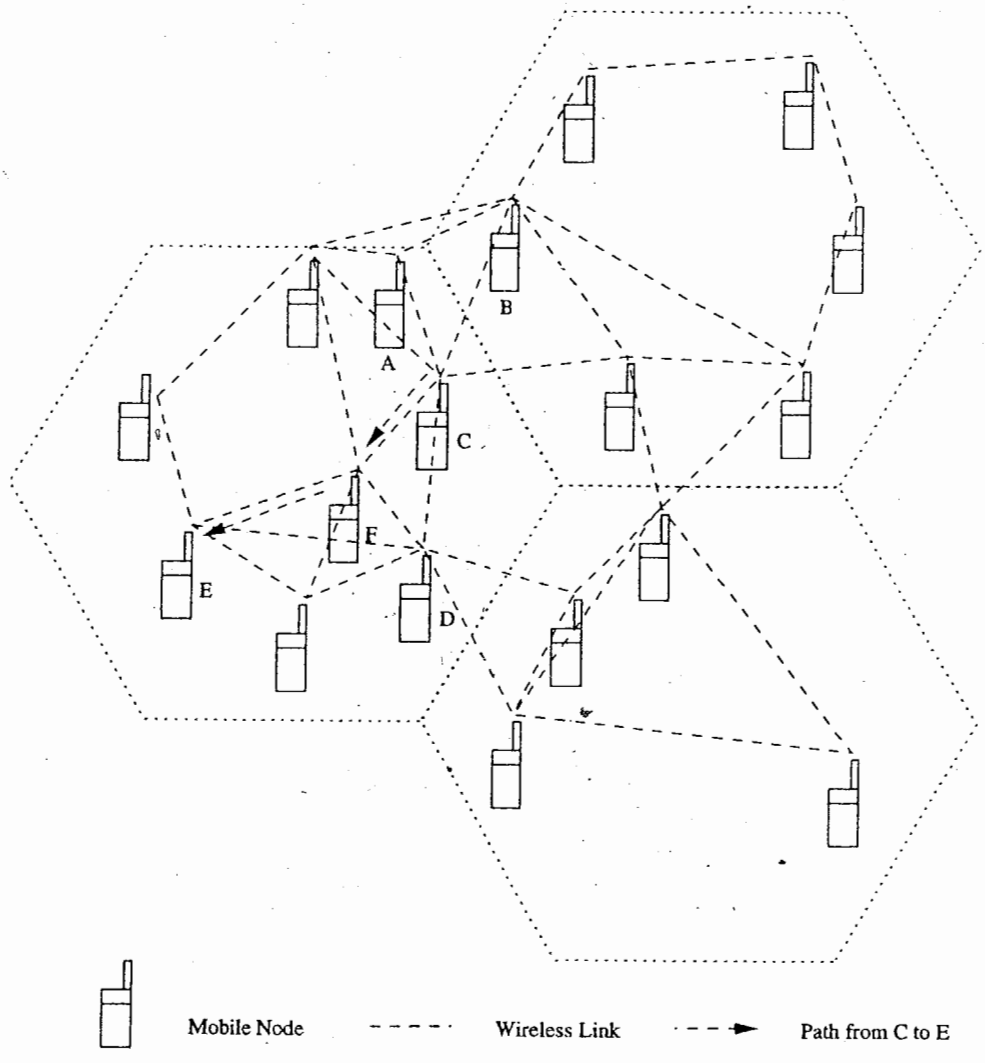


Figure An ad hoc wireless network.

* The presence of base station simplifies routing & resource mgmt in a cellular n/w.

But in adhoc networks, routing & resource mgmt are done in a distributed manner in which all nodes co-ordinate to enable comm^n amg themselves.

list out the difference b/w cellular networks & adhoc wireless networks.

Cellular Networks	Ad Hoc Wireless Networks
Fixed infrastructure-based	Infrastructure-less
Single-hop wireless links	Multi-hop wireless links
Guaranteed bandwidth (designed for voice traffic)	Shared radio channel (more suitable for best-effort data traffic)
Centralized routing	Distributed routing
Circuit-switched (evolving toward packet switching)	Packet-switched (evolving toward emulation of circuit switching)
Seamless connectivity (low call drops during handoffs)	Frequent path breaks due to mobility
High cost and time of deployment	Quick and cost-effective deployment
Reuse of frequency spectrum through geographical channel reuse	Dynamic frequency reuse based on carrier sense mechanism
Easier to achieve time synchronization	Time synchronization is difficult and consumes bandwidth
Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control protocols
Application domains include mainly civilian and commercial sectors	Application domains include battlefields, emergency search and rescue operations, and collaborative computing
High cost of network maintenance (backup power source, staffing, etc.)	Self-organization and maintenance properties are built into the network
Mobile hosts are of relatively low complexity	Mobile hosts require more intelligence (should have a transceiver as well as routing/switching capability)
Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	Main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths
Widely deployed and currently in the third generation of evolution	Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense

Applications of Ad Hoc Wireless Network

{Hint : MECH WW}

1. Military Applications

* Adhoc wireless n/w's can be very useful in establishing communication amng a group of soldiers for tactical operations.
* Setting up of a fixed infrastructure for comm^n amng group of soldiers in enemy territories or in inhospitable terrains may not be possible. In such a case, adhoc wireless networks provide reqd comm^n mechanism quickly.
* The primary nature of the comm^n reqd in a military environment enforces certain impt requirements on adhoc wireless n/w's namely, reliability, efficiency, secure comm^n & support for multicast routing.

2. Emergency Operations

* In environments where the conventional infrastructure based comm^n facilities are destroyed due to a war or due to natural calamities, immediate deployment of adhoc wireless networks would be a good sol^n for co-ordinating rescue activities.

3. Collaborative & Distributed Computing

* Adhoc wireless n/w helps in collaborative computing, by establishing temporary comm^n infrastructure for quick comm^n with minimal configuration amng a group of ppl in a confuence.
* In distributed file sharing appl^n reliability is of high importance which would be provided by adhoc n/w.

4. Wireless Mesh Networks

* Wireless mesh networks are adhoc wireless n/w that are formed to provide an alternate comm^n infrastructure for mobile or fixed nodes/users, without the spectrum reuse constraint & requirement of n/w planning of cellular n/w.
* It provides the most economical data transfer capability coupled with the freedom of mobility.
* The infrastructure built is in the form of small radio relaying devices fixed on the roof tops of the house in residential zone or highway, or in campus.
* It operates at the license-free ISM band around 2.4 GHz & 5 GHz. It is scaled well to provide support to large no. of points.
* Major adv is the support for a high data rate, quick & low cost of deployment, enhanced services, high scalability, easy extendability, high availability & low cost per bit.

5. Wireless Sensor Networks

* Sensor networks are special category of adhoc wireless n/w that are used to provide a wireless comm^n infrastructure amg the sensors deployed in a specific appl^n domain.
* Sensor nodes are tiny devices that have capability of sensing physical parameters processing the data gathered, & comm^n to the monitoring system.
* The issues that make sensor n/w a distinct category of adhoc wireless n/w are the following:

- Mobility of nodes
- Size of the n/w
- Density of deployment
- Power constraints
- Data or information fusion
- Traffic distribution.

6. Hybrid Wireless Network

* One of the major appln area of adhoc wireless n/w is in the hybrid wireless architecture such as multi-hop cellular network (MCN) & integrated cellular adhoc relay (iCAR).
* MCN's combine the reliability & support of fixed base station of cellular n/w with flexibility & multi-hop relaying of adhoc wireless networks.
* Major adv are as follows:
  (a) Higher capacity than cellular n/w's due to the better channel reuse.
  (b) Increased flexibility & reliability in routing.
  (c) Better coverage & connectivity in holes of a cell can be provided by means of multiple hops through intermediate nodes in a cell.

ISSUES IN AN AD-HOC NETWORK (Hint: MTR MESS ADS PQ)

The major issues that affect the design, deployment, & performance of an adhoc wireless n/w system are.

1. Medium Access scheme
2. Transport layer protocol
3. Routing.
4. Multicasting.
5. Energy management
6. Self-organisation
7. Security.
8. Addressing & service discovery
9. Deployment considerations
10. Scalability
11. Pricing scheme
12. Quality of service provisioning.

Medium Access Scheme

The primary responsibility of a medium access control (MAC) protocol in adhoc wireless networks is the distributed arbitration for the shared channel for transmission of packets.

The major issues to be considered in designing a MAC protocol for adhoc wireless networks are as follows:

1. Distributed operation
2. Synchronization
3. Hidden terminals
4. Exposed terminals
5. Throughput
6. Access delay
7. Fairness

} Self Explanatory

8. Real-time traffic support
9. Resource reservation
10. Ability to measure resource availability
11. Capability for power control.
12. Adaptive rate control
13. Use of directional antennas.

} Self Explanatory

Routing

The responsibilities of a routing protocol include exchanging the route info^{n}; finding a feasible path to a destination.

The **major challenges** that a routing protocol faces are as follows:

1. Mobility
2. Bandwidth constraint
3. Error-prone & shared channel
4. Location-dependent contention

} Self Explanatory

5. Other resource constraints, such as computing power, battery power & buffer storage.

The **major requirements** of a routing protocol in adhoc wireless networks are the following:

1. Minimum route acquisition delay.
2. Quick route reconfiguration.
3. Loop-free routing.
4. Distributed routing approach
5. Minimum control overhead
6. Scalability
7. Provisioning of QoS
8. Support for time-sensitive traffic

} Self Explanatory

Multicasting

* It plays impt role in emergency search & rescue operations & in military communication.
* Use of single-link connectivity amg the nodes in a multicast group results in a tree-shaped multicast routing topology. Such a tree-shaped topology provides high multicast efficiency, with low pkt delivery ratio due to the frequent tree breaks.
* The major issues in designing multicast routing protocols are as follows.
  1. Robustness → refers to recovering & reconfiguring quickly the data.
  2. Efficiency
  3. Control overhead
  4. Quality of service
  5. Efficient group mgmt
  6. Scalability
  7. Security

  } Self Explanatory

Transport layer Protocols

* The main objectives of the transport layer protocols include:- setting up & maintaining end-to-end connections, reliable end-to-end delivery of data pkts, flow control & congestion control.

Eg: Some transport layers

UDP (connectionless) → neither perform flow control, nor congestion control

TCP (connection-oriented)

↳ perform flow control & congestion control

Pricing Scheme

Assume that an optimal route from node A to node B passes through node C, & node C is not powered on. Then node A will have to set up a costlier & non-optimal route to B. The non-optimal path consumes more-resources & affects the throughput of the system.

As the intermediate nodes in a path that relay the data pkts expend their resources such as battery charge & computing power, they should be properly compensated.

Hence pricing schemes that incorporate service compensation or service reimbursement are required.

Quality of service Provisioning

* QoS is the performance level of services offered by a service provider or a n/w to the user.
* QoS provising often requires.
  - ⇝ negotiation b/w host & the n/w.
  - ⇝ resource reservation schemes
  - ⇝ priority scheduling. &
  - ⇝ call admission control.

QoS parameters

Applications	corresponding QoS parameter
Multimedia appl^n	bandwidth & delay.
Military appl^n	security & reliability.
Defense appl^n	finding trustworthy intermediate hosts & routing.
Emergency operation	availability.
Hybrid wireless n/w	max available link, delay, bandwidth & channel utilization.

QoS-aware routing

* Finding the path is the 1st step in this.
* The parameters that can be considered for routing decisions are
  - ⇝ n/w throughput
  - ⇝ pkt delivery ratio
  - ⇝ reliability
  - ⇝ delay
  - ⇝ jitter
  - ⇝ pkt loss rate
  - ⇝ bit error rate &
  - ⇝ path loss.

QoS framework

* A framework for QoS is a complete system that attempts to provide the promised services to each user or application.
* The key component of QoS framework is a QoS service model which defines the way user requirements are served.

Self-Organization

* One very impt property that an adhoc wireless n/w should exhibit is organizing & maintaining the n/w by itself.
* The major activities that an adhoc wireless n/w is req'd to perform for self-organization are
  - ⇝ neighbour discovery
  - ⇝ topology organization &
  - ⇝ topology reorganization. (updating topology info^n)

Addressing & Service Discovery

* Addressing & service discovery assume significance in adhoc wireless n/w due to the absence of any centralised coordinator.

Security

* Security is an impt issue in adhoc wireless n/w as the information can be hacked.

* Attacks against n/w are of 2 types
  - (i) Passive attack → made by malicious node to obtain info^n transacted in the n/w without disrupting the opeation.
  - (ii) Active attack → they disrupt the oper^n of n/w.

* The major security threats that exist in adhoc wireless n/w's are as follows.
  1. Denial of service (Unavailable of service to nodes due to overload on system)
  2. Resource consumption — 2 major types → Energy depletion / Buffer overflow
  3. Host impersonation (Internal node creating wrong entries and terminating automatically before reaching destn)
  4. Information disclosure
  5. Interference (refers to jamming wireless comm^n by creating a wide-spectrum noise)

Energy Management

* Energy mgmt is defined as the process of managing the sources & consumers of energy in a node or in the n/w for enhancing the lifetime of a network.

* Features of energy mgmt are :
  - → Shaping the energy discharge pattern of a node's battery to enhance battery life.
  - → finding routes that consumes min energy
  - → using distributed scheduling schemes to improve battery life
  - → handling the processor & interface devices to minimize power consumption.

* Energy mgmt can be classified into the following categories:

1. Transmission power mgmt
2. Battery energy mgmt
3. Processor power mgmt
4. Devices power mgmt

Scalability

* Scalability is the ability of the routing protocol to scale well in a n/w with a large no. of nodes.

* It requires minimization of control overhead & adaptation of the routing protocol to the n/w size.

Deployment Considerations

* The deployment of a commercial adhoc wireless n/w has the following benefits when compared to wired networks.

(i) Low cost of deployment
(ii) Incremental deployment
(iii) Short deployment time
(iv) Reconfigurability.

* The following are the major issues to be considered in deploying an adhoc wireless network.

1. Scenario of deployment.

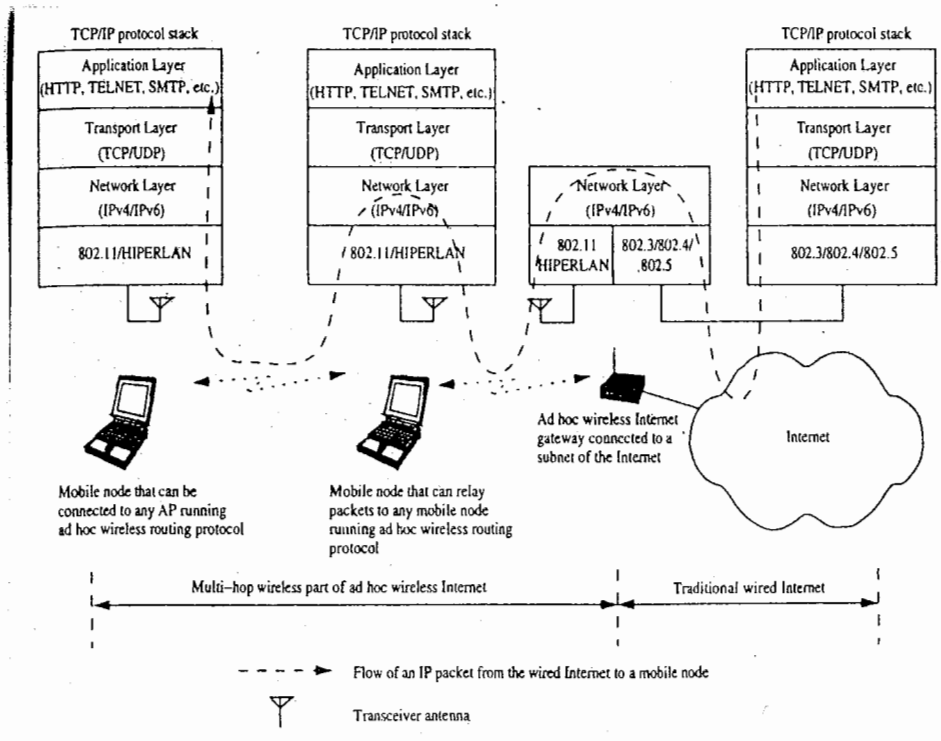
Some scenarios are

- Military deployment
- Emergency deployment
- Commercial wide-area deployment
- Home network deployment

2. Required longevity of n/w.
3. Area of coverage
4. Service availability
5. Operational integration with other infrastructure
6. Choice of protocols.

AD HOC WIRELESS INTERNET

* Ad hoc wireless internet extends the services of the internet to the end users over an adhoc wireless n/w.
* Some of the applications of adhoc wireless internet are:
  - → wireless mesh n/w
  - → provisioning of temporary internet services to major conference venues.
  - → sports venues
  - → temporary military settlements.
  - → battlefields.
  - → broadband Internet services in rural regions.
* Schematic dia of adhoc wireless internet is shown below.



The major issues to be considered for a successful adhoc wireless Internet are the following.

1. Gateways

↳ They are the entry points to the wired internet
↳ They perform following tasks
- Keeping track of end users
- bandwidth mgmt
- load balancing
- traffic shaping
- packet filtering
- width fairness &
- address, service & location discovery.

2. Address mobility

↳ This problem is worse here as the nodes operate over multiple wireless hops.

3. Routing

↳ It is a major problem in adhoc wireless internet, due to dynamic topological changes, the presence of gateways, multi-hop relaying, & the hybrid character of the n/w.
↳ Possible soln is to use separate routing protocol. for the wireless part of adhoc wireless internet.

4. Transport layer protocol

↳ Several factors are to be considered here, the major one being the state maintenance overhead at the gateway nodes.

5. Load balancing

↳ They are essential to distribute the load so as to avoid the situation where the gateway nodes become

6. Pricing / billing

↳ Since Internet bandwidth is expensive, it becomes very important to introduce pricing/billing strategies for the adhoc wireless Internet.

7. Provisioning of security.

↳ Security is a prime concern since the end users can utilize the adhoc wireless internet infrastructure to make e-commerce transaction.

8. QoS support

↳ With the widespread use of voice over IP (VoIP) & growing multimedia applications over the Internet, provisioning of QoS support in the adhoc wireless Internet becomes a very impt issue.

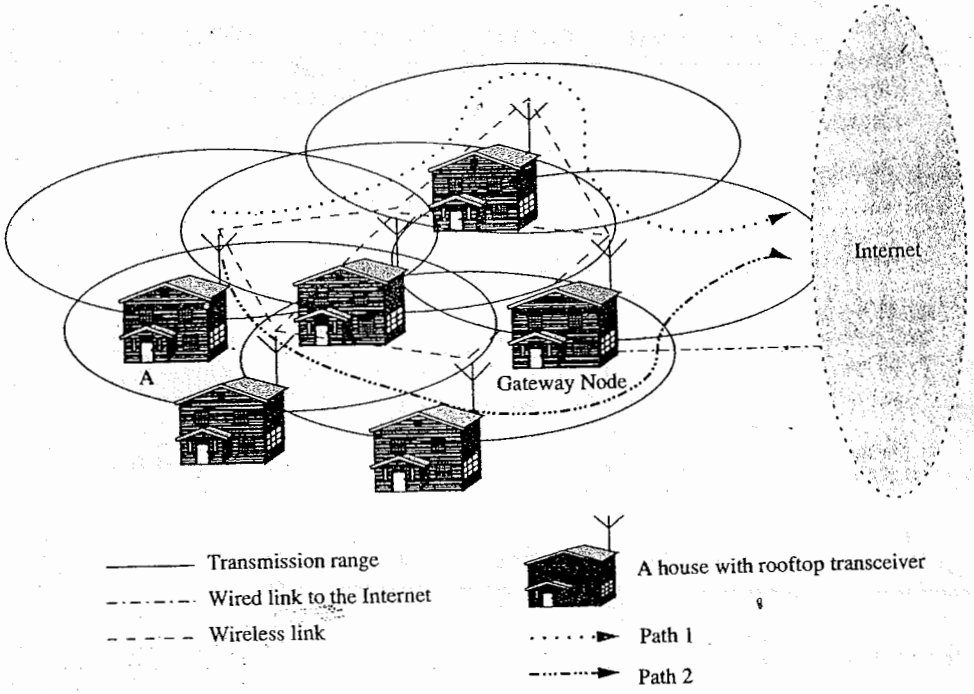
9. Service, address & location discovery

↳ Service discovery refers to the activity of discovering or identifying the party which provides service or resource.

↳ Address discovery refers to the services such as those provided by address resolution protocol (ARP) or domain name service (DNS) operating within the wireless domain.

↳ Location discovery refers to different activities such as detecting the location of a particular mobile node in the n/w or detecting the geographical location of nodes.

* Figure below shows a wireless mesh n/w that connects several house to the Internet through a gateway node. Fig shows that house A is connected to the internet over multiple paths (path 1 & path 2).



Rakesh.S
VKIT

Syllabus

* Introduction
* Issues in designing a MAC protocol for Adhoc wireless n/w
* Design goals for AdHoc wireless networks using MAC protocol
* Classification of MAC protocol
* Contention-based protocols with reservation mechanism

INTRODUCTION

Nodes in an adhoc wireless network share a common broadcast radio channel. Since the radio spectrum is limited, the bandwidth available for communication in such n/w is also limited.

Access to shared medium should be controlled in such a manner that all nodes receive a fair allocation of bandwidth. MAC protocol would help this.

ISSUES IN DESIGNING A MAC PROTOCOL FOR AD HOC WIRELESS NETWORKS

The following are the main issues in designing a MAC protocol for adhoc wireless networks : (BQ SH ED M

1. Bandwidth efficiency

↳ It is defined as follows

$$\text{b/w efficiency} = \frac{\text{actual data transmission}}{\text{total available bandwidth}}$$

↳ MAC protocol must be designed in such a way that the scare b/w is utilised in an efficient manner.

↳ MAC protocol must try to maximize this b/w efficiency.

2. Quality of Service Support

↳ QoS support is essential for supporting time-critical traffic sessions such as in military communications.

3. Synchronization

↳ MAC protocol must take into consideration the synchronization between nodes in the n/w.

↳ It is impt., for bandwidth reservations by nodes.

4. Hidden & Exposed terminal problem.

These problems are uniaue to wireless n/w.

* The hidden terminal problem refers to the collision of pkts at receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the the transmission range of receiver.

collision occurs when 2 nodes transmit pkt at same time without knowing abt transmission of each other.

In fig., both node S1 & S2 transmit pkt to node R1 at the same time, their pkts collide at R1. This is because both nodes S1 & S2 are hidden from each other as they are not within the direct transmission range of each other & hence do not know abt the presence of each other.

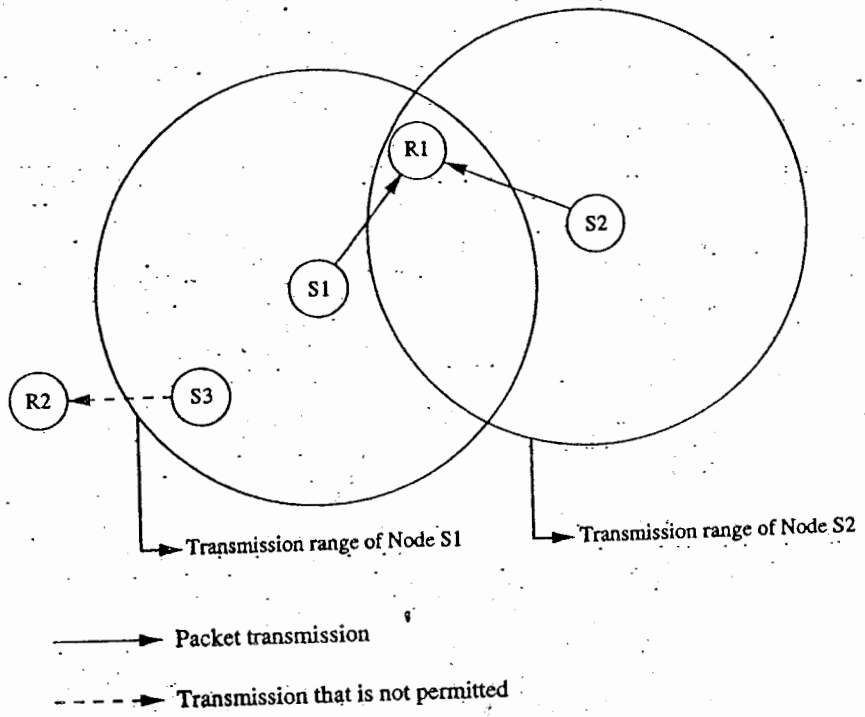


Figure . Hidden and exposed terminal problems.

* The exposed terminal problem refers to the inability of node, which is blocked due to transmission of a pkt by a nearby node to another node

In figure, if a transmission from node S1 to another node R1 is already in progress, S3 cant transmit to node R2, as it concludes that its neighbour node S1 is in transmitting node & hence it should not interfere with on-going transmission.

* These problems reduce throughput of a n/w when the traffic load is high

Hence desirable MAC protocol must be free

5. Error-prone shared broadcast channel

↳ A MAC protocol should grant channel access to nodes in such a manner that collisions are minimized.

↳ Also, the protocol must ensure that all nodes are treated fairly wrt bandwidth allocation.

6. Distributed Nature / lack of central co-ordinators.

↳ Ad hoc wireless n/ws do not have centralized co-ordinators.

↳ The MAC protocol that we design must implement it.

7. Mobility of Nodes

↳ MAC protocol must not degrade the performance of a system due to mobility of nodes.

DESIGN GOALS OF A MAC PROTOCOL FOR AD HOC WIRELESS NETWORKS

The following are the impt, goals to be met while designing MAC protocol for an adhoc wireless networks.

1. The operation of a protocol must be **distributed.**
2. The protocol should provide **QoS support for real-time traffic.**
3. The **access delay**, which refers to the delay experienced by any pkt to get transmitted, must be kept low.
4. The available **bandwidth** must be efficiently utilised.
5. The protocol should ensure **fair allocation of bandwidth** to nodes
6. **Control overhead** must be kept as low as possible.
7. The protocol must be **scalable to large network**

8. The protocol must minimize the effects of hidden & exposed terminal problem.
9. It should have power control mechanism.
10. It should have adaptive data rate control mechanism.
11. Protocol should provide time synchronization amg nodes.
12. It should try to use directional antennas which can provide advantages such as reduced interface, reduced power consumption & increased spectrum reuse.

CLASSIFICATION OF MAC PROTOCOLS

Ad hoc network MAC protocol can be classified into 3 basic types:

1. Contention-based protocol
2. Contention-based protocol with reservation mechanisms.
3. Contention-based protocol with scheduling mechanisms.

Contention-based protocols

These protocols follow a contention-based channel access policy. This is further divided into 2 types.

(i) *Sender-initiated protocols*

↳ Packet transmission are initiated by the sender node.

↳ This is further divided into 2 types.

a) Single-channel sender-initiated protocol in which, the total available bandwidth is used as it as, without being divided.

b) Multichannel sender-initiated protocol in which, the available bandwidth is divided into multiple channels.

(ii) Receiver Initiated protocols

↳ The receiver node initiates the contention resolution protocol.

Contention-based protocols with Reservation Mechanism

These protocols provide QoS support to time-sensitive traffic sessions. These protocols can be further divided into 2 types.

(i) Synchronous Protocols

↳ They require time synchronization amg all nodes in the network, so that reservations made by a node are known to other nodes in its neighbourhood

↳ Global time synchronization is very difficult to achieve.

(ii) Asynchronous Protocols

↳ They do not require any global synchronization amg nodes in the network.

↳ These protocols use relative time info for effective reservations.

Contention-Based Protocols with Scheduling Mechanism

↳ These protocols focus on pkt scheduling at nodes, & also scheduling nodes for access to channel.

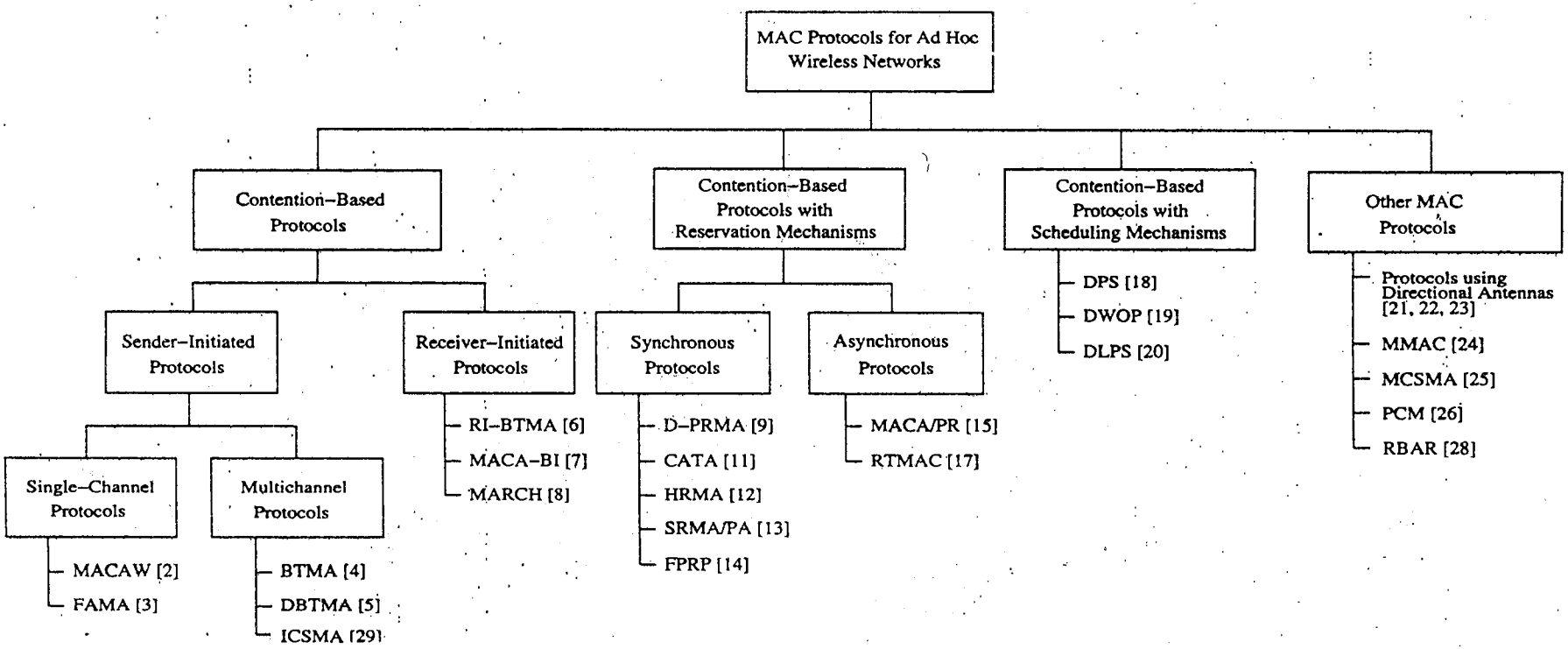


Figure Classifications of MAC protocols.

CONTENTION BASED PROTOCOLS WITH RESERVATION MECHANISMS

1. Distributed Packet Reservation Multiple Access Protocol

* The D-PRMA protocol extends the earlier centralized pkt reservation multiple access (PRMA) scheme into a distributed scheme that can be used in adhoc wireless n/w.
* D-PRMA extends this protocol for providing voice support in adhoc wireless networks.
* D-PRMA is a TDMA-based scheme.
* The channel is divided into fixed & equally shared frames as shown in below figure.

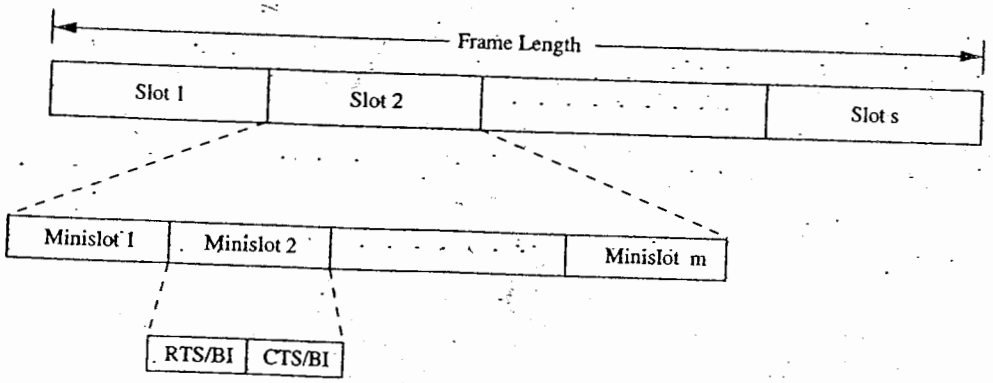


Figure Frame structure in D-PRMA.

Each frame is composed of s slots, & each slot consists of m minislots. Each minislots can be further divided into 2 control fields, RTS/BI & CTS/BI (BI stands for Busy Induction).

These control fields are used for slot reservation & for overcoming the hidden termina problem.

* All nodes having pkts ready for transmission contend for the minislot of each slot. The remaining (m-1) minislots are granted to the node that wins the contention.
* Within a reserved slot, comm^n b/w the source & receiver nodes takes place by means of either **time division duplexing** (TDD) or **frequency division duplexing (FDD)**. Any node that wants to transmit pkts has to first reserve slots, if they have not been already reserved.
* If a sender node detects the channel to be idle at the beginning of a slot (minislot), it transmits an RTS pkt (slot reservation request) to the intended destination through the RTS/BI part of the current minislot. On successfully receiving this RTS pkt, the receiver node responds by sending a CTS pkt. through the CTS/BI of the same minislot.
* In D-PRMA to avoid hidden terminal problem, all nodes hearing the CTS sent by the receiver are not allowed to transmit during the remaining period of that same slot.
* TO avoid exposed terminal problem, a node hearing RTS but not the CTS is still allowed to transmit pkt.
* D-PRMA is **more suited for voice traffic than for data traffic applications**.

2. Collision Avoidance Time Allocation Protocol

* The CATA protocol is based on **dynamic topology-dependent transmission scheduling**.
* CATA supports broadcast, unicast & multicast transmission simultaneously.
* The operation of CATA is based on 2 basic principles
  1. The receiver(s) must inform the potential source nodes abt the reserved slot on which it is currently receiving pkts. Similarly, the source node must inform the potential destination node(s) abt interferences in the slot.
  2. Usage of negative acknowledgments for reservation requests, & control pkt transmissions at the beginning of each slot, for distributing slot reservation info" to senders of broadcast or multicast sessions.
* Time is divided into equal-sized frames, & each frame consists of S slots as shown in figure.

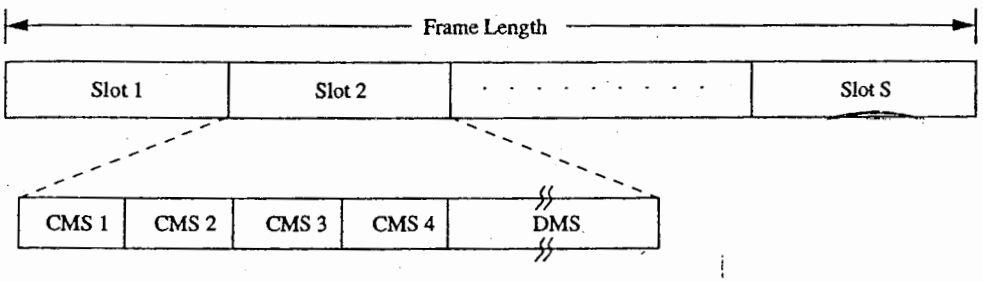


Figure Frame format in CATA.

Each slot is further divided into 5 minislots. The first 4 minislots are used for transmitting control pkts & are called control minislots (CMS1, CMS2, CMS3, CMS4). The 5th & last minislot, called data

* Each node that receives data during the DMS of current slot transmits a **slot reservation** (SR) pkt during the CMS1 of the slot.

Every node that transmits data during DMS of the current slot transmits a **request-to-send** (RTS) pkt during CMS2 of the slot.

> The sender of an intended reservation, if it senses the channel to be idle during CMS1, transmits an RTS packet during CMS2. The receiver node of a unicast session transmits a clear-to-send (CTS) packet during CMS3. On receiving this packet, the source node understands that the reservation was successful and transmits data during the DMS of that slot,

> Once the reservation has been made successfully in a slot, from the next slot onward, both the sender and receiver do not transmit anything during CMS3, and during CMS4 the sender node alone transmits a not-to-send (NTS) packet,

* The length of the frame is very impt in CATA. For any node (say, node A) to broadcast successfully there must be no other node (say node B) in its two-hop neighbourhood that transmits simultaneously. If such a node B exists, then if node B is within node A's one-hop neighbourhood, node A & node B cannot heal the pkt transmitted by each other.

* CATA works well with simple single-channel half-duplex radios. It provides support for collision-free broadcast & multicast traffic.

3. Hop Reservation Multiple Access Protocol (HRMA)

* The HRMA protocol is a multichannel MAC protocol which is based on simple half-duplex, very slow frequency-hopping spread spectrum (FHSS) radios.

* It uses a reservation & handshake mechanism to enable a pair of communicating nodes to reserve a frequency hop, thereby gauranteeing collision-free data transmission even in the presence of hidden terminals.

> Out of the available L frequency channels, HRMA uses one frequency channel, denoted by f_0, as a dedicated synchronizing channel. The nodes exchange synchronization information on f_0. The remaining $L-1$ frequencies are divided into $M = \lfloor \frac{(L-1)}{2} \rfloor$ frequency pairs (denoted by (f_i, f_i^*), $i = 1, 2, 3, .., M$), thereby restricting the length of the hopping sequence to M. f_i is used for transmitting and receiving hop-reservation (HR) packets, request-to-send (RTS) packets, clear-to-send (CTS) packets, and data packets. f_i^* is used for sending and receiving acknowledgment (ACK) packets for the data packets received or transmitted on frequency

* In HRMA, time is slotted & Each slot it assigned a separate frequency hop, which is one amg the M frequency hops in the hopping sequence.

Each time slot is divided into 4 periods, namely synchronization period, HR period, RTS & CTS period, each period is meant for receiving the synchronization pkt, FR pkt, RTS pkt & CTS pkt respectively.

* Frame format in HRMA is as shown below. It is composed of a single synchronization slot, followed by M consecutive normal slots

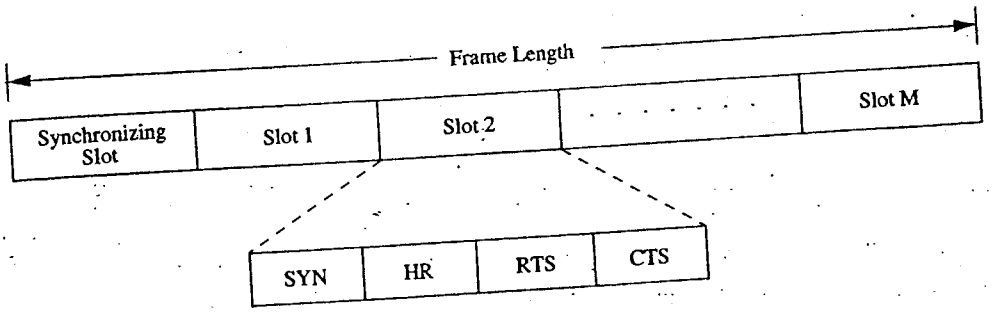


Figure Frame format in HRMA.

Figure : depicts the worst-case frequency overlap scenario. In the figure, the maximum number of frequency hops $M = 5$. It is evident from the figure that within any time period equal to the duration of a HRMA frame, any two nodes from the two disconnected partitions always have at least two overlapping time periods of length μ_s on the synchronizing frequency f_0. Therefore, nodes belonging to disconnected network components can easily merge into a single network.

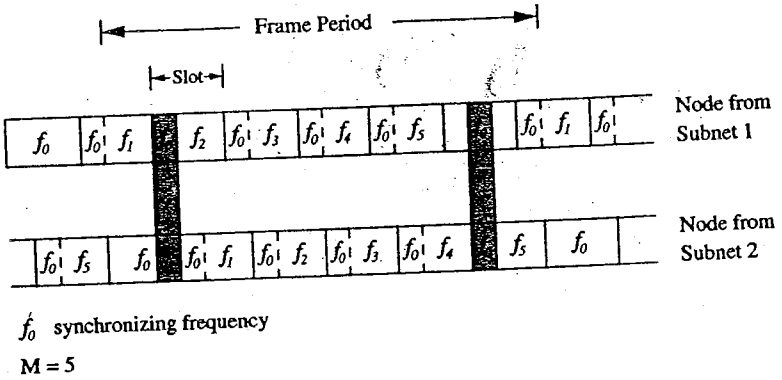


Figure Merging of subnets.

* when a node receives data to be transmitted, it first listens to the HR period of the immediately following slot.

If it finds the channel to be free during the SR period, it transmits an RTS pkt to the destination during the RTS period of the slot & wait for the CTS pkt.

On receiving the RTS, the destination nodes transmits the CTS pkt during the CTS period of the same slot,

If the source node receives the CTS pkt correctly, it implies that the source & receiver nodes have succesfully reserved the current hop.

* After transmitting each data pkt, the source node hops onto this acknowledgement frequency. The receiver sends an acknowledgement (ACK) pkt back to the source on this acknowledgment frequency.
* Data pkts transmitted can be of any size.

4. Soft Reservation Multiple Access with Priority Assignme

* SRMA/PA was developed with the main objective of supporting integrated services of real-time & non-real-time appl^n in an adhoc wireless n/w's, at the same time maximizing the statistical multiplexing gain.
* Nodes use a collision-avoidance handshake mechanism & a soft-reservation mechanism in order to contend for & effect reservation of time-slots.
* Main features of SRMA/PA are
  - → a unique frame str & soft reservation capability for distributed & dynamic slot scheduling
  - → dynamic & distributed access priority assignment & update policies
  - → time-constrained back-off algorithm.

* Time is divided into frames, The frame str is shown below.

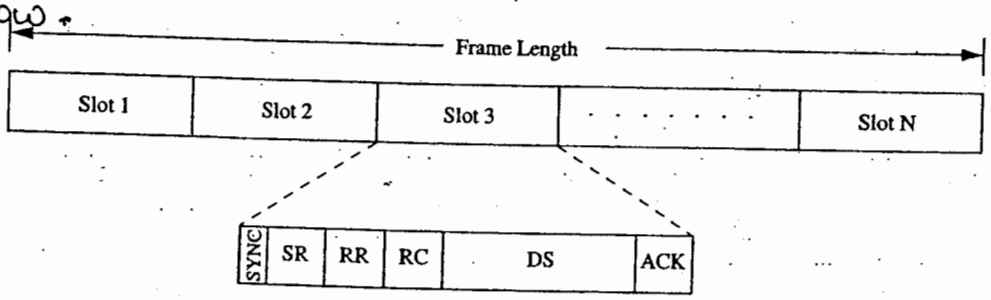


Figure Frame structure in SRMA/PA.

Each slot is further divided into 6 different fields, SYNC, soft reservation (SR), reservation request (RR), reservation confirm (RC), data sending (DS), & acknowledgment (ACK).

The SYNC field is used for sychronization purposes. The SR, RR, RC & ACK fields are used for transmitting & receiving the corresponding control pkts. The DS field is used for data transmission.

* In case of a voice terminal node, the node tries to take control of the slot already reserved by a data terminal if it finds its priority level to be higher than that of the data terminal. This process is called <u>soft reservation</u>.

* Priority levels are initially assigned to nodes based on the service classes in a static manner.

The node is assigned a prespecified priority, $P_v^{(R)}$ or $P_d^{(R)}$, respectively for voice & data terminals. R denotes that the node is a reserved node, that is, a node that has successfully reserved the slot. It is reqd that $P_v^{(R)} > P_d^{(R)}$, such that delay.

data applications.

* A node that is currently transmitting is said to be in the **active state**.

A node is said to be in **idle state** if it does not have any pkt to be transmitted.

In active state itself node can be in one of the following 2 states

(i) **Access state**, the one in which the node is backlogged & is trying to reserve a slot for transmission.

(ii) The node is said to be in **reserved state** if it has already reserved slot for transmission.

* In order to avoid collisions in SRMA/PA, a binary exponential back-off algorithm is used for non-real time connections & a modified exponential back-off algorithm is used for real-time connection

5. Five-Phase Reservation Protocol

* The FPRP is a single-channel TDMA-based broadcast scheduling protocol.
* The protocol is insensitive to the n/w size i.e., it is scalable.
* This protocol also ensures that no collisions occur due to the hidden-terminal problem.
* Time is divided into frames. There are 2 types of frames: reservation frame (RF) & information frame (IF

Each RF's is followed by a sequence of IF's. Each RF has N reservation slots (RS), & each IF has N information slots (IS).

The structure of frame is shown below.

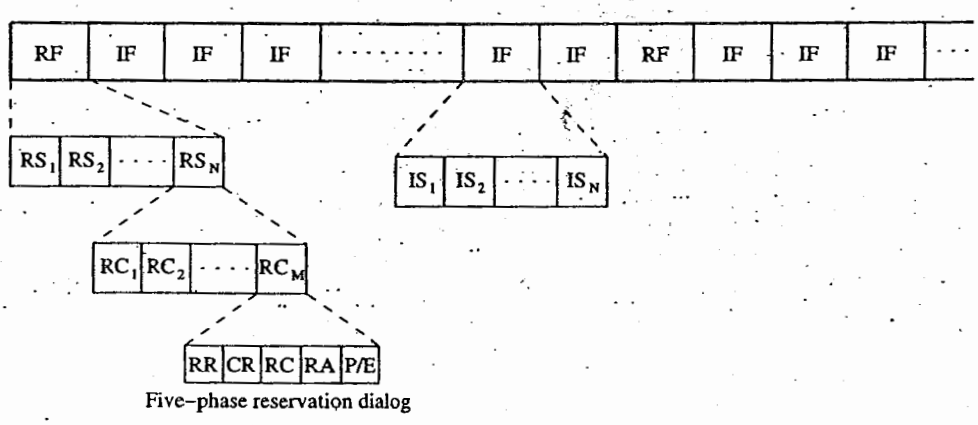


Figure Frame structure in FPRP.

Each RS is composed of M reservation cycles (R within each RC, a 5-phase dialog takes place, using which a node reserves slots.

During IS, a node would be in one of the following 3 states: transmit (T), receive (R) or blocked (B).

* Each node knows when a five-phase cycle would start. The five-phase of the reservation process are as follows.

1. Reservation request phase: Nodes that need to transmit packets send reservation request (RR) packets to their destination nodes.

2. Collision report phase: If a collision is detected by any node during the reservation request phase, then that node broadcasts a collision report (CR) packet. The corresponding source nodes, upon receiving the CR packet, take necessary action.

3. Reservation confirmation phase: A source node is said to have won the contention for a slot if it does not receive any CR messages in the previous phase. In order to confirm the reservation request made in the reservation request phase, it sends a reservation confirmation (RC) message to the destination node in this phase.

4. Reservation acknowledgment phase: In this phase, the destination node acknowledges reception of the RC by sending back a reservation acknowledgment (RA) message to the source. The hidden nodes that receive this message defer their transmissions during the reserved slot.

5. Packing and elimination (P/E) phase: Two types of packets are transmitted during this phase: packing packet and elimination packet.

In this phase, a packing packet (PP) is sent by each node that is located within two hops from a TN, and that had made a reservation since the previous P/E phase. A node receiving a PP understands that there has been a recent success in slot reservation three hops away from it, and because of this some of its neighbors would have been blocked during this slot. The node can take advantage of this and adjust its contention probability p, so that convergence is faster.

In an attempt to resolve a non-isolated deadlock, each TN is required to transmit an elimination packet (EP) in this phase, with a probability 0.5. A deadlocked TN, on receiving an EP before transmitting its own EP, gets to know about the deadlock. It backs off by marking the slot as reserved and does not transmit further during the slot.

* consider the following figure.

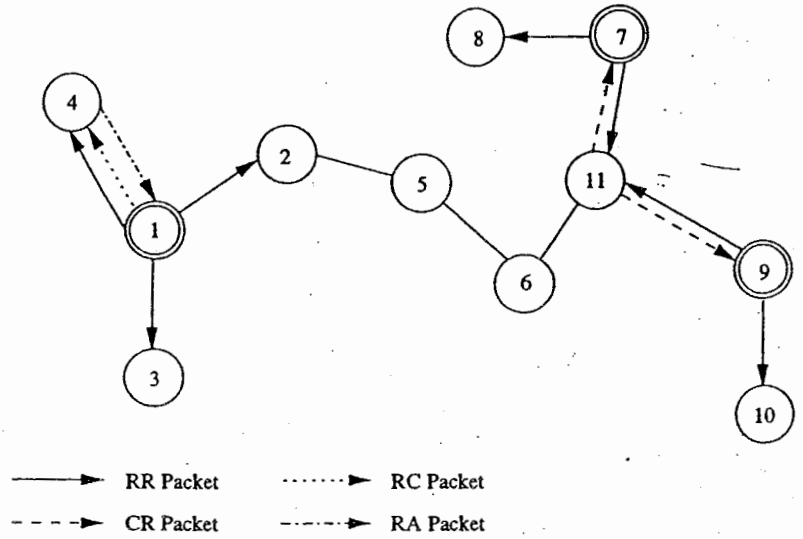


Figure (FPRP Example

Here nodes 1, 7 & 9 have pkts ready to be transmitted to nodes 4, 8 & 10 respectively.

During the **reservation-request phase**, all three nodes transmit RR pkts. Since no other node in the two-hop neighbourhood of node 1 transmits simultaneously, node 1 does not receive any CR msg in the **collision-report phase**. So node 1 transmits an RC message in the next phase for which node 4 sends back RA msg.

Node 7 & 9 both transmit RR pkt in the reservation-request phase. Here node 9 is within 2-hops from node 7. So if both nodes 7 & 9 transmit simultaneously, their RR pkts collide at common neighbour node 11. Node 11 sends a CR pkt which is heard by 7 & 9. On receiving CR pkt, nodes 7 & 9 stop contending for the current slot.

(2 more protocols have been left. Plz refer text book)

UNIT 5 : ROUTING - 2

Syllabus

* Hybrid Routing Protocol
* Routing protocols with effective flooding mechanisms.
* Hierarchical Routing protocols
* Power aware Routing protocols

— 6 Hours.

HYBRID ROUTING PROTOCOLS

* Here, each node maintains the network topology information up to m nodes.
* We discuss following Hybrid Routing protocols
  1. Core Extraction Distributed Ad Hoc Routing (CEDAR) protocol.
  2. Zone Routing Protocol (ZRP)
  3. Zone Based Hierarchical Link State Routing (ZHLS) protocol

Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR)

* CEDAR integrates routing and support for QoS.
* It is based on extracting core nodes (also called as Dominator nodes) in the network

Basic concept:

→ core nodes together approximate the minimum Dominating set (DS).
A DS of a graph is defined as a set of nodes such that every nodes in the graph is either present in the DS or is a neighbor of some node present in the DS.

→ There exists at least one core node within every three hops.

→ The nodes that choses a core node as their dominating node are called core member nodes of the core node concerned.

→ The path b/w two core nodes is termed a virtual link.

→ CEDAR employs a distributed Algorithm to select core nodes
The selection of core nodes represents the core extraction phase

→ CEDAR uses the core broadcast mechanism to transmit any packet throughout the n/w in the unicast mode, involving as min. no. of nodes as possible.

~~Route Establishment in CEDAR.~~

~~phase 1~~

→ ~~Finding core nodes:~~
~~The nodes that takes part in the core broadcast process are called core nodes~~
~~It involves substantial control overhead~~

→ ~~Establishing virtual link:~~
~~The path b/w two core nodes are is termed as virtual link~~

~~phase 2.~~

→ ~~check local topology:~~

* Route Establishment in CEDAR:

It is carried out in two phase.

i.) The first phase finds a core path from source to destination.
The core path is defined as the path from the dominator of the source node (source core) to the dominator of the destination node (Destination core)

ii.) In the second phase, a QoS feasible path is found over the core path.

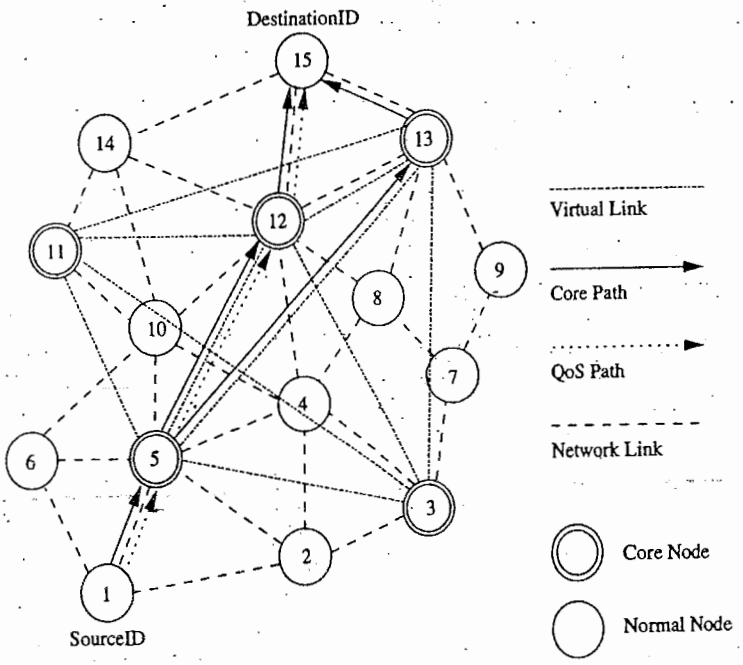
→ A node initiates a RouteRequest if the destination is not in the local topology table of its core node; otherwise the path is immediately established.

→ For establishing a route, the source core initiates a core broadcast in which the RouteRequest is sent to all neighboring core nodes which inturn fawards it.

→ A core node which has the destination node as its core member replies to the source core.

→ Once the core path is established, a path with the required QoS support is then choosen.

* Illustration: (refer fig)


DestinationID
15
14
13
12
11
9
8
10
7
4
6
5
3
2
1
SourceID
Virtual Link
Core Path
QoS Path
Network Link
Core Node
Normal Node

PTO

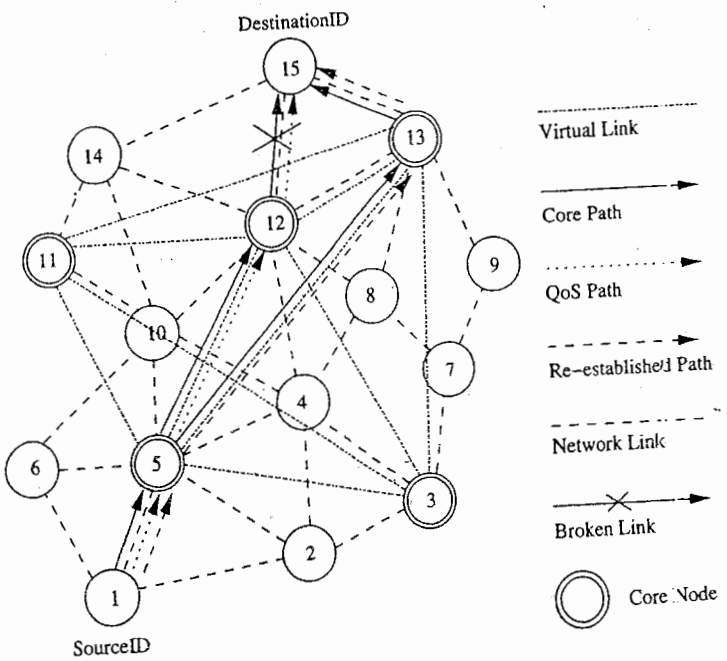
* Route maintainence in CEDAR.

CEDAR attempts to repair a broken route locally when a path break occurs.

→ A node after which the break occured:
- sends a notification of failure
- begins to find a new path from it to the destn.
- rejects every received packet till the moment it finds the new path to the destn.

→ Meanwhile, as the source receives the notification message;
- it stops to transmit
- tries to find a new route to the destn.

→ If the new route is found by either of these two nodes, a new path from the source to the destn is established.



* Advantages:

→ performs both routing & QoS path computation very efficiently with the help of core nodes.

→ Utilization of core nodes reduces traffic overhead.

→ Core broad casts provide a reliable mechanism for establishing paths with QoS support.

* Disadvantages:

→ Since route establishment is carried out at core nodes, the movement of core nodes adversely affects the performance of the protocol.

→ Core node update information causes control overhead.

Zone Routing Protocol (ZRP)

* Effectively combines the best features of both proactive and Reactive routing protocols.

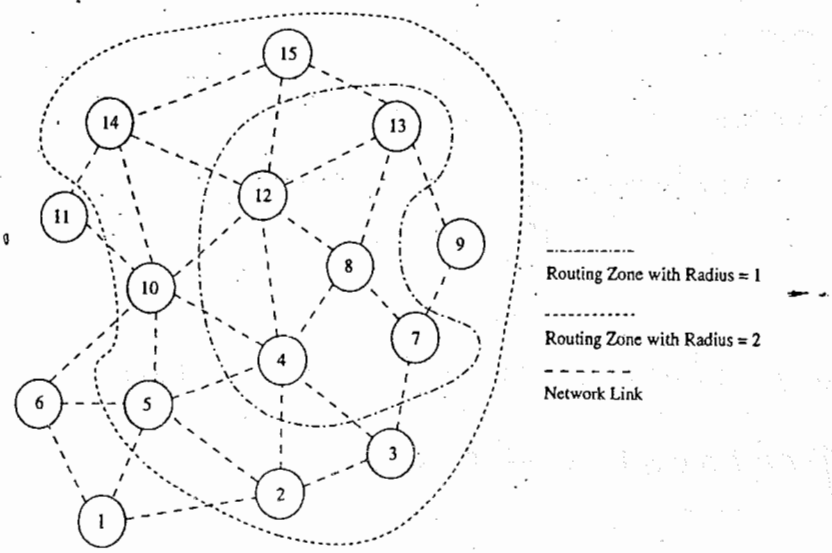
* concept: → use a proactive routing scheme within a limited zone in the r-hop neighborhood of every node.

→ use a reactive routing scheme for nodes beyond this.

* An intra-zone Routing protocol (IARP) is used in the ~~node~~ zone where a particular node employs proactive routing.
The reactive routing protocol used beyond this zone is referred to as inter-zone routing protocol (IERP)

* The routing zone of a given node is a subset of the network, within which all nodes are reachable within less than or equal to zone radius hops.

eg: (refer fig)



Routing Zone for Node 8

* Route Establishment:

→ when a node s (here node 8 in below fig) has packets to be sent to a destn node d (node 15 in fig), it checks whether node d is within its zone.

→ If the destn belongs to its own zone, then it delivers the packets directly. Otherwise, node 8 bordercasts the RouteRequest to its peripheral nodes in fig, node 8 bordercasts ~~RouteReply~~ RouteRequests to node 2, 3, 5, 7, 9, 10, 13, 14, & 15)

→ If any peripheral node finds node d to be located within its routing zone, it sends a

otherwise, the node reborder casts the RouteRequest packet to the peripheral nodes.

→ This process continues until node 'd' is located.

* Advantages:

→ Reduces control overhead by combining the best features of proactive & Reactive protocols.

* Disadvantages:

→ control overhead may increase due to the large overlapping of nodes' routing zones.

Zone Based Hierarchical link State Routing protocol (ZHLS)

* ZHLS uses the geographical location info. of the nodes to form non-overlapping zones. A Hierarchical addressing that consists of a zone ID and a node ID is employed.
* Similar to ZRP, ZHLS also employs a proactive approach inside the geographical zone and a reactive approach behind the zone.
* Every node requires GPS support for obtaining its own geographical ~~suppor~~ location that is used to map itself into the corresponding zone.

* the assignment of zone addresses to geographical areas is important and is done during a phase called the n/w design phase or n/w deployment phase.

* Each node maintains two link state packets: (LSP)
  → node level LSP: list of connected neighbours
  → zone LSP: list of connected zones.

* Route Establishment:

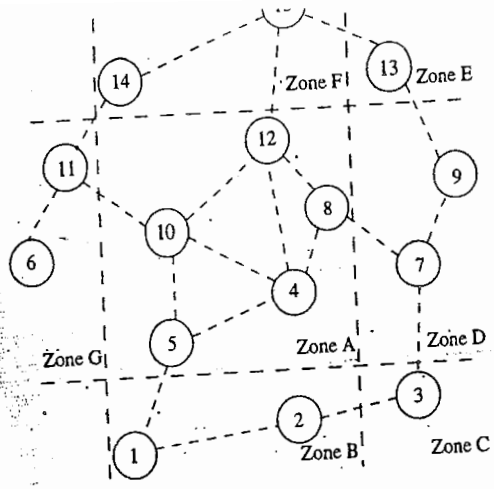
→ If a source node src wants to communicate with a destination node dest, Src checks whether Dest resides in its own zone.

→ If Dest belongs to same zone, then packets are delivered to Dest as per the intra zone routing table

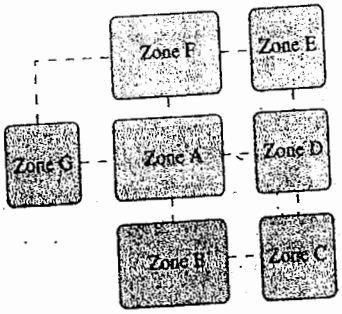
→ If Dest does not belong to the zone, then the src originates a location request packet containing the sender's & destination's information. This location info is forwarded to every other zone.

→ The gateway node of a zone at which the location request packet is received verifies its routing table for the destination node.

→ The gateway node that finds the destination node required by a location request packet originates a location response packet containing the zone information to the sender.



(a) Node–level topology in ZHLS



(b) Zone topology for the node–level topology in (a)

Table 7.1. Zone link state packets

Source Zone	Zone Link State Packet
A	B, D, F, and G
B	C and A
C	B and D
D	A, C, and E
E	A, D, and F
F	A, E, and G
G	A and F

* Route maintainence

→ If a given gateway node moves away, causing a zonelevel connection failure, routing can still take place with the help of the other gateway nodes.

→ This is due to the hierarchical addressing that makes use of zone ID & node ID.

* Advantages:

→ Reduces storage requirements & commⁿ overhead

→ Robust & resilient to path breaks.

→ non overlapping zones.

* Disadvantages:

→ Additional overhead incurred in creation of zonelevel topology.

→ path to dstn is suboptimal

→ Geographical info. may not be available in all environments

ROUTING PROTOCOLS WITH EFFICIENT FLOODING MECHANISMS

* Many protocols flood the network with RouteRequest packets in order to obtain a path to the destination.
* Flooding of control packets results in
  → wastage of band width
  → Increase in number of collisions.
* protocols with efficient flooding mechanisms:
  1. Preferred link-based routing (PLBR) protocols
  2. Optimized link state routing (OLSR) protocols.

Preferred Link Based Routing (PLBR) protocols

* uses the preferred link approach in an implicit manner by processing a RouteRequest packet only if it is received through a strong link.
* Here a node selects a subset of nodes from its neighbors List (NL). This subset is referred to as the preferred list (PL) Selection of this subset may be based on link or node characteristics.

* All neighbors ~~copy~~ receive RouteRequest packets because of the broadcast radio channel, but only neighbors present in the PL forward them further.
* Each node maintains information about its neighbors and their neighbors in a table called Neighbor's neighbor table (NNT)
It periodically transmits a beacon containing the changed neighbor's information
* PLBR has three main phases:
  → Route Establishment
  → Route Selection.
  → Route Maintainence.

1. Route Establishment

→ If Dest is in Src's NNT, the route is established directly.
otherwise, Src transmits a RouteRequest packet containing
  - Source node's address (SrcID)
  - Destn node's address (DestID)
  - unique sequence no (SeqNum)
  - Traversed path (TP)
  - PL
  - TTL flag
  - NoDelay flag.

→ A node is eligible for forwarding a RouteRequest only if it satisfies the following criteria:

- The node ID must be present in the received RouteRequest packet's PL.
- RouteRequest packet must not have been already forwarded by the node, and the TTL on the packet must be greater than zero

→ If the Dest is in the eligible nodes' NNT, the RouteRequest is forwarded as a unicast packet to the neighbor.

→ If the computed PLT is empty, the RouteRequest packet is discarded and marked as sent.

→ If the RouteRequest reaches the destn, the route is selected by the route selection procedur given below.

2. Route Selection:

→ When multiple RouteRequest packets reach Dest, the route selection procedure selects the best route among them.

→ The criterion for selecting the best route can be the shortest path, or the least delay path, or the most stable path.

→ Dest starts a timer after receiving the first RouteRequest packet. The timer expires after a certain RouteSelectWait period, after which no more RouteRequest packets would be accepted.

→ From the received RouteRequest packets, a route is selected as follows:

- For every routeRequest i that reached Dest during the RouteSelectWait period, $Max(W^i_{min})$ is selected, where W^i_{min} is the min. weight of the link in the path followed by i.
  If two or more paths have the same value for $max(W^i_{min})$, the shortest path is selected.
- After selecting a route, all subsequent RouteRequest packets from the same src with a SeqNum less than or equal to the SeqNum of the selected RouteRequest are discarded.
- If the NoDelay flag is set, the route selection procedure is ommitted & TP of the first RouteRequest reaching the Dest is selected as the route.
  (done if fast connection setup is needed)

Algorithms for preferred Links computation,

1. Neighbor-Degree-Based preferred Link Algorithm (NDPL)
2. Weight Based preferred link Algorithm (WBPL)

NDPL

Let d → node that calculates the preferred list table PLT.

TP → Traversed path

$OLDPL_L$ → prefered list of the received RouteRequest packet.

NNT_d → NNT of node d.

N(i) → neighbors of node i and itself

INL → Include list, a set containing all reachable ~~node~~ neighbors by transmitting the RouteRequest packet.

EXL → Exclude list, a set containing all neighbors that are unreachable by transmitting the RouteRequest packet after execution of the algorithm

Step 1: Node 'd' marks the nodes that are not eligible for further forwarding the RouteRequest packet.

(a) If a node i of TP is a neighbor of node d mark all neighbors of i as reachable. ie add N(i) to INL.

(b) If a node i of $OLDPL_L$ is a neighbor of node d and i<d, then include N(i) in INL.

(c) If neighbor i of node d has a neighbor 'n' present in TP, add N(i) to INL.

(d) If neighbor i of node d has a neighbor 'n' present in $OLDPL_L$ & n<d, add N(i) to INL.

Step 2:
If neighbor i of node d is not in INL, put i in PLT and mark all neighbors of i as reachable.
If i is present in INL, mark the neighbors of i as unreachable by adding them to EXL.

Step 3:
If neighbor i of 'd' has a neighbor 'n' present in EXL, put i in PLT and mark all neighbors of i as reachable. Delete all neighbors of i from EXL.

Step 4:
Reduction steps are applied here in order to remove overlapping neighbors from PLT without compromizing on reachability.

(a) Remove each neighbor ~~of~~ i from PLT if N(i) is covered by remaining neighbors of PLT. Here the minimum degree neighbor is selected every time

(b) Remove neighbor i from PLT whose N(i) is covered by node d itself.

Weight-Based Preferred Link Algorithm.

* Here node finds the preferred links based on stability (weight).

step 1: Weight given to i based on time stability (WT^i_{time}) is

$$WT_{time} = \begin{cases} 1 & \text{if } BCnti > TH_{Bcon} \\ \dfrac{BCnti}{THbcon} & \text{otherwise} \end{cases}$$

where $BCnti_i$ → count of beacons received from a neighbor i.

TH_{bcon} → no. of beacons generated during a time period equal to that required to cover twice the transmission range

$$TH_{bcon} = \frac{2 \times \text{TransmissionRange}}{\text{max. Velocity} \times \text{period of beacon}}$$

step 2: Estimate the distance (D^i_{Est}) to i from the received power of the last few packets using appropriate propagation models.

The weight based on spatial stability is

$$WT^i_{spatial} = \frac{R - D_{Est}}{R}$$

step 3: The weight assigned to the link i is the combined weight given to time stability and spatial stability

$$W_i = WT^i_{time} + WT^i_{spatial}$$

Step 4: Arrange the neighbors in non-increasing order of their weights. The nodes are put into PLT in this order.

Step 5: If a link is overloaded, delete the associated neighbor from PLT. Execute Step 1 of NDPL & delete $\forall i, i \in PLT \cap i \in INL$. Also delete those neighbors from PLT that satisfy step 4 of NDPL.

* Advantages:
  - → minimizes broadcast storm problem. Hence highly scalable
  - → Reduction in control overhead results in a decrease in the no. of collisions & improvement in efficiency of the protocol.
* Disadvantages:
  - → Computationally more complex.

Optimized Link State Routing (OLSR)

* It is a proactive routing protocol that employs an efficient link state packet forwarding mechanism called multipoint Relaying (MPR)
* This protocol optimizes the pure link state routing protocol.

* optimizations are done in two ways:
1. By reducing the size of control packets
2. By reducing the no. of links that are used for forwarding the link state packets.

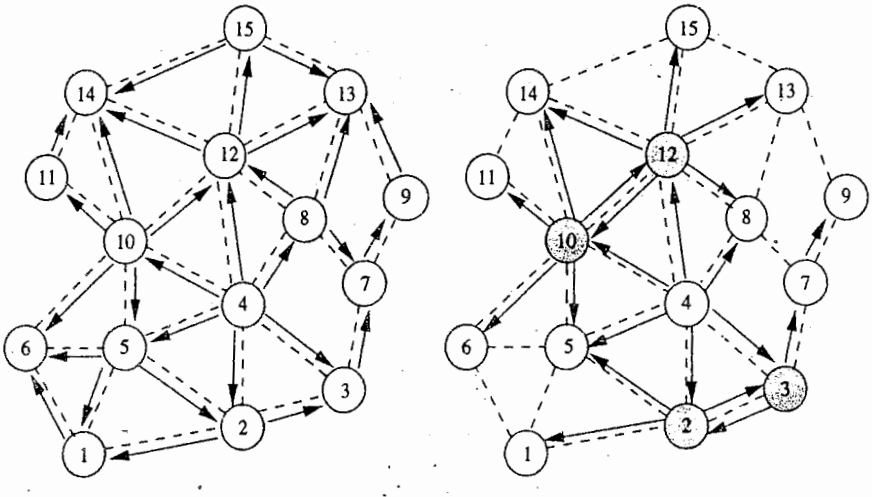
* The subset of links or neighbors that are designated for link state updates and are assigned the responsibility of packet forwarding are called multipoint relays

* The set consisting of nodes that are multipoint relays is referred to as MPR set Each node (say, P) in the n/w selects an MPRset that processes & forwards every link state packet that node P originates. The neighbor nodes that do not belong to the MPRset process the link state packets originated by node P but do not forward them.

* Similarly, each node maintains a subset of neighbors called MPR selectors, which is nothing but the set of neighbors that have selected the node as a multipoint relay.

* In order to decide on the membership of the nodes in the MPRset, a node periodically sends Hello messages that contain
  - → list of neighbors with which the node has bidirectional links
  - → list of neighbors whose transmissions were received in the recent past but with whom bidirectional links have not yet been confirmed.

* The ~~selection of~~ nodes that receive this Hello packet update their own two-hop topology tables.
  The selection of multipoint relays is also indicated in the Hello packet.
* The Data structure called neighbor table is used to store the list of neighbors, the two-hop neighbors, and the status of neighbor nodes.
* The neighbor nodes can be in one of the three possible link status states, ie
  → unidirectional
  → Bidirectional
  → multipoint relay.



Node 4 selects MPRset <2, 3, 10, 12>

Network Link

Node belonging to MPRset of Node 4

Broadcast packets forwarded by members of MPRset

(a) Flooding the network takes as many transmissions as the number of nodes

(b) Flooding the entire network with six transmissions using MPR scheme

Selection of Multipoint Relay Nodes. (refer fig b)

$N_i(x)$ → i^{th} hop neighbor set of node x

$MPR(x)$ → MPRset of node x.

Step 1: $MPR(x) \leftarrow \phi$ /* initializing empty MPRset */

Step 2: $MPR(x) \leftarrow$ { those nodes that belong to $N_1(x)$ and which are the only neighbors of nodes in $N_2(x)$ }

Step 3: While there exists some node in $N_2(x)$ which is not covered by $MPR(x)$

(a) For each node in $N_1(x)$, which is not in $MPR(x)$, compute the maximum number of nodes that it covers among the uncovered nodes in the set $N_2(x)$.

(b) Add to $MPR(x)$ the node belonging to $N_1(x)$ for which this number is maximum.

* Advantages:

→ Reduces the routing overhead

→ Reduces the no. of broadcasts done.

Hence low connection ~~step~~ setup time and reduced control overhead.

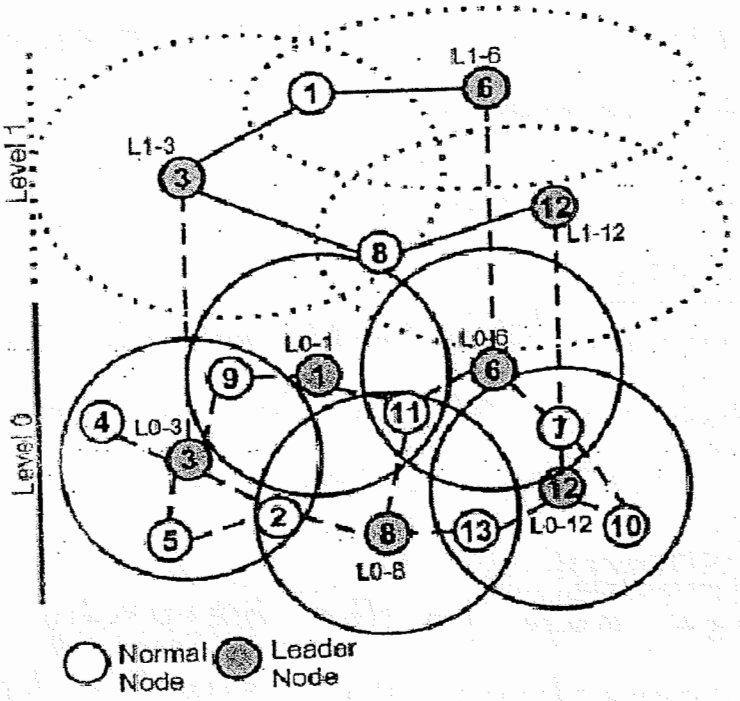
HIERARCHICAL ROUTING PROTOCOLS

* the use of routing hierarchy has several advantages
  → reduction in size of routing tables and better scalability.
* We discuss two routing protocols here
  1. Hierarchical State Routing (HSR) protocol
  2. Fisheye State Routing protocol.

Hierarchical State Routing (HSR) protocol.

* It is a distributed multi-level hierarchical routing protocol that employs clustering at different levels with efficient membership management at every level of clustering.
* Each cluster has its leader.
* clustering is organized in levels:
  → physical: between nodes that have physical wireless one-hop links b/w them.
  → logical: based on certain relations.

* Fig shows an ex for multilevel clustering



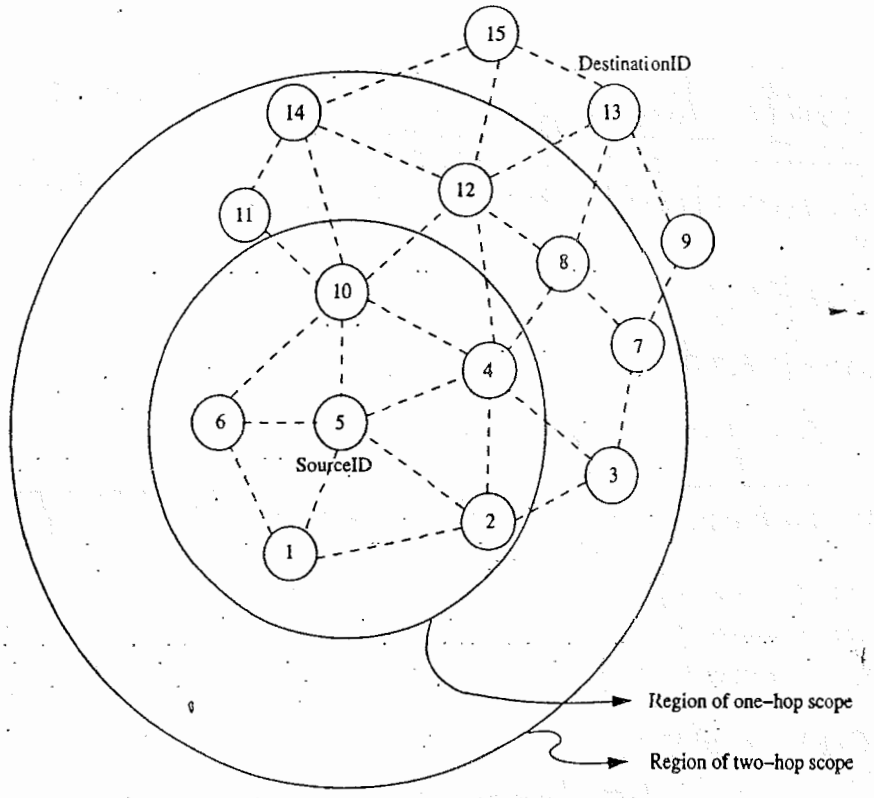
* Node 8 is described as L0 - 8
  → its node ID = 8
  → It leads a cluster at level zero.
  Node 3 is described as L1 - 3
  → Its node ID = 3
  → It leads a cluster at first ~~zero~~ level.
* The path between two cluster leaders is called <u>virtual link</u>
* The path b/w L1 - 3 L1 - 2 is :
  (3 - 2 - 8 - 13 - 12) → hierarchical ID.
* HSR address is <HID - nodeID>
  HSR address of node 10 is :
  <12, 12 - 10>

* Every node maintains information about its peers' topology and the status of links to them. This info. is broadcast to all the members of the cluster periodically.
* cluster leaders exchange similar info with their peers.
Each cluster leader broadcasts the info to the lower level informing all the nodes about the hierarchical topology of the n/w.
* Route Establishment
→ Go to highest node in the hierarchy
→ Establish connections on virtual links.
→ Send data thru' channel.

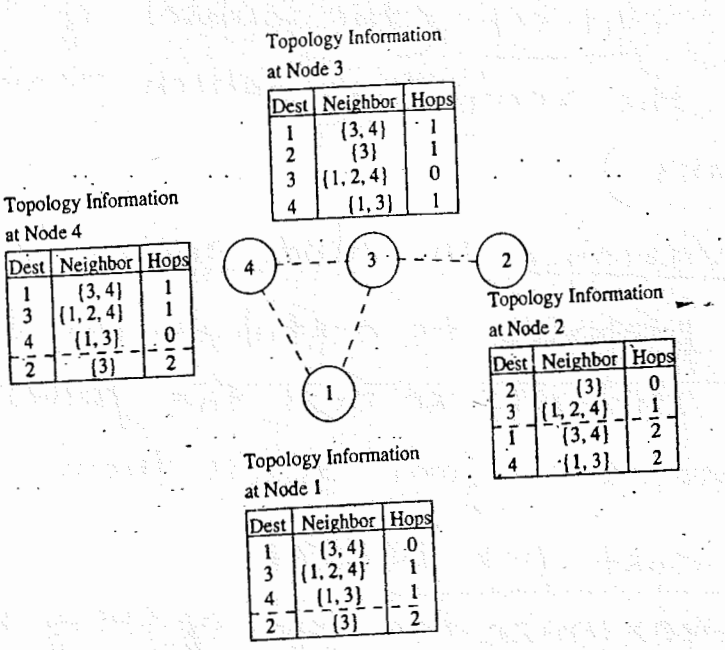
* Advantages:
→ Reduces routing table size. Storage required is $O(n \times m)$. for flat topology, it is $O(n^m)$.
n → ave no. of nodes.
m → no. of levels.
* Disadvantages:
→ ~~problem of~~ process of exchanging information concerned all the levels of the hierarchy as well as the process of leader election in every cluster makes it quite problematic for adhoc n/ws.

Fish Eye State Routing protocol (FSR)

* It is a generalization of the GSR protocol.
* It uses Fisheye technique to reduce the routing overhead.
* principle: A fish eye has the ability to see object the better when they are nearer to its focal point That means that:
  Each node maintains accurate information about near nodes
* nodes exchange topology information only with their neighbors.
* FSR defines routing scope, which is the set of nodes that are reachable in a specific no. of hops.
  The scope of a node at two hops is the set of nodes that can be reached in two hops.
  fig below shows scope of node 5 with one hop and two hops.



* the link state info. for the nodes belonging to the smallest scope is exchanged at the highest frequency. Frequency of exchanges decreases with an increase in scope.
* Fig below illustrates an ex. depicting the n/w topology information maintained at nodes in a n/w.
info. regarding nodes that are more than one hop away from the current node are listed below the dotted line in the topology table.



* Advantages:
→ Reduces bandwidth consumption by link state update packets.
→ Suitable for large & highly mobile ad hoc wireless n/w.

* Disadvantages:
→ Very poor performance in small ad hoc n/ws

POWER AWARE ROUTING PROTOCOLS

Power Aware Routing metrics.

1. minimal Energy Consumption per packet
→ This metric aims at minimizing the power consumed by a packet in traversing from source node to the dest node.

2. Maximize network connectivity

→ This metric attempts to balance the routing load among the cut set (the subset of the nodes in the n/w, the removal of which results in n/w partitions)

3. Maximum Variance in Node power levels

→ This metric proposes to distribute the load among all nodes in the n/w so that the power consumption pattern remains uniform across them.

4. Minimum cost per packet.

→ In order to maximize the life of every node in the n/w, this routing metric is made as a function of the state of the node's battery.

→ A node's cost decreases with an increase in its battery change & vice versa.

5. Minimize maximum node cost.

→ This metric minimizes the maximum cost per node for a packet after routing a no. of packets or after a specific period.

UNIT 7: TRANSPORT LAYER

Syllabus

* Introduction
* Issues in designing a transport layer protocol for Adhoc wireless n/w
* Design goals of a transport layer protocol for Adhoc wireless n/w.
* classification of Transport layer solutions
* TCP over Adhoc wireless n/w s.
* other transport layer protocols for Adhoc wireless n/w.

– 7 Hours.

INTRODUCTION.

* The objectives of transport layer protocol include the setting up of an end-to-end connection, end-to-end delivery of data packets, flow control, and congestion control.

ISSUES IN DESIGNING A TRANSPORT LAYER PROTOCOL FOR AD HOC WIRELESS NETWORKS

1. Induced Traffic:

* Induced Traffic affects the throughput achieved by the transport layer protocol.
* The traffic at any given link (or path) due to the traffic through neighbouring links (or paths) is referred to as induced traffic.

2. Induced throughput unfairness:

* This refers to the throughput unfairness at the transport layer due to the throughput/delay unfairness existing at the lower layers such as the n/w and MAC layers.

3. Separation of congestion control, reliability, and flow control.

* A TL protocol can provide better performance if end to end reliability, flow control, & congestion control are handled separately.

4. Power and Bandwidth constraints:

* The performance of a TL protocol is significantly affected by these resource constraints.

5. Misinterpretation of congestion:

* Interpretation of network congestion as used in traditional n/ws is not appropriate in ad hoc wireless n/ws.

6. Completely decoupled transport layer:

* Another challenge faced by TL protocol is the interaction with the lower layers.

7. Dynamic topology:

* performance is affected by rapid changes in n/w topology.

DESIGN GOALS OF A TRANSPORT LAYER PROTOCOL FOR AD HOC WIRELESS NETWORKS.

1. The protocol should maximize the throughput per connection.
2. It should provide throughput fairness across contending flows.
3. It should incur min. connection set up and connection maintainence overheads.
4. It should have mechanisms for congestion control and flow control in the n/w

5. It should be able to provide both reliable and unreliable connections as per the requirements of the application layer.

6. It should be able to adapt to the dynamics of the n/w.

7. Bandwidth must be used efficiently.

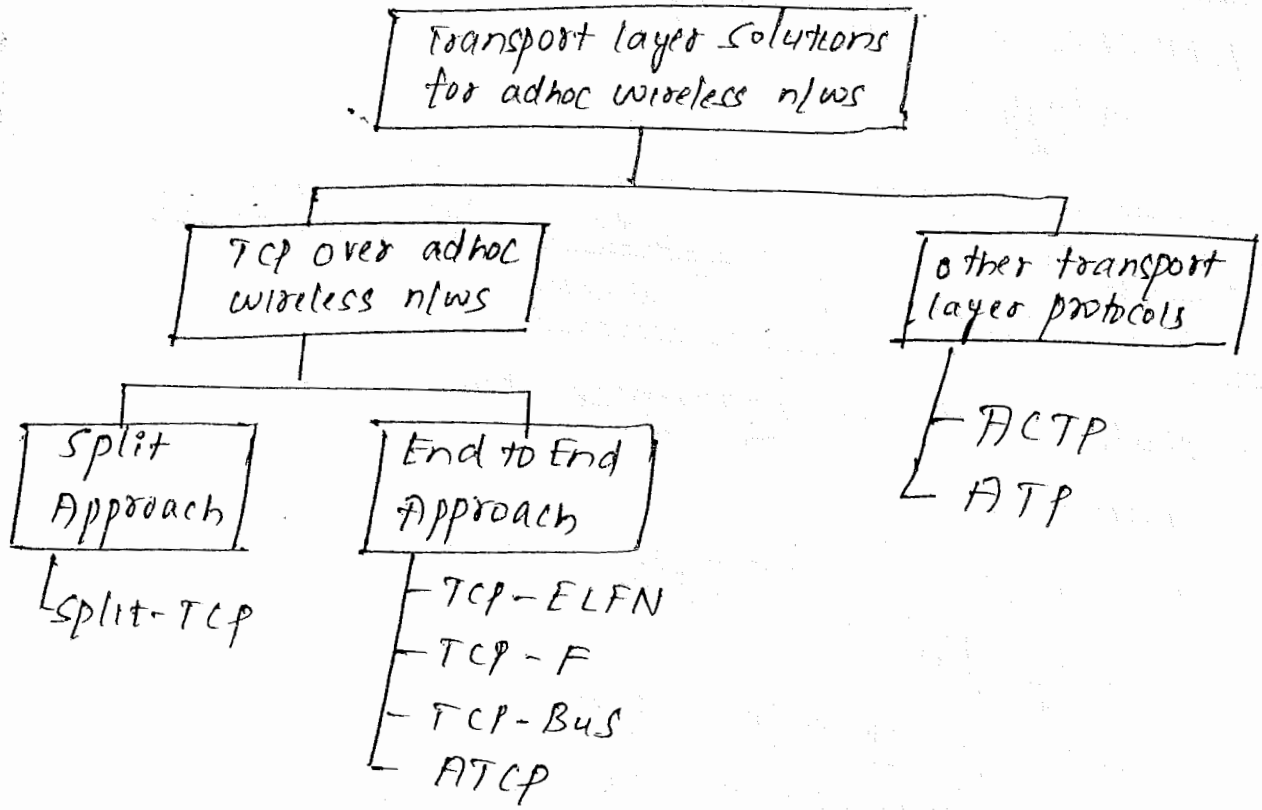
8. It should be aware of resource constraints

9. It should make use of information from the lower layers.

10. It should have a well-defined cross-layer interaction framework.

11. It should maintain end-to-end semantics.

CLASSIFICATION OF TRANSPORT LAYER SOLUTIONS.



TCP OVER ADHOC WIRELESS NETWORKS

* TCP is a reliable, end-to-end, connection-oriented TL protocol that provides a byte stream based service.

* major responsibilities of TCP include
  - Congestion control
  - Flow control
  - In-order delivery of packets
  - reliable transportation of packets.

Why does TCP not Perform well in Adhoc wireless network?

~~1. misinterpretation of packet loss~~:

The major reasons behind throughput degradation that TCP faces when used in ad hoc wireless n/ws are the following.

1. Misinterpretation of packet loss:

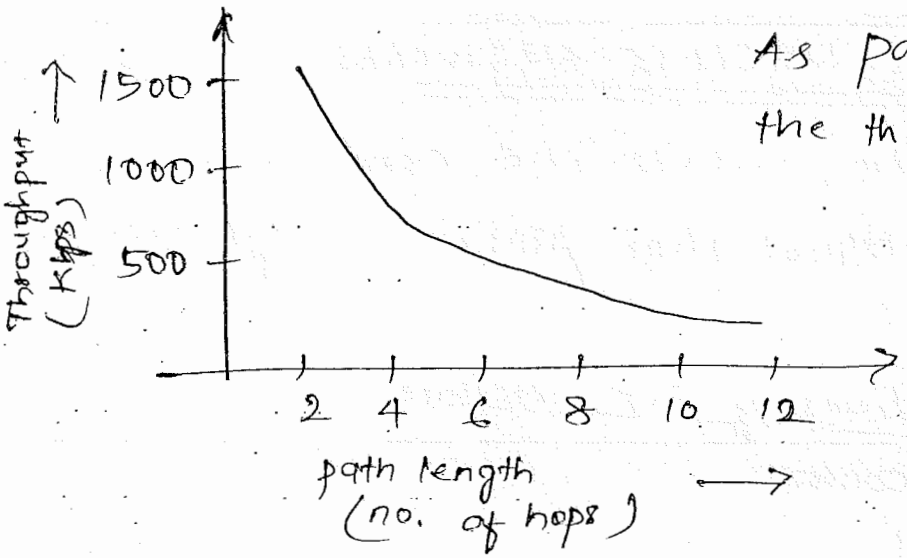
* In traditional TCP design, the packet loss is mainly attributed to network congestion.

Adhoc wireless n/ws experience a much higher packet loss due to
- high bit rate
- increased collisions etc

2. Frequent path breaks:

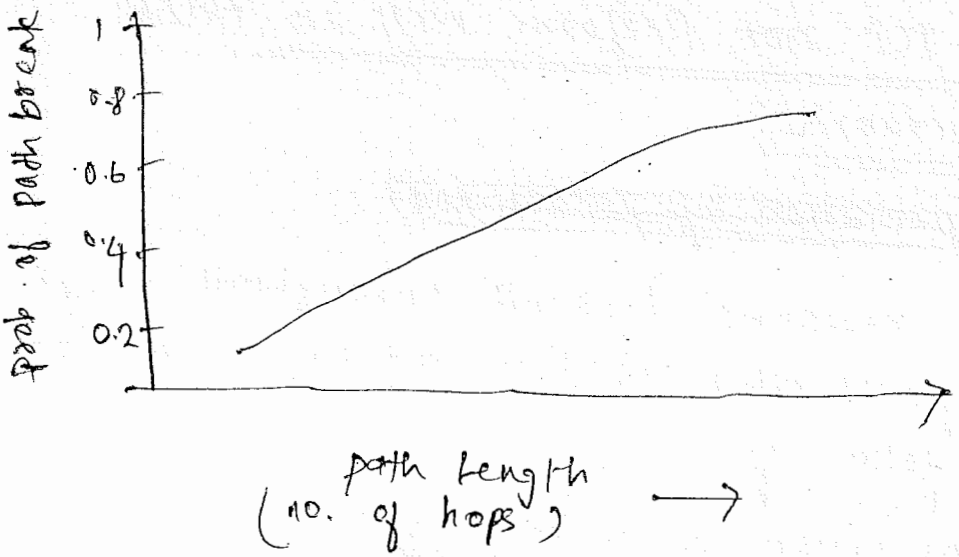
* If the route re establishment time is greater than the RTO period of TCP sender, then the TCP sender assumes congestion in the n/w, retransmits lost packets, & initiates congestion control algorithm. This leads to wastage of

3. Effect of path length:



As path length increases, the throughput decreases.

4. ~~Misinterpretation of congestion window~~



4. Misinterpretation of congestion window.

* when these are frequent path breaks, the congestion window may not reflect the maximum transmission rate acceptable to the n/w and the receiver.

5. Assymmetric link behavior:

* Radio channel used in ad hoc wireless n/w has different properties such as location dependent contention, directional properties etc leading to asymmetric links.
* This can lead to TCP invoking the congestion control algorithm and several retransmissions.

6. Uni directional path

* TCP relies on end-to-end ACK for ensuring reliability. Path break on an entirely different reverse path can affect the performance of the n/w as much as a path break in the forward path.

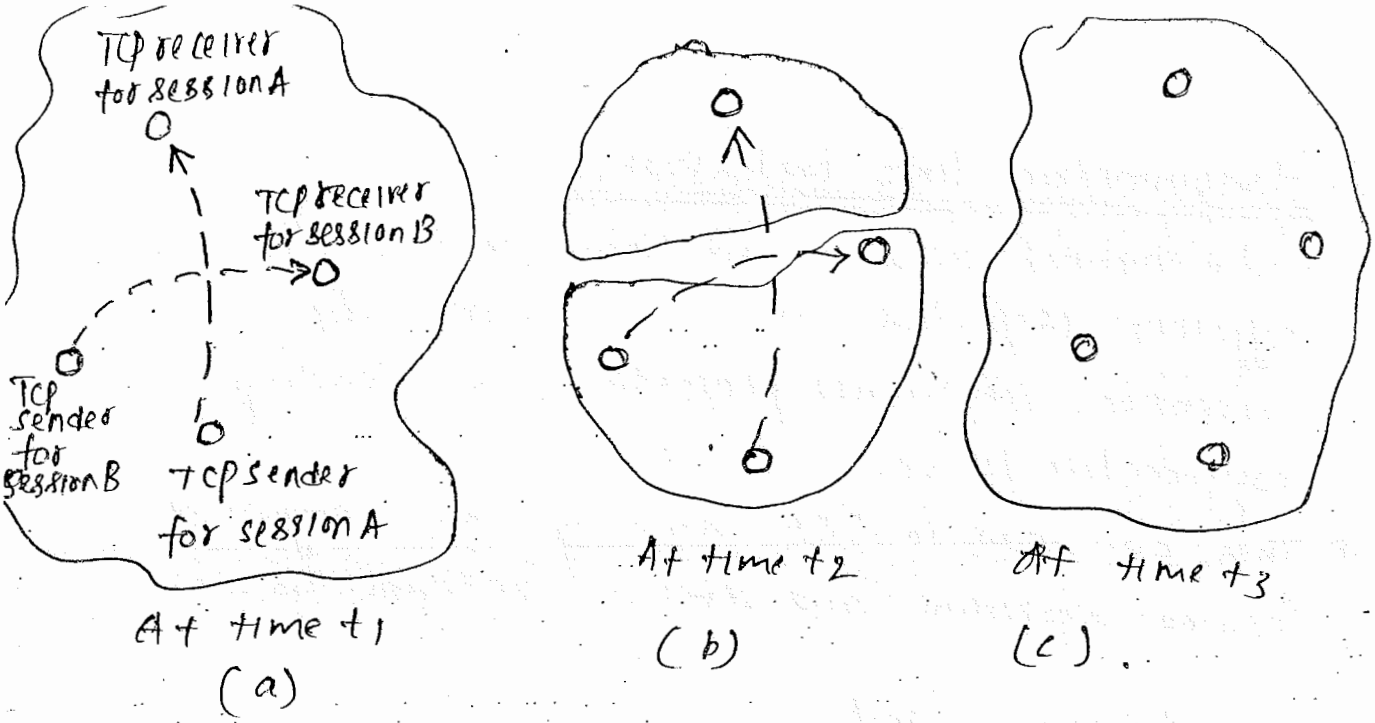
7. Multipath Routing:

* For TCP, multipath routing leads to significant amount of out of order packets, which inturn generates a set of duplicate acknowledgement (DUPACKs), which cause additional power consumption and invocation of congestion control.

8. Network partitioning and Remerging:

* Fig below illustrates the effect of n/w partitions in ad hoc wireless n/ws.
* A n/w with two TCP sessions A & B is shown in (a) at time t1.
* At time t2, the n/w gets partitioned into two as shown in (b) due to dynamic topological changes.

now TCP session A's sender & receiver belong to two diff. partitions & TCP session B experiences path break.



Q. The use of sliding window based Transmission!

* TCP uses a sliding window for flow control. This can contribute to degraded performance in bandwidth constrained ad hoc wireless n/w. It can also lead to burstiness in traffic due to the subsequent transmission of TCP segments.

Feed Back Based TCP (TCP-F)

* improves performance of TCP
* used a feedback based approach.
* the routing protocol is expected to repair the broken path within a reasonable time period.
* operation:

→ In TCP-F, an intermediate node, upon detection of a path break, originates route failure notification (RFN) packet. This intermediate node is called Failure point (FP)

→ This RFN packet is routed toward the sender of the TCP session. sender info. is obtained from TCP packets.

→ if any intermediate nodes that receive RFN has an alternate route to the same destn, then it discards the RFN packet and uses the alternate path for forwarding further data packets, thus reducing control overhead involved in the route reconfiguration process.

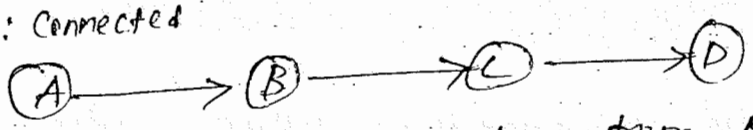
→ when TCP sender receives an RFN packet, it goes into a state called snooze. In this state, a sender
- stops sending any more packets to the destn.
- cancels all timers.
- Freezes its congestion window
- freezes the retransmission timer
- sets up a route failure timer.

→ when route failure timer expires, the TCP sender changes from snooze state to connected state.

→ when the route reestablishment has been done, then the Failure point sends Route reestablishment notification (RRN) packet to the sender and the TCP state is updated back to the connected state

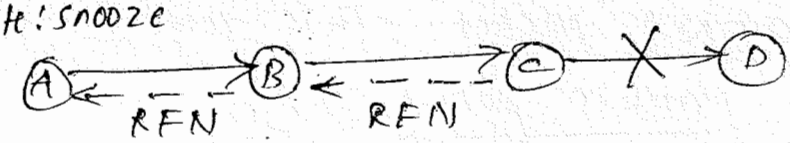
Example:

TCP state: Connected



(a) TCP-F connection from A to D

TCP state: snooze



(b) Link C-D breaks & C originates RFN

TCP state: connected

(c) link C-D rejoins and C originates RRN.

* Advantages

→ simple feed back soln for problems arising from path breaks.

→ permits TCP congestion control mechanism to respond to congestion in the n/w.

Disadvantages

~~→ finding sender is quite difficult.~~

→ If a route to sender is not available at the FP, then additional control packets may need to be generated for routing RFN packets.

→ TCP-F has an additional state compared to tradition TCP state m/c.

→ congestion window used after a new route is obtained may not reflect the achievable transmission rate acceptable to the n/w and the TCP-F receiver.

TCP with Explicit Link Failure Notification (TCP-ELFN)

* improves TCP performance in ad hoc wireless n/w.
* similar to TCP-F
* operation
  → ELFN is originated by the node detecting a path breaks upon detection of a link failure to the TCP sender.
  → This can be implemented in two ways
    i.) by sending an ICMP destination unreachable (DUR) message to the sender.
    (or)
    ii.) By piggy-backing this information to the RouteError message that is sent to the sender
  → once the TCP sender receives the ELFN packet, it disables its retransmission timers and enters a standby state
  → In this state, it periodically originates probe packets to see if a new route is established.
  → upon reception of an ACK by the TCP receiver for the probe packets, it leaves the standby state, and continues to function as normal.

* Advantages
  → improves TCP performance by decoupling the path break info. from the congestion info. by the use of ELFN
  → less dependent on routing protocol & requires only link failure notification about the path break.

* Disadvantages:

→ when the n/w is temporarily partitioned, the path failure may last longer & this can lead to the origination of periodic probe packets consuming bandwidth & power.

→ Congestion window used after a new route is obtained may not reflect the achievable transmission rate acceptable to the network and the TCP receiver.

TCP-BuS (TCP with Buffering capability and sequence information)

* It is similar to TCP-F and TCP-ELFN in its use of feedback info from an intermediate node on detection of a path break. But it is more dependent on the routing protocol.

* TCP-BuS was proposed, with Associativity-based Routing (ABR) protocol as the routing scheme. Hence it makes use of some special messages such as LQ and REPLY for finding partial path.

* operation:

→ upon detection of a path break, an upstream intermediate node, called pivot node (PN), originates an explicit route disconnection notification (ERDN) message to the TCP-BuS sender.

↳ propagated in a reliable way

→ Upon receiving ERDN packet, the TCP-Bus sender stops transmission and freezes all timers and windows as in TCP-F.

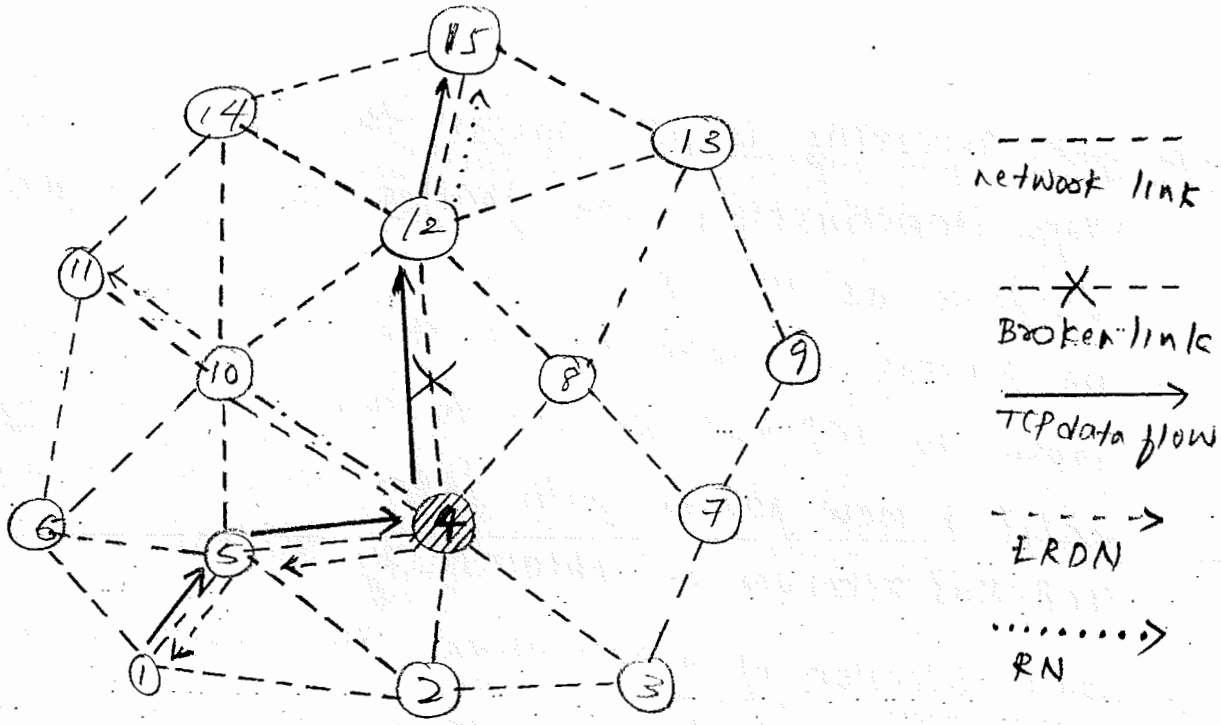
→ The packets in transit at the intermediate nodes from the TCP-Bus sender to the PN are buffered until a new partial path from the PN to the TCP-Bus receiver is obtained by the PN.

→ Upon detection of a path break, the downstream node originates a Route Notification (RN) packet to the TCP-Bus receiver, which is forwarded by all the downstream nodes in the path.

→ PN attempts to find new partial path (route) to the TCP-Bus receiver, and the availability of such a partial path to destination is intimated to the TCP-Bus sender through an explicit route successful notification (ERSN) packet.
TCP utilizes route reconfiguration mechanism of ABR to obtain partial path to the destn.

→ Upon a successful LQ-REPLY process to obtain a new route to the TCP-Bus receiver, PN informs the TCP-Bus sender of the new partial path using ERSN packet. (It is sent reliably)
TCP-Bus sender also periodically originates probe packets to check the availability of a path to the destn.

* Below fig illustrates the operation of TCP-Bus.



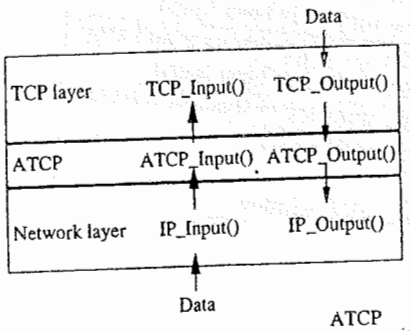
* Advantages:
→ performance improvement
→ Avoidance of fast retransmission due to the use of buffering, sequence numbering, and selective acknowledgement.
→ Also takes advantage of the underlying routing protocols.

* Disadvantages.
→ Increased dependency on the routing protocol and the buffering at the intermediate nodes.
→ The failure of intermediate nodes that buffer the packets may lead to loss of packets and performance degradation.
→ The dependency on the routing protocol may degrade its performance with other routing protocols that do not have similar control messages as in ABR.

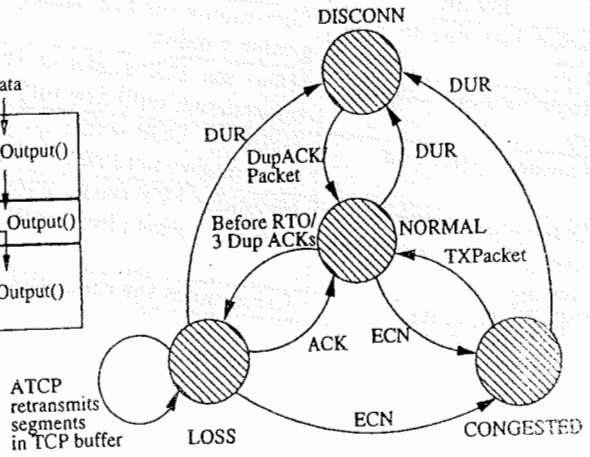
Ad Hoc TCP.

* Based on feedback information received from the intermediate nodes, the TCP sender changes its state to the
  - → persist state
  - → congestion control state, or
  - → Retransmission state.
* when an intermediate node finds that the n/w is partitioned, then the TCP sender state is changed to the persist state where it avoids unnecessary retransmissions.
* Fig shows the thin layer implementation of ATCP between the ~~transmiss~~ traditional TCP layer and the IP layer. This does not require changes in the existing TCP protocol.
  This layer is active only at the TCP sender.

~~* The main~~



(a) ATCP thin layer implementation



(b) State transition diagram for the ATCP sender

TCP sender in persist state

DUR – Receive destination unreachable

TXPacket – TCP transmits a packet

major function of the ATCP is to monitor the

→ packets sent and received by TCP sender,
→ the state of TCP sender.
→ state of the network.

fig (b) shows the state transmission diagram for the ATCP at the TCP sendor.

The four states in the ATCP are

1. NORMAL
2. CONGESTED
3. LOSS
4. DISCONN

when a TCP connection is established, the ATCP sender state is in NORMAL, here ATCP does not interfere with the operation of TCP and it remains invisible.

ATCP tries to perform the activities listed below:

Event	Action
Packet loss due to high BER	Retransmits the lost packets without reducing congestion window
Route recomputation delay	Makes the TCP sender go to persist state and stop transmission until new route has been found
Transient partitions	Makes the TCP sender go to persist state and stop transmission until new route has been found
Out-of-order packet delivery due to multipath routing	Maintains TCP sender unaware of this and retransmits the packets from TCP buffer
Change in route	Recomputes the congestion window

* Advantages:
→ it maintains the end to end semantics of TCP.
→ It is compatible with traditional TCP.
→ improves throughput of TCP in adhoc wireless n/ws.

* Disadvantages:
→ Dependency on the n/w layer protocol to detect the route changes and partitions.
→ Addition of thin ATCP layer to TCP/IP protocol stack requires changes in the interface functions currently being used.

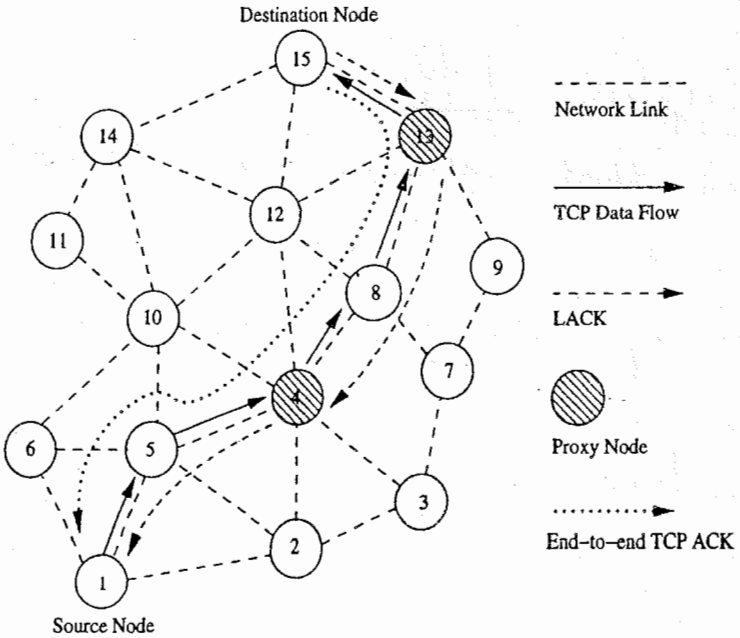
Split TCP.

* Channel capture Effect:
→ major issues that affects the performance of TCP over adhoc wireless n/w is the degradation of throughput with increasing path length,
→ This can also lead to unfairness among TCP sessions where one session may obtain much higher thru'put than other sessions.
→ This unfairness problem is further worsened by the use of MAC protocols, which are found to give a higher throughput for certain link level sessions, leading to an effect known as channel capture

* Split TCP provides a unique solution to this problem by splitting the transport layer objectives into
  → congestion control
  → End to End Reliability.

* In addition, split-TCP splits a long TCP connection into a set of short concatenated TCP connections (called segments or zones) with a no. of selected intermediate nodes (known as proxy nodes) as terminating points of these short connections.

* Fig illustrates the operation of split-TCP where a three segment split-TCP connection exists between source node 1 and destination node 15.



* A proxy node receives the TCP packets, reads its contents, stores it in its local buffer, and sends an acknowledgement to the source (or the previous proxy)
* this acknowledgement is called Local acknowledgement (LACK) does not guarantee end to end delivery.
* The responsibility of further delivery of packets is assigned to the proxy node.

* In fig, node 1 initiates a TCP session to node 15 node 4 and node 13 are choosen as proxy nodes
* The no. of proxy nodes in a TCP session is determined by the length of the path b/w source & destn node
* Based on a distributed algorithm, the intermediat nodes that receive TCP packets determine whether to act as a proxy node or just as a simple forwarding node.
* In fig, the path b/w nodes ~~4 & 13~~ is 1 and 4 is the first zone (segment), the path b/w nodes 4 to 13 is the second zone (segment), and the last zone is b/w node 13 and 15.
* The proxy node 4, upon receipt of each TCP packet from source node 1, acknowledges it with a LACK packet, & buffers the received packets. This buffered packets is forwarded to the next proxy node at a transmission rate proportiona to the arrival of LACKs from the next proxy node or

* Advantages
→ improved throughput
→ improved throughput fairness
→ lessened impact of mobility.

* Disadvantages
→ Requires modifications to TCP protocol.
→ End to End connection handling of traditional TCP is violated.
→ the failure of proxy nodes can lead to throughput degradation.

Comparision of TCP solutions for Ad Hoc Wireless networks

Issue	TCP-F	TCP-ELFN	TCP-BuS	ATCP	Split-TCP
Packet loss due to BER or collision	Same as TCP	Same as TCP	Same as TCP	Retransmits the lost packets without invoking congestion control	Same as TCP
Path breaks	RFN is sent to the TCP sender and state changes to snooze	ELFN is sent to the TCP sender and state changes to standby	ERDN is sent to the TCP sender, state changes to snooze, ICMP DUR is sent to the TCP sender, and ATCP puts TCP into persist state	Same as TCP	Same as TCP
Out-of-order packets	Same as TCP	Same as TCP	Out-of-order packets reached after a path recovery are handled	ATCP reorders packets and hence TCP avoids sending duplicates	Same as TCP
Congestion	Same as TCP	Same as TCP	Explicit messages such as ICMP source quench are used	ECN is used to notify TCP sender. Congestion control is same as TCP	Since connection is split, the congestion control is handled within a zone by proxy nodes
Congestion window after path reestablishment	Same as before the path break	Same as before the path break	Same as before the path break	Recomputed for new route	Proxy nodes maintain congestion window and handle congestion
Explicit path break notification	Yes	Yes	Yes	Yes	No
Explicit path reestablishment notification	Yes	No	Yes	No	No
Dependency on routing protocol	Yes	Yes	Yes	Yes	No
End-to-end semantics	Yes	Yes	Yes	Yes	No
Packets buffered at intermediate nodes	No	No	Yes	No	Yes

Topic left:
other TL protocols for
Adhoc wireless n/w

Syllabus

* Network security requirements
* Issues & challenges in security provisioning.
* Network Security Attacks.
* Key management
* Secure routing in Ad Hoc wireless networks.

NETWORK SECURITY REQUIREMENTS

A security protocol for adhoc wireless networks should satisfy the following requirements.

1. Confidentiality

- The data sent by the sender must be comprehensible only to the intended receiver.
- Though an intruder might get hold of the data being sent, he/she must not be able to derive any useful information out of the data.
- One of the popular techniques used for ensuring confidentiality is **data encryption**.

2. Integrity

- The data sent by source node should reach the destination node **without being altered**.

3. Availability

- The n/w should remain **operational** all the time.
- It must be robust enough to **tolerate link failures** & also be **capable of surviving various attacks** mounted on it.
- It should be able to provide **gauranteed services** whether an authorized user requires them.

4. **Non-repudiation**

↳ It is a mechanism to gaurantee that the sender of a msg cannot later deny having sent the msg & that the recipient cannot deny having received the message.

↳ **Digital signatures** are used for this purpose.

ISSUES & CHALLENGES IN SECURITY PROVISIONING (SLIP L^2) → Hint

Designing a foolproof security protocol for adhoc wireless is a very challenging task. The below discussed characteristics causes difficulty in providing security in adhoc wireless networks.

1. **Shared broadcast radio channel.**

↳ The radio channel used for communication in adhoc wireless networks is **broadcast in nature** & is shared by all nodes within its direct transmission range.

↳ Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network.

↳ This problem can be minimized to a certain extent by using **directional antennas.**

2. **Limited resource availability**

↳ Resources such as bandwidth, battery power, & computational power are scarce in adhoc wireless networks.

↳ Hence it is difficult to implement complex cryptography-based security mechanisms in such networks.

3. **Insecure Operational environment**

↳ The operating environments where adhoc wireless are used may **not always be secure.** One impt appl^n of such networks is in battlefields.

4. **Physical vulnerability**

↳ Nodes in these networks are usually **compact & hand-held** in nature.

↳ They could **get damaged easily** & are also **vulnerable to theft.**

5. **Lack of central authority**

↳ In wired n/w's & infrastructure-based wireless n/w's, it would be possible to monitor the traffic on the n/w through certain impt central points & implement security mechanisms at such points.

↳ Since adhoc-wireless n/w's **do not have central points**, these mechanisms cannot be applied in adhoc wireless networks.

6. **Lack of associations.**

↳ Since these n/w's are **dynamic in nature**, a node can join or leave the n/w at any point of time.

↳ If no proper authentication mechanism is used for associating nodes in a n/w, an intruder would be able to join into the n/w quite easily & carry out his/her attacks.

NETWORK SECURITY ATTACKS

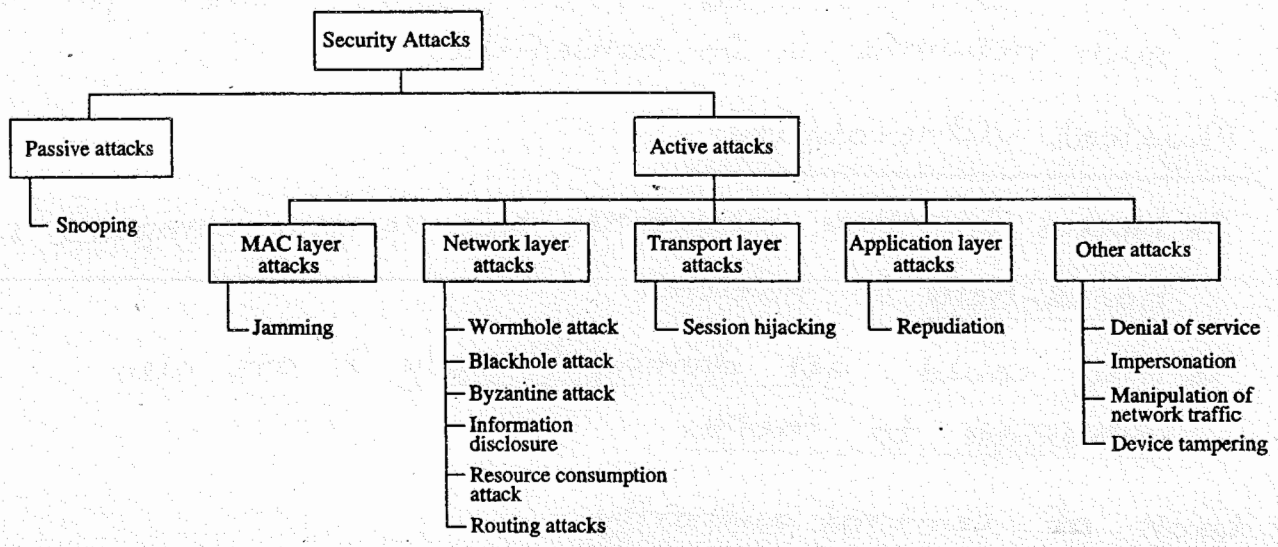


Figure Classifications of attacks.

Attacks on adhoc wireless n/w's can be classified into 2 broad categories, namely.

1. Passive Attack
   - ↳ It does not disrupt the operation of the network; the adversary snoops the data exchanged in the n/w without altering it.
   - ↳ One way to overcome such problems is to use powerful **encryption mechanisms to encrypt the data being transmitted.**

2. Active Attack.
   - ↳ An active attack attempts to **alter or destroy** the data being exchanged in the n/w, thereby disrupting the normal functioning of the n/w.
   - ↳ They can be further classified into 2 categories
     (i) ***External*** attacks which are carried out by nodes that do not belong to the network.

They can be prevented using standard encryption techniques and firewalls.

(ii) **Internal attacks** are from compromised nodes that are actually part of the network.

There are many types of active attacks which are discussed below:

NETWORK LAYER ATTACKS

There are many type of attacks pertaining to the n/w layer in n/w protocol stack. Some of them are as follows:

(i) Wormhole attack

↳ In this attack, an attacker receives pkts at one location in the n/w & tunnels them (possibly selectively) to another location in the n/w, where the pkts are resent into the n/w.

This tunnel b/w 2 colluding attackers is reffred to as a **wormhole**.

↳ If proper mechanisms are not employed to defend the n/w against wormhole attacks, existing routing protocols for adhoc wireless n/w's **may fail to find valid routes**.

(ii) Blackhole attack

↳ In this attack, a **malicious node falsely advertise good paths** to dest^n node during path-finding process. or in route update msgs.

↳ The intention of malicious node could be to **hinder the path-finding process** or to **intercept all data pkts** being sent to the dest^n node.

(iii) Byzantine attack

↳ Here, a compromised intermediate note or a set of compromised intermediate nodes work in collusion & carries out attack such as creating routing loops, routing pkts on non-optimal paths & selectively dropping pkts.

(iv) Information disclosure

↳ A compromised node may leak confidential or important information to unauthorized nodes in the network

(v) Resource consumption attack

↳ In this attack, a malicious node tries to consume/waste resources of other nodes present in the network.

↳ The resources targetted are battery power, bandwidth. & computational power, which are limitedly available in adhoc wireless networks.

(vi) Routing attacks

There are several types of attacks mounted on routing protocol & they are as follows:

a) Routing table overflow

* In this type of attack, an adversary node advertises routes to non-existent nodes, to the authorized nodes present in the n/w.
* The main objective of this attack is to cause an overflow of routing tables, which would in turn prevent the creation of entries corresponding to new routes to

b) Routing table poisioning

* Here, the compromised nodes in the n/w's send **fictitious routing updates** or **modify genuine route update pkts** sent to other uncompromised nodes.
* This may result in **sub-optimal routing**, **conjestion in n/w** or even **make some parts of n/w inaccessible**.

c) Packet replication

* In this attack, an adversary node would **replicate stale pkts.**

d) Route cache poisoning

* Similar to routing table poisioning, an adversary can also poison the route cache to achieve similar activities.

e) Rushing attack

* On-demand routing protocols that use duplicate supression during the route discovery process are vulnerable to this attack.

TRANSPORT LAYER ATTACKS

(i) Session hijacking

↳ Here, an adversary takes control over a session b/w 2 nodes.

↳ Since most authentication processes are carried out only at the start of session, once the session b/w 2 nodes get established, the adversary node masquerades as one of the end-nodes of the session & hijacks the sessions.

APPLICATION LAYER ATTACKS

(i) Repudiation

↳ It refers to the denial or attempted denial by a node.

OTHER ATTACKS

This section discusses security attacks that cannot strictly be associated with any specific layer.

Multi-layer Attacks

Multi-layer attacks are those that could occur in any layer of the n/w protocol stack. Some of the multi-layer attacks in adhoc wireless networks are

(i) Denial of Service

↳ In this type of attack, an adversary attempts to prevent legitimate & authorized users of services offered by the n/w from accessing those services.

↳ This may lead to a failure in the delivery of guaranteed services to the end users.

↳ Some of the DoS attacks are as follows:

a) Jamming
b) SYN flooding
c) Distributed DoS attack.

} Self Explanatory

(ii) Impersonation

↳ In this attacks, an adversary assumes the identity & privileges of an authorized node, either to make use of n/w resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the n/w by "injecting

↳ A **man-in-the-middle** attack is another type of impersonation attack.

(iii) **Device Tampering**

↳ Unlike nodes in a wired n/w, nodes in adhoc wireless n/w's are usually compact, soft, and hand-held in nature

↳ They could get **damaged or stolen easily**.

KEY MANAGEMENT

Having seen the various kinds of attacks possible on adhoc wireless n/w's, we now look at various techniques employed to overcome the attacks.

* **Cryptography** is one of the most common & reliable means to ensure security & can be applied to any communication network.

* In the parlance of cryptography, the original info" to be sent from one person to another is called **plaintext**. The plaintext is converted into **ciphertext** by the process of **encryption**.

* An authentic receiver can **decrypt/decode** the ciphertext back into plaintext by the process of **decryption**.

* The process of encryption and decryption are governed by **keys**, which are small amounts of info" used by the cryptographic algorithms. When the key is to be kept secret to ensure the security of the system, it is called a **secret key**.

* The secure administration of cryptographic keys is called

* The 4 main goals of cryptography are **confidentiality, integrity, authentication & non-repudiation.**

* There are 2 major kinds of cryptographic algorithms:
  (i) **Symmetric Key algorithms**, which use the same key for encryption & decryption.
  (ii) **Asymmetric Key algorithms**, which use two different keys for encryption & decryption.

* The asymmetric key algorithms are based on some mathematical principles which make it feasible or impossible to obtain one key from another; therefore, one of the keys can be made **public** while the other is kept secret (private). This is called **public key cryptography.**

SYMMETRIC KEY ALGORITHMS

* Symmetric key algorithms rely on the presence of **shared key at both the sender & receiver**, which has been exchanged by some previous arrangement.

* There are 2 kinds of symmetric key algorithms.
  - One involving **block ciphers** &
  - the **stream ciphers**.

* A *block cipher* is an encryption scheme in which plaintext is broken into fixed-length segments called **blocks**, & the blocks are encrypted one at a time.

* The simplest eg., include **substitution** & **transposition**

* In **substitution**, each alphabet of plaintext is substituted by another in the ciphertext, & this table mapping of the original & the substituted alphabet is available at both the sender & receiver.
* A **transposition cipher** permutes the alphabet in plaintext to produce the ciphertext.
* Fig (a) shows encryption using substitution & fig (b) shows a transposition cipher. The block length used is 5.

Original Alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Substitution	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
Plaintext	EVERYDAY CREATES A HISTORY EVERY DAYCR EATES AHIST ORY
Ciphertext	IZIVC HECGV IEXIW ELMWX SVC

(a)

Transposition	1 2 3 4 5 ↓ 3 5 1 4 2
Plaintext	EVERYDAY CREATES A HISTORY EVERY DAYCR EATES AHIST ORY
Ciphertext	EYERV YRDCA TSEEA ITASH YOR

(b)

Figure Substitution and transposition.

* A **stream cipher** is, in effect, a **block cipher of block length one**.
* One of the simplest stream ciphers is **Vernam cipher**, which uses a key of same length as the plaintext for encryption.

For eg.. if the plaintext is the binary string 10010100 & key is 01011001, then the encrypted string

is given by the XOR of the plaintext & Key, to be 1100 1101. The plaintext is again recovered by XOR-ing the ciphertext with the same Key.

ASYMMETRIC KEY ALGORITHMS

* Asymmetric Key (or public Key) algorithms use different Keys at the sender end & receiver ends for encryption & decryption, respectively.
* Let the encryption process be represented by a function E, & decryption by D.

  Then plaintext 'm' is transformed into the ciphertext 'c' as $c = E(m)$

  The receiver then decodes c by applying D. Hence D is such that $m = D(c) = D(E(m))$
* When this asymmetric key concept is used in public key algorithms, the Key E is made public, while D is made private, known only to the intended receiver.
* RSA algorithm is the best eg. of public key cryptography.
* Digital signatures scheme are also based on public key encryption.

KEY MANAGEMENT APPROACHES

* The primary goal of Key mgmt., is to share a secret (some information) amg a specified set of participants.
* The main approaches to Key management are **Key predistribution**, **Key transport**, **Key arbitration** and **Key agreement**.

KEY PREDISTRIBUTION

* Key predistribution, as the name suggests, involves distributing key to all interested parties before the start of communication.
* This method involves much less communication & computation, but all participats must be known a priori, during the initial configuration.
* Once deployed, there is no mechanism to include new members in the group or to change the key.
* As an improvement over predistribution scheme, sub-groups may be formed within a group, and some communication may be restricted to a subgroup. However, formation of sub-groups is also an priori decision.

KEY TRANSPORT

* In Key transport systems, one of the **communicating entities** generates Keys & transports them to the other members.

* The simplest scheme assumes that a shared key already exists among the participating members. This shared key is used to encrypt a new key & is transmitted to all corresponding nodes. Only those nodes which have the prior shared key can decrypt it.

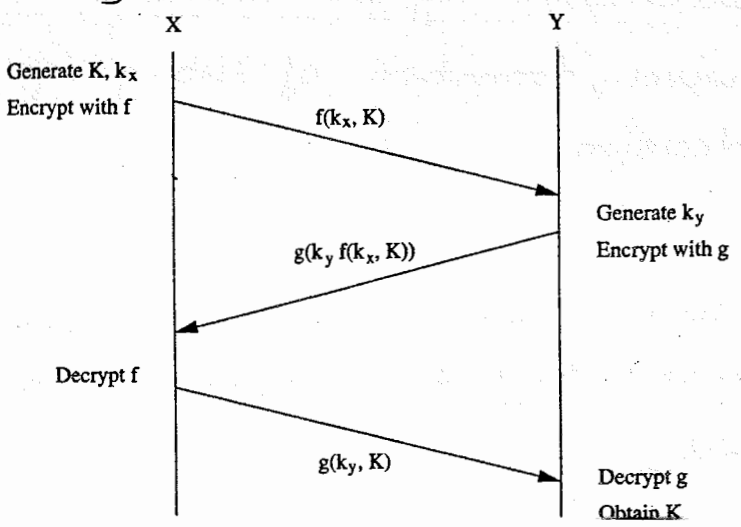
This is called the **Key encrypting key (KEK) method.**

* An interesting method for key transport without prior shared keys is the **Shamir's three-pass protocol.**

The scheme is based on a special-type of encryption called **communicative encryption schemes.**

Consider 2 nodes X & Y which wish to communicate. Node X selects a key K which it wants to use in its communication with node Y. It then generates a random key K_x, using which it encrypts K with f, & sends to node Y. Node Y encrypts this with a random key K_y using g, & sends this back to node X.

Now, node X decrypts this msg with its key K_x, & after applying inverse func^n f^{-1}, sends it to node Y. Finally, node Y decrypts the msg using K_y & g^{-1} to obtain key K.



KEY ARBITRATION

* Key arbitration schemes use a central arbitrator to create & distribute keys among all participants.

  Hence, they are a class of key transport schemes.

KEY AGREEMENT

* Key agreement protocols are used to establish a secure context over which a session can be run, starting with many parties who wish to communicate & an insecure channel.
* In group key agreement schemes, each participant contributes a part to the secret key.
* The most popular key agreement schemes use the **Diffie-Hellman exchange**, an assymetric key algorithm based on discrete logarithms.

KEY MANAGEMENT IN ADHOC WIRELESS NETWORKS

* Adhoc wireless networks pose certain specific challenges in key mgmt., due to the lack of infrastructure in such networks.
* 3 types of infrastructure have been identified; which are absent in adhoc wireless networks.
  - → The first is the n/w infrastructure, such as dedicated routers & stable links, which ensure communication with all nodes.
  - → The second missing infrastructure is services such as name resolution, directory & TTP's.
  - → The third missing infrastructure in adhoc wireless n/w is the administrative support of certifying authorities.

Password-Based Group Systems

* A password-based system has been explored where, in the simplest case, a long string is given as the password for users for one session.
* However, human beings tend to favour natual language phrases as passwords, over randomly generated strings.

  Such passwords, if used as keys directly during a session, are very week & open to attack because of high redundancy, & the possibility of reuse over diffuent sessions.
* Hence, protocols have been proposed to derive a strong key (not vulnerable to attacks).
* This password-based system could be **two-party**, with a separate exchange b/w any 2 participants, or it could be for the whole group, with a leader being elected to preside over the session.
* The protocol used is as follows.

  Each participant generates a random number, & sends it to all others. When every node has received the random number of every other node, a common predecided function is applied on all the numbers to calculate a **reference value**. The nodes are ordered based on the difference b/w their random number & the reference value.

Threshold Cryptography

* Public Key Infrastructure (PKI) enables the **easy distribution of keys** & is a **scalable method.**
* Each node has a **public/private key pair**, & a **certifying authority** (CA) can bind the keys to a particular node.

  But CA has to be present at all times, which may not be feasible in an adhoc wireless networks.
* A scheme based on threshold cryptography has been proposed by which **n servers** exist in an adhoc wireless network, out of which any (t+1) servers can jointly perform arbitration or authorization successfully, but **t servers** cannot perform the same. This is called an $(n, t+1)$ configuration, where $n \geq 3t+1$
* To sign a certificate, each server generates a **partial signature** using its private key & submits it to a **combiner**. The combiner can be any one of the servers.

  In order to ensure that the key is combined correctly, t+1 combiners can be used to account for at most t malicious servers.

  Using t+1 partial signatures, the combiner computes a signature & verifies its validity using a public key.

  If verification fails, it means that atleast one of the t+1 keys is not valid, so another subset of t+1 partial signatures is tried. If combiner itself is malicious, it cannot get a valid key, because partial key itself is always invalid.

Self-organised Public Key Management for Mobile Adhoc n/w's

* Self-organised public key system makes use of absolutely no infrastructure.
* The users in the adhoc wireless network issue certificates to each other based on **personal acquaintance**.

  A certificate is **binding** b/w a node & its **public key**. These certificates are stored & distributed by the users themselves. Certificates are issued only for specific period of time. Before it expires, the certificate is updated by the user who had issued the certificate.
* Each certificate is initially stored twice, by the issuer & by the person for whom it is issued.
* If any of the certificates are conflicting (eg., the same public key to different users, or the same user having different public keys), it is possible that a malicious node has issued a false certificate.

  A node then enables such certificates as **conflicting** & tries to resolve the conflict.

  If the certificates issued by some node are found to be wrong, then that node may be assumed to be malicious.

SECURE ROUTING IN AN ADHOC WIRELESS NETWORKS

Ensuring secure communication in adhoc wireless networks include the mobility of nodes, a promiscuous mode of operation, limited processing power & limited availability of resources such as battery power, bandwidth & memory.

Requirements of a secure routing protocol for adhoc wireless n/ws

The fundamental requirements for a secure routing protocol for adhoc wireless networks are listed as below:

1. **Detection of malicious nodes.**
   - ↳ A secure routing protocol should be able to detect the presence of any malicious node in the n/w & should avoid the participation of such nodes in the routing process.

2. **Gaurantee of correct route discovery**
   - ↳ If a route b/w the source & destination node exists, the routing protocol should be able to find the route, & should also ensure the correctness of the selected route.

3. **Confidentiality of network topology**
   - ↳ Once the n/w topology is known, the attacker may try to study the traffic pattern in the network. If some of the nodes are found to be more active compared to others, the attacker may try to mount attacks. This may ultimately affect the on-going routing [illegible], confidentiality of n/w topology is impt.

4. Stability against attacks

↳ The routing protocols must be self-stable in the sense that it must be able to revert to its normal operating state within a finite amount of time after a passive or an active attack.

Some of the security-aware routing protocols proposed for adhoc wireless networks are discussed.

SECURITY - AWARE AD-HOC ROUTING PROTOCOL

* This routing protocol uses **security** as one of the key metrics in path finding.
* In adhoc wireless networks, communication b/w end nodes through possibly multiple intermediate nodes is based on the fact that the two end nodes trust the intermediate nodes.
* SAR defines ***level of trust*** as a metric for routing & as one of the attributes for security to be taken into consideration while routing.
* The routing protocol based on level of trust is explained in below figure.

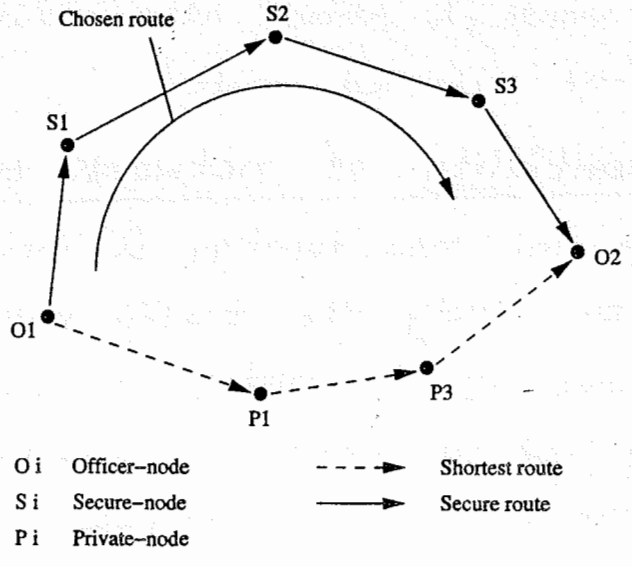


Figure Illustration of the level of trust metric

* As shown in fig., two path exists b/w the 2 offices O1 & O2 who want to communicate with each other. One of these paths is a shorter path which runs through private nodes whose trust levels are low.
  Hence, the protocol choose a longer but secure path which passes through other secure nodes.
* The SAR mechanisms can be easily **incorporated into both on-demand & table-driven routing protocols.**
* The SAR protocols allows the application to **choose the level of security it requires.** But the protocol requires different keys for different levels of security.

SECURE EFFICIENT AD HOC DISTANCE VECTOR ROUTING PROTOCOL

* SEAD routing protocol, is a secure adhoc routing protocol based on **destination-sequenced distance vector (DSDV) routing protocol.**
* This protocol is mainly designed **to overcome security attacks** such as DoS & **resource consumption attacks.**
* The protocol uses **one-way hash function** & does not involve any asymmetric cryptographic operation.

Distance Vector Routing

* This belongs to the category of **table-driven routing protocols.**
* Each node maintains a **routing table** containing the list of all known routes to various destination nodes in the network.
* The metric used for routing is the distance measured in terms of **hop-count.**

* The routing table is updated periodically by exchanging routing information. An alternative to this approach is **triggered updates**, in which each node broadcasts routing updates only if its routing table gets altered.

One-Way Hash Function

* SEAD uses authentication to differentiate b/w updates that are received from non-malicious nodes & malicious nodes. This **minimizes resource consumption attacks** caused by malicious nodes.

* SEAD uses one-way hash function for **authenticating the updates**.

* A one-way hash function (H) generates a one-way hash chain $(h_1, h_2, \ldots)$. The function H maps an i/p bit string of any length to a fixed length bit-string, that is, $H : (0,1)^* \longrightarrow (0,1)^\rho$, where ρ is the length in bits of the o/p bit-string.

  To create a one-way hash chain, a node generates a random no. with initial value $x \in (0,1)^\rho$. h_0, the first no. in the hash chain is initialized to x. The remaining values in the chain are computed using general formula,

  $$h_i = H(h_{i-1}) \text{ for } 0 \le i \le n, \text{ for some } n.$$

* The SEAD protocol assumes an upper bound value m-1 defines the max diameter of adhoc wireless n/w.

If the sequence of values calculated by a node using the hash function H is given by $(h_1, h_2, \ldots, h_n)$, where n is divisible by m, then for a routing table entry with sequence number i, let $k = \frac{k}{m} - i$. If the metric j (distance) used for that routing table entry is $0 \le j \le m-1$, then the value h_{km+j} is used to authenticate the routing update entry for that [illegible] metric j. Whenever a route update message is sent, the node appends the value used for authentication

along with it. If the authentication value used is h_{km+j}, then the attacker who tries to modify this value can do so only if he/she knows h_{km+j-1}. Since it is a one-way hash chain, calculating h_{km+j-1} becomes impossible.

* SEAD avoids routing loops.
* This protocol is robust against multiple uncoordinated attacks.

AUTHENTICATED ROUTING FOR AD HOC NETWORKS

* ARAN is a secure routing protocol which successfully defeats all identified attacks in the n/w layer.
* During the route discovery process of ARAN, the source node broadcasts RouteRequest packets. The destination node, on receiving the RouteRequest packets, responds by unicasting back a reply packet on the selected path.
* The ARAN protocol uses a preliminary **cryptographic certification process**, followed by **end-to-end route authentication process**, which ensures secure route establishment.

Issue of Certificates

* There exists an authenticated trusted server whose public key is known to all legal nodes in the network.
* The ARAN protocol assumes that keys are generated *a priori* by the server & distributed to all the nodes in the network.
* On joining the n/w, each node receives a certificate from the trusted server.

* The certificate received by a node A from the trusted server T looks like the following :

$$T \rightarrow A : \; cert_A = [IP_A, K_{A+}, t, e] K_{T-}$$

Where IP_A ⇝ represents the IP address of node A

K_{A+} ⇝ the public key of node A

t ⇝ the time of creation of the certificate

e ⇝ time expiry of the certificate

K_{T-} ⇝ private key of the server.

End-to-End Route Authentication

* The main goal of this end-to-end route authentication process is to ensure that the correct intended destination is reached by the packets sent from the source node.

The source node S broadcasts a Route Request / Route Discovery pkt destined to the destination node D.

The RouteRequest pkt contains the pkt identifier [route discovery process (RDP)], the IP address of the destination (IP_D), the certificate of the source node S ($Cert_S$), the current time (t), & nonce N_S.

The process can be denoted as below.

$$S \rightarrow broadcasts := [RDP, IP_D, Cert_S, N_S, t] K_{S-}$$

K_{S-} ⇝ private key of the source node S.

Whenever the source sends a route discovery message, it increments the value of nonce. Nonce is a counter used in conjunction with the time-stamp in order to make the nonce recycling easier. When a node receives an RDP packet from the source with a higher value of the source's nonce than that in the previously received RDP packets from the same source node, it makes a record of the neighbor from which it received the packet, encrypts the packet further with its own certificate, and broadcasts it further. The process can be denoted as follows:

$$A \rightarrow broadcasts := [[RDP, IP_D, Cert_S, N_S, t] K_{S-}] K_{A-}, Cert_A$$

An intermediate node B, on receiving an RDP packet from a node A, removes its neighbor's certificate, inserts its own certificate, and broadcasts the packet further. The destination node, on receiving an RDP packet, verifies node S's certificate and the tuple (N_S, t) and then replies with the *RouteReply* packet (REP). The destination unicasts the REP packet to the source node along the reverse path as follows:

$$D \rightarrow X := [REP, IP_S, Cert_D, N_S, t]K_{D-}$$

where node X is the neighbor of the destination node D, which had originally forwarded the RDP packet to node D. The REP packet follows the same procedure on the reverse path as that followed by the route discovery packet. An error message is generated if the time-stamp or nonce do not match the requirements or if the certificate fails. The error message looks similar to the other packets except that the packet identifier is replaced by the ERR message.

SECURITY - AWARE AODV PROTOCOL

* AODV is a on-demand routing protocol where the route discovery process is initiated by sending RouteRequest pkts only when data pkts arrive at a node for transmission.
* A malicious intermediate node could advertise that it has the shortest path to the destination, thereby redirecting all the pkts through itself. This is known as **blackhole attack**. It is illustrated in the following figure.

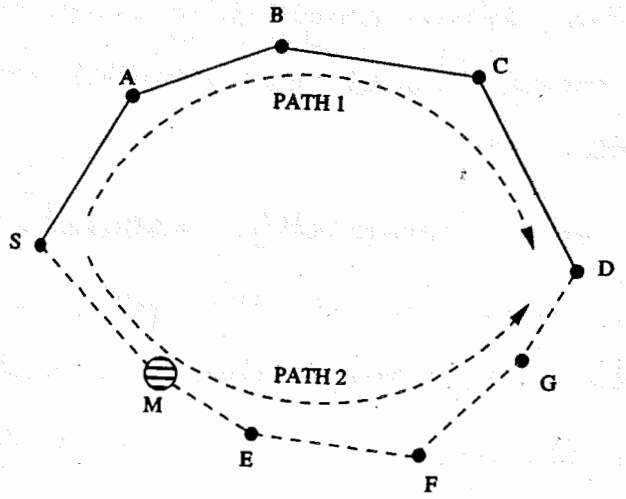


Figure Illustration of blackhole problem.

* Let node M be the malicious node that enters the n/w. It advertises that it has the shortest path to the destination node D when it receives the RouteRequest pkt sent by node S.

The attacker may not be able to succeed if node A, which also receives the RouteRequest pkt from node S, replies earlier than node M.

But a major advantage for the malicious node is that it does not have to search its routing table. for route to the destination. Also, the RouteReplay pkts originate directly from the malicious node & not from the destination node. Hence malicious node would reply faster than node A,

Thus node S may tend to establish a route to destination D through the malicious node M, allowing node M to listen to all pkts meant for the destination node.

Solutions for the Blackhole Problem.

* One of the solutions for this problem is to restrict the intermediate nodes from originating RouteReply pkts. Only the destination node would be permitted to initiate RouteReply pkts.
* Security is still not completely assured, since the malicious node may lie in the path chosen by the destination node. Also, the delay involved in the route discovery process increases as the size of the n/w increases.
* As soon as the RouteReply pkt is received from one of the intermediate nodes, another route request pkt from

intermediate node in the path. This is to ensure that such a path exists from the intermediate node to the destination node.

* For example, let the source node send RouteRequest pkts & receive RouteReply through the intermediate malicious node M. The RouteReply pkt of node M contains info" regarding its next-hop neighbour nodes. Let it contain info" abt the neighbour node E. Then as shown in below fig the source node S sends FurtherRouteRequest pkts to this neighbour node E. Node E responds by sending a FurtherRouteReply pkt to source node S.

Since node M is a malicious node which is not present in the routing list of node E, the FurtherRouteReply pkt sent by node E will not contain a route to the malicious node M. But if it contains a route to the Destination node D, then the new route to the dest" through node E is selected, & the earlier selected route through node M is rejected.

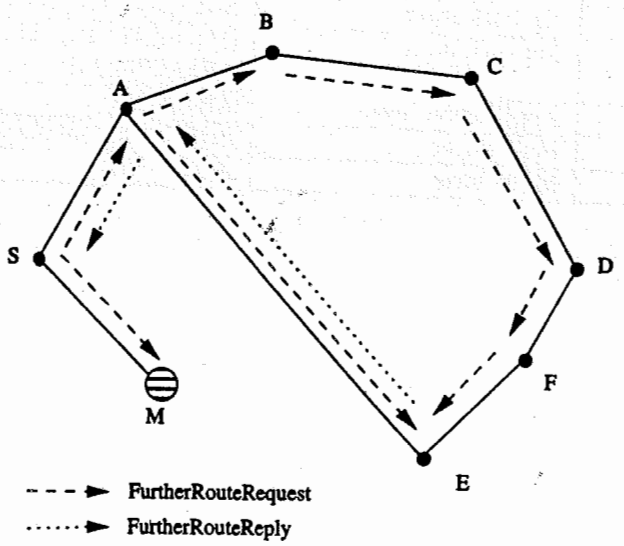


Figure Propagation of *FurtherRouteRequest* and *FurtherRouteReply*.

* This protocol completely eliminates the blackhole attack caused by a single attacker. The major disadvantage of this scheme is that the control overhead of the routing protocol increases considerably

Also, if the malicious nodes work in a group, this protocol fails miserably.

Summary

Table below lists out various attacks possible in adhoc wireless n/w's along with the soln proposed for countering these attacks.

Table Defense against attacks

Attack	Targeted Layer in the Protocol Stack	Proposed Solutions
Jamming	Physical and MAC layers	FHSS, DSSS
Wormhole attack	Network layer	Packet Leashes [16]
Blackhole attack	Network layer	[25], [29]
Byzantine attack	Network layer	[17]
Resource consumption attack	Network layer	SEAD [26]
Information disclosure	Network layer	SMT [30]
Location disclosure	Network layer	SRP [30], NDM [31]
Routing attacks	Network layer	[19], SEAD [26], ARAN [28], ARIADNE [32]
Repudiation	Application layer	ARAN [28]
Denial of Service	Multi-layer	SEAD [26], ARIADNE [32]
Impersonation	Multi-layer	ARAN [28]