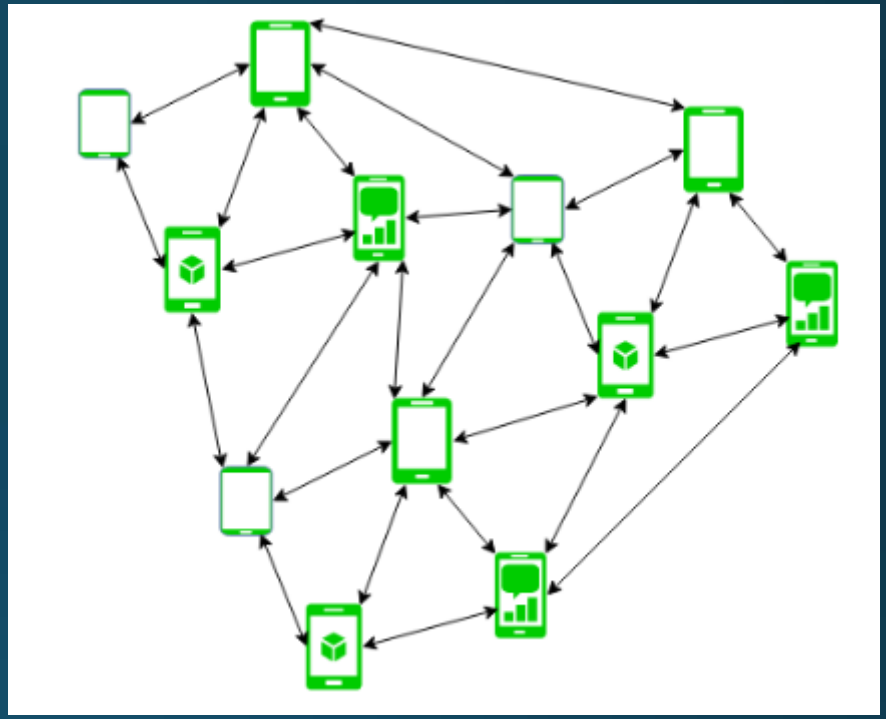
Unit 4-Part1

MANETS

Content

- Mobile Ad-hoc networks
- Characteristics and applications
- Coverage and connectivity problems
- Routing in MANETs.



MANET

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

Characteristics

- **Dynamic Topologies:**
  Network topology which is typically multihop may change randomly and rapidly with time, it can form unidirectional or bi-directional links.
- **Bandwidth constrained, variable capacity links:**
  Wireless links usually have lower reliability, efficiency, stability, and capacity as compared to a wired network
- **Autonomous Behavior:**
  Each node can act as a host and router, which shows its autonomous behavior.
- **Energy Constrained Operation:**
  As nodes rely on batteries or other exhaustible means for their energy. Mobile nodes are characterized by less memory, power, and lightweight features.

Characteristics

- **Limited Security:**
  Wireless networks are more prone to security threats. A centralized firewall is absent due to the distributed nature of the operation for security, routing, and host configuration.
- **Less Human Intervention:**
  They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature.

MANETS-PROS and CONS

Pros:

- Separation from central network administration.
- Each node can play both the roles ie. of router and host showing autonomous nature.
- Self-configuring and self-healing nodes do not require human intervention.
- Highly scalable and suits the expansion of more network hub.

Cons:

- Resources are limited due to various constraints like noise, interference conditions, etc.
- Lack of authorization facilities.
- More prone to attacks due to limited physical security.
- High latency i.e. There is a huge delay in the transfer of data between two sleeping nodes.

Types of MANETS

- **Vehicular Ad hoc Network (VANETs) –**
  Enable effective communication with another vehicle or with the roadside equipments. Intelligent vehicular ad hoc networks(InVANETs) deals with another vehicle or with roadside equipments.

- **Smart Phone Ad hoc Network (SPANC) –**
  To create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. Here peers can join or leave the network without destroying it.

- **Internet based Mobile Ad hoc Network (iMANETs) –**
  It supports internet protocols such as TCP/UDP and IP. To link mobile nodes and establish routes distributed and automatically.

Types of MANETS

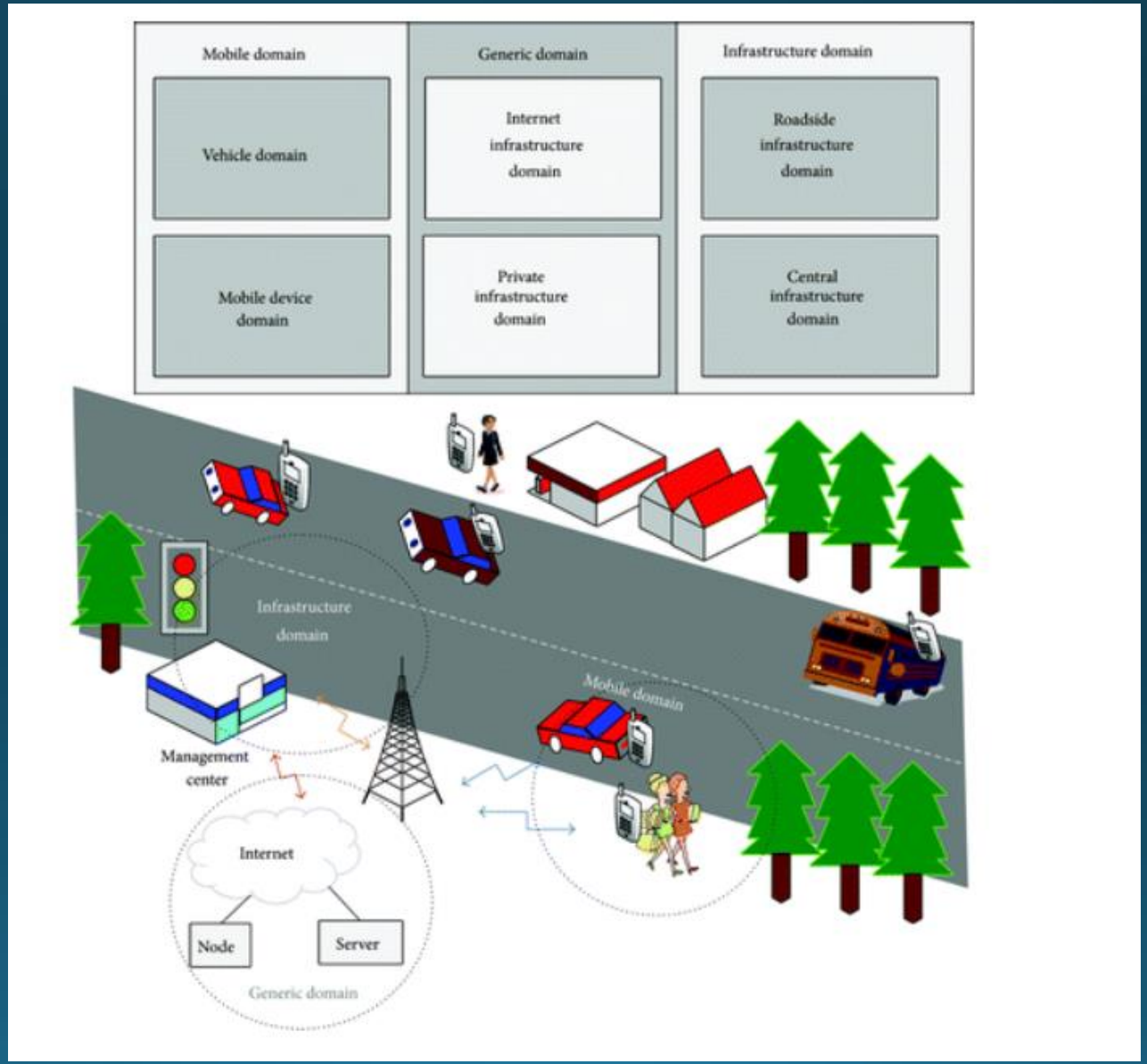
- **Hub-Spoke MANET:**
  Multiple sub MANET's may be connected in hub-spoke VPN to create a geographically distributed MANET. Normal Ad-hoc routing algorithm does not apply directly.

- **Military or Tactical MANETs –**
  This is used by the military units. Emphasis on data rate, real-time demand, fast re-routing during mobility, security, radio range, etc.

- **Flying Ad hoc Network (FANETs) –**
  This is composed of unmanned aerial vehicles (commonly known as drones). Provides links to remote areas and mobility.

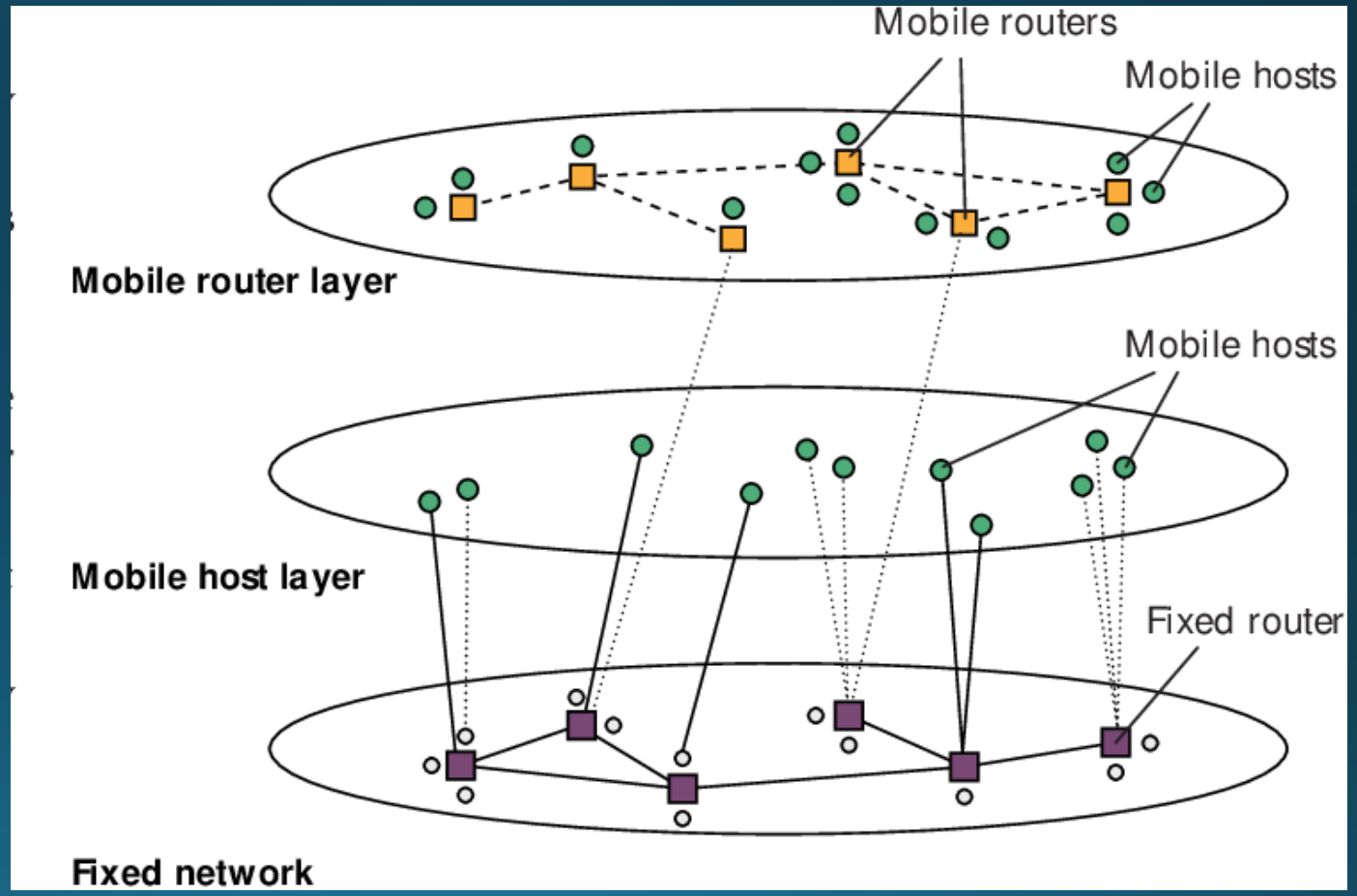
VANET

- The mobile domain consists of two parts: the vehicle domain and the mobile device domain.
- The vehicle domain comprises all kinds of vehicles such as cars and buses.
- The mobile device domain comprises all kinds of portable devices like personal navigation devices and smartphones.



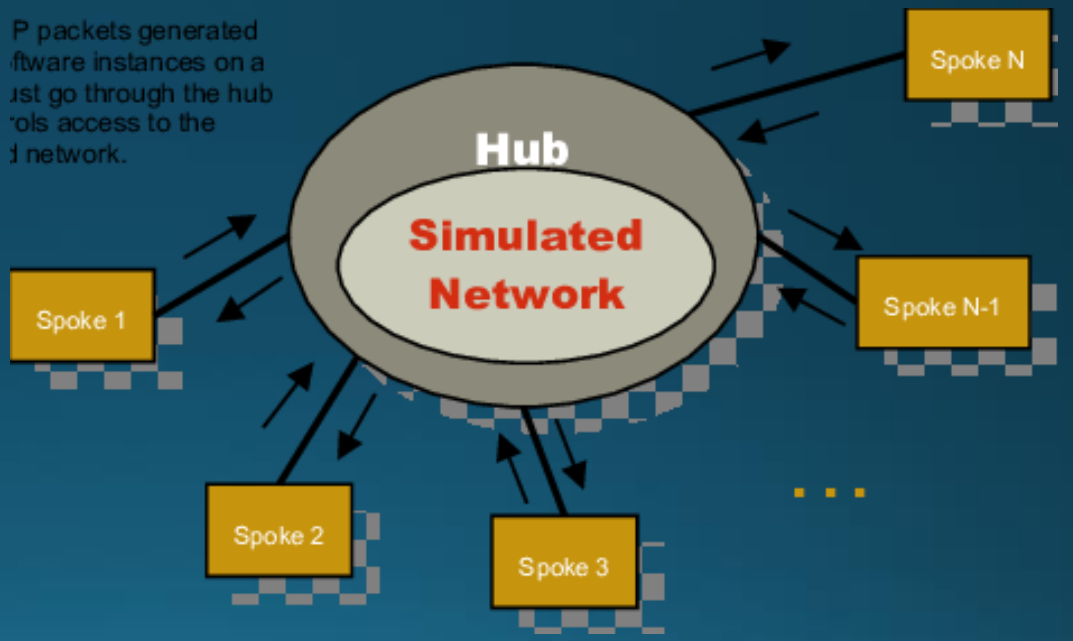
iMANETS

Internet based mobile ad hoc network (IMANET) is **an emerging technique that combines a wired network (e.g. Internet) and a mobile ad hoc network (manet) for developing a ubiquitous communication infrastructure**.

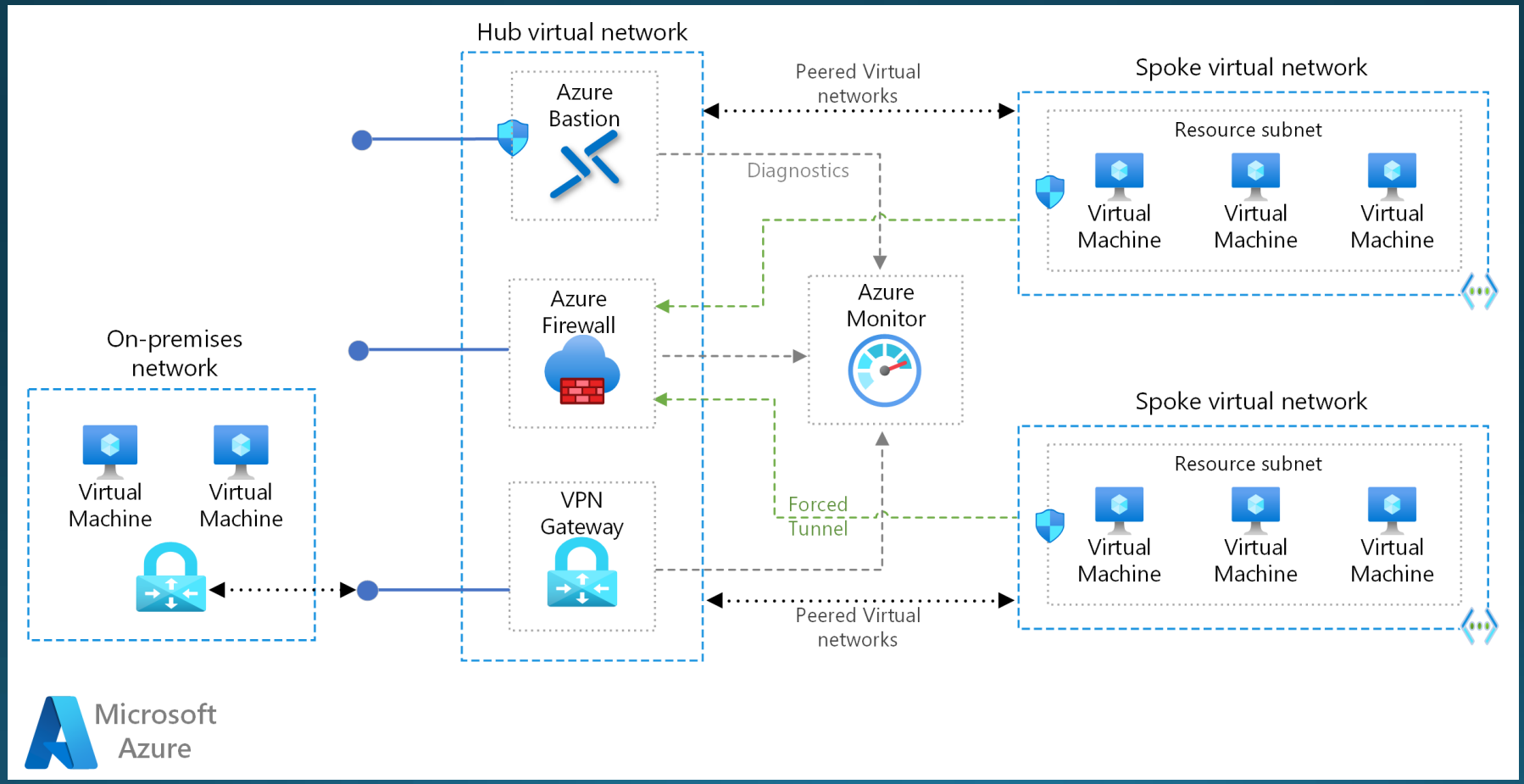


HUB-SPOKE MANETS

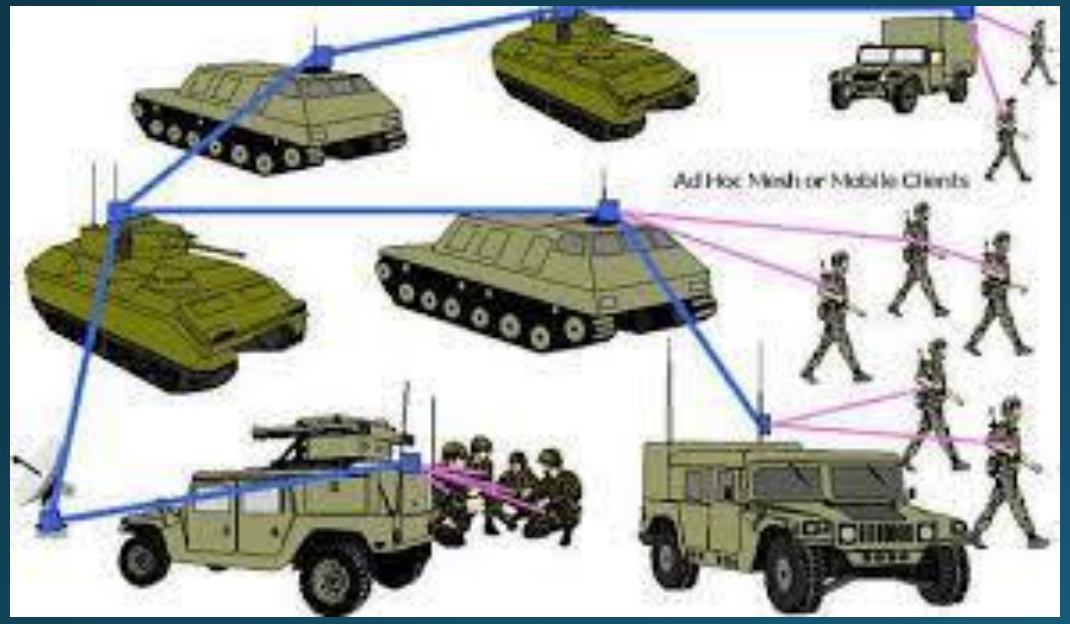
The communication is not made between pairs of applications, but between each application (spoke) and the central hub [1]. The broker functionalities include routing and messages transformation to the receiver spoke.



Azure with Hub-Spoke Architecture

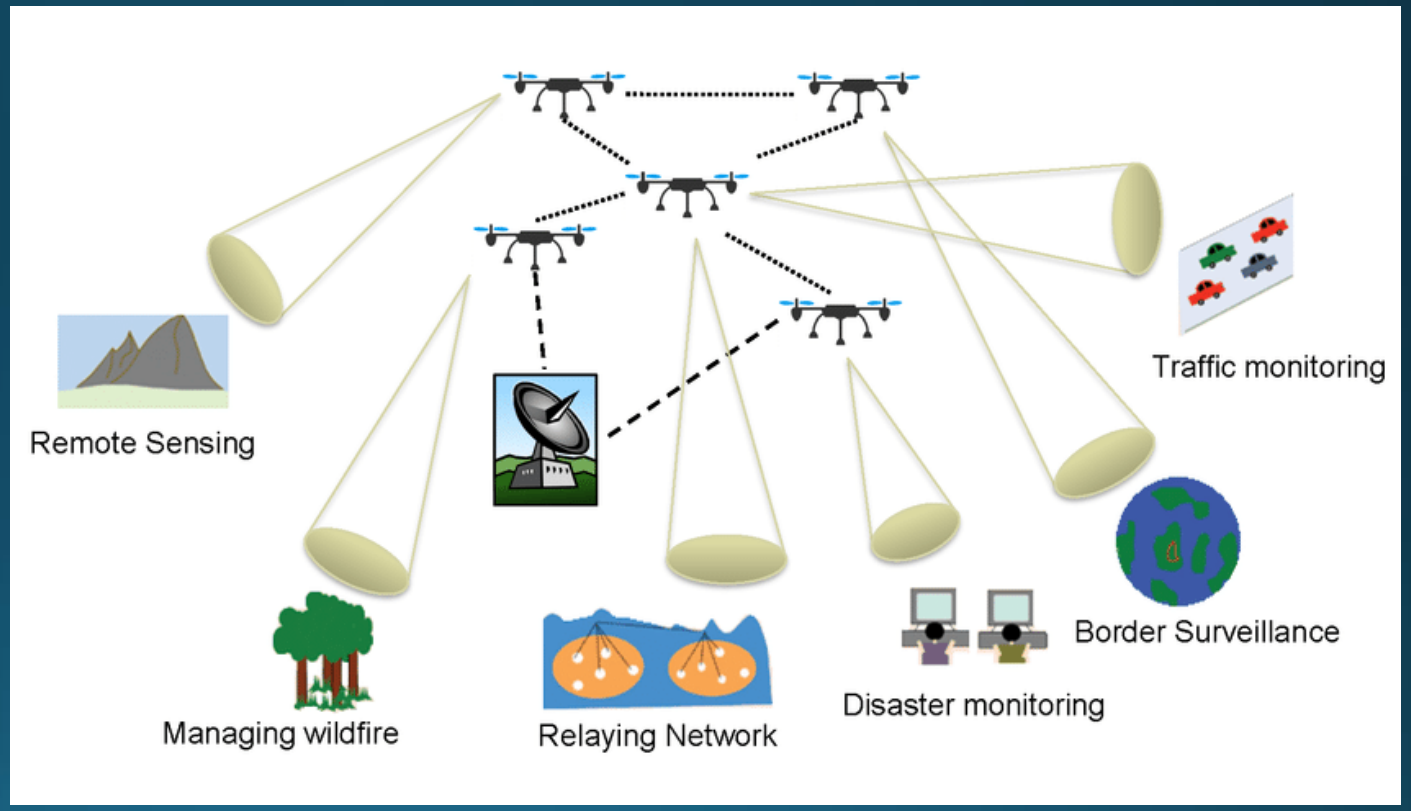


Tactical Manets



FANETS

- A Flying Ad hoc Networks (FANETs) is **such kind of network that consists of a group of small UAVs connected in ad-hoc manner, which are integrated into a team to achieve high level goals.**



Applications

- Military field: Ad-Hoc networking can permit army to exploit benefit of conventional network expertise for preserving any info network among vehicles, armed forces, and headquarters of information.
- Cooperative work: To facilitate the commercial settings, necessity for concerted computing is very significant external to office atmosphere and surroundings as compared to inner environment. People want getting outside meetings for exchanging the information plus cooperating with each other regarding any assigned task.
- Confined level: Ad-Hoc networks are able to freely associate with immediate, in addition momentary hypermedia network by means of laptop computers for sharing the info with all the contestants' e.g. classroom and conference. Additional valid and confined level application may be in domestic network where these devices can interconnect straight in exchanging the information.
- PAN and Bluetooth: A PAN is localized and tiny range network whose devices are generally belong to a specified individual. Limited-range MANET such as Bluetooth can make simpler the exchange among several portable devices like a laptop, and a cell phone.

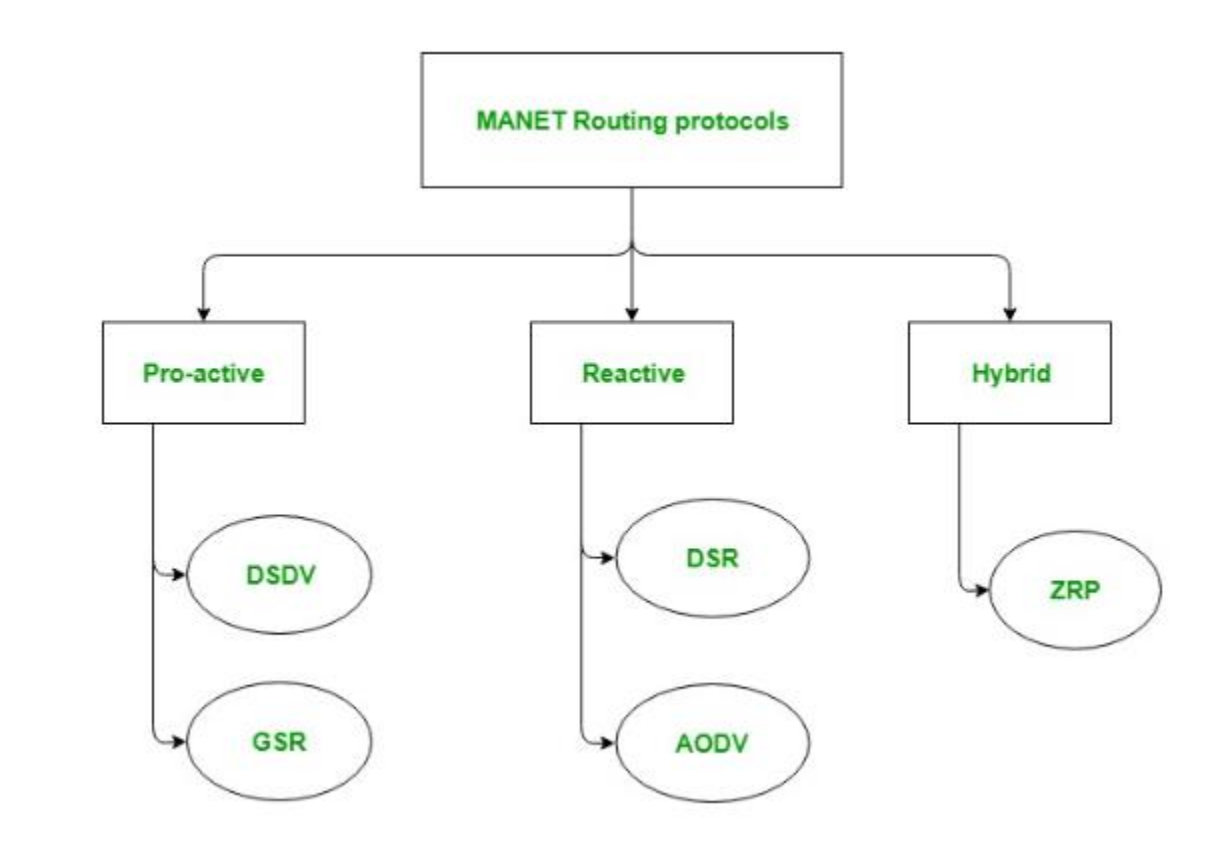
Applications

- Business Sector: Ad-hoc network could be used for rescuing and emergency processes for adversity assistance struggles, for instance, in flood, fire or earthquake. Emergency saving procedures should take place where damaged and non-existing transmissions structure and quick preparation of a transmission network is required .
- Sensor Networks: managing home appliances with MANETs in both the case like nearby and distantly. Tracking of objects like creatures. Weather sensing related activities.
- Backup Services: liberation operations, tragedy recovery, diagnosis or status or record handing in hospitals, replacement of stationary infrastructure.
- Educational sector: arrangement of communications facilities for computer-generated conference rooms or classrooms or laboratories [10] .

Routing in MANETS

- nodes do not know the topology of their network, instead they have to discover it by their own as the topology in the ad-hoc network is dynamic topology.
- The basic rules is that a new node whenever enters into an ad-hoc network, must announce its arrival and presence and should also listen to similar announcement broadcasts made by other mobile nodes.

Types of Routing



ProActive

- These are also known as table-driven routing protocols. Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes.
- Since the topology in the mobile ad-hoc network is dynamic, these routing tables are updated periodically as and when the network topology changes.
- It has a limitation that it doesn’t work well for the large networks as the entries in the routing table becomes too large since they need to maintain the route information to all possible nodes.

Reactive Routing

- These are also known as on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed.
- The process of route discovery occurs by flooding the route request packets throughout the mobile network.
- It consists of two major phases namely, route discovery and route maintenance.

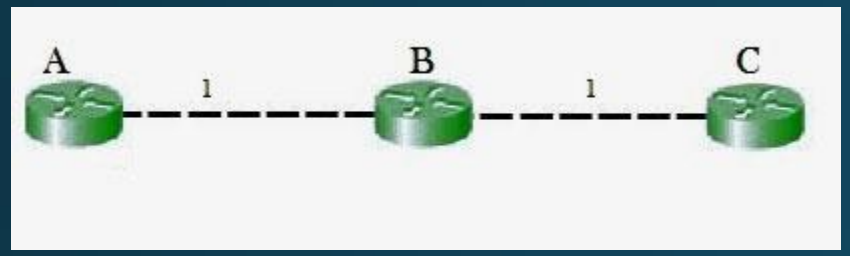
Hybrid Routing Protocol

- It basically combines the advantages of both, reactive and pro-active routing protocols. These protocols are adaptive in nature and adapts according to the zone and position of the source and destination mobile nodes. One of the most popular hybrid routing protocol is **Zone Routing Protocol (ZRP)**.
- The whole network is divided into different zones and then the position of source and destination mobile node is observed. If the source and destination mobile nodes are present in the same zone, then proactive routing is used for the transmission of the data packets between them. And if the source and destination mobile nodes are present in different zones, then reactive routing is used for the transmission of the data packets between them.

Proactive- DSDV protocol

- Distance vector routing protocol was not suited for mobile ad-hoc networks due to count-to-infinity problem.
- Hence, as a solution Destination Sequenced Distance Vector Routing Protocol (DSDV) came into picture.
  Destination sequence number is added with every routing entry in the routing table maintained by each node.
- A node will include the new update in the table only if the entry consists of the new updated route to the destination with higher sequence number.

Count to infinity Problem



- B will know that it can get to C at a cost of 1, and A will know that it can get to C via B at a cost of 2.
- if the link between B and C is disconnected, then B will know that it can no longer get to C via that link and will remove it from its table.
- Before it can send any updates it's possible that it will receive an update from A which will be advertising that it can get to C at a cost of 2.
- B can get to A at a cost of 1, so it will update a route to C via A at a cost of 3. A will then receive updates from B later and update its cost to 4.
- They will then go on feeding each other bad information toward infinity which is called as **Count to Infinity problem**.

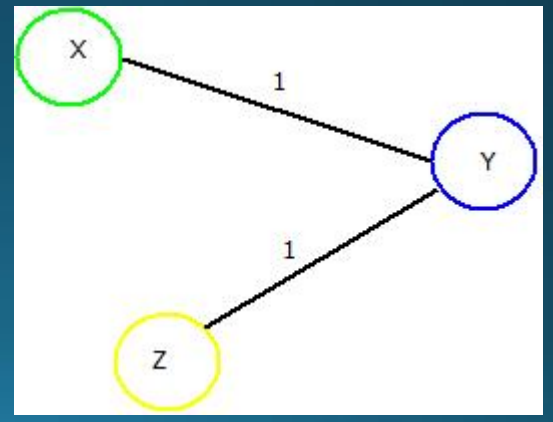
DSDV

- 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 neighboring nodes along with the sequence number(SEQ No means the time at which table is updated).
- This image describes the header format of Destination Sequenced Distance Vector Routing protocol
- Destination Sequenced Distance Vector Routing : 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.

DSDV 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 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.



Routing tables at each node

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 red 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

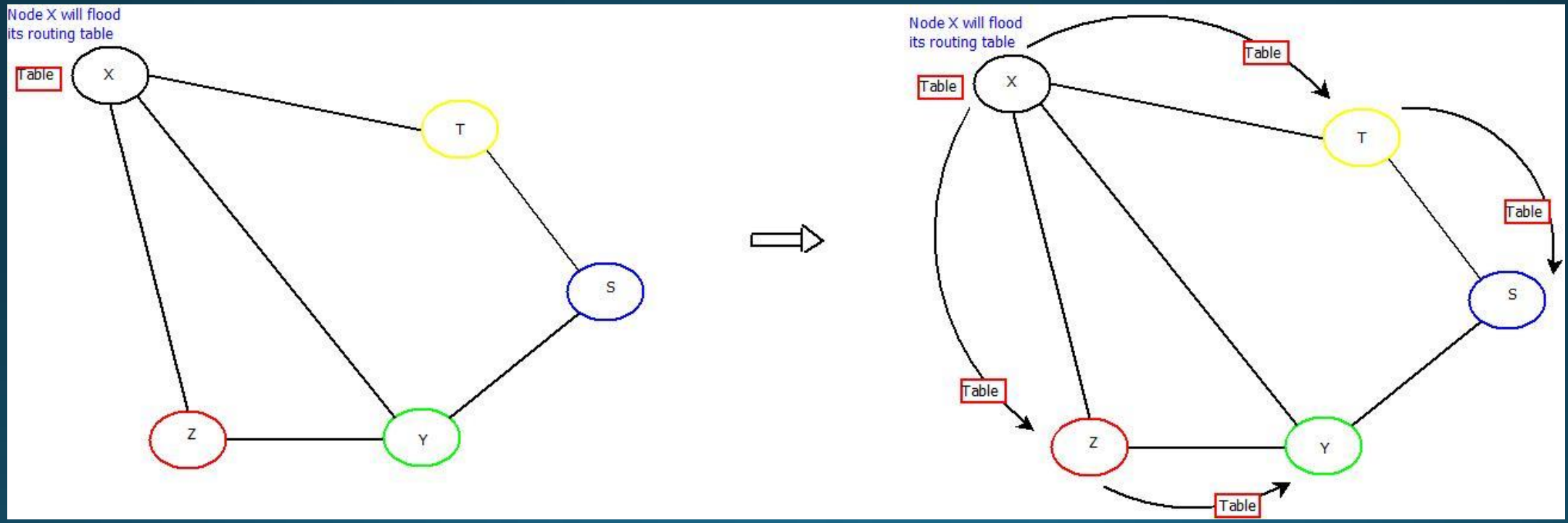
Pros and Cons

- Advantages : Destination Sequenced Distance Vector Routing Protocol
- Can't be implemented commercially or on larger scale.
- Efficient results will be produced if applied on small networks.
- Disadvantages : Destination Sequenced Distance Vector Routing Protocol
- Slower protocol processing time.
- Less bandwidth.
- Not suitable for large number of networks which are dynamic in nature.

GSR

- Global State Routing is based upon the fundamental concepts of link state routing.
- In Link State Routing(LSR), one of the node floods out a single routing table information to its neighbors and those neighbors floods out that table to further nodes. This process continue to take place until the routing table is received by all the nodes throughout the network.
- But in case of Global State Routing, the routing table of a particular node is broadcast-ed to its immediate neighbors only. Then initial tables of those neighboring nodes are updated. These updated tables are further broadcast one by one and this process continue to take place until all the nodes broadcasts their tables to each node in the network.
-

GSR working

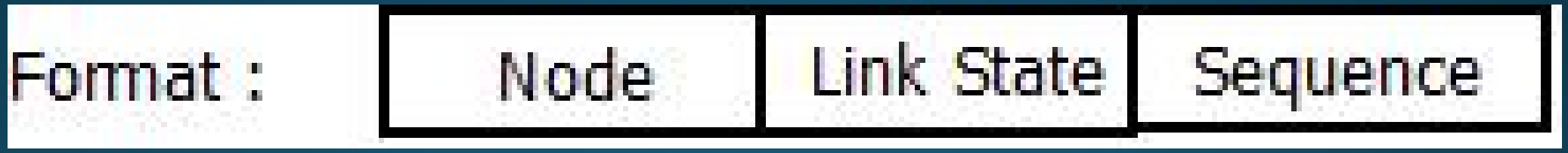

Node X will flood
its routing table
Table
X
T
S
Z
Y
Node X will flood
its routing table
Table
Table
X
T
Table
S
Table
Z
Y
Table

GSR concept

- GSR protocol uses and maintains three tables for every node individually. These tables are:

1. Distance Table : This table contains the distance of a node from all the nodes in network.

2. Topology Table : This table contains the information of Link state data along with the sequence number which can be used to determine when the information is updated last.



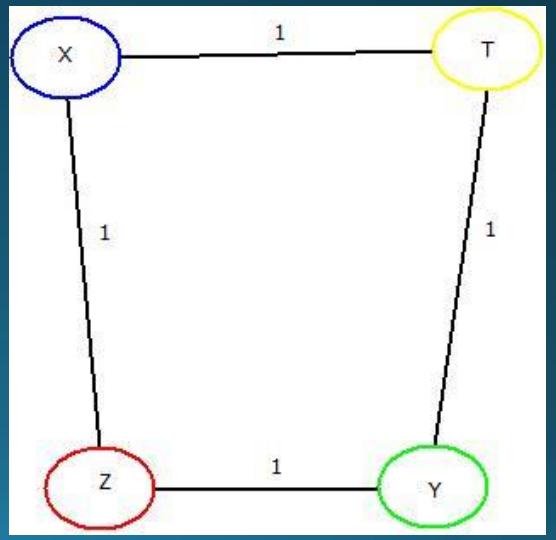
GSR concept

3. Next Hop Table : Next hop table will contain the information about the immediate neighbor of a particular node.

These tables are updated on every step and ensures that each node receives correct information about all the nodes including their distances.

Example

- GSR broadcasts the routing tables to its immediate neighbors rather than flooding it to all the nodes as Link State Routing protocol does.
- Consider a network of 4 nodes having a distance of "1" on each of its edge. Below mentioned steps will let you know how GSR works and how its routing tables are updated.



GSR

- For Node "X" : Firstly three tables as mentioned above will be maintained which includes distance table, Topology table and Next hop tables. This same process will be done for rest of the nodes too.

Topology Table

Node	Link State	Sequence
X	{}	----
Y	{}	----
Z	{}	----
T	{}	----

Next Hop Table

Node	Link State
X	X
Y	-1
Z	-1
T	-1

Distance Table

Node	Distance
X	0
Y	Infinite
Z	Infinite
T	Infinite

GSR

- Secondly, broadcasting of all the tables will be done to all the immediate neighbors of “X” i.e. “Y” and “Z”.
- These tables are updated at “X”, “Y” & “T” nodes respectively.
- Same will be done for node “Y”. After first updation from “X”, node “Y” will broadcast the tables to its immediate neighbors i.e. “X” & “T” and those tables will be updated accordingly. This will be done for “T” & “Z” also.
- Once done, all the nodes “X”, “Y”, “Z” & “T” will be having the updated routing tables containing distances from each, with the help of which an optimal path can be chosen if data needs to be transferred from one node to other.

GSR updated tables

Distance Table

Node	Distance
X	0
Y	1
Z	1
T	∞

Next Hop Table

Node	Next
X	X
Y	Y
Z	Z
T	-1

Topology Table

Node	Link State	SEQ Number
X	{Y,Z}	1
Y	{}	----
Z	{X,T}	----
T	{}	----

Node X

Distance Table

Node	Distance
X	1
Y	0
Z	∞
T	1

Next Hop Table

Node	Next
X	X
Y	Y
Z	-1
T	T

Topology Table

Node	Link State	SEQ Number
X	{}	----
Y	{X,T}	1
Z	{}	----
T	{}	----

Node Y

Distance Table

Node	Distance
X	1
Y	∞
Z	0
T	1

Next Hop Table

Node	Next
X	X
Y	-1
Z	-Z
T	T

Topology Table

Node	Link State	SEQ Number
X	{}	----
Y	{}	----
Z	{X,T}	1
T	{}	----

Node Z

GSR

- Now, broadcasting of topology tables of "X" will take place to its neighbour i.e. "Y" & "Z" and updated tables will be like as mentioned below.

For Y:

Distance Table

Node	Distance
X	1
Y	0
Z	2
T	1

Next Hop Table

Node	Next
X	X
Y	Y
Z	X
T	T

Topology Table

Node	Link State	SEQ Number
X	{Y,Z}	1
Y	{X,T}	1
Z	{}	----
T	{}	----

For Z:

Distance Table

Node	Distance
X	1
Y	2
Z	0
T	1

Next Hop Table

Node	Next
X	X
Y	X
Z	Z
T	T

Topology Table

Node	Link State	SEQ Number
X	{Y,Z}	1
Y	{}	----
Z	{X,T}	1
T	{}	----

Similarly, these tables are further updated with topology tables of "Y", "Z" & "T" as done in case of "X.

Pros and Cons

Advantages : Global State Routing Protocol

- Higher accuracy of GSR in generating optimal path as compared to LSR.
- Broadcasting reduces error rate as compare to flooding used in LSR.

Disadvantages : Global State Routing Protocol

- Large bandwidth consumption.
- Higher operational cost.
- Large Message size resulting in more time consumption.

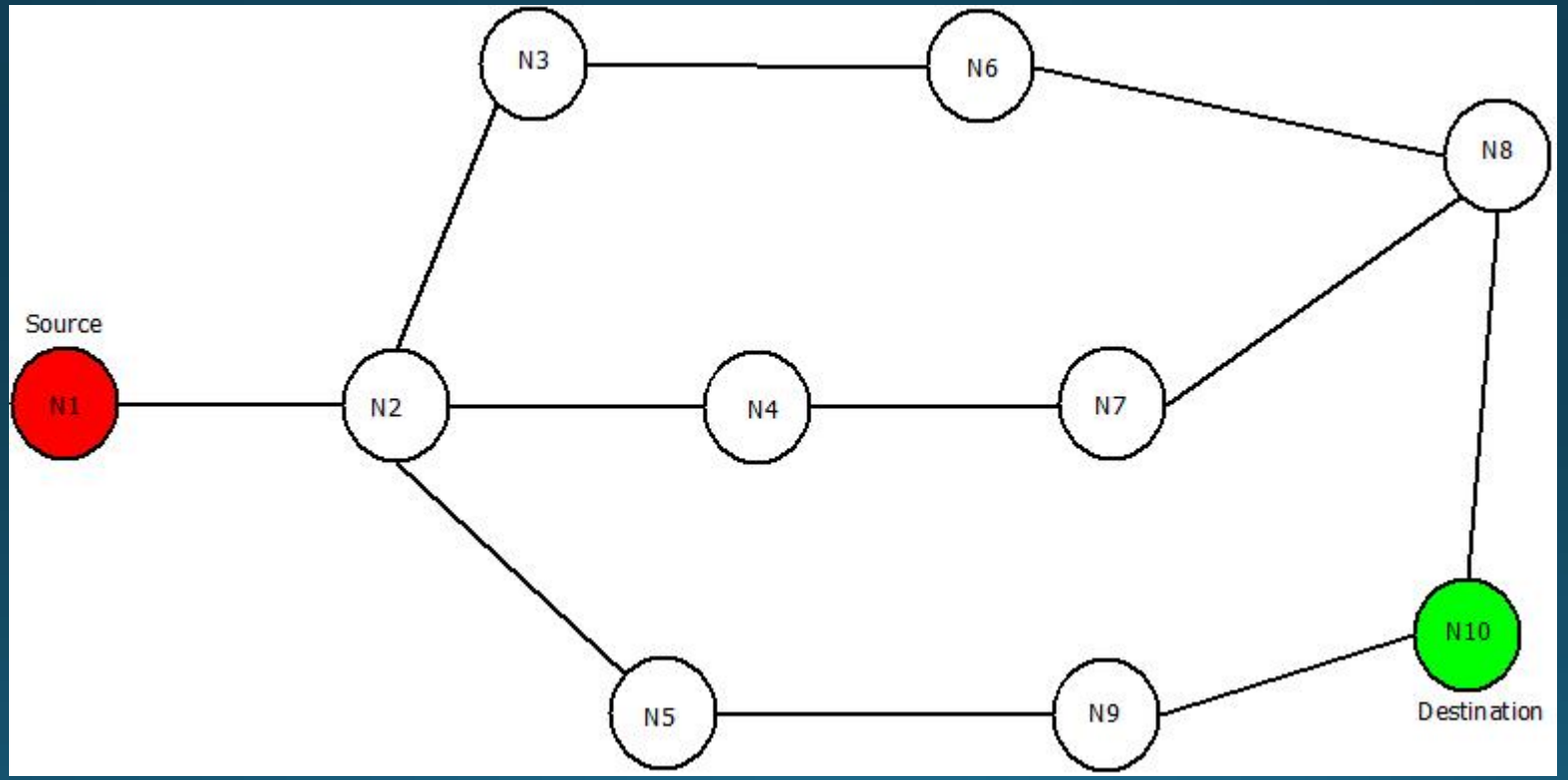
Reactive Protocols –Dynamic Source Routing

- Dynamic Source Routing (DSR) comes under the reactive routing protocol category, as it is capable of discovering the route from source to destination only when required and needed.
- Dynamic Source Routing protocol uses a process called "Route Discovery Mechanism" that is capable of discovering the route for data packets from source node to destination nodes using intermediate nodes.
- As like proactive routing protocols such as Global State Routing an Dynamic Sequence Distance Vector Routing no separate table is maintained.
- The major change in DSR as compare to GSR and DSDV is, in DSDV after asking a requirement of route from source to destination, path via intermediate nodes is checked for its length.
- Then a "Re-Request" packet is sent back from destination to source via the smallest route possible in the whole network. The "Re-Request" packet does contains its unique ID also.
- This process of separately sending a "Re-Request" packet from destination to source makes it easier for the sender to send the data packets on fixed path rather than sending it on multiple paths to check for total distance.

DSR working

- Dynamic Source Routing does broadcast the route to its neighbors but does not floods the information. It only trace the route by calculating the total distance or by calculating the number of nodes present in between source and destination nodes.
- Consider a network containing 10 nodes where node N1 being the source and node N10 being the destination nodes. Below mentioned steps will let you know how DSR protocol works and how Re-Request packet is transmitted through the network.

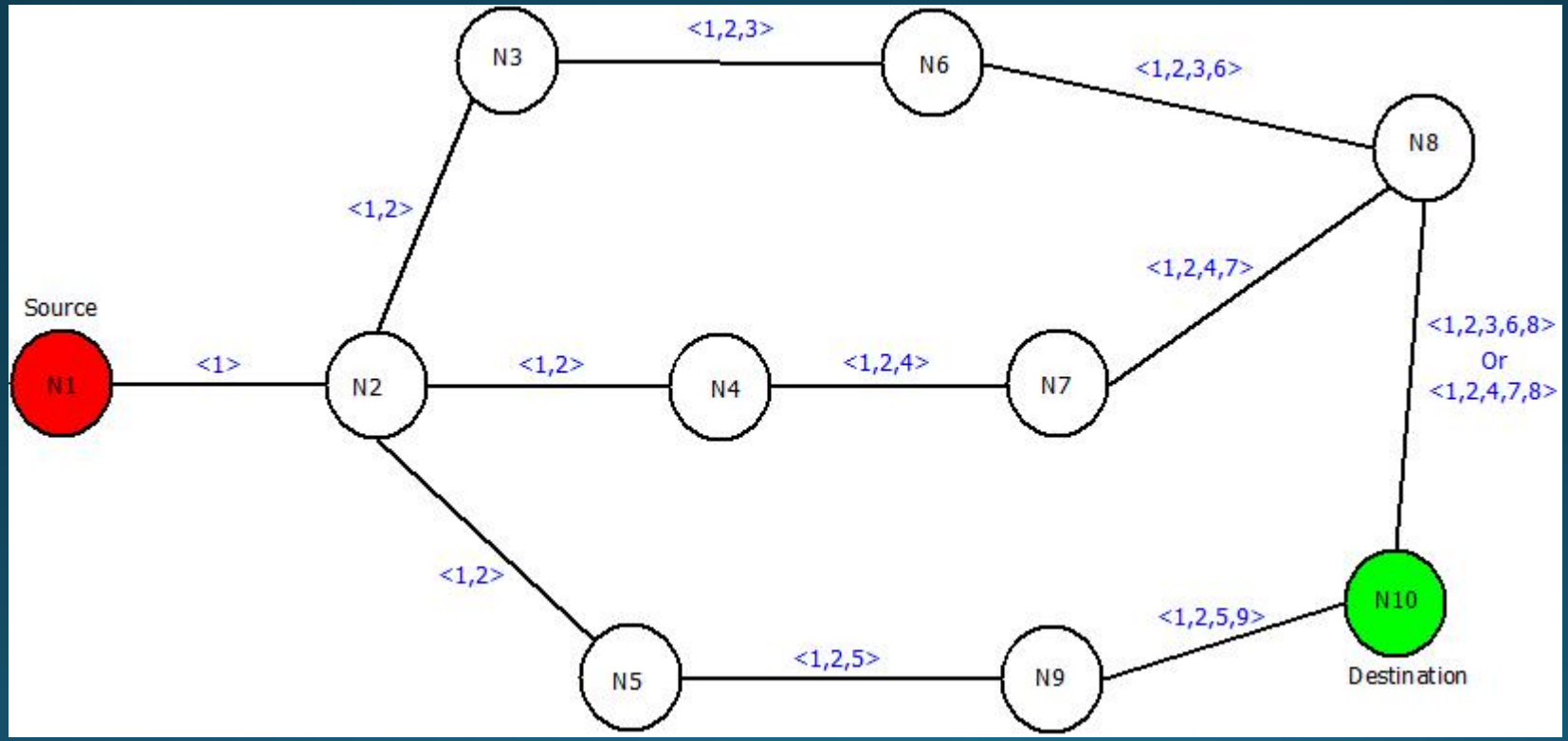
Example



DSR

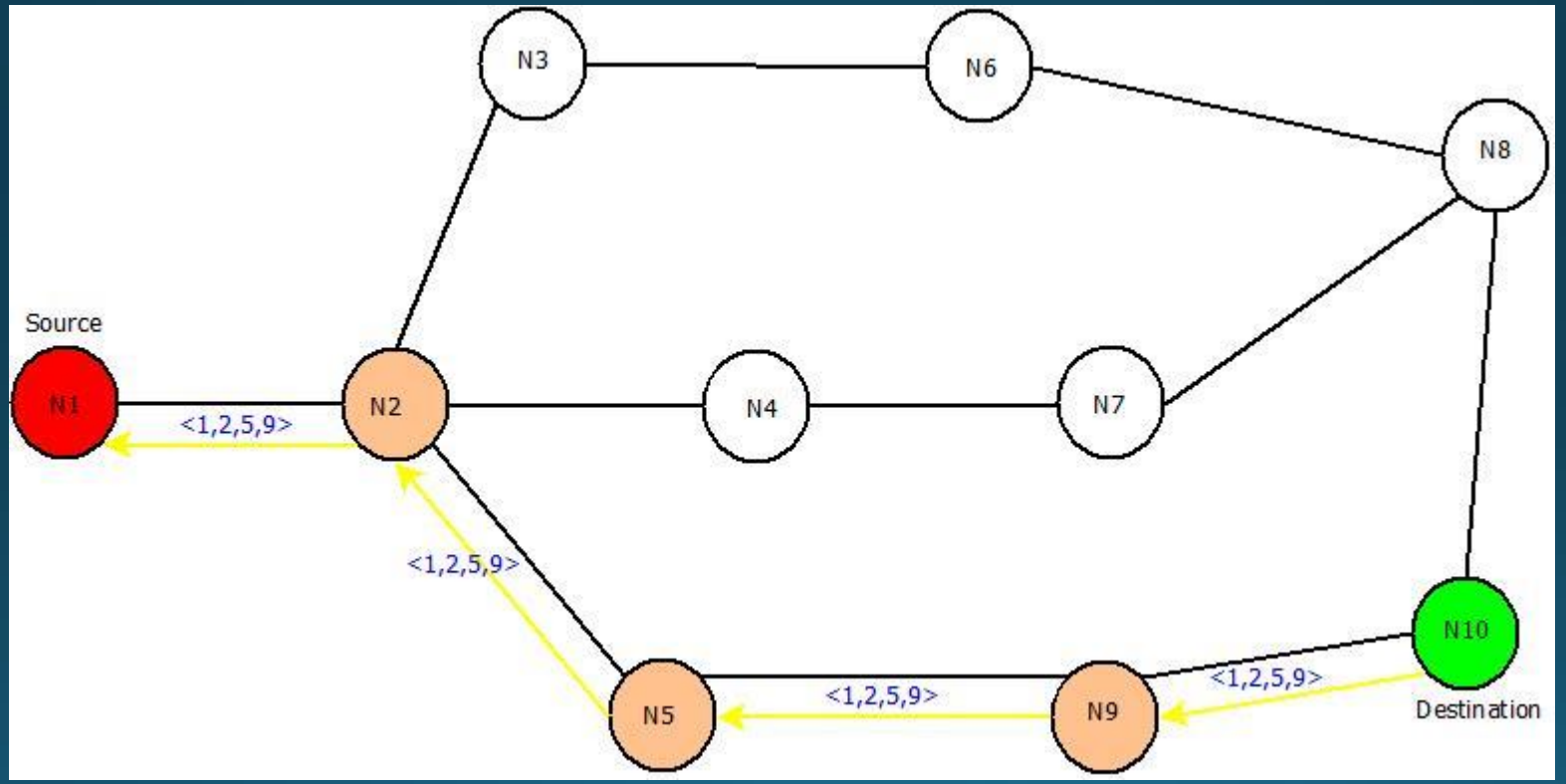
- Step 1: Start from source node N1 and broadcast the information about it to its neighbors i.e. in this case the route information is “<1>”, because of its one-to-one link between node N1 and N2.
- Step 2: Broadcast previous route information to neighbors of node N2 i.e. to node N3, N4, N5. The new route will remain same “<1,2>” in all the cases.
- Step 3: Take node N3 and broadcast previous route(<1,2>) to next neighboring nodes i.e. node N6. New route till node N6 will be “<1,2,3>” and same process can be done for other nodes i.e. Node N4 and N5.
- Step 4 : Further, broadcast the new routes i.e. <1,2,3,6> , <1,2,4> , <1,2,5> to nodes N8, N7 & N9 respectively.
- Step 5: Repeat the above steps until destination node is reached via all the routes.
- The updated routes will be as:

DSR-Updated Network



DSR

- After this, “Re-Request” packet will be sent in backward direction i.e. from destination node “N10” to source node “N1”. It will trace the shortest route by counting the number of nodes from route discovered in previous steps.
- The three possible routes are :
- Route 1: <1,2,3,6,8>
- Route 2: <1,2,4,7,8>
- Route 3: <1,2,5,9>
- Route 3 i.e. "<1,2,5,9>” will be chosen as it contains the least number of nodes and hence it will definitely be the shortest path and then data can be transferred accordingly.
- The Re-Request Packet route can be located as:


N3
N6
N8
Source
N1
<1,2,5,9>
N2
N4
N7
<1,2,5,9>
N10
N5
<1,2,5,9>
N9
<1,2,5,9>
Destination

Pros and Cons

Advantages : Dynamic Source Routing Protocol

- A perfect route is discovered always.
- Highly efficient.
- Low bandwidth Consumption.

Disadvantages : Dynamic Source Routing Protocol

- If the route gets broke, data transmission cannot happen.
- Time taking algorithm-Slow.
- If network is large , then it is impossible for the data packets header to hold whole information of the routes.

Ad-Hoc On Demand Distance Vector Routing Protocol(AODV)

- Another type of reactive routing protocol which does not maintain routes but build the routes as per requirements is Ad-Hoc On Demand Distance Vector Routing Protocol.
- 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.

AODV

- 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.

AODV 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 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.

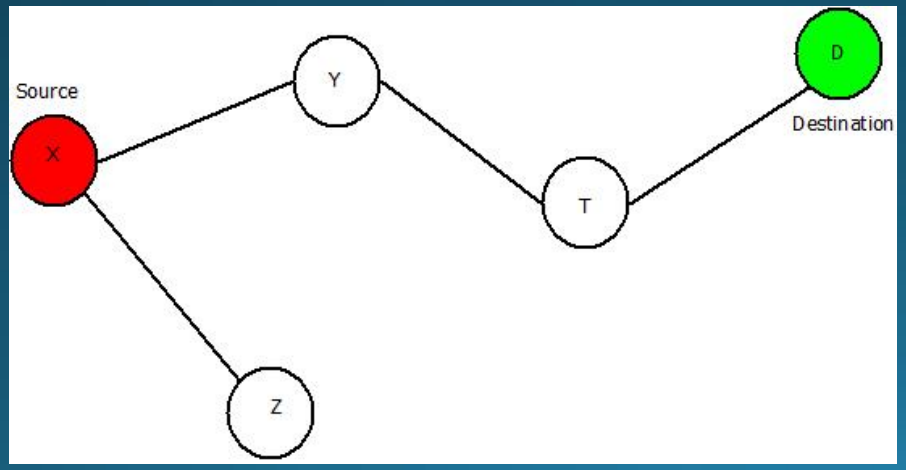
The IP addresses of source node "X" and destination node "D" is already known. Below mentioned steps will let you know how AODV works and concept of Route Request(REREQ) and Route Response(RRESP) is used.

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

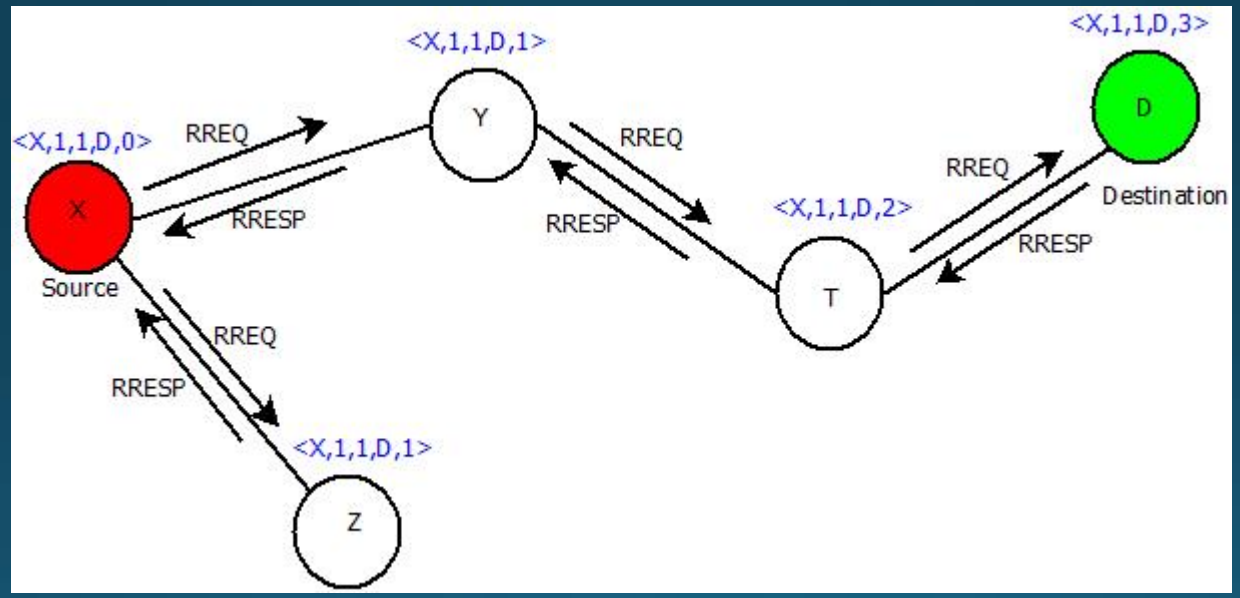
Step 2: Node "Y" & "Z" will check for route and will respond using RRESP packet back to source "X". Here in this case "Z" is the last node but the destination. It will send the RREQ packet to "X" stating "Route Not Found". But node "Y" will send RRESP packet stating "Route Found" and it will further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



Adhoc on demand DSR network

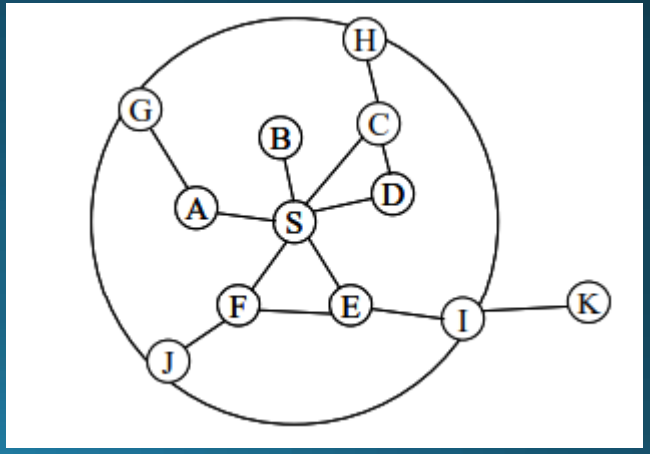


Pros and Cons

- Advantages : Ad-Hoc On Demand Distance Vector Routing Protocol
- Dynamic networks can be handled easily.
- No loop generation.
- Disadvantages : Ad-Hoc On Demand Distance Vector Routing Protocol
- A delayed protocol because of its route discovery process.
- High bandwidth requirement.

Hybrid - **Zone Routing Protocol (ZRP).**

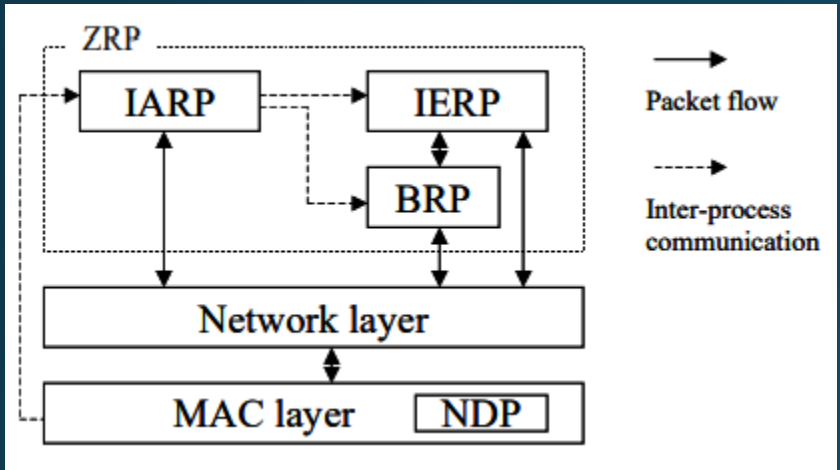
- The Zone Routing Protocol, as its name implies, is based on the concept of zones.
- A routing zone is defined for each node separately, and the zones of neighboring nodes overlap.
- The routing zone has a radius ρ expressed in hops. The zone thus includes the nodes, whose distance from the node in question is at most ρ hops.
- zone is defined in hops, not as a physical distance.



ZRP

- The nodes of a zone are divided into peripheral nodes and interior nodes.
- Peripheral nodes are nodes whose minimum distance to the central node is exactly equal to the zone radius

ZRP Architecture



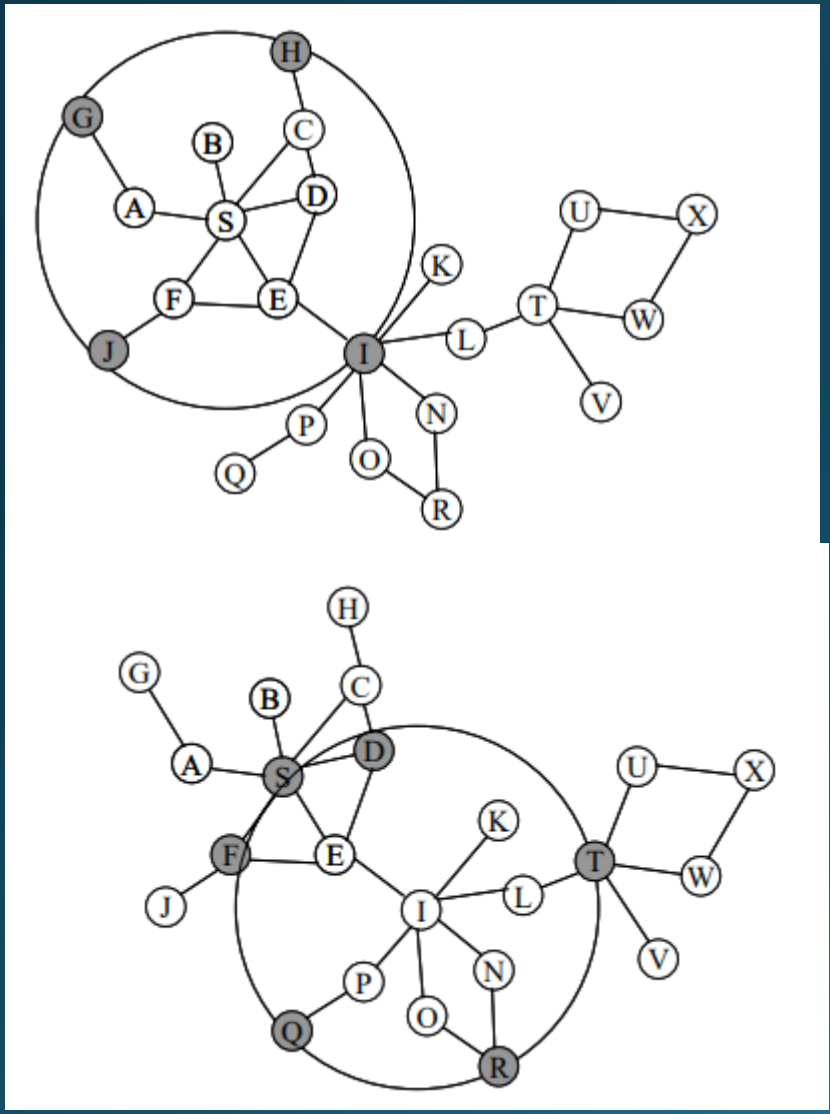
- ZRP refers to the locally **proactive routing** component as the IntrA-zone Routing Protocol **(IARP).**
- The globally reactive routing component is named IntEr-zone Routing Protocol (IERP).
- IARP is a family of limited-depth, proactive link-state routing protocols. IARP maintains routing information for nodes that are within the routing zone of the node.
- IERP is a family of reactive routing protocols that offer enhanced route discovery and route maintenance services based on local connectivity monitored by IARP.

Routing using ZRP

- A node that has a packet to send first checks whether the destination is within its local zone using information provided by IARP. In that case, the packet can be routed proactively.

- Reactive routing is used if the destination is outside the zone.

Example



The node S has a packet to send to node X. The zone radius is ρ=2.

- The node uses the routing table provided by IARP to check whether the destination is within its zone.
- Since it is not found, a route request is issued using IERP. The request is broadcast to the peripheral nodes (gray in the picture).
- Each of these searches their routing table for the destination
- Node I does not find the destination in its routing table. it broadcasts the request to its peripheral nodes.
- query control mechanisms, the request is not passed back to nodes D, F and S.
- Finally, the route request is received by node T, which can find the destination in its routing zone.
- Node T appends the path from itself to node X to the path in the route request. A route reply, containing the reversed path is generated and sent back to the source node.