CHAPTER: II

AN OUTLINE OF ROUTING IN WIRELESS NETWORKS
2.1 **Wireless Networks:**

Whether it’s because you have made a call using a mobile phone, received a message on your pager, checked your email from a PDA or even just seen an advert related to it, we have all come across a wireless data or voice network.

If a user, application or company wishes to make data portable, mobile and accessible then wireless networking is the answer. A wireless networking system would rid of the downtime you would normally have in a wired network due to cable problems. It would also save time and money due to the fact that you would spare the expense of installing a lot of cables. Also, if a client computer needs to relocate to another part of the office then all you need to do is move the machine with the wireless network card.

Wireless networking can prove to be very useful in public places – libraries, guest houses, hotels, cafeterias, and schools are all places where one might find wireless access to the Internet. From a financial point of view, this is beneficial to both the provider and the client. The provider would offer the service for a charge – probably on a pay per use system, and the client would be able to take advantage of this service in a convenient location; away from the office or home.

A drawback of wireless Internet is that the QoS (Quality of Service) is not guaranteed and if there is any interference with the link then the connection may be dropped.

**2.1.1 Task of different layer in wireless network**

The physical layer must tackle the path loss, fading, and multi-user interference to maintain stable communication links between peers. The data link layer (DLL) must make the physical link reliable and resolve contention among unsynchronized users transmitting packets on shared
channel. The latter task is performed by the medium access control (MAC) sub layer in the DLL. The network layer must track changes in the network topology and appropriately determine the best route to any desired destination. The transport layer must match the delay and packet loss characteristics specific to such a dynamic wireless network. Even the application layer needs to handle frequent disconnections.

2.1.2 Media access control
The media access control (MAC) data communication protocol sub-layer, also known as the medium access control, is a sub layer of the data link layer specified in the seven-layer OSI model. It provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. The hardware that implements the MAC is referred to as a medium access controller.

The MAC sub-layer acts as an interface between the logical link control (LLC) sub layer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

- Functions performed in the MAC sub layer
  According to 802.3-2002 section 4.1.4, the functions required of a MAC are:
  - Receive/transmit normal frames
  - Half-duplex retransmission and back off functions
  - Append/check FCS (frame check sequence)
  - Inter frame gap enforcement
  - Discard malformed frames
- Append/ remove preamble, SFD, and padding
- Half-duplex compatibility: append/ remove MAC address

In 100Mbps and faster MACs, the MAC address is not actually handled in the MAC layer. Doing so would make it impossible to implement IP because the ARP layer of IP-Ethernet needs access to the MAC address.

**Addressing mechanism**

In 100Mbps and faster Ethernet MACs, there is no required addressing mechanism. However, the MAC address inherited from the original MAC layer specification is used in many higher level protocols such as Internet Protocol (IP) over Ethernet.

The local network address used in IP-Ethernet is called MAC address because it historically was part of the MAC layer in early Ethernet implementations. The MAC layer's addressing mechanism is called physical address or MAC address. A MAC address is a unique serial number. Once a MAC address has been assigned to a particular network interface (typically at time of manufacture), that device should be uniquely identifiable amongst all other network devices in the world. This guarantees that each device in a network will have a different MAC address (analogous to a street address). This makes it possible for data packets to be delivered to a destination within a sub network, i.e. hosts interconnected by some combination of repeaters, hubs, bridges and switches, but not by IP routers. Thus, when an IP packet reaches its destination (sub) network, the destination IP address (a layer 3 or network layer concept) is resolved with the Address Resolution Protocol for IPv4, or by Neighbour Discovery Protocol (IPv6) into the MAC address (a layer 2 concept) of the destination host.
An example of a physical network is an Ethernet network, perhaps extended by wireless local area network (WLAN) access points and WLAN network adapters, since these share the same 48-bit MAC address hierarchy as Ethernet.

A MAC layer is not required in full-duplex point-to-point communication, but address fields are included in some point-to-point protocols for compatibility reasons.

- **Channel access control mechanism**

  The channel access control mechanisms provided by the MAC layer are also known as a multiple access protocol. This makes it possible for several stations connected to the same physical medium to share it. Examples of shared physical media are bus networks, ring networks, hub networks, wireless networks and half-duplex point-to-point links. The multiple access protocol may detect or avoid data packet collisions if a packet mode contention based channel access method is used, or reserve resources to establish a logical channel if a circuit switched or channelization based channel access method is used. The channel access control mechanism relies on a physical layer multiplex scheme.

  The most widespread multiple access protocol is the contention based CSMA/CD protocol used in Ethernet networks. This mechanism is only utilized within a network collision domain, for example an Ethernet bus network or a hub network. An Ethernet network may be divided into several collision domains, interconnected by bridges and switches.

  A multiple access protocol is not required in a switched full-duplex network, such as today's switched Ethernet networks, but is often available in the equipment for compatibility reasons.
- **Common multiple access protocols**

Examples of common packet mode multiple access protocols for wired multi-drop networks are:

- CSMA/CD (used in Ethernet and IEEE 802.3)
- Token bus (IEEE 802.4)
- Token ring (IEEE 802.5)
- Token passing (used in FDDI)

Examples of common multiple access protocols that may be used in packet radio wireless networks are:

- CSMA/CA (used in IEEE 802.11/WiFi WLANs)
- Slotted ALOHA
- Dynamic TDMA
- Reservation ALOHA (R-ALOHA)
- Mobile Slotted Aloha (MS-ALOHA)
- CDMA
- OFDMA

The logical link control (LLC) data communication protocol layer is the upper sub-layer of the data link layer (which is itself layer 2, just above the physical layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

The LLC sub-layer acts as an interface between the media access control (MAC) sublayer and the network layer.
• **Operation**

The LLC sublayer is primarily concerned with:

- Multiplexing protocols transmitted over the MAC layer (when transmitting) and decoding them (when receiving).
- Providing node-to-node flow and error control

In today's networks, flow control and error management is typically taken care of by a transport layer protocol such as the TCP protocol, or by some application layer protocol, in an end-to-end fashion, i.e. retransmission is done from source to end destination. This implies that the need for LLC sublayer flow control and error management has reduced. LLC is consequently only a multiplexing feature in today's link layer protocols. An LLC header tells the data link layer what to do with a packet once a frame is received. It works like this: A host will receive a frame and look in the LLC header to find out to what protocol stack the packet is destined - for example, the IP protocol at the network layer or IPX. However, today most non-IP network protocols are abandoned.

• **Application examples**

  • **X.25 and LAPB**

An LLC sublayer was a key component in early packet switching networks such as X.25 networks with the LAPB data link layer protocol, where flow control and error management were carried out in a node-to-node fashion, meaning that if an error was detected in a frame, the frame was retransmitted from one switch to next instead. This extensive handshaking between the nodes made the network slow.
Local area network (LAN) and metropolitan area network (MAN) protocols

The IEEE 802.2 standard specifies LLC sublayer for all IEEE 802 local area networks, such as IEEE 802.3/Ethernet (if the EtherType field isn't used), IEEE 802.5, and IEEE 802.11, and in some non-IEEE 802 networks such as FDDI.

- **Ethernet**
  Since bit errors are very rare in wired networks, Ethernet does not provide flow control or automatic repeat request (ARQ), meaning that incorrect packets are detected but only cancelled, not retransmitted (except in case of collisions detected by the CSMA/CD MAC layer protocol). Instead, retransmissions rely on higher layer protocols. As the Ethertype in an Ethernet II framing formatted frame is used to multiplex different protocols on top of the Ethernet MAC header it can be seen as LLC identifier. However, If Ethernet is used without EtherType field, Ethernet is considered as lacking LLC sublayer.

- **Wireless LAN**
  In wireless communications, bit errors are very common. In wireless networks such as IEEE802.11, flow control and error management is part of the CSMA/CA MAC protocol, and not part of the LLC layer. The LLC sublayer follows the IEEE 802.2 standard.

- **HDLC**
  Some non-IEEE 802 protocols can be thought of as being split into MAC and LLC layers. For example, while HDLC specifies both MAC functions (framing of packets) and LLC functions (protocol
multiplexing, flow control, detection, and error control through a retransmission of dropped packets when indicated), some protocols such as Cisco HDLC can use HDLC-like packet framing and their own LLC protocol.

- **PPP and modems**
  Over telephone network modems, PPP link layer protocols can be considered as a LLC protocol, providing multiplexing, but it does not provide flow control and error management. In a telephone network, bit errors might be common, meaning that error management is crucial, but that is today provided by modern modem protocols. Today's modem protocols have inherited LLC features from the older LAPM link layer protocol, made for modem communication in old X.25 networks.

  **Cellular systems**
  The GPRS LLC layer also does ciphering and deciphering of SN-PDU (SNDCP) packets.

  **Power lines**
  Another example of a data link layer which is split between LLC (for flow and error control) and MAC (for multiple access) is the ITU-T G.hn standard, which provides high-speed local area networking over existing home wiring (power lines, phone lines and coaxial cables).

### 2.1.3 Network layer
The network layer is layer 3 of the seven-layer OSI model of computer networking.
The network layer is responsible for packet forwarding including routing through intermediate routers, whereas the data link layer is responsible for media access control, flow control and error checking.

The network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination host via one or more networks while maintaining the quality of service functions.

**Functions of the network layer include:**

- **Connection model: connectionless communication**
  For example, IP is connectionless, in that a frame can travel from a sender to a recipient without the recipient having to send an acknowledgement. Connection-oriented protocols exist at other, higher layers of that model.

- **Host addressing**
  Every host in the network needs to have a unique address which determines where it is. This address will normally be assigned from a hierarchical system, so you can be "Fred Murphy" to people in your house, "Fred Murphy, 1 Main Street" to Dubliners, or "Fred Murphy, 1 Main Street, Dublin" to people in Ireland, or "Fred Murphy, 1 Main Street, Dublin, Ireland" to people anywhere in the world. On the Internet, addresses are known as Internet Protocol (IP) addresses.

- **Message forwarding**
  Since many networks are partitioned into subnet works and connect to other networks for wide-area communications, networks use specialized hosts, called gateways or routers to forward packets between networks. This is also of interest to mobile applications, where a user may move from one location to another, and it must be arranged that his messages follow him. Version 4 of the Internet
Protocol (IPv4) was not designed with this feature in mind, although mobility extensions exist. IPv6 has a better designed solution. Within the service layering semantics of the OSI network architecture the network layer responds to service requests from the transport layer and issues service requests to the data link layer.

2.2 Mobile Ad Hoc Networks

A mobile ad hoc network, such as the one shown in Figure 2, is a collection of digital data terminals equipped with wireless transceivers that can communicate with one another without using any fixed networking infrastructure. Communication is maintained by the transmission of data packets over a common wireless channel. The absence of any fixed infrastructure, such as an array of base stations, makes ad hoc networks radically different from other wireless LANs. Whereas communication from a mobile terminal in an “infrastructure” network, such as a cellular network, is always maintained with a fixed base station, a mobile terminal (node) in an ad hoc network can communicate directly with another node that is located within its radio transmission range. In order to transmit to a node that is located outside its radio range, data packets are relayed over a sequence of intermediate nodes using a store-and-forward “multihop” transmission principle. All nodes in an ad hoc network are required to relay packets on behalf of other nodes. Hence, a mobile ad hoc network is sometimes also called a multihop wireless network.
Figure 2: Adhoc Network

Since no base stations are required, ad hoc networks can be deployed quickly, without having to perform any advance planning or construction of expensive network infrastructure. Hence, such networks are ideally suited for applications where such infrastructure is either unavailable or unreliable. Typical applications include military communication networks in battlefields, emergency rescue operations, undersea operations, environmental monitoring, and space exploration.

Deployment quality and relatively low cost of implementation, ad hoc networks is also used in places where they are cheaper than their infrastructure counterparts. Examples of these applications consist of a network of laptop computers in conference rooms, network of digital electronic equipment and appliances [6, 7]. There has been a growing interest of using ad hoc networks of wireless sensors to perform unmanned distributed surveillance and tracking operations [8].

The design of ad hoc networks faces many unique challenges. Most of these arise due to two principal reasons. The first is that all nodes in an ad hoc network, including the source nodes, the corresponding destinations, as well as the routing nodes forwarding traffic between them, may be mobile. As the wireless transmission range is limited, the wireless link
between a pair of neighbouring nodes breaks as soon as they move out of range. Hence, the network topology that is defined by the set of physical communication links in the network (wireless links between all pairs of nodes that can directly communicate with each other) can change frequently and unpredictably. This implies that the multihop path for any given pair of source and destination nodes also changes with time. Mobility also causes unpredictability in the quality of an existing wireless link between neighbors. A second reason that makes the design of ad hoc networks complicated is the absence of centralized control. All networking functions, such as determining the network topology, multiple accesses, and routing of data over the most appropriate multihop paths, must be performed in a distributed way. These tasks are particularly challenging due to the limited communication bandwidth available in the wireless channel.

These challenges must be addressed in all levels of the network design. The physical layer must tackle the path loss, fading, and multi-user interference to maintain stable communication links between peers. The data link layer must make the physical link reliable and resolve contention among unsynchronized users transmitting packets on a shared channel. The latter task is performed by the medium access control (MAC) sub layer in the data link layer. The network layer must track changes in the network topology and appropriately determine the best route to any desired destination. The transport layer must match the delay and packet loss characteristics specific to such a dynamic wireless network. Even the application layer needs to handle frequent disconnections.

Although this area has received a lot of attention in the past few years, the idea of ad hoc networking started in the 1970s when the U.S. Defense
Advanced Research Projects Agency (DARPA), sponsored the PRNET (Packet Radio Network) project in 1972 [9]. This was followed by the SURAN (Survivable Adaptive Radio Network) project in the 1980s [10]. These projects supported research on the development of automatic call setup and maintenance in packet radio networks with moderate mobility. However, interest in this area grew rapidly in the 1990s due to the popularity of a large number of portable digital devices such as laptop and palmtop computers, and the common availability of wireless communication devices. The rising popularity of the Internet added to the interest to develop internetworking protocols for mobile ad hoc networks operating in.

2.3 Routing in ad hoc Networks

Movements of nodes in a mobile ad hoc network cause the nodes to move in and out of range from one another. As a result, there is a continuous making and breaking of links in the network, causing the network connectivity (topology) to vary dynamically with time.

Since the network relies on multihop transmissions for communication, this imposes major challenges for the network layer to determine the multihop route over which data packets can be transmitted between a given pair of source and destination nodes. Figure 3 demonstrates how the movement of a single node (C) changes the network topology, rendering the existing route between A and E (i.e., A–C–E) unusable. The network needs to evaluate the changes in the topology caused by this movement and establish a new route from A to E (such as A–D–C–E).
Because of the time-varying nature of the topology of mobile ad hoc networks, traditional routing techniques, such as the shortest-path and link-state protocols that are used in fixed networks, cannot be directly applied to ad hoc networks. A fundamental quality of routing protocols for ad hoc networks is that they must dynamically adapt to variations of the network topology. This is implemented by devising techniques for efficiently tracking changes in the network topology and rediscovering new routes when older ones are broken. Since an ad hoc network is infrastructure less, these operations are to be performed in a distributed fashion with the collective cooperation of all nodes in the network. Some of the desirable qualities of dynamic routing protocols for ad hoc networks are:

2.3.1 Desirable qualities of dynamic routing protocols

Routing overhead: Tracking changes of the network topology requires exchange of control packets among the mobile nodes, these control packets must carry various types of information, such as node identities, neighbor lists, distance metrics, and so on, which consume additional bandwidth for transmission. Since wireless channel bandwidth is at a premium, it is desirable that the routing protocol minimizes the number and size of control packets for tracking the variations of the network.
**Timeliness:** Since link breakages occur at random times, it is hard to predict when an existing route will expire. The timeliness of adaptation of the routing protocol is crucial. A broken route causes interruption in an ongoing communication until a new route is established. Often the newly rediscovered route may be largely disjoint from the older route, which creates problems in rerouting the packets that were already transferred along the route and could not be delivered to the destination. Ideally, a new route should be determined before the existing one is broken, which may not be possible. Alternatively, a new route should be established with minimum delay.

**Path optimality:** With constraints on the routing overhead, routing protocols for mobile ad hoc networks are more concerned with avoiding interruptions of communication between source and destination nodes rather than the optimality of the routes. Hence, in order to avoid excess transmission of control packets, the network may be allowed to operate with suboptimal (which are not necessarily the shortest) routes until they break. However, a good routing protocol should minimize overhead as well as the path lengths. Otherwise, it will lead to excessive transmission delays and wastage of power.

**Loop freedom:** Since the routes are maintained in a distributed fashion, the possibility of loops within a route is a serious concern. The routing protocol must incorporate special features so that the routes remain free of loops.

**Storage complexity:** Another problem of distributed routing architectures is the amount of storage space utilized for routing. Ad hoc networks may be applied to small portable devices, such as sensors,
which have severe constraints in memory and hardware. Hence, it is desirable that the routing protocol be designed to require low storage complexity.

**Scalability:** Routing protocols should be able to function efficiently even if the size of the network becomes large. This is not very easy to achieve, as determining an unknown route between a pair of mobile nodes becomes more costly in terms of the required time, number of operations, and expended bandwidth when the number of nodes increases.

### 2.3.2 The issues that require further investigation:

**MAC:** How can we design improved and robust MAC schemes that would dynamically adjust to variations of the wireless link characteristics and simultaneously cater to the need for higher data rates, quality-of-service requirements, and power savings, and that would be crucial in many future applications?

**Routing:** By far the biggest issue in mobile ad hoc networking research is routing. With the rapid and diverse nature of growth of mobile ad hoc networks, the choice of the routing protocol is likely to depend on the network size, mobility, and application requirements. However, it will be interesting to see if an approach to generate a unified standard for ad hoc routing is achievable.

**Transport:** The issues of transport layer protocols for mobile ad hoc networks require special attention. It is often said that optimizing ad hoc network performance requires a multilayer approach, where design
problems at different layers of the protocol stack are addressed together for a unified solution. How can we arrive at such a design solution?

**Scalability:** Many applications are already being conceived where hundreds of thousands of nodes are being considered for ad hoc networking. How do we design protocols for these large scale networks?

**Internet connectivity:** What is the best paradigm for extending the reach of the Internet to mobile terminals that form a mobile ad hoc network with access points to the Internet?

**Security:** All wireless networks are susceptible to security problems such as eavesdropping and jamming. How can we provide security to mobile ad hoc networks?

**Power:** One of the major limitations of portability arises from limitations of battery power. In addition to developing improved battery technology, future ad hoc networking protocols have to be made more power efficient so that the network can survive longer without replacement of batteries. These items are far from comprising a complete list of challenging research problems that ad hoc networking has posed.

Based on when routing activities are initiated, routing protocols for mobile ad hoc networks may be broadly classified [13, 14, 15, and 16] in three basic categories: (1) *proactive or table-driven* protocols, (2) *reactive or on-demand* routing protocols, and (3) *hybrid* routing protocols.
2.4 Taxonomy of Ad hoc Routing Protocols

![Taxonomy of Adhoc routing protocol](image)

**Figure 4:** Taxonomy of Adhoc routing protocol

2.5 Proactive routing protocols

Proactive protocols perform routing operations between all source destination pairs periodically, irrespective of the need of such routes. E.g. DSDV [18], OLSR [19].

2.5.1 Issues in Proactive Routing

The key characteristic of proactive routing protocols is that updates are sent periodically irrespective of need. Another issue is that they are table-driven[20]. These two properties cause serious problems for making proactive routing protocols scale with network size.

2.6 Reactive Routing Protocols

Reactive protocols are designed to minimize routing overhead. Instead of tracking the changes in the network topology to continuously maintain shortest path routes to all destinations, these protocols determine routes only when necessary. Typically, these protocols perform a *route discovery* operation between the source and the desired destination when the source needs to send a data packet and the route to the destination is
not known. As long as a route is live, reactive routing protocols only perform *route maintenance* operations and resort to a new route discovery only when the existing one breaks. E.g. DSR[21], AODV[22]

### 2.6.1 Issues in Reactive Routing

Since reactive routing protocols only transmit routing packets when needed, these protocols are comparatively more efficient when there are fewer link breakages, such as under low mobility conditions. In addition, when there are only a few communicating nodes in the network, the routing functions are only concerned with maintaining the routes that are active. Because of these benefits, reactive or on-demand routing protocols have received more attention than proactive protocols for mobile ad hoc networks.

### 2.7 Hybrid Routing Protocols

The use of *hybrid routing* is an approach that is often used to obtain a better balance between the adaptability to varying network conditions and the routing overhead. These protocols use a combination of reactive and proactive principles, each applied under different conditions, places, or regions. For instance, a hybrid routing protocol may benefit from dividing the network into clusters and applying proactive route updates within each cluster and reactive routing across different clusters. E.g. ZRP[23], LANMAR

### 2.8 Geographic Position Aided Routing

The fundamental problems of routing in ad hoc networks arise due to the random movements of the nodes. Such movements make topological information stale, and hence, when an on-demand routing protocol needs
to find the route, it often has to flood the entire network looking for the destination. One of the ways of reducing the wastage of bandwidth in transmitting route request packets to every node in the network is to confine the search using geographical location information. Geographical positioning systems (GPS) can detect the physical location of a terminal using universal satellite-transmitted wireless signals [24, 25, and 26]. In recent times, GPS have become smaller, more versatile, and more cost-effective. Hence, several protocols have been proposed that assume the presence of a GPS receiver in each node and utilize the location information in routing one of the approaches for utilizing geographic location information in routing is to forward data packets in the direction of the location of the destination node, as proposed in various references. It may be required to define geographic location–specific addresses instead of logical node addresses to do that.

An alternative concept is proposed in the Location Aided Routing (LAR) protocol, which uses location information in on-demand routing to limit the spread of request packets for route discoveries. LAR uses information such as the last known location and speed of movements of a destination to determine a REQUEST ZONE, which is defined as a restricted area within which the REQUEST packets are forwarded in order to find the destination. Two different ways of defining REQUEST ZONES have been proposed. The idea is to allow route request packets to be forwarded by only those nodes that lie within the REQUEST ZONE, specified by the source. This limits the overhead of routing packets for route discovery, which would normally be flooded over the whole network.

A related protocol that uses spatial locality based on hop counts to confine the spread of request packets was proposed by Castaneda and Das. This protocol uses the concept that once an existing route is broken, a new route can be determined within a certain distance (measured in
number of hops) from the old route. The protocol confines the spread of route request packets while searching for a new route to replace one that is freshly broken. For a new route discovery where no earlier routes were on record, the protocol still uses traditional flooding. However, this *query localization* technique for rediscovering routes still saves routing overhead.

### 2.9 Stability-Based Routing

A different approach to improve the performance of routing in mobile ad hoc networks is based on using routes that are selected on the basis of their *stability*. The Associativity-Based Routing (ABR) [27] protocol maintains association *stability metric* that measures the duration of time for which a link has been stable. While discovering a new route, the protocol selects paths that have high aggregate-association stability. This is done with the idea that a long-lived link is likely to be stable for a longer interval than a link that has been relatively short-lived Signal Stability-Based Routing (SSR) [28] uses signal strengths to determine stable links. It allows the discrimination between “strong” and “weak” links when a route request packet is received by a node. The request packet is forwarded by the node if it has been received over a strong link. This allows the selection of routes that are expected to be stable for a longer time.

### 2.10 Multipath Routing

On-demand or reactive routing protocols suffer from the disadvantage that data packets cannot be transmitted until the route discovery is completed. This delay can be significant under heavy traffic conditions when the REQUEST or the REPLY packet may take a considerable
amount of time in traversing its path. This characteristic, along with the fact that each route discovery process consumes additional bandwidth for the transmission of REQUEST and REPLY packets, motivates us to find ways to reduce the frequency of route discoveries in on-demand protocols. One way of doing that is to maintain multiple alternate routes between the same source-destination pair such that when the primary route breaks, the transmission of data packets can be switched over to the next available path in the memory. Under the assumption that multiple paths do not break at the same time, which is most often true if the paths are sufficiently disjoint, the source may delay a fresh route discovery if the alternate paths are usable. As a result, many routing protocols have been designed to maintain multiple paths or routes for each pair of source and destination nodes.

The Temporally Ordered Routing Algorithm (TORA) [29] provides multiple alternate paths by maintaining a “destination oriented” directed acyclic graph from the source. The DSR protocol also has an option of maintaining multiple routes for each destination in the route cache, so that an alternate route can be used upon failure of the primary route. Two multipath extensions of DSR were proposed by Nasipuri, Castaneda, and Das that aggressively determine multiple disjoint paths for each destination. Here, two different schemes for selecting alternative routes were considered, both benefiting from reducing the frequency of route discoveries caused by link breakages. Several other multipath routing protocols that derive benefits using the same principle have also been proposed.
2.11 Pre-emptive Routing

A purely reactive routing protocol typically does not avoid a multihop communication from being interrupted before the route breaks due to a link failure. Most reactive routing protocols initiate a fresh route discovery when an ERROR packet is received at the source due to a link breakage. This introduces a pause in the communication until a new route is found. The goal of pre-emptive routing protocols is to avoid such pauses by triggering a route discovery and switching to a new (and, it is hoped, better) route before the existing route breaks. Such protocols can be viewed as a combination of proactive and reactive routing, where the route maintenance is performed proactively but the basic routing framework is reactive. The crucial design issue in such protocols is to detect when to initiate a pre-emptive route discovery to find a “better” route. The protocol proposed by Goff and colleagues uses the technique of determining this by observing when the signal strength falls below a predetermined threshold. If the wireless channel is relatively static, then this correctly detects the initiation of link failure due to increasing distance between the two nodes in the link.

However, multipath fading and shadowing effects might lead to false alarms while using this technique. Alternatively, using a time-to-live parameter was proposed by Nasipuri [26] and colleagues. In this protocol, a pre-emptive route discovery is initiated when a route has been in use for a predetermined threshold of time. The pre-emption obviously makes the route discoveries more frequent than what would be observed in a purely reactive scheme. To keep the routing overhead low, the pre-emptive routing protocol use of query localization in the pre-emptive searches.