Unit - I

AD HOC NETWORKS INTRODUCTION AND ROUTING PROTOCOLS

Elements of Ad hoc Wireless Networks, Issues in Ad hoc wireless networks, Example commercial applications of Ad hoc networking, Ad hoc wireless Internet, Issues in Designing a Routing Protocol for Ad Hoc Wireless Networks, Classifications of Routing Protocols, Table Driven Routing Protocols – Destination Sequenced Distance Vector (DSDV), On–Demand Routing protocols –Ad hoc On–Demand Distance Vector Routing (AODV).

TABLE OF CONTENTS

1.1 Introduction

1.1.1 Computer Networks

- A computer network is the interconnection of multiple nodes through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The

links connecting the nodes are known as communication channels.

- The computer network uses distributed processing in which task is divided among several computers. Instead, a single computer handles an entire task, each separate computer handles a subset

Advantages of Distributed processing

- **Security:** It provides limited interaction that a user can have with the entire system. For example, a bank allows the users to access their own accounts through an ATM without allowing them to access the bank's entire database.
- **Faster problem solving:** Multiple computers can solve the problem faster than a single machine working alone.
- **Security through redundancy:** Multiple computers running the same program at the same time can provide the security through redundancy. For example, if four computers run the same program and any computer has a hardware error, then other computers can override it.

Applications of Distributed Systems

- E-mail
- Online Ticket Reservation
- Banking, etc.,

1.1.2 Types of Communication

- Communication medium refers to the physical channel through which data is sent and received. Data is sent in the form of voltage levels which make up the digital signal. A digital signal consists of 0s and 1s. There are basically two types of networks:
  - **Wired network**
  - **Wireless network**

Wired Network

- In a wired network, data is transmitted over a physical medium.
- There are three types of physical cables used in a wired network.
  - Twisted Pair
  - Coaxial Cable
  - Fiber Optic

  Examples: Cable TV, Broadband Telephone Communication.

Wireless Network

- A wireless network uses radio waves as the sole medium for transmitting and receiving data. There are no wires involved.
- Radio waves are electromagnetic waves which are transverse in nature and they have the longest wavelength on the electromagnetic spectrum.

  Examples: Infrared, Bluetooth, WiFi.

1.2 Elements of Ad hoc Wireless Networks

- The word "ad hoc" comes from Latin Language, which means 'for this purpose only', Ad hoc Networks are the small area networks, especially designed with Wireless/Temporary connections to the different computer assisted nodes.
- A wireless ad-hoc network (WANET) is a type of local area network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring a central device, such as a router or access point. When Wi- Fi networks are in ad-hoc mode, each device in the network forwards data to the others.
- Since the devices in the ad-hoc network can access each other's resources directly through a basic point-to-point wireless connection, central servers are unnecessary for functions such as file shares or printers.
- In a wireless ad-hoc network, a collection of devices (or nodes) is responsible for network operations, such as routing, security, addressing and key management. Figure 1.1 shows, multi-hop wireless ad hoc networks, it defined as a collection of nodes that communicate with each other wirelessly by using radio signals with a shared common channel.

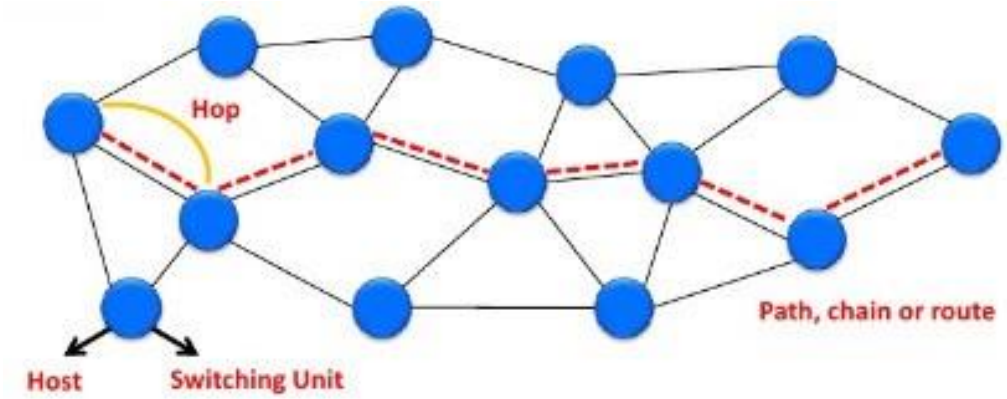


Figure 1.1 Multi- Hop Wireless Ad-Hoc Networks

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

Types of Wireless Ad Hoc Networks

Wireless ad hoc networks are categorized into different classes. They are:

- **Mobile ad hoc network (MANET)**: An ad hoc network of mobile devices.
- **Vehicular ad hoc network (VANET)**: Used for communication between vehicles. Intelligent VANETs use artificial intelligence and ad hoc technologies to communicate what should happen during accidents.
- **Smartphone ad hoc network (SPAN)**: Wireless ad hoc network created on smartphones via existing technologies like Wi-Fi and Bluetooth.
- **Wireless mesh network**: A mesh network is an ad hoc network where the various nodes are in communication directly with each other to relay information throughout the total network.
- **Army tactical MENT**: Used in the army for "on-the-move" communication, a wireless tactical ad hoc network relies on range and instant operation to establish networks when needed.
- **Wireless sensor network**: Wireless sensors that collect everything from temperature and pressure readings to noise and humidity levels, can form an ad hoc network to deliver information to a home base without needing to connect directly to it.
- **Disaster rescue ad hoc network**: Ad hoc networks are important when disaster strikes and established communication hardware isn't functioning properly.

Advantages of Ad Hoc Networks

- Ad-hoc networks can have more flexibility.
- It is better in mobility.
- It can be turn up and turn down in a very short time.
- More economical
- It considered as a robust network because of its non-hierarchical distributed control and management mechanisms.

Disadvantages of Ad Hoc Networks

- Unpredictable Topology
- Limited Bandwidth
- Lose of data
- Interference
- Limited Security
- Energy Constraints

1.3 Issues in Ad hoc wireless networks

➢ The major issues that affect the design, deployment, and performance of an ad hoc wireless system are as follows:

- Medium Access Control (MAC)
- Routing
- Multicasting
- Transport layer protocol
- Quality of Service (QOS)
- Self-organization
- Security
- Energy management
- Addressing and service discovery
- Scalability
- Deployment considerations

1.3.1 Medium Access Control

➢ The purpose of this protocol is to achieve a distributed FIFO schedule among multiple nodes in an ad hoc network. When a node transmits a packet, it adds the information about the arrival time of queued packets. It provide fair access to shared broadcast radio channel. The major issues in MAC protocol are as follows:

- **Distributed Operation:** The MAC protocol design should be fully distributed involving minimum control overhead, because it need to operate in environment without centralized device.
- **Synchronization:** The synchronization is mandatory for TDMA-based systems for management of transmission and reception slots.
- **Hidden Terminals Problem:** Hidden terminals are nodes that are hidden (or not reachable) from the sender of a data transmission session, but are reachable to the receiver of the session. (Figure 1.2)

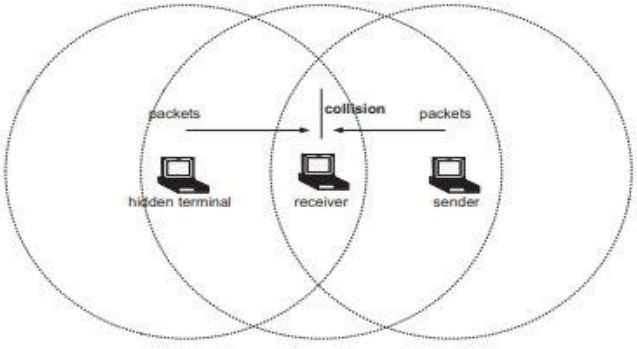


Figure 1.2 Hidden Terminal Problem

Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- Collisions at receiver node -> inefficient bandwidth utilization, reduce throughput.

- **Exposed Terminals Problem:** The nodes that are in the transmission range of the sender of an on-going session, are prevented from making a transmission. The exposed nodes should be allowed to transmit in a controlled fashion without causing collision to the on-going data transfer. (Figure 1.3)

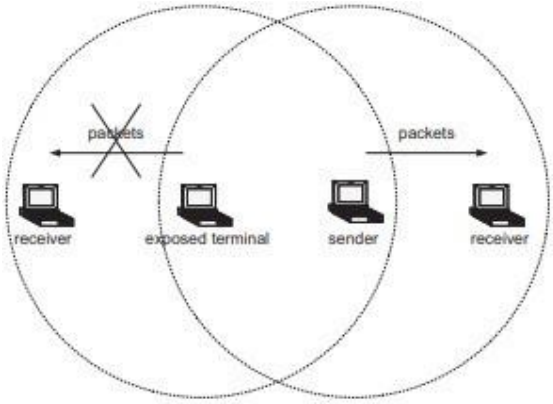


Figure 1.3 Exposed Terminal Problem

Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- **Throughput:** The MAC protocol employed in ad hoc wireless networks should attempt to maximize the throughput of the system. The important considerations for throughput enhancement are
  - Minimizing the occurrence of collisions.
  - Maximizing channel utilization
  - Minimizing control overhead.
- **Access delay:** The average delay that any packet experiences to get transmitted. The MAC protocol should attempt to minimize the delay.
- **Fairness:** Fairness refers to the ability of the MAC protocol to provide an equal share or weighted share of the bandwidth to all competing nodes. Fairness can be either node-based or flow-based.
- **Real-time Traffic support:** In a contention-based channel access environment, without any central coordination, with limited bandwidth, and with location-dependent contention, supporting time- sensitive traffic such as voice, video, and

real-time data requires explicit support from the MAC protocol.

- **Resource reservation:** The provisioning of QoS defined by parameters such as bandwidth, delay, and jitter requires reservation of resources such as bandwidth, buffer space, and processing power.

- **Ability to measure resource availability:** In order to handle the resources such as bandwidth efficiently and perform call admission control based on their availability, the MAC protocol should be able to provide an estimation of resource availability at every node. This can also be used for making congestion control decisions.

- **Capability for power control:** The transmission power control reduces the energy consumption at the nodes, causes a decrease in interference at neighboring nodes, and increases frequency reuse.

- **Adaptive rate control:** This refers to the variation in the data bit rate achieved over a channel. A MAC protocol that has adaptive rate control can make use of a high data rate when the sender and receiver are nearby & adaptively reduce the data rate as they move away from each other.

1.3.2 Routing

➢ The responsibilities of a routing protocol include exchanging the route information; finding a feasible path to a destination. The major challenges that a routing protocol faces are as follows:

- **Mobility:** The Mobility of nodes results in frequent path breaks, packet collisions, transient loops, stale routing information, and difficulty in resource reservation.

- **Bandwidth constraint:** Since the channel is shared by all nodes in the broadcast region, the bandwidth available per wireless link depends on the number of nodes & traffic they handle.

- **Error-prone and shared channel:** The Bit Error Rate (BER) in a wireless channel is very high [10^{-5} to 10^{-3}] compared to that in its wired counterparts [10^{-12} to 10^{-9}].

- **Location-dependent contention:** The load on the wireless channel varies with the number of nodes present in a given geographical region. This makes the contention for the channel high when the number of nodes increases. The high contention for the channel results in a high number of collisions & a subsequent wastage of bandwidth.

- **Other resource constraints:** The constraints on resources such as computing power, battery power, and buffer storage also limit the capability of a routing protocol.

The major requirements of a routing protocol in ad hoc wireless networks are the following.

- **Minimum route acquisition delay**
- **Quick route reconfiguration**
- **Loop-free routing**
- **Distributed routing approach**
- **Minimum control overhead**
- **Scalability**
- **Provisioning of QoS**
- **Support for time-sensitive traffic**
- **Security and privacy**

1.3.3 Multicasting

➢ It plays important role in emergency search & rescue operations & in military communication. Use of single link connectivity among 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 packet delivery ratio due to the frequency tree breaks. The major issues in designing multicast routing protocols are as follows:

- **Robustness:** The multicast routing protocol must be able to recover & reconfigure quickly from potential mobility-induced link breaks thus making it suitable for use in high dynamic environments.
- **Efficiency:** A multicast protocol should make a minimum number of transmissions to deliver a data packet to all the group members.
- **Control overhead:** The scarce bandwidth availability in ad hoc wireless networks demands minimal control overhead for the multicast session.
- **Quality of Service:** QoS support is essential in multicast routing because, in most cases, the data transferred in a multicast session is time-sensitive.

- **Efficient group management:** Group management refers to the process of accepting multicast session members and maintaining the connectivity among them until the session expires.
- **Scalability:** The multicast routing protocol should be able to scale for a network with a large number of node
- **Security:** Authentication of session members and prevention of non-members from gaining unauthorized information play a major role in military communications.

1.3.4 Transport Layer Protocol

➢ The main objectives of the transport layer protocols include :

- Setting up & maintaining end-to-end connections,
- Reliable end-to-end delivery of packets,
- Flow control &
- Congestion control.

Examples of some transport layers protocols are,

a) UDP (User Datagram Protocol) :

- It is an unreliable connectionless transport layer protocol.
- It neither performs flow control & congestion control.
- It do not take into account the current network status such as congestion at the intermediate links, the rate of collision, or other similar factors affecting the network throughput.

b) TCP (Transmission Control Protocol):

- It is a reliable connection-oriented transport layer protocol.
- It performs flow control & congestion control.
- Here performance degradation arises due to frequent path breaks, presence of stale routing information, high channel error rate, and frequent network partitions.

1.3.5 Quality of Service (QoS)

➢ QoS is the performance level of services offered by a service provider or a network to the user.

- QoS provisioning often requires,
  - Negotiation between host & the network.
  - Resource reservation schemes.
  - Priority scheduling &
  - Call admission control.

- **QoS parameters**

Applications	Corresponding QoS parameter
1.Multimedia application	1. Bandwidth & Delay.
2.Military application	2.Security & Reliability.
3.Defense application	3.Finding trustworthy intermediate hosts & routing
4.Emergency search and rescue operations	4.Availability.
5.Hybrid wireless network	5.Maximum available link life, delay, bandwidth & channel utilization.
6.communication among the nodes in a sensor network	6.Minimum energy consumption, battery life & energy conservation

- **QoS-aware routing**
  - Finding the path is the first step toward a QoS-aware routing protocol.
  - The parameters that can be considered for routing decisions are,
    - Network throughput.
    - Packet delivery ratio.
    - Reliability.
    - Delay.
    - Delay jitter.
    - Packet loss rate.
    - Bit error rate.

1.3.6 Self-Organization

- One very important property that an ad hoc wireless network should exhibit is organizing & maintaining the network by itself.
- The major activities that an ad hoc wireless network is required to perform for self-organization are,

- Neighbour discovery.
- Topology organization &
- Topology reorganization (updating topology information)

1.3.7 Security

- Security is an important issue in ad hoc wireless network as the information can be hacked.
- Attacks against network are two types
  - Passive attack → Made by malicious node to obtain information transacted in the network without disrupting the operation.
  - Active attack → They disrupt the operation of network.
- Further active attacks are two types
  - External attack: The active attacks that are executed by nodes outside the network.
  - Internal attack: The active attacks that are performed by nodes belonging to the same network.
- The major security threats that exist in ad hoc wireless networks are as follows :
  - **Denial of service** – The attack affected by making the network resource unavailable for service to other nodes, either by consuming the bandwidth or by overloading the system.
  - **Resource consumption** – The scarce availability of resources in ad hoc wireless network makes it an easy target for internal attacks, particularly aiming at consuming resources available in the network. The major types of resource consumption attacks are,
    - Energy depletion
      - ✓ Highly constrained by the energy source
      - ✓ Aimed at depleting the battery power of critical nodes.
    - Buffer overflow
      - ✓ Carried out either by filling the routing table with unwanted routing entries or by consuming the data packet buffer space with unwanted data.

- ✓ Lead to a large number of data packets being dropped, leading to the loss of critical information.

- **Host impersonation** – A compromised internal node can act as another node and respond with appropriate control packets to create wrong route entries, and can terminate the traffic meant for the intended destination node.
- **Information disclosure** – A compromised node can act as an informer by deliberate disclosure of confidential information to unauthorized nodes.
- **Interference** – A common attack in defense applications to jam the wireless communication by creating a wide spectrum noise.

1.3.8 Addressing and Service Discovery

- Addressing & service discovery assume significance in ad hoc wireless network due to the absence of any centralised coordinator.
- An address that is globally unique in the connected part of the ad hoc wireless network is required for a node in order to participate in communication.
- Auto-configuration of addresses is required to allocate non-duplicate addresses to the nodes.

1.3.9 Energy Management

- Energy management is defined as the process of managing the sources & consumers of energy in a node or in the network for enhancing the lifetime of a network.
- Features of energy management are:
  - Shaping the energy discharge pattern of a node's battery to enhance battery life.
  - Finding routes that consumes minimum energy.
  - Using distributed scheduling schemes to improve battery life.
  - Handling the processor & interface devices to minimize power consumption.
- Energy management can be classified into the following categories:
  - **Transmission power management**
    - The power consumed by the Radio Frequency (RF) module of a mobile node is determined by several factors such as
      - ✓ The state of operation.
      - ✓ The transmission power and
      - ✓ The technology used for the RF circuitry.

- **Battery energy management**
  - The battery management is aimed at extending the battery life of a node by taking advantage of its chemical properties, discharge patterns, and by the selection of a battery from a set of batteries that is available for redundancy.
- **Processor power management**
  - The clock speed and the number of instructions executed per unit time are some of the processor parameters that affect power consumption.
  - **T**he CPU can be put into different power saving modes during low processing load conditions.
  - The CPU power can be completely turned off if the machines is idle for a long time.
- **Devices power management**
  - Intelligent device management can reduce power consumption of a mobile node significantly.
  - This can be done by the operating system (OS) by selectively powering down interface devices that are not used or by putting devices into different power saving modes, depending on their usage.

1.3.10 Scalability

- Scalability is the ability of the routing protocol to scale well in a network with a large number of nodes.
- It requires minimization of control overhead & adaptation of the routing protocol to the network size.

1.3.11 Deployment Considerations

- The deployment of a commercial ad hoc wireless network has the following benefits when compared to wired networks
  - **Low cost of deployment**
    - The use of multi-hop wireless relaying eliminates the requirement of cables & maintenance in deployment of communication infrastructure.
    - The cost involved is much lower than that of wired networks.

- **Incremental deployment**
  - Deployment can be performed incrementally over geographical regions of the city.
  - The deployed part of the network starts functioning immediately after the minimum configuration is done.
- **Short deployment time**
  - Compared to wired networks, the deployment time is considerably less due to the absence of any wired links.
- **Reconfigurability**
  - The cost involved in reconfiguring a wired network covering a Metropolitan Area Network (MAN) is very high compared to that of an ad hoc wireless network covering the same service area.

1.4 Commercial Applications of Ad Hoc Networking

➢ Ad Hoc wireless networks, due to their quick and economically less demanding deployment, find applications in several areas. Some important applications are:

- Military Applications
- Collaborative and Distributed computing
- Energy Operations
- Wireless Mesh Networks
- Wireless Sensor Networks
- Hybrid Wireless Networks

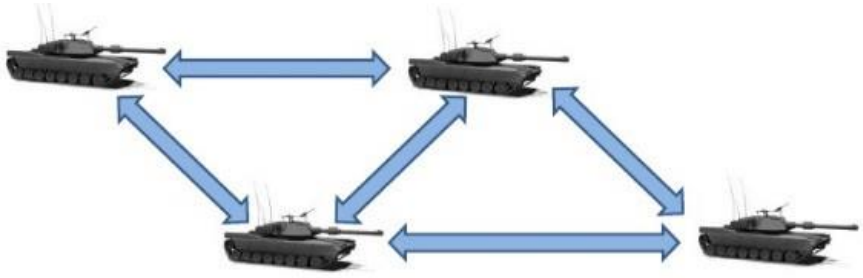
1.4.1 Military Applications

➢ Ad hoc wireless networks can be very useful in establishing communication among a group of soldiers for tactical operations.

➢ Setting up of a fixed infrastructure for communication among group of soldiers in enemy territories or in inhospitable terrains may not be possible.

➢ In such a case, adhoc wireless networks provide required communication mechanism quickly.

- The primary nature of the communication required in a military environment enforces certain important requirements on adhoc wireless networks namely, Reliability, Efficiency, Secure communication & Support for multicast routing.



Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

1.4.2 Collaborative & Distributed computing

- Adhoc wireless network helps in collaborative computing, by establishing temporary communication infrastructure for quick communication with minimal configuration among a group of people in a conference.
- In distributed file sharing application reliability is of high importance which would be provided by adhoc network.
- Other applications such as streaming of multimedia objects among participating nodes in ad hoc wireless networks require support for soft real-time communication
- Devices used for such applications could typically be laptops with add -on wireless interface cards, enhanced personal digital assistants (PDAs) or mobile devices with high processing power

1.4.3 Emergency Operations

- Ad hoc wireless networks are very useful in emergency operations such as search and rescue, crowd control and commando operations.
- The major factors that favour ad hoc wireless networks for such tasks are self-configuration of the system with minimal overhead, independent of fixed or centralised infrastructure, the freedom and flexibility of mobility, and unavailability of conventional communication infrastructure.

- In environments, where the conventional infrastructure based communication facilities are destroyed due to a war or due to natural calamities, immediate deployment of adhoc wireless networks would be a good solution for co-ordinating rescue activities.
- They require minimum initial network configuration with very little or no delay

1.4.4 Wireless Mesh Network

- Wireless mesh networks are adhoc wireless network that are formed to provide an alternate communication infrastructure for mobile or fixed nodes/users, without the spectrum reuse constraint & requirement of network planning of cellular network.(Figure 1.4)

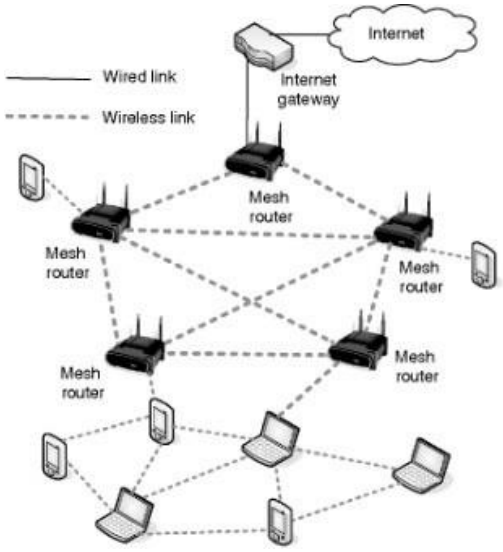


Figure 1.4 Wireless Mesh Netowrks

Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- It provides many alternate paths for a data transfer session between a source & destination, resulting in quick reconfiguration of the path when the existing path fails due to node failure.
- Since the infrastructure built is in the form of small radio relaying devices, the investment required in wireless mesh networks is much less than what is required for the cellular network counterpart.
- The possible deployment scenarios of wireless mesh networks include: residential zones, highways, business zones, important civilian regions and university campuses
- Wireless mesh networks should be capable of self-organization and maintenance.
- It operates at license-free ISM band around 2.4 GHz & 5 GHz.

- It is scaled well to provide support to large number of points.
- Major advantage is the support for a high data rate, quick & low cost of deployment, enhanced services, high scalability, easy extendibility, high availability & low cost per bit.

1.4.5 Wireless Sensor Networks

- The Wireless Sensor Networks (WSN) are special category of Adhoc wireless network that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain.(Figure 1.5)
- Sensor nodes are tiny devices that have capability of sensing physical parameters processing the data gathered, & communication to the monitoring system.

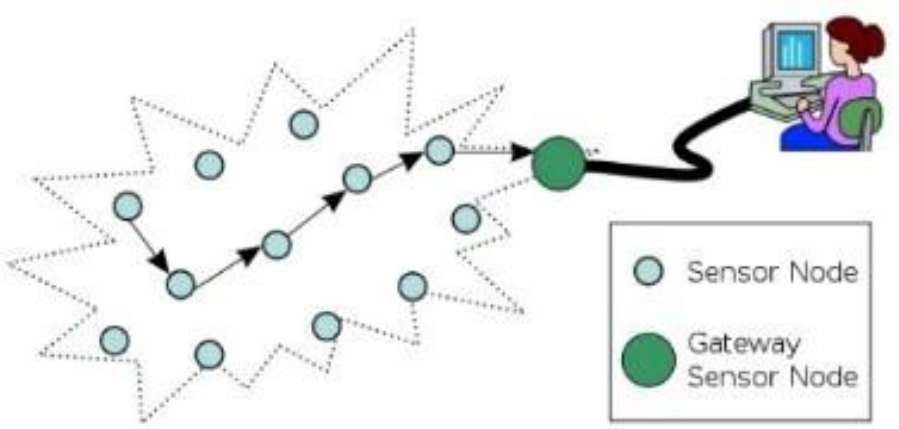


Figure 1.5 Wireless Sensor Networks

Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- The issue that make sensor network a distinct category of adhoc wireless network are the following:

Mobility of nodes

- Mobility of nodes is not a mandatory requirement in sensor networks.
- For example, the nodes used for periodic monitoring of soil properties are not required to be mobile & the nodes that are fitted on the bodies of patients in a post-surgery ward of a hospital are designed to support limited or partial mobility.
- In general, sensor networks need not in all cases be designed to support mobility of sensor nodes.

Size of the network

- The number of nodes in sensor network can be much larger than that in a typical ad hoc wireless network.

Density of deployment

- The density of nodes in a sensor network varies with the domain of application.
- For example, Military applications require high availability of the network, making redundancy a high priority.

Power constraints

- The power constraints in sensor networks are much more stringent than those in ad hoc wireless networks. This is mainly because the sensor nodes are expected to operate in harsh environmental or geographical conditions, with minimum or no human supervision and maintenance.
- In certain case, the recharging of the energy source is impossible.
- Running such a network, with nodes powered by a battery source with limited energy, demands very efficient protocol at network, data link, and physical layer.
- The power sources used in sensor networks can be classified into the following 3 categories:
  - Replenishable Power source: The power source can be replaced when the existing source is fully drained.
  - Non-replenishable Power source: The power source cannot be replenished once the network has been deployed. The replacement of sensor node is the only solution.
  - Regenerative Power source: Here, Power source employed in sensor network have the capability of regenerating power from the physical parameter under measurement.

Data / Information fusion

- Data fusion refers to the aggregation of multiple packets into one before relaying it.

- Data fusion mainly aims at reducing the bandwidth consumed by redundant headers of the packets and reducing the media access delay involved in transmitting multiple packets.

- Information fusion aims at processing the sensed data at the intermediate nodes and relaying the outcome to the monitor node.

Traffic Distribution

- The communication traffic pattern varies with the domain of application in sensor networks.
- For example, the environmental sensing application generates short periodic packets indicating the status of the environmental parameter under observation to a central monitoring station.
- This kind of traffic requires low bandwidth.
- Ad hoc wireless networks generally carry user traffic such as digitized & packetized voice stream or data traffic, which demands higher bandwidth.

1.4.6 Hybrid Wireless Networks

- One of the major application area of ad hoc wireless network is in the hybrid wireless architecture such as Multi-hop Cellular Network [MCN] & Integrated Cellular Adhoc Relay [iCAR].
- The primary concept behind cellular networks is geographical channel reuse.
- Several techniques like cell sectoring, cell resizing and multi-tier cells increase the capacity of cellular networks.
- MCNs combine the reliability & support of fixed base station of cellular network with flexibility & multi - hop relaying adhoc wireless networks.
- Major advantages are:
  - Higher capacity than cellular networks due to the better channel reuse.
  - Increased flexibility & reliability in routing.
  - Better coverage & connectivity in holes of a cell can be provided by means of multiple hops through intermediate nodes in a cell.

1.5 Ad hoc wireless Internet

- Ad hoc wireless internet extends the services of the internet to the end users over an ad hoc wireless network. It shows in figure 1.6.
- Some of the applications of ad hoc wireless internet are :
  - Wireless mesh network.
  - Provisioning of temporary internet services to major conference venues.
  - Sports venues.
  - Temporary military settlements.
  - Battlefields
  - Broadband internet services in rural regions.
- The major issues to be considered for a successful ad hoc wireless internet are the following :
  - **Gateway**
    - They are the entry points to the wired internet.
    - Generally owned & operated by a service provider.
    - They perform following tasks ,
      - ✓ Keeping track of end users.
      - ✓ Bandwidth management.
      - ✓ Load balancing.
      - ✓ Traffic shaping.
      - ✓ Packet filtering.
      - ✓ Width fairness &
      - ✓ Address, service & location discovery.
  - **Address mobility**
    - This problem is worse here as the nodes operate over multiple wireless hops.
    - Solution such as Mobile IP can provide temporary alternative.

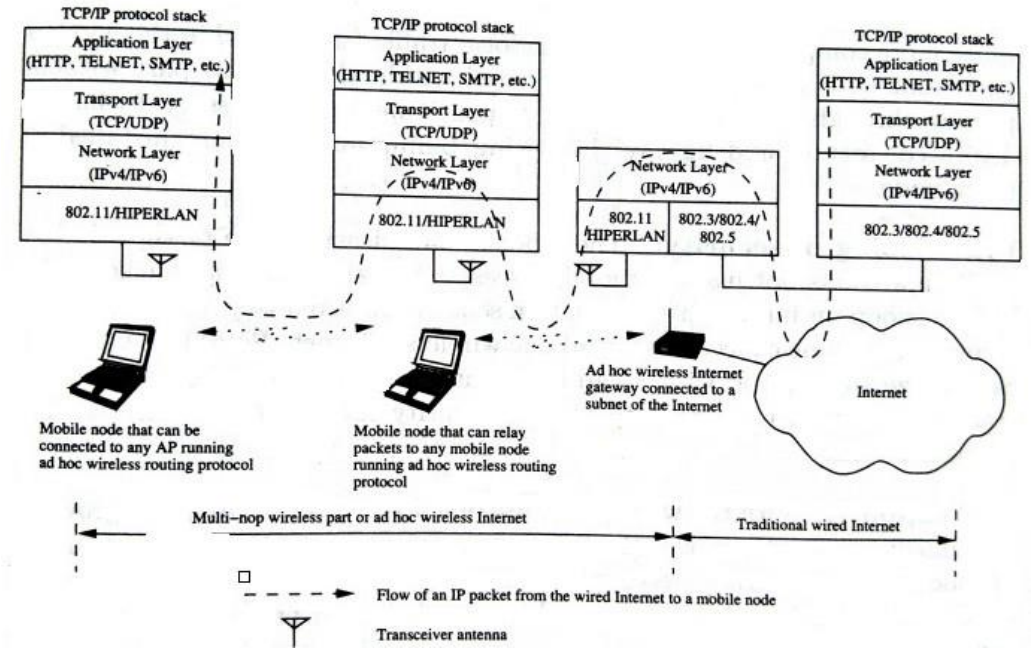


Figure 1. 6 Ad Hoc Wireless Internet

Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- **Routing**
  - It is a major problem in ad hoc wireless internet, due to dynamic topological changes, the presence of gateways, multi-hop relaying, & the hybrid character of the network.
  - Possible solution is to use separate routing protocol for the wireless part of ad hoc wireless internet.
- **Transport layer protocol**
  - Several factors are to be considered here, the major one being the state maintenance overhead at the gateway nodes.
- **Load balancing**
  - They are essential to distribute the load so as to avoid the situation where the gateway nodes become bottleneck nodes.
- **Pricing / Billing**
  - Since internet bandwidth is expensive, it becomes very important to introduce pricing/billing strategies for the ad hoc wireless internet.

- **Provisioning of security**
  - Security is a prime concern since the end users can utilize the ad hoc wireless internet infrastructure to make e-commerce transaction.
- **QoS support**
  - With the widespread use of Voice Over IP (VOIP) & growing multimedia applications over the internet, provisioning of QoS support in the ad hoc wireless internet becomes a very important issue.
- **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 network or detecting the geographical location of nodes.

1.6 Routing Protocols for Ad Hoc Wireless Networks

- Routing is the exchange of information from one station of networks to other and Protocol is the set of standard or rules to exchange data between two devices.
- An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network.
- An ad hoc wireless network consists of a set of mobile nodes (hosts) that are connected by wireless links. The network topology (the physical connectivity of the communication network) in such a network may keep changing randomly.
- Routing protocols that find a path to be followed by data packets from a source node to a destination node used in traditional wired networks cannot be directly applied in ad hoc wireless networks due to their highly dynamic topology absence of established infrastructure for centralized administration (e.g., base stations or access points), bandwidth-constrained wireless links, and resource (energy)-constrained nodes.

1.7 Issues in Designing a Routing Protocol for Ad Hoc Wireless Networks

- The major challenges that a routing protocol designed for ad hoc wireless networks faces are:
  - Mobility of nodes
  - Bandwidth Constraints
  - Error-Prone channel state
  - Hidden Terminal Problem
  - Exposed Terminal Problems
  - Resource Constraints

1.7.1 Mobility

- Network topology is highly dynamic due to movement of nodes. Hence, an ongoing session suffers frequent path breaks.
- Disruption occurs due to the movement of either intermediate nodes in the path or end nodes.
- Wired network routing protocols cannot be used in adhoc wireless networks because the nodes are here are not stationary and the convergence is very slow in wired networks.
- Mobility of nodes results in frequently changing network topologies
- Routing protocols for ad hoc wireless networks must be able to perform efficient and effective mobility management.

1.7.2 Bandwidth Constraint

- Abundant bandwidth is available in wired networks due to the advent of fiber optics and due to the exploitation of wavelength division multiplexing (WDM) technologies.
- In a wireless network, the radio band is limited, and hence the data rates it can offer are much less than what a wired network can offer.
- This requires that the routing protocols use the bandwidth optimally by keeping the overhead as low as possible.

- The limited bandwidth availability also imposes a constraint on routing protocols in maintaining the topological information.

1.7.3 Error-prone shared broadcast radio channel

- The broadcast nature of the radio channel poses a unique challenge in ad hoc wireless networks.
- The wireless links have time-varying characteristics in terms of link capacity and link-error probability.
- This requires that the adhoc wireless network routing protocol interact with the MAC layer to find alternate routes through better-quality links.
- Transmissions in ad hoc wireless networks result in collisions of data and control packets.
- Therefore, it is required that ad hoc wireless network routing protocols find paths with less congestion.

1.7.4 Hidden Terminal Problem

- The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the receiver, but are within the transmission range of the receiver.
- Collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other.

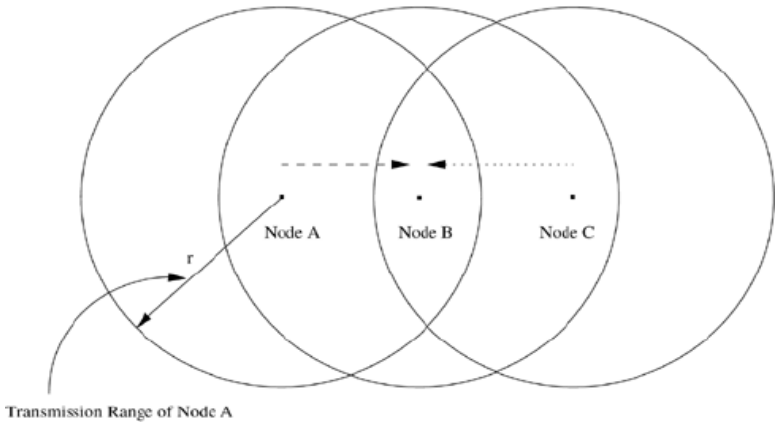


Figure 1. 7 Hidden Terminal Problem

Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- For example, consider figure 1.7. Here, if both node A and node C transmit to node B at the same time, their packets collide at node B. This is due to the fact that both node A and C are hidden from each other, as they are not within the direct transmission range of each other and hence do not know about the presence of each other.
- Solution for this problem (figure 1.8), include medium access collision avoidance (MACA)

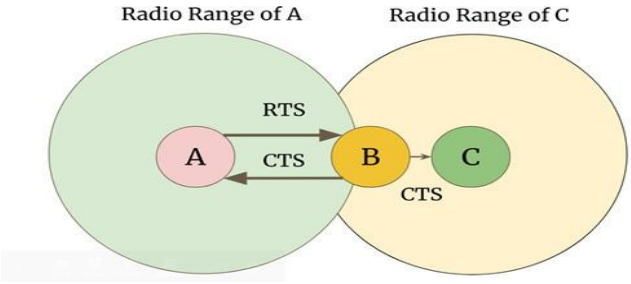


Figure 1.8 Solution for Hidden Terminal Problem

- Transmitting node first explicitly notifies all potential hidden nodes about the forthcoming transmission by means of a two way handshake control protocol called RTS-CTS protocol exchange. This may not solve the problem completely but it reduces the probability of collisions.

1.7.5 Exposed Terminal Problem

- The exposed terminal problem refers to the inability of a node which is blocked due to transmission by a nearby transmitting node to transmit to another node.
- For example, consider the figure 1.9, Here, if a transmission from node B to another node A is already in progress, node C cannot transmit to node D, as it concludes that its neighbor node B, is in transmitting mode and hence should not interfere with the on-going transmission. Thus, reusability of the radio spectrum is affected.

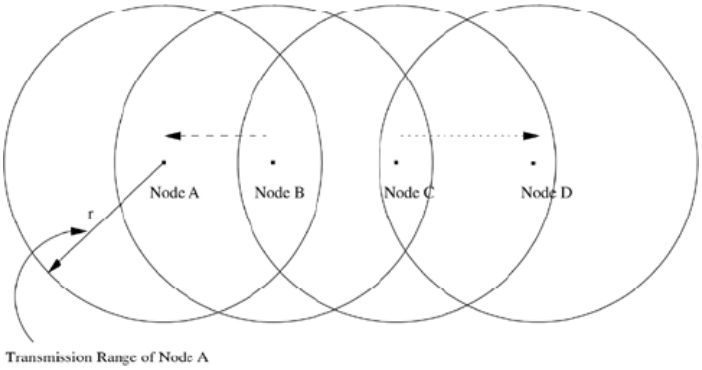


Figure 1. 9 Exposed Terminal Problem

Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- Solution for this problem, illustrated in figure 1.10. In this case, node A did not successfully receive the CTS originated by node R and hence assumes that there is no on-going transmission in the neighborhood. Since node A is hidden from node T, any attempt to originate its own RTS would result in collision of the on-going transmission between nodes T and R.

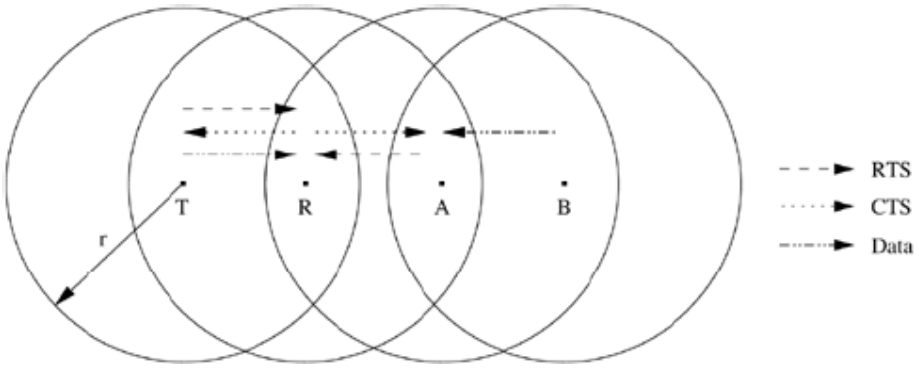


Figure 1. 10 Solution for Exposed Terminal Problem

Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

1.7.6 Resource Constraints

- Two essential and limited resources are battery life and processing power.
- Devices used in adhoc wireless networks require portability, and hence they also have size and weight constraints along with the restrictions on the power source.
- Increasing the battery power and processing ability makes the nodes bulky and less portable.

1.8 Characteristics of an Ideal Routing Protocol for Ad Hoc Wireless Networks

- A routing protocol for ad hoc wireless networks should have the following characteristics:
  - It must be fully distributed as centralized routing involves high control overhead and hence is not scalable.
  - It must be adaptive to frequent topology changes caused by the mobility of nodes.
  - Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes, that is, minimum connection setup time is desired.
  - It must be localized, as global state maintenance involves a huge state propagation control overhead.
  - It must be loop-free and free from state routes.

- The number of packet collisions must be kept to a minimum by limiting the number of broadcasts made by each node. The transmissions should be reliable to reduce message loss and to prevent the occurrence of state routes.
- It must converge to optimal routes once the network topology becomes stable. The convergence must be quick.
- It must optimally use scarce resources such as bandwidth, computing power, memory, and battery power.
- Every node in the network should try to store information regarding the stable local topology only. Changes in remote parts of the network must not cause updates in the topology information maintained by the node.
- It should be able to provide a certain level of quality of service (QoS) as demanded by the applications, and should also offer support for time-sensitive traffic.

1.9 Classifications of Routing Protocols

➢ Routing protocols for ad hoc wireless networks can be classified into several types based on different criteria. A classification tree is shown in Figure 1.11.

➢ The routing protocol for adhoc wireless networks can be broadly classified into 4 categories based on

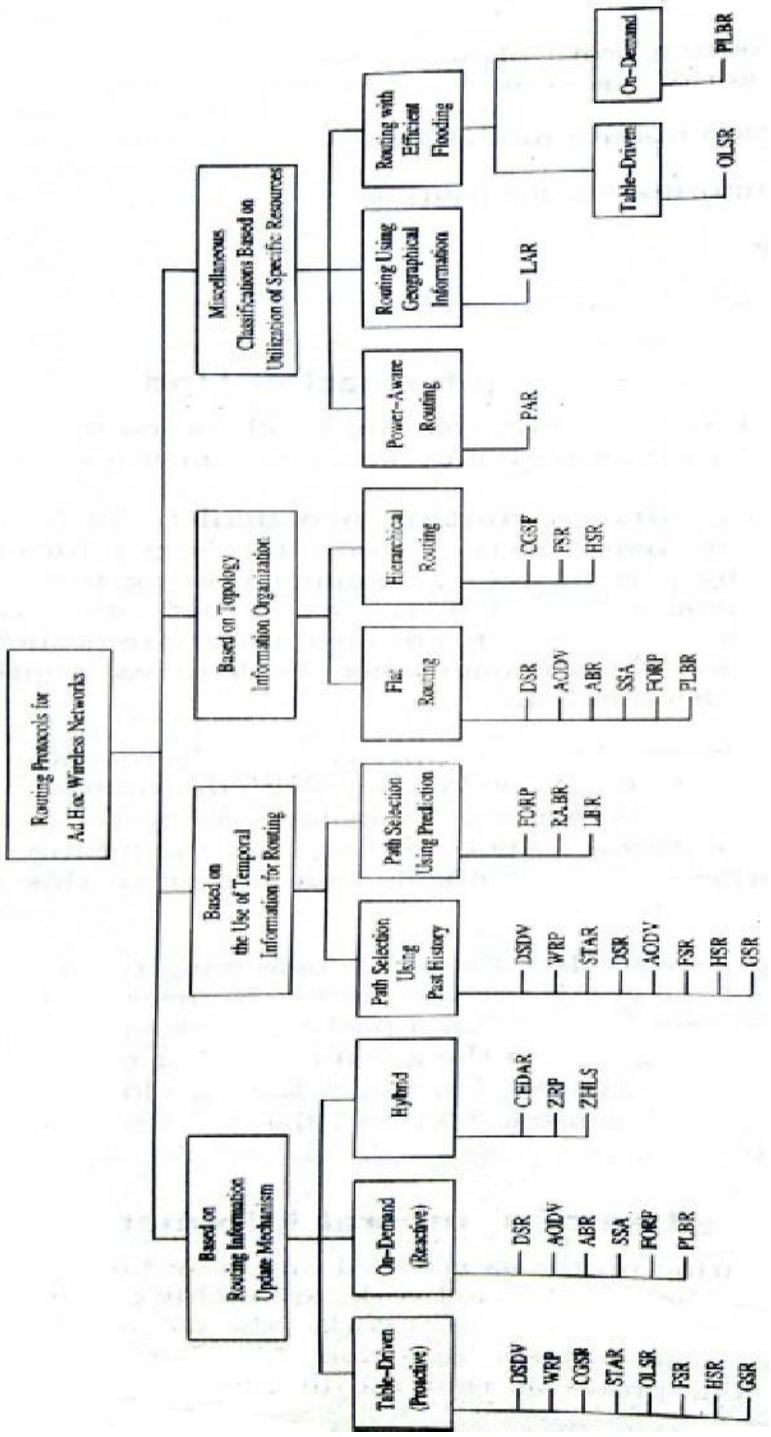
- Routing information update mechanism.
- Use of temporal information for routing
- Routing topology
- Utilization of specific resources.

1.9.1 Based on the routing information update mechanism

➢ Ad hoc wireless network routing protocols can be classified into 3 major categories based on the routing information update mechanism. They are:

- **Proactive or table-driven routing protocols**
  - Every node maintains the network topology information in the form of routing tables by periodically exchanging routing information.
  - Routing information is generally flooded in the whole network.
  - Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains.
- **Reactive or on-demand routing protocols**
  - Do not maintain the network topology information.
  - Obtain the necessary path when it is required, by using a connection establishment process.

Figure 1.11 Classification of Sensor Network Protocols



Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- **Hybrid routing protocols**
  - Combine the best features of the above two categories.
  - Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node.
  - For routing within this zone, a table-driven approach is used.
  - For nodes that are located beyond this zone, an on-demand approach is used.

1.9.2 Based on the use of temporal information for routing

➢ The protocols that fall under this category can be further classified into two types

- **Routing protocols using past temporal information**
  - Use information about the past status of the links or the status of links at the time of routing to make routing decisions.
- **Routing protocols that use future temporal information**
  - Use information about the about the expected future status of the wireless links to make approximate routing decisions.
  - Apart from the lifetime of wireless links, the future status information also includes information regarding the lifetime of the node, prediction of location, and prediction of link availability.

1.9.3 Based on the Routing Topology

➢ Ad hoc wireless networks, due to their relatively smaller number of nodes, can make use of either a flat topology or a hierarchical topology for routing.

- **Flat topology routing protocols**
  - Make use of a flat addressing scheme similar to the one used in IEEE 802.3 LANs.
  - It assumes the presence of a globally unique addressing mechanism for nodes in an ad hoc wireless network.

- **Hierarchical topology routing protocols**
  - Make use of a logical hierarchy in the network and an associated addressing scheme.
  - The hierarchy could be based on geographical information or it could be based on hop distance.

1.9.4 Based on the utilization of specific resources

- **Power-aware routing**
  - Aims at minimizing the consumption of a very important resource in the ad hoc wireless networks: the battery power.
  - The routing decisions are based on minimizing the power consumption either logically or globally in the network.
- **Geographical information assisted routing**
  - Improves the performance of routing and reduces the control overhead by effectively utilizing the geographical information available.

1.10 Table Driven Routing Protocols

- These protocols are extensions of the wired network routing protocols.
- They maintain the global topology information in the form of tables at every node.
- Tables are updated frequently in order to maintain consistent and accurate network state information.
- Example:
  - **Destination Sequenced Distance Vector Routing Protocol (DSDV)**
  - **Wireless Routing Protocol (WRP)**
  - **Source-Tree Adaptive Routing Protocol (STAR)**
  - **Cluster-head Gateway Switch Routing Protocol (CGSR)**

1.10.1 Destination Sequenced Distance Vector Routing Protocol (DSDV)

- Destination Sequenced Distance Vector (DSDV) is a hop-by-hop vector routing protocol requiring each node to periodically broadcast routing updates. Destination Sequenced Distance Vector Routing protocol is a modified version of Bellman Ford Algorithm and is based upon the concepts of Distance Vector Routing.
- In Distance Vector Routing (DVR), each node broadcasts a table containing its distance from nodes which are directly connected and based upon this, other nodes broadcasts the updated routing. Those nodes which are unreachable directly are labelled as "infinite".
- But, this updation of routing tables keeps on happening and an infinite loop is generated which is commonly known as Count-To-Infinityproblem.
- To overcome this problem of count to infinity by generating sequence number in the routing table, every time the routing table is updated. The process of DSDV is same as that of Distance Vector Routing but an extra attribute of sequence number is added.

Destination Sequenced Distance Vector Routing: Concept

- DSDV protocol uses and maintains a single table only, for every node individually. The table contains the following attributes.
  - Routing Table: It contains the distance of a node from all the neighbouring nodes along with the sequence number (SEQ No means the time at which table is updated).

Node	Destination	Next Hop	Distance	SEQ No

Table: 1.1 DSDV Table Format

- This table is updated on every step and ensures that each node broadcast as well as receives correct information about all the nodes including their distance and sequence number.

Destination Sequenced Distance Vector Routing Protocol: Working

- In DSDV, nodes broadcasts their routing tables to immediate neighbors with the sequence number. Every time any broadcasting occurs, the sequence number is also updated along with distances of nodes.

- Consider a network (Figure 1.12) of 3 nodes having distances of "1" on each of the edges respectively. Below mentioned steps will let you know how DSDV works and routing tables are updated.

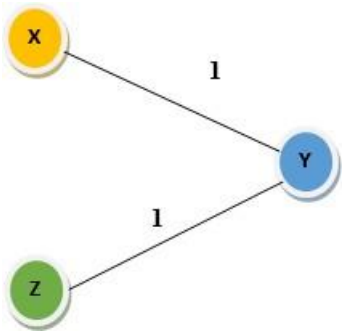


Figure 1.12 Sample Network of DSDV

Step-1: Draw separate tables for all the nodes "X", "Y" & " Z" along with the distance and sequence number.

For X:

Source	Destination	Next Hop	Cost	SEQ No
X	X	X	0	100-X
X	Y	Y	1	200-Y
X	Z	Y	2	300-Z

For Y:

Source	Destination	Next Hop	Cost	SEQ No
Y	X	X	1	100-X
Y	Y	Y	0	200-Y
Y	Z	Y	1	300-Z

For Z:

Source	Destination	Next Hop	Cost	SEQ No
Z	X	Y	2	100-X
Z	Y	Y	1	200-Y
Z	Z	Z	0	300-Z

- If "Y" wants to broadcast the routing table. Then updated routing tables of all the nodes in the network will look like as depicted in the below tables where Bold marked cell denotes the change in sequence number.

For X:

Source	Destination	Next Hop	Cost	SEQ No
X	X	X	0	100-X
X	Y	Y	1	**210-Y**
X	Z	Y	2	300-Z

For Y:

Source	Destination	Next Hop	Cost	SEQ No
Y	X	X	1	100-X
Y	Y	Y	0	**210-Y**
Y	Z	Z	1	300-Z

For Z:

Source	Destination	Next Hop	Cost	SEQ No
Z	X	Y	2	100-X
Z	Y	Y	1	**210-Y**
Z	Z	Z	0	300-Z

Advantages

- Less delay involved in the route setup process.
- Mechanism of incremental update with sequence number tags makes the existing wired network protocols adaptable to ad hoc wireless networks.
- The updates are propagated throughout the network in order to maintain an up-to-date view of the network topology at all nodes.

Disadvantages

- The updates due to broken links lead to a heavy control overhead during high mobility.
- Even a small network with high mobility or a large network with low mobility can completely choke the available bandwidth.
- Suffers from excessive control overhead.
- In order to obtain information about a particular destination node, a node has to wait for a table update message initiated by the same destination node.

1.11 On–Demand Routing protocols

➢ In table-driven protocols, each node maintain up-to-date routing information to all the nodes in the network where in **on-demand protocols** a node finds the route to a destination when it desires to send packets to the destination.

1.11.1 Ad hoc On–Demand Distance Vector Routing (AODV)

- This protocol is an example of reactive routing protocol which does not maintain routes but build the routes as per requirements. That means, Route is established only when it is required by a source node for transmitting data packets.
- AODV is used to overcome the drawbacks of Dynamic Source Routing Protocol and Distance Vector Routing Protocol i.e. Dynamic Source Routing is capable of maintaining information of the routes between source and destination which makes it slow. If the network is very large containing a number of routes from source to destination, it is difficult for the data packets header to hold whole information of the routes.
- In case of Dynamic Source Routing, multiple routes are present for sending a packet from source to destination but AODV overcomes this disadvantage too.
- In AODV, along with routing tables of every node, two counters including Sequence Number (SEQ NO) and broadcast ID are maintained also.
- The destination IP is already known to which data is to be transferred from source. Thus, the destination Sequence Number (SEQ NO) helps to determine an updated path from source to destination.
- Along with these counters, Route Request (RREQ) and Route Response (RRESP) packets are used in which RREQ is responsible for discovering of route from source to destination and RRESP sends back the route information response to its source.

Ad-Hoc On - Demand Distance Vector Routing Protocol: Working

- In Ad-Hoc On-Demand Distance Vector Routing, the source node and destination nodes IP addresses are already known.
- The goal is to identify, discover and maintain the optimal route between source and destination node in order to send/receive data packets and informative.
- Each node comprises of a routing table along with below mentioned format of Route Request (RREQ) packet.
- RREQ {Destination IP, Destination Sequence Number, Source IP, Source Sequence Number, Hop Count}.

- Consider a network (Figure 1.13) containing 5 nodes that are “X”, “Y”, “Z”,”T”,”D” present at unit distance from each other, where “X” being the source node and “D” being the destination node.

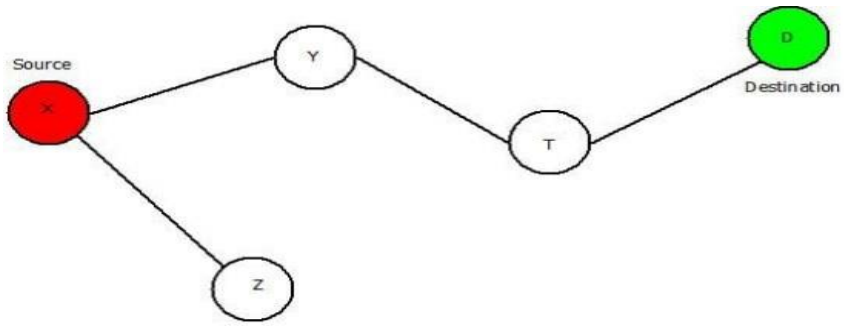


Figure 1.13 Sample Network of AODV

Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- The IP addresses of source node “X” and destination node “D” is already known. Below mentioned steps will let you know how AODV works and concept of Route Request (REREQ) and Route Response (RRESP) is used.(Figure 1.14)

  - **Step 1:** Source node “X” will send Route Request i.e. RREQ packet to its neighbours “Y” and “Z”.

  - **Step 2:** Node “Y” & “Z” will check for route and will respond using RRESP packet back to source “X”. Here in this case “Z” is the last node but the destination. It will send the RREQ packet to “X” stating “Route Not Found”. But node “Y” will send RRESP packet stating “Route Found” and it will further broadcast the RRESP to node “T”.

  - **Step 3:** Now the field of net hop in the RREQ format will be updated, Node “T” will send back the “Route Found” message to Node “Y” and will update the next hop field further.

  - **Step 4:** Then Node “T” will broadcast and RREQ packet to Node “D”, which is the destination and the next hop field is further updated. Then it will send RRES packet to “T” which will further be sent back to the source node “X” via node “Y” and Node “T” resulting in generation of an optimal path. The updated network would be:

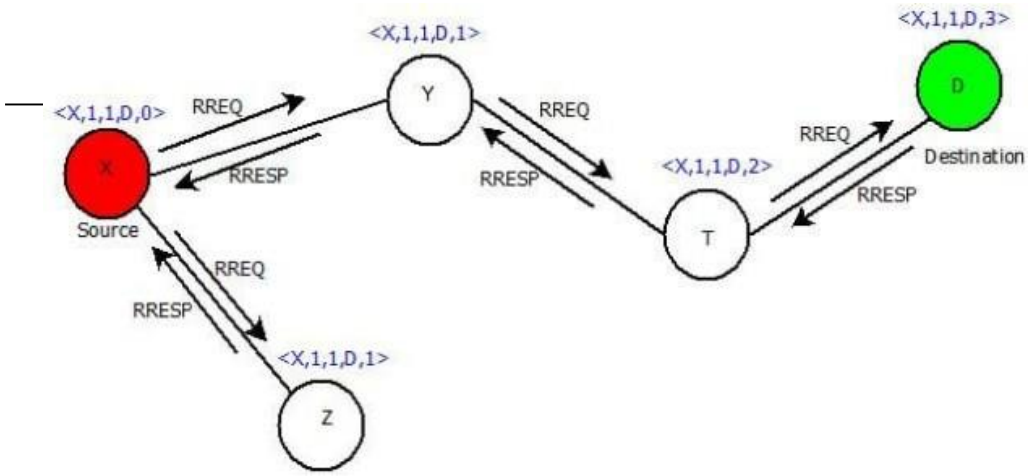


Figure 1.14 Example of AODV Network

Source **:** Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

Advantages

- Dynamic networks can be handled easily.
- No loop generation.

Disadvantages

- A delayed protocol because of its route discovery process.
- High bandwidth requirement.