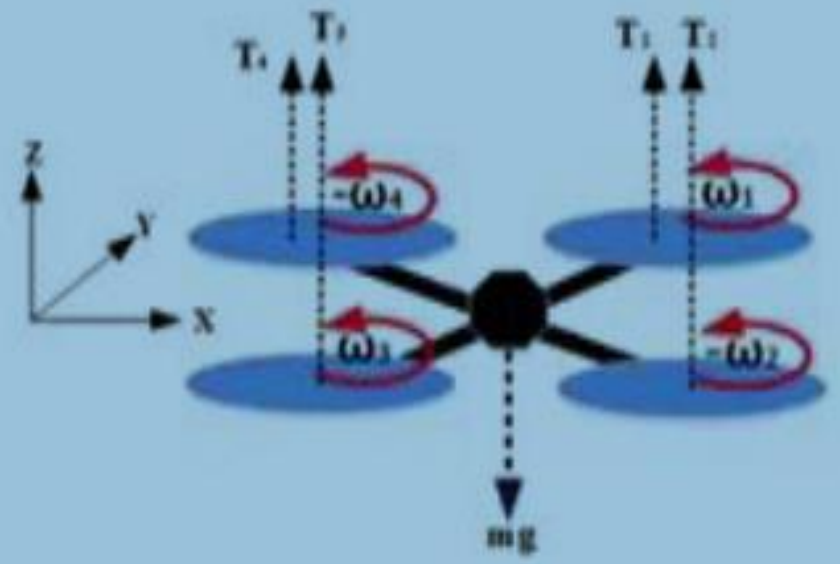
UAV NETWORKS

UAV: An unmanned aerial vehicle (also known as a drone) refers to a pilotless aircraft, a flying machine without an onboard human pilot or passengers.

- The FAA(Federal Aviation Administration) has defined an Unmanned Aircraft or UA as “A device used or intended to be used for flight in the air that has no onboard pilot”.
- This includes all classes of airplanes, helicopters, airships, and translational lift aircraft that have no onboard pilot.
- Unmanned aircraft are understood to include only those aircraft controllable in three axes and therefore, exclude traditional balloons.
- Control functions for unmanned aircraft may be either onboard or off-board (remote control).

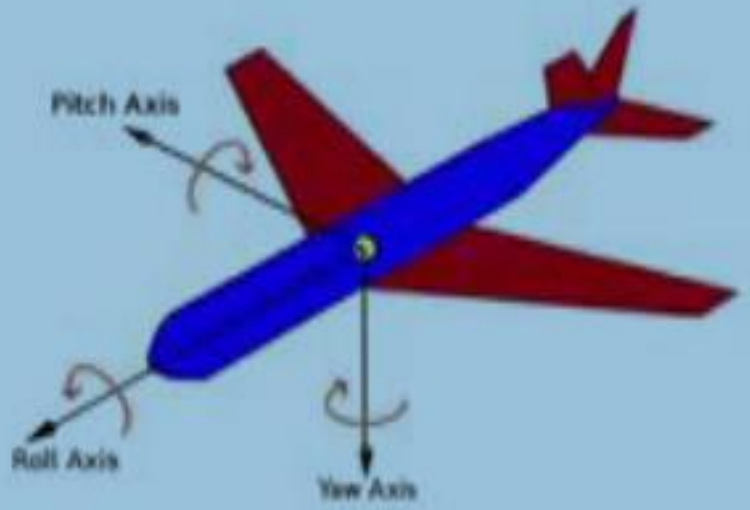
Basics of Aerial Systems



$$T = T1 + T2 + T3 + T4$$

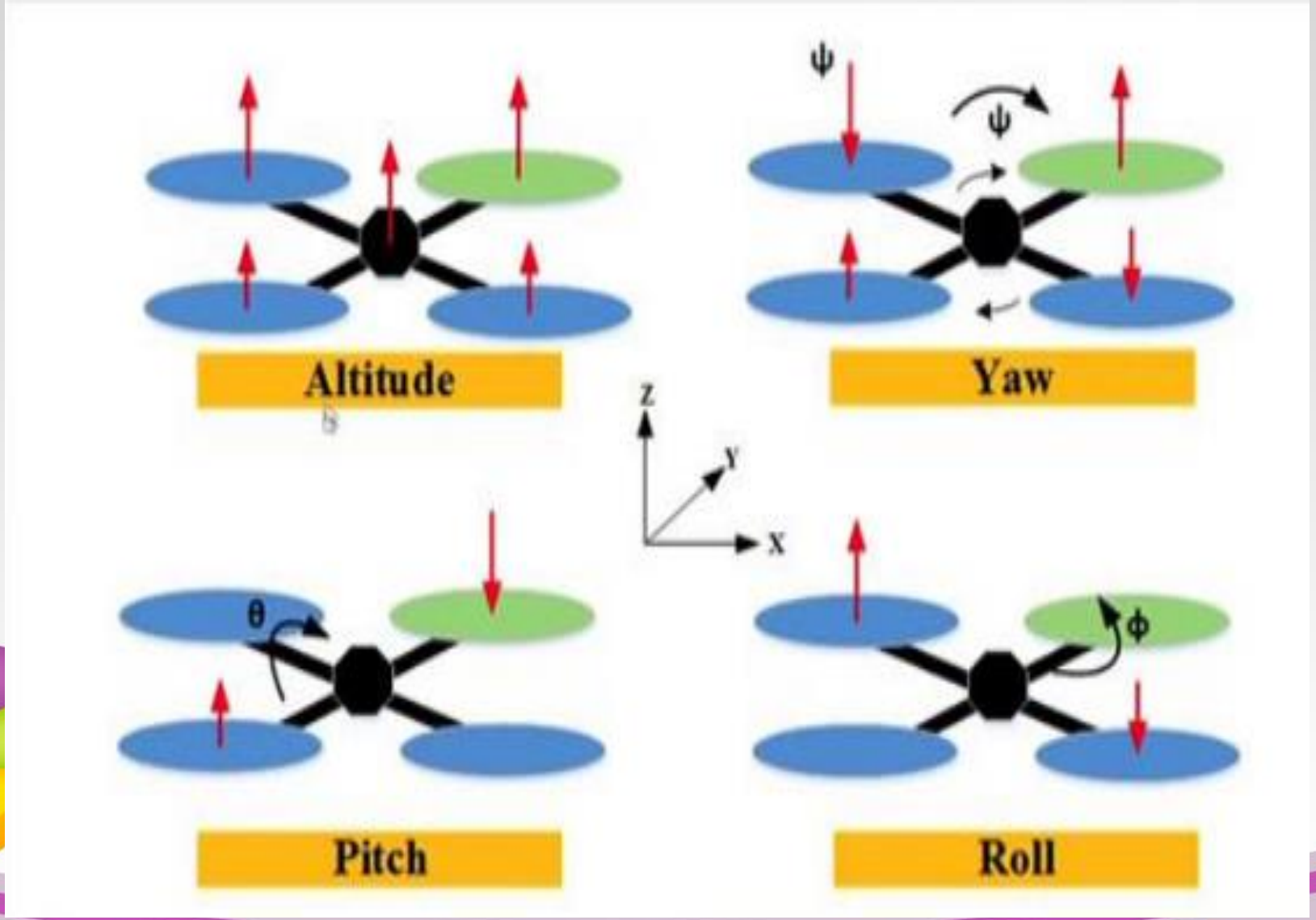
$$T > mg$$

- Forces:-
  - Thrust (T)
  - Angular velocity of motors (ω)



- Actions:
  - Yaw (along z-axis): ψ
  - Pitch (along y-axis): θ
  - Roll (along x-axis): ϕ

Aerial Systems: Actions



The Customisable Hex Copter

Ready to Fly Quad Copter

UAV

- Unmanned Aerial Vehicles
- Aircraft without an on-board human pilot or controller.
- May have various degrees of autonomy.
- Operated-
  - Remotely by a human operator Manual
  - Autonomously to achieve a defined mission- Autonomous
  - Autonomously, with minor human interventions - Hybrid

UAV Applications

- Unmanned aerial vehicles (UAVs), commonly known as drones, have been the subject of concerted research over the past few years, owing to their autonomy, flexibility, and broad range of application domains.

- UAVs are an emerging technology that can be harnessed for military, public and civil applications.

- Military use of UAVs is more than 25 years old primarily consisting of border surveillance, reconnaissance and strike.

- Public use is by the public agencies such as police, public safety and transportation management. They are likely to become invaluable inclusions in the operations of police departments, fire brigades and other homeland security organizations in the near future.

UAV Applications

- UAVs can provide timely disaster warnings and assist in speeding up rescue and recovery operations when the public communication network gets crippled.

- They can carry medical supplies to areas rendered inaccessible.

- In situations like poisonous gas infiltration, wildfires and wild animal tracking UAVs could be used to quickly envelope a large area without risking the safety of the personnel involved.

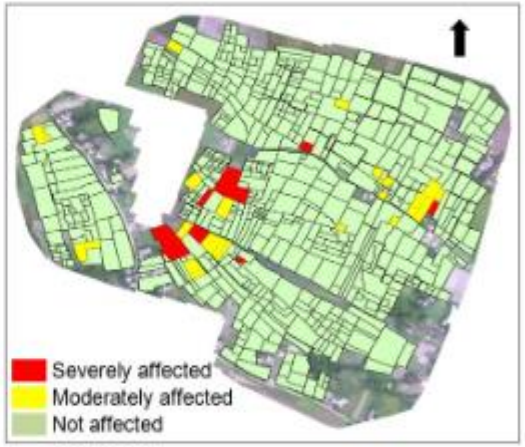
- Besides, advances in electronics and sensor technology have widened the scope of UAVs to include applications as diverse as traffic monitoring, wind estimation, powerline and pipeline inspection as well as remote sensing.

CASE STUDIES

3D View of Landslide

Mapping of Landslide Affected Area in **Meghalaya**

Infested Fields in Naramari Village, Morigaon District, Assam



Categorisation of BPH Infested Rice Fields

Infested Crop Damage Assessment

3D Reconstruction: MUDA Shopping Complex, Nongpoh

3-Dimensioinal Terrain Model Construction in Nongpoh, NE

UAV Classification

- **Classification based on MTOW:**

MTOW(Mean TakeOff Weight) is a good metric to classify aircraft for regulatory purposes since it correlates well with the expected kinetic energy imparted at impact, which in turn is considered to be the primary factor affecting safety of operations.

Class	MTOW (kg)	Range category	Typical max altitude (ft)
0	<25	Close range	1,000 ft
1	25–500	Short range	15,000 ft
2	501–2,000	Medium range	30,000 ft
3	>2,000	Long range	Above 30,000 ft

- **Classification based on Autonomy:**

ACL	Level descriptor
0	Remotely piloted vehicle
1	Execute preplanned mission
2	Changeable mission
3	Robust response to real-time faults/events
4	Fault/event adaptive vehicle
5	Real-time multi-vehicle coordination
6	Real-time multi-vehicle cooperation
7	Battlespace knowledge
8	Battlespace cognizance
9	Battlespace swarm cognizance
10	Fully autonomous

ACL: Autonomous control level

- **Classification based on function**

- Target and decoy – providing ground and aerial gunnery a target that simulates an enemy aircraft or missile
- Reconnaissance – providing battlefield intelligence
- Combat – providing attack capability for high-risk missions
- Logistics – delivering cargo
- Research and development – improve UAV technologies
- Civil and commercial UAVs – agriculture, aerial photography, data collection

- **NASA UAS Classification**

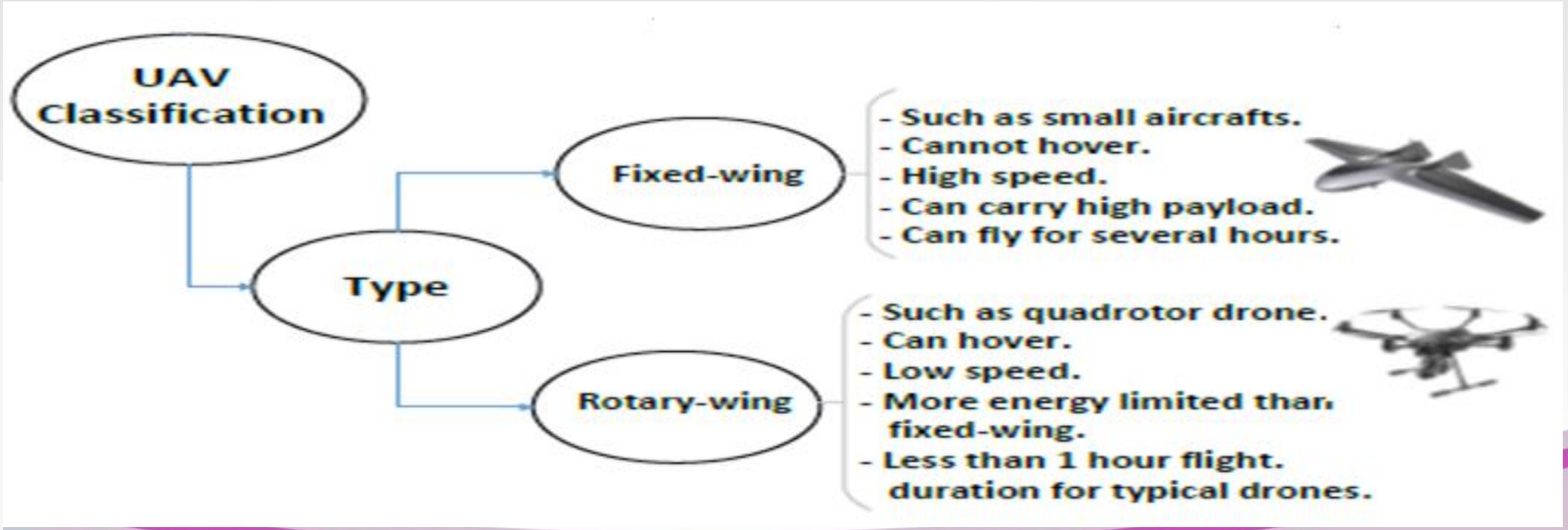
Category	I	II	III
Weight	< 55 lb (25 kg)	55-330 lb (25-150 kg)	> 330 lb (150 kg)
Airspeed (kt)	≤ 70	≤ 200	> 200
Type	Model or sUAS	sUAS	UAS

- **Classification based on weight, altitude and endurance**

	Mass (kg)	Range (km)	Flight alt. (m)	Endurance (h)
Micro	<5	<10	250	1
Mini	<20/25/30/150[a]	<10	150/250/300	<2
Tactical				
Close range (CR)	25–150	10–30	3.000	2–4
Short range (SR)	50–250	30–70	3.000	3–6
Medium range (MR)	150–500	70–200	5.000	6–10
MR endurance (MRE)	500–1500	>500	8.000	10–18
Low altitude deep penetration (LADP)	250–2500	>250	50–9.000	0.5–1
Low altitude long endurance (LALE)	15–25	>500	3.000	>24
Medium altitude long endurance (MALE)	1000–1500	>500	3.000	24–48
Strategic				
High altitude long endurance (HALE)	2500–5000	>2.000	20.000	24–48
Stratospheric (Strato)	>2.500	>2.000	>20.000	>48
Exo-stratospheric (EXO)	TBD	TBD	>30.500	TBD
Special task				
Unmanned combat AV (UCAV)	>1.000	1.500	12.000	2
Lethal (LET)	TBD	300	4.000	3–4
Decoys (DEC)	150–250	0–500	50–5.000	<4

- **Classification Based on Ownership:**
-
- **Public/State: O**wned and operated by public entities like federal agencies or local law enforcement agencies.
- **Civil: O**wned by industry or private parties.

- **Classification Based on Type:**



Federal Aviation Authority(FAA) guidelines on UAV Operations (2015, for a govt. public safety agency)

- Weight must be 4.4 pounds or less.
- Must be within the line of sight of the operator.
- Must fly less than 400 feet above the ground, during daylight conditions.
- Must be outside of 5 statute miles from any airport, heliport, seaplane base, spaceport, or other location.
- Should be flown a sufficient distance from populated areas and full scale aircraft.
- Must not be used for business purposes.

History of UAVs

- The earliest recorded use of UAV was in 1849 when Austria attacked Venice using UAVs.
- However the idea of building “flying machines” was first conceived close to 2,500 years ago, in ancient Greece and China!
- In 425 BC Archytas built a mechanical bird called “the pigeon” which flew for about 200m.

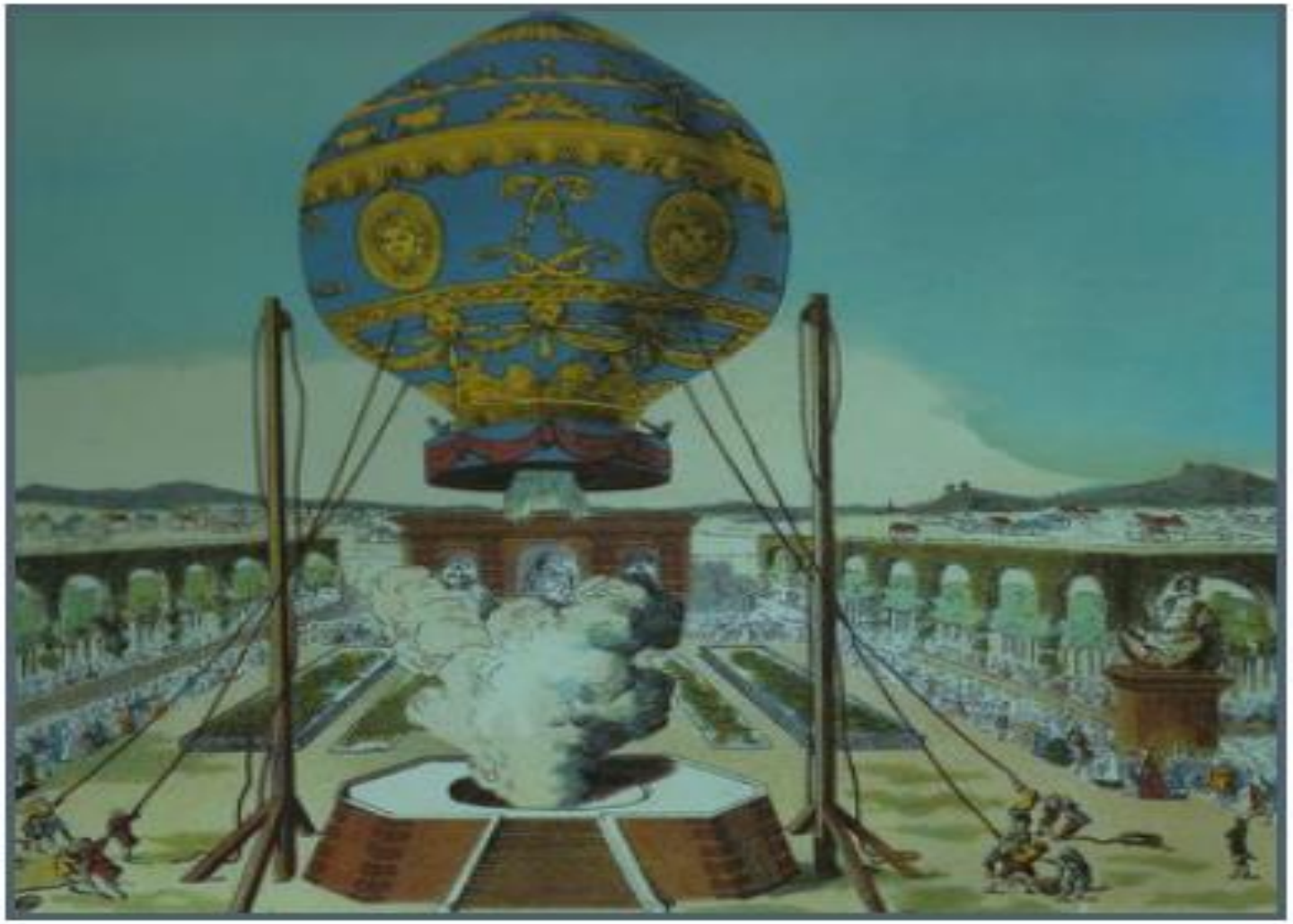
History of UAVs

- During and after World War I, UAVs were used by US Army.
- In World War II Nazi Germany produced and used various UAVs.
- The V-1 flying bomb was the first cruise missile ever built. It was first tested in 1942. The V-1 was intended to target London and was massively fired, achieving more than one hundred launches a day.
- Target drones evolved post World War II.
- The use of drones as decoys goes back to at least 1950s.

- In 1946, eight B-17 Flying Fortresses were transformed by American airmen into drones for collecting radioactive data from the radioactive cloud.

History of UAVs

- During 1960s both USA and USSR developed reconnaissance drones.
- UAVs were used in Vietnam War during1966-1971.
- On August 21, 1998, *Laima* becomes the first Endurance UAV to cross the Atlantic Ocean, completing the flight in 26 hours.
- During 1980s solar powered UAVs were popular.
- As of 2012: US army employed 7494 UAVs.
- Recreational drones became popular in the United States in 2015.



The first manned flight using a hot air balloon in 1783 in France

History of UAVs

The SD-1, also known as the MQM-57 Falconer, was the first reconnaissance drone of the US Army and remained in service until the 1970s (Photo Credit: National Museum of the USAF)

The Neptune, a reconnaissance UAV capable of water landings (Photo Credit: US Navy)

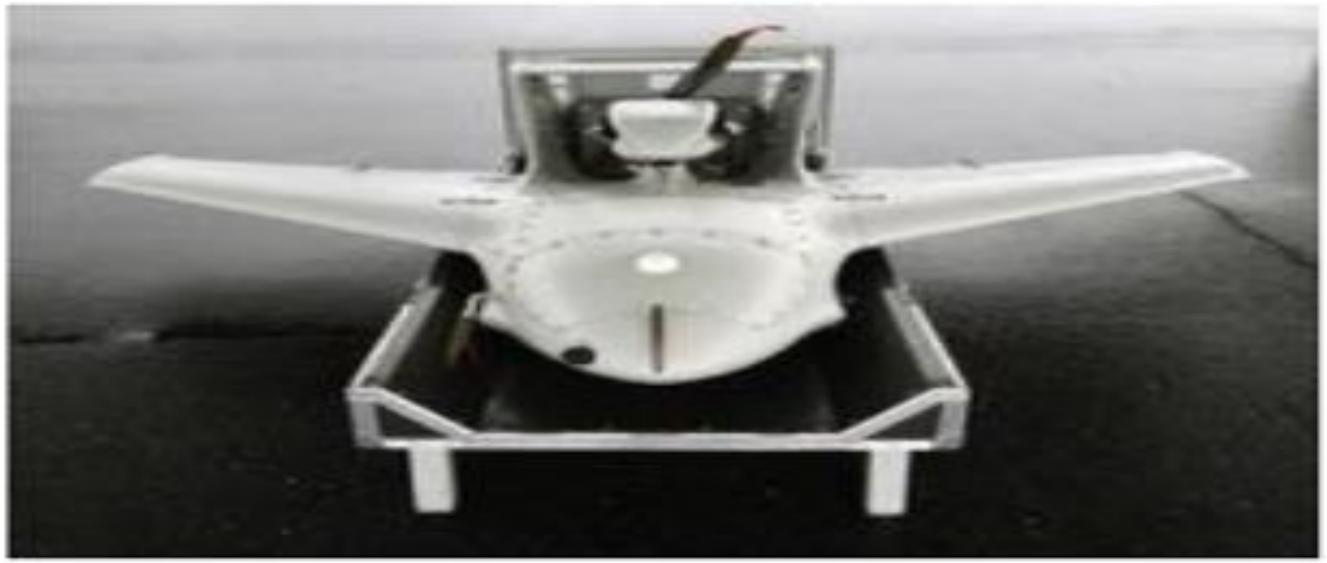


Fig. The Helios UAV developed by NASA and AeroVironment. During its second high-altitude flight, it reached 96,863 ft, shattering the existing world altitude record for sustained level flight for both propeller and jet-powered aircraft (Photo Credit: NASA)

- World War I: Hewitt-Sperry Automatic Airplane
- 1935: The first scaled remote pilot vehicle was developed
- World War II: Nazi Germany produced and used various UAVs
- 1959: US Air Force began planning use of UAVs to reduce pilot loss
- 1964: UAVs were used for combat missions in Vietnam War

UAV NETWORKS

A network of UAVs can be viewed as a flying wireless network in which each UAV serves as a node transmitting its own information to other nodes or receiving the information intended for it or relaying information meant for others in the network.

The network could be ad hoc without any supporting infrastructure or it could be supported by ground-based and/or satellite-based communication infrastructures.

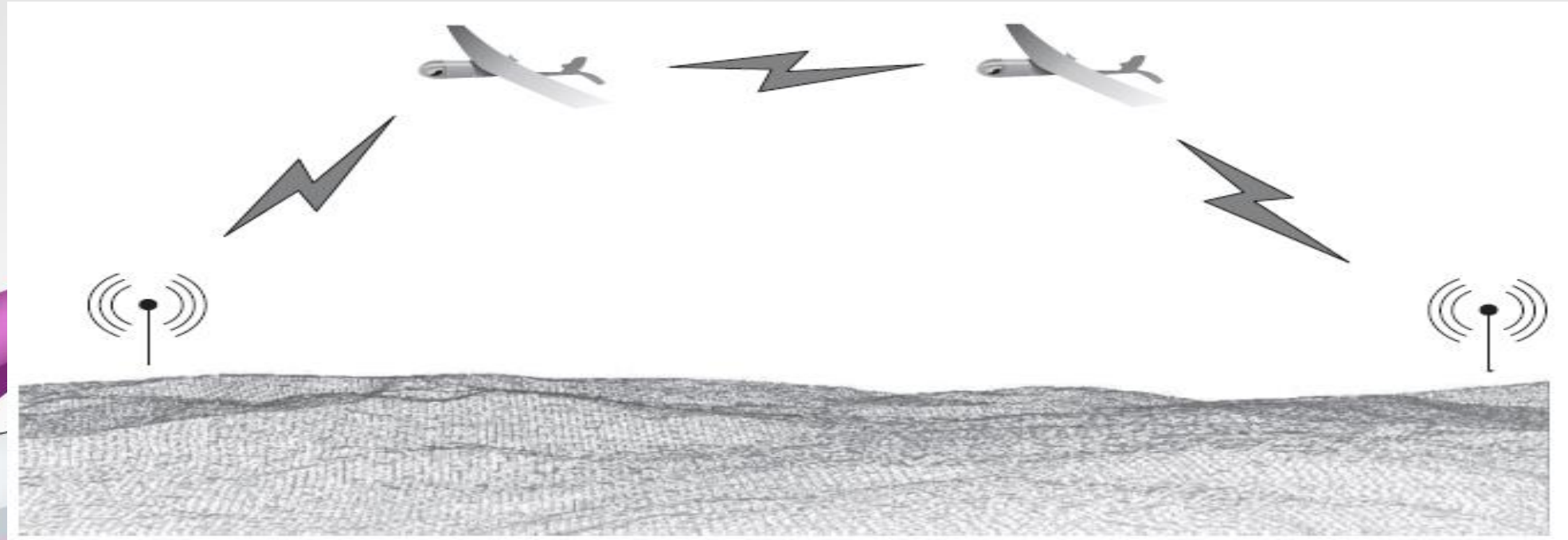


Figure Two UAVs working together as a simple relay network extending the range of coverage on the ground

UAV networks are basically not about single UAVs, but multiple UAVs which can communicate with one another.

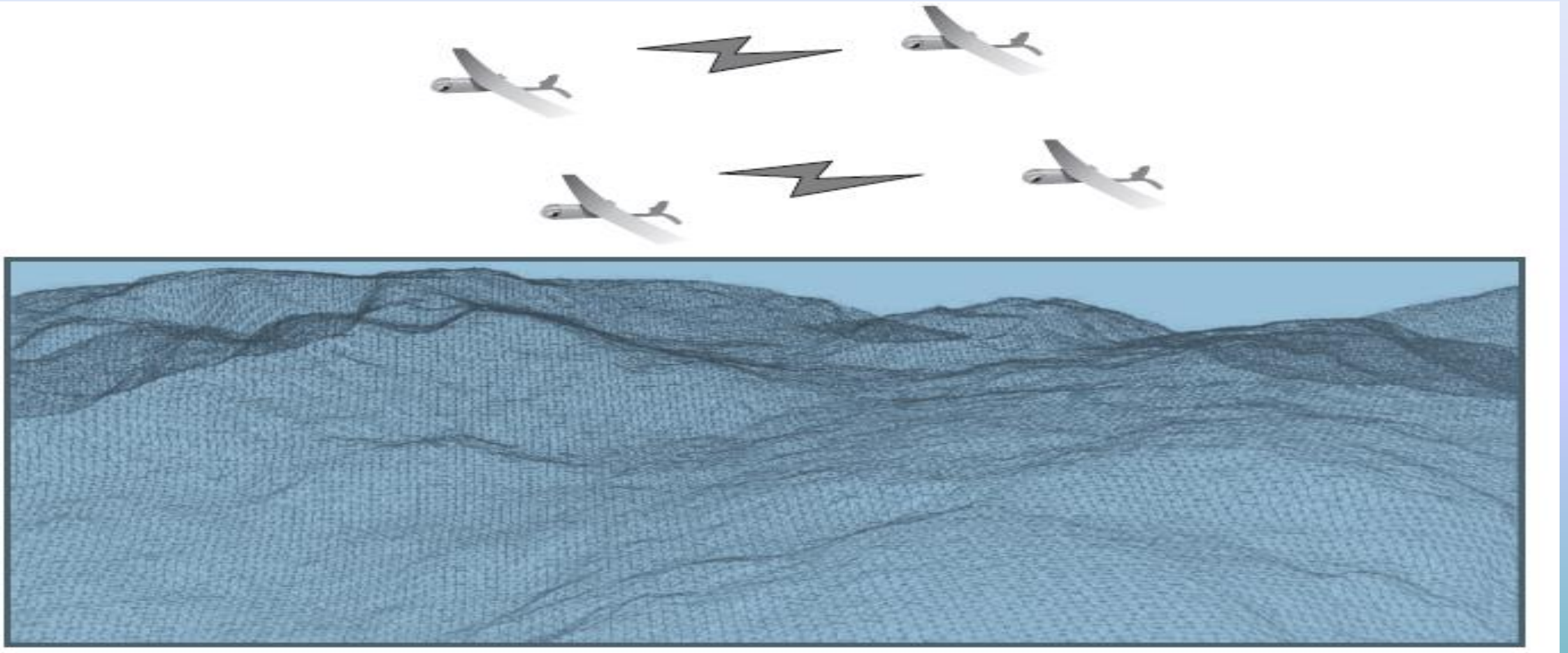


Figure Multiple UAVs forming an aerial mobile ad hoc network

Multi-UAV Network

- More than one UAV associated with the network
- UAVs are smaller and less expensive.
- Communication between UAVs and between ground node is important.
- Co-operation of UAVs.
- Degree of mobility

The topology or configuration of the UAV network: Mesh, star, or even a straight line. It primarily depends on the application and use case scenario.

A UAV enabled communication infrastructure provides a better alternative to ground based infrastructure, especially when a clear line of sight between a transmitter and receiver is not available due to uneven terrain or cluttered environment.

An aerial MANET is a multi-hop networking solution for delivering information over long distances.

Each node in the aerial MANET acts as a terminal as well as a relay node or router carrying information within the network.

In an ad hoc configuration, there is no need for any other infrastructure such as satellites or centralized servers to support the UAV swarm.

Global Positioning System (GPS) sensor helps to estimate and exchange geolocation information among the UAVs.

A UAV network with ground- and satellite-based communication infrastructure is commonly known as an airborne network.

Since aerial nodes move much faster than nodes on the ground, the topology of an aerial network will be very dynamic.

The extremely changing dynamics require specific protocols for routing and secure information exchange.

In addition, sense-and-avoid and situational awareness strategies are necessary to make sure that the nodes maintain a minimum safe distance during their flight.

Airborne networks are unique and significantly different from vehicular networks involving only ground vehicles in many perspectives.

Classical mobility models and security strategies designed for MANETs and ground vehicular networks are not suitable for airborne networks.

An airborne network is a cyber physical system (CPS) in which there is an intense interaction between its physical and cyber components.

The fundamental challenge for airborne networks is to bring the synergistic interactivity between its cyber and physical components.

Mobility Models in MANET

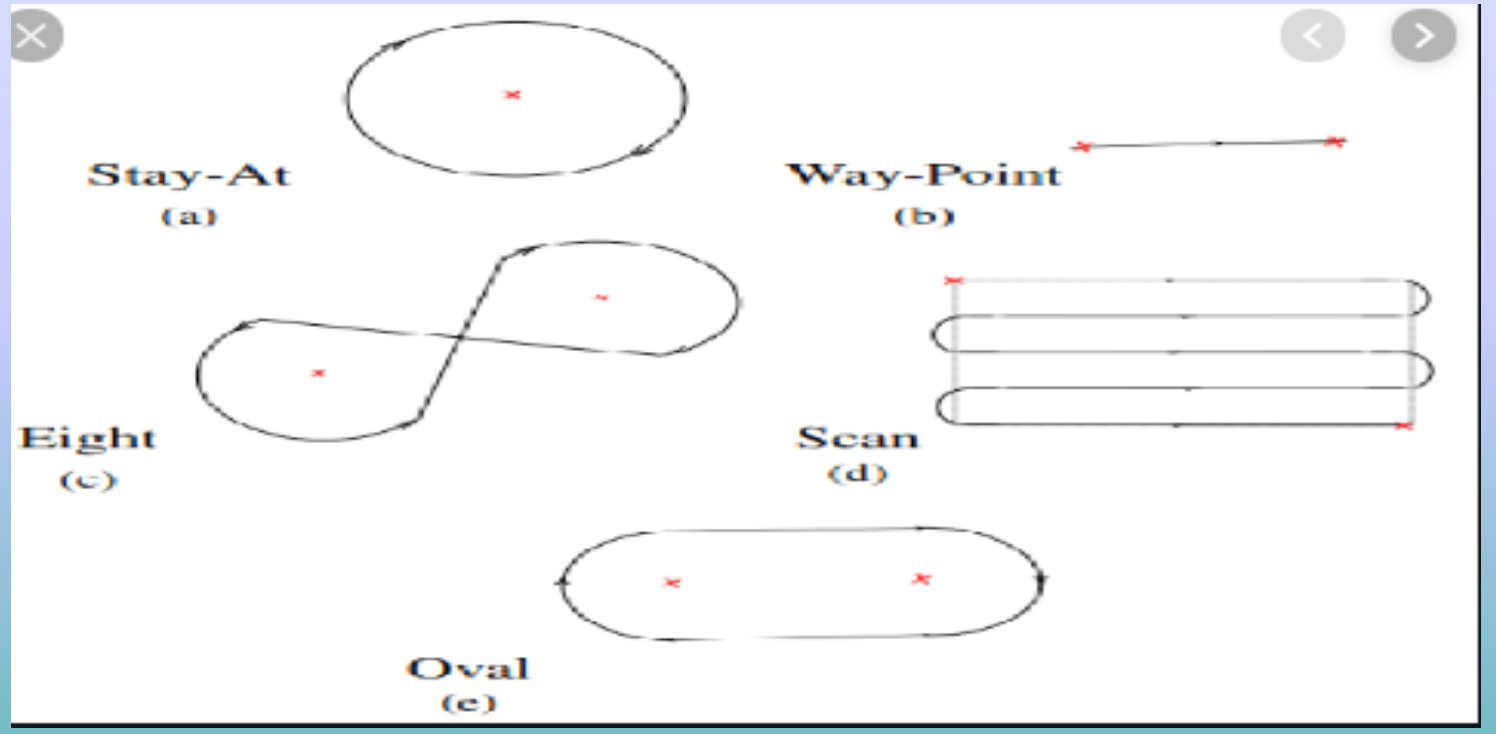
- Random Walk Mobility Model
- Random Waypoint Mobility Model
- Random Direction Mobility Model
- A Boundless Simulation Area Mobility Model
- Gauss-Markov Mobility Model
- A Probabilistic version Random Walk Mobility Model

Mobility Models in UAV Networks

- 3D Gauss Markov Mobility Model
- Semi-Random Circular Movement Mobility Model
- Smooth Turn Mobility Model
- 3-Way Random Mobility Model
- Flight –Plan Based Mobility Model
- Multi-Tier Mobility Model.

Mobility Models in UAV Networks

- **Pheromone Mobility Model**
- **Paparazzi Mobility Model**



5 movements in Paparazzi Mobility Model

UAV Systems: Features

Feature	Single UAV System	Multi-UAV System
Failures	High	Low
Scalability	Limited	High
Survivability	Poor	High
Speed of Mission	Slow	Fast
Cost	Medium	Low
Bandwidth required	High	Medium
Antenna	Omni-directional	Directional
Complexity of Control	Low	High
Failure to coordinate	Low	Present

Features of the UAV Networks

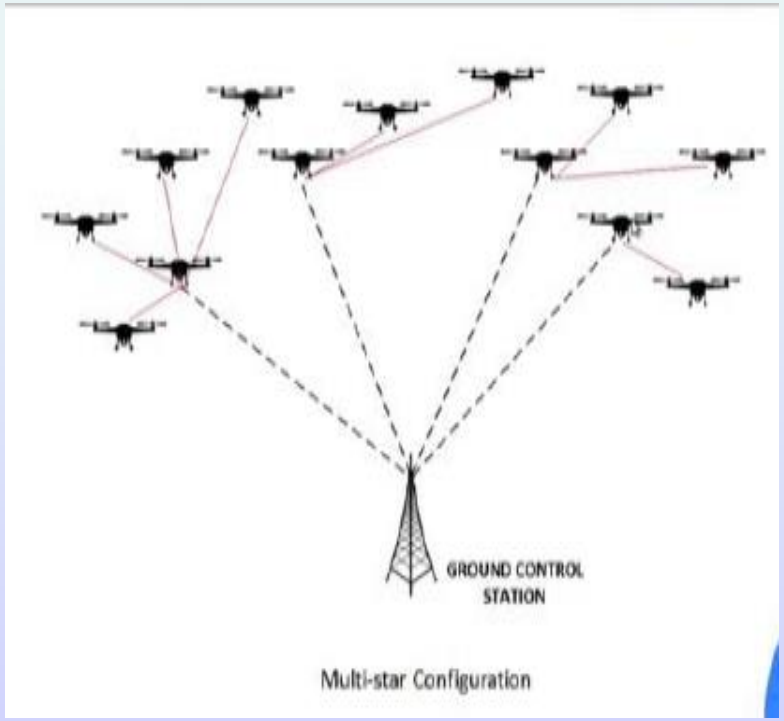
- Infrastructure-based or Ad Hoc?
  - Constant inter network with UAVs and a control center may be treated as infrastructure based network
  - Highly mobile nodes change their position and communicate, co-operate and establish the network dynamically in Ad Hoc manner.

- Server or client?
  - Usually server.
  - Routing packets for clients.
  - Relaying sensor data to control centers.

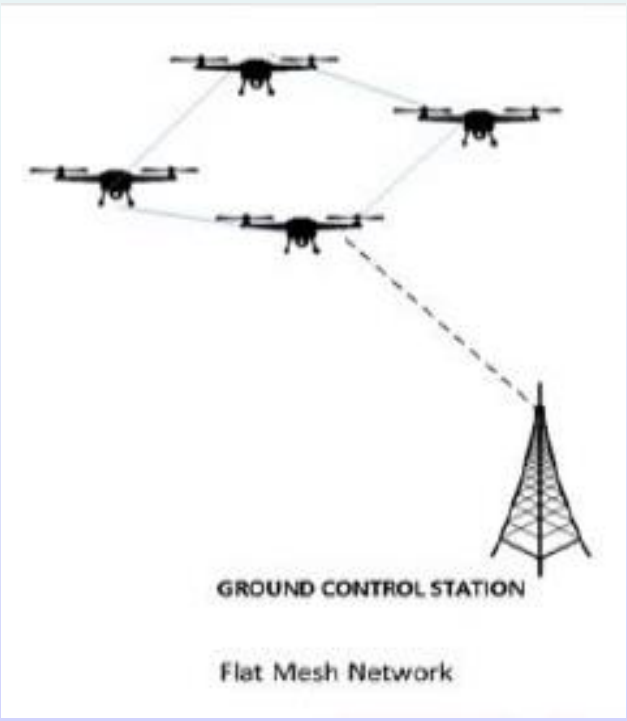
Star or Mesh?

- Star :
  - Typically two types –
    - Star Configuration,
    - Multi-star Configuration .
  - In Star Configuration, UAV is directly connected to the ground station.
  - In Multi-star Configuration, UAVs form multiple star topology. One node from each group connects to the ground station.
  - High latency.
  - Highly dependent on ground station.

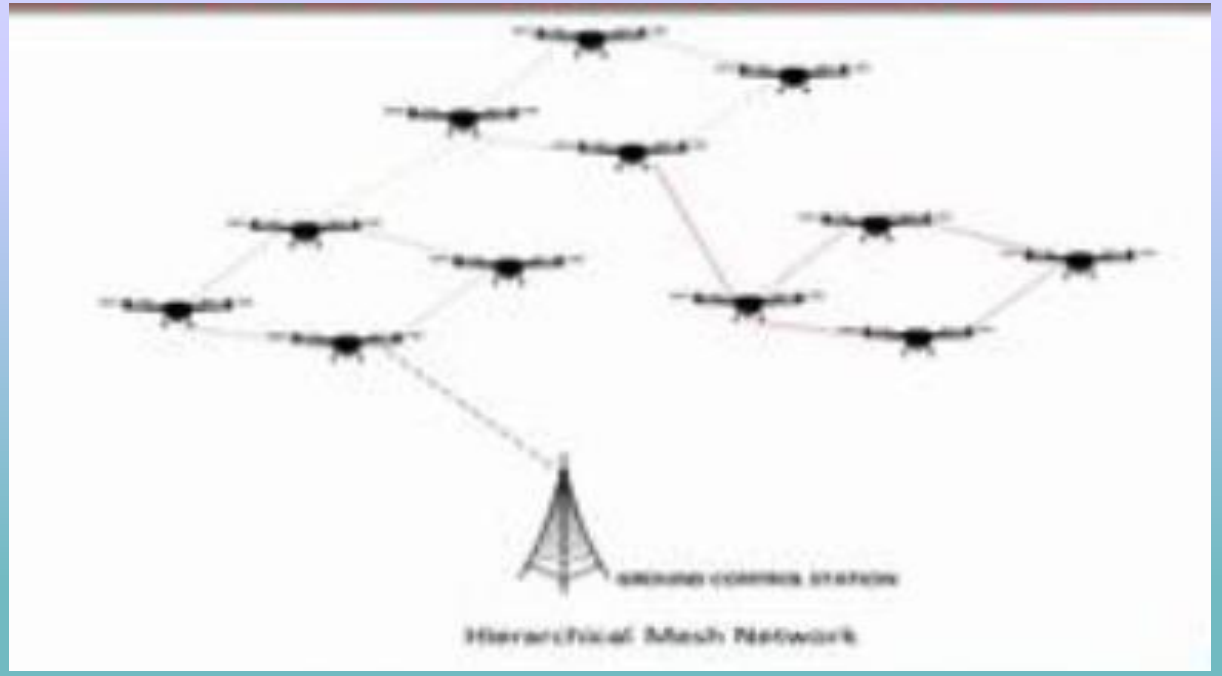
Star Configuration



Multi-star Configuration



Flat Mesh Network


Hierarchical Mesh Network

Star Network	Mesh Network
Point-to-point	Multi-point to multi-point
Central control point present	Infrastructure based may have a control center, Ad hoc has no central control center
Infrastructure based	Infrastructure based or Ad hoc
Not self configuring	Self configuring
Single hop from node to central point	Multi-hop communication
Devices cannot move freely	In ad hoc devices are autonomous and free to move. In infrastructure based movement is restricted around the control center
Links between nodes and central points are configured	Inter node links are intermittent
Nodes communicate through central controller	Nodes relay traffic for other nodes

UAV Topologies are prone to different types of disruptions and Delays.

- Disruptions depend on mobility, power transmission, inter-UAV distances, extraneous noise.
- Delay depends on poor link quality, end-to-end path not being available.

Multi-UAV Network : Constraints

- Frequent link breakages
- Prone to malfunction
- Huge power requirements
- Very complex
- Physically prone to environmental effects: winds, rain, etc.

Multi-UAV Network : Advantages

- High Reliability
- High Survivability
- Single Malfunction Proof
- Cost Effective
- Efficient
- Speeded up missions

Challenges in UAV Networks

- UAV networks remain fluid: Topology, number of nodes, links, etc change fast.
- Challenges for simple proactive or a reactive routing scheme.
- Conserving energy.
- Prone to environmental disturbances such as winds, rain, birds, animals, etc.
- Localization
- Maintaining coverage
- Path planning

COMPARATIVE STUDY

	MANET	VANET	UAV Networks
Description	Mobile wireless nodes connect with other nodes within communication range in an ad-hoc manner(No centralized infrastructure required)	Ad-hoc networks in which vehicles are the mobile nodes. Communication is among vehicles and between vehicles and road side units.	Ad-hoc or infrastructure based networks of airborne nodes. Communication among UAVs and with the control station
Mobility	Slow. Typical speeds 2 m/sec. Random movement. Varying density, higher at some popular places	High-speed,typically 20-30 m/s on highways, 6-10 m/s in urban areas. Predictable, limited by road layout,traffic and traffic rules	Speeds from 0 to typically as high as 100 m/s. Movement could be in 2 or 3 dimensions, usually controlled according to mission
Topology	Random, ad-hoc	Star with roadside infrastructure and ad-hoc among vehicles	Star with control center, ad-hoc/mesh among UAVs.

COMPARATIVE STUDY

	MANET	VANET	UAV Networks
Topology Changes	Dynamic - nodes join and leave unpredictably. Network prone to partitioning.	More dynamic than MANETs. Movement linear. Partitioning common.	Stationary, slow or fast. May be flown in controlled swarms. Network prone to partitioning
Energy Constraints	Most nodes are battery powered so energy needs to be conserved.	Devices may be car battery powered or own battery powered.	Small UAVs are energy constrained. Batteries affect weight and flying time
Typical use cases in public and Civil domains	Information distribution (emergencies,advertising,shopping, events) Internet hot spots	Traffic & weather info, emergency warnings, location based services, infotainment	Rescue operations, Agriculture-crop survey , Wildlife search, Oil rig surveillance

COMPARATIVE STUDY

Characteristics	MANETs	VANETs	UAV Networks
Density	High	High	Low
Network connectivity	High	Medium	Low
Energy autonomy	Low	High	High (Depends on UAV kind)
Topology variation	Occasionally	Frequently	Very frequently
Scalability	Medium	High	Low
QoS	Low	High (Depends on the application)	High (Depends on the application)
Mobility models	Random	Restricted through roads pattern	Predefined by mobility models
Node speed	Medium	High	Very high

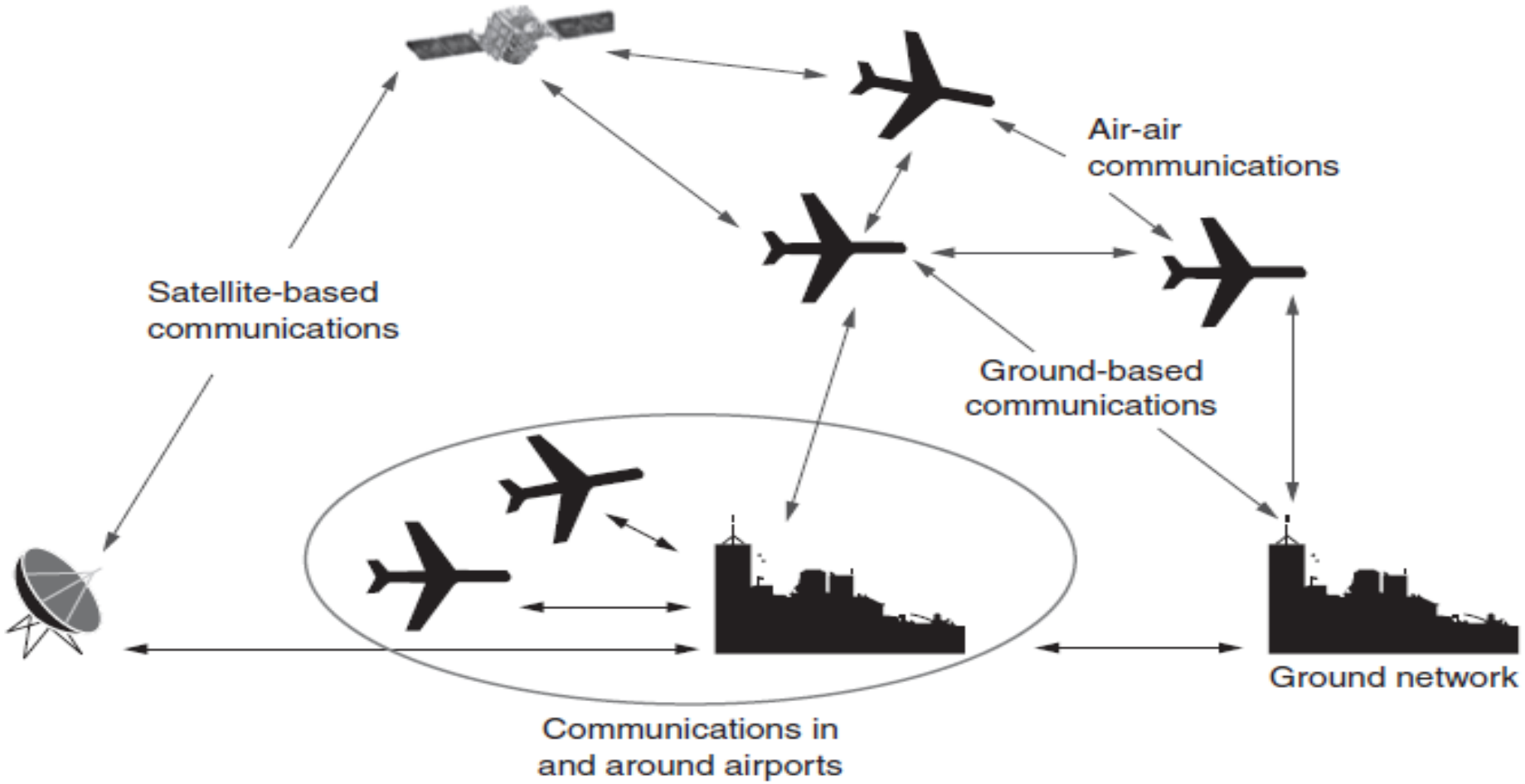
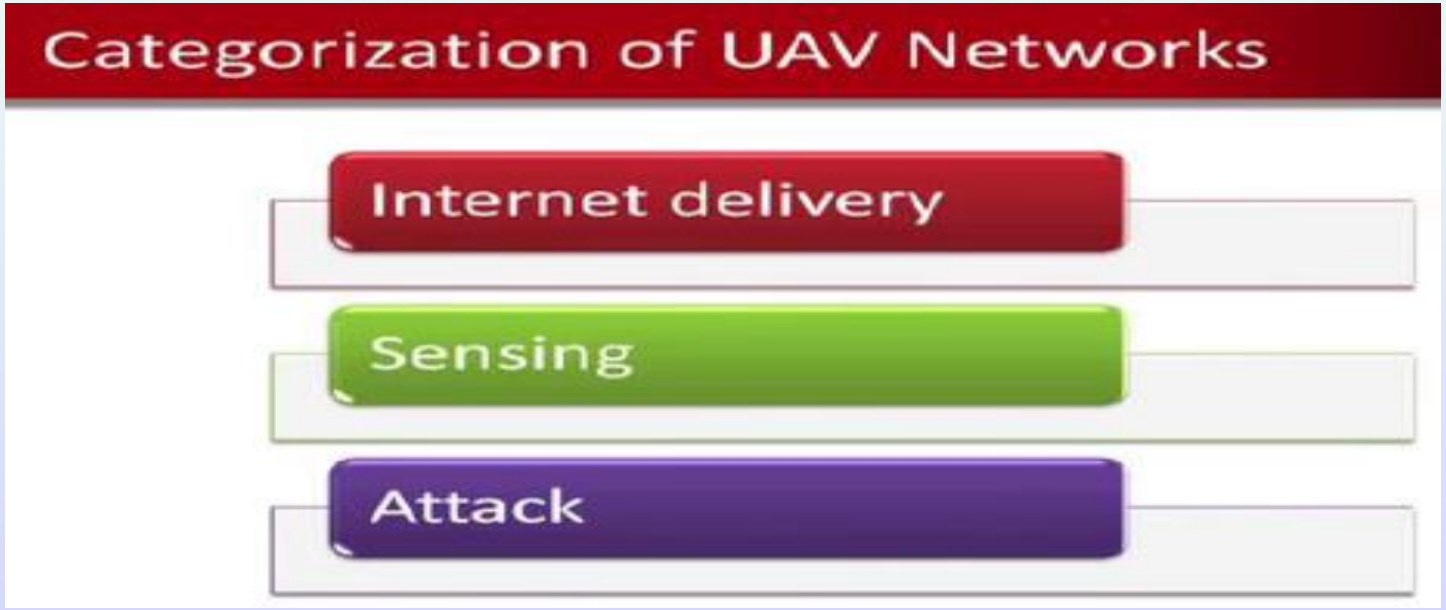


Figure A real-world airborne network consisting of unmanned aerial systems as well as the satellite- and ground-based communication infrastructure

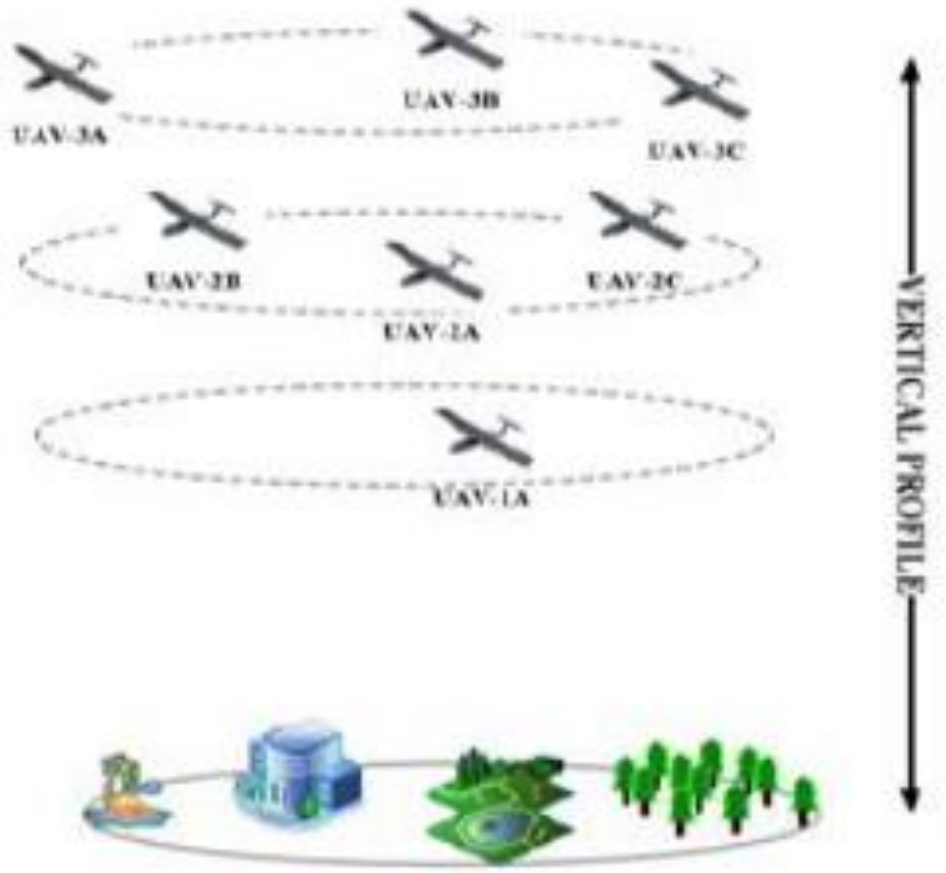


- Internet Delivery :
  - Application: Disaster communication , Oil exploration , Remote health etc.
  - Network : Infrastructure based, base station in the sky.
  - Topology : Star/Mesh.
  - Control (communication) : Centralized (position control based).
  - Client or Server: Server (routes communication and control).
  - Routing: Through server

- Sensing :
  - Application : Reconnaissance, search, detecting forest fires, tracking wild animals etc.
  - Network : Infrastructure based.
  - Topology : Mesh.
  - Control (communication) : Centralized (task control based).
  - Client or Server: Server (when receiving from sensors) / client(when carrying sensors)
  - Routing: Central or mesh (control from central data to central, also data among UAVs)

- Attack :
  - Application : War Multi-UAV attack
  - Network : Infrastructure based/Infrastructure less, Ad-hoc
  - Topology : Mesh.
  - Control (communication) : Distributed (task control based),Individuals controlling each UAV.
  - Client or Server: Server (delivering info to formations) /client (for attack).
  - Routing: Mesh routing (control from central, data among UAVs).

FANETs: Flying Ad Hoc Networks

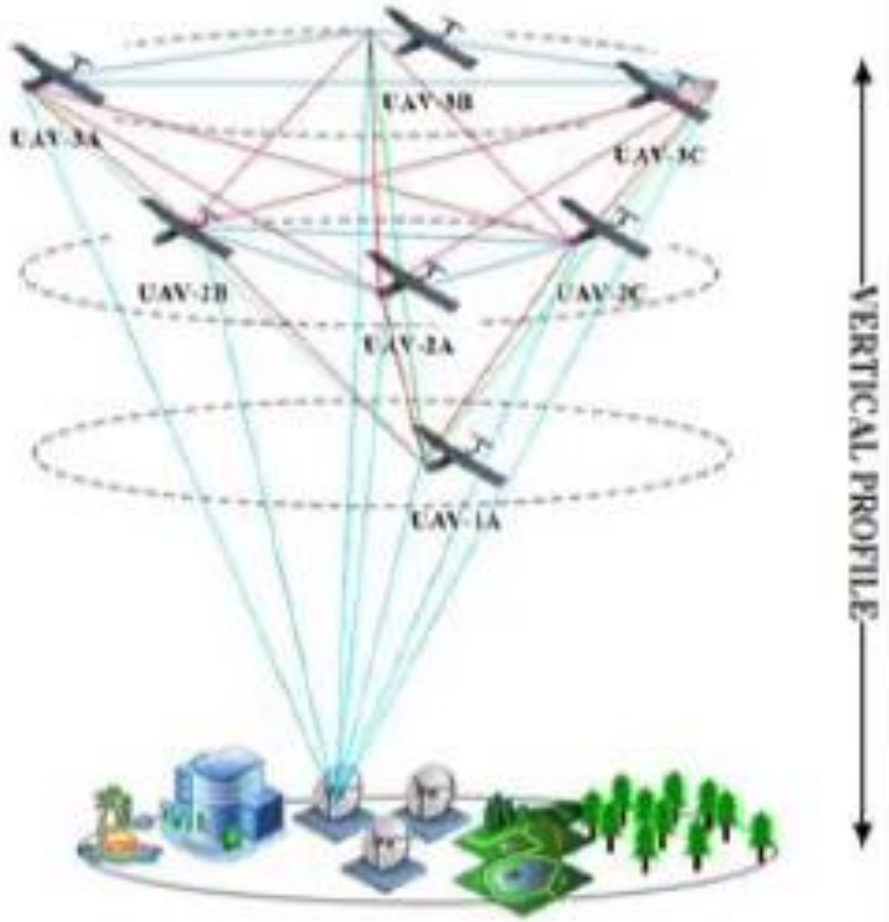


- Network formation using UAVs which ensures longer range, clearer line of sight propagation and environment-resilient communication.
- UAVs may be in same plane or organized at varying altitudes.
- Besides self-control, each UAV must be aware of the other flying nodes of the FANET to avoid collision.
- Popular for disaster-time and post-disaster emergency establishment.

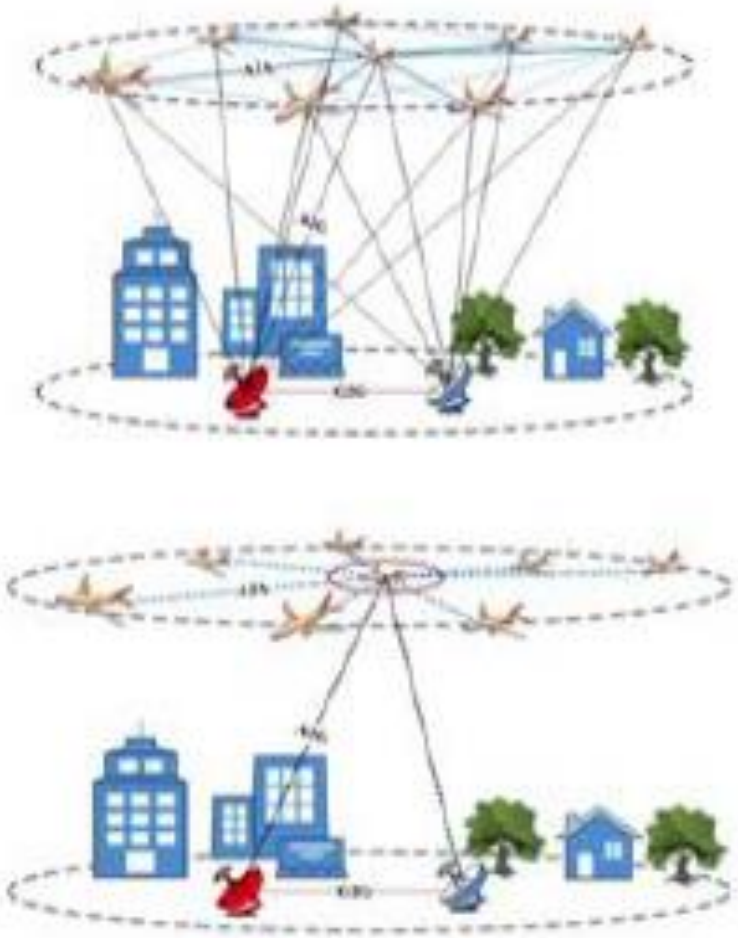
FANETs: Flying Ad Hoc Networks (Contd...)

Features:

- FANET Inter-plane communication
- FANET Intra-plane communication
- FANET- Ground Station communication
- FANET- Ground Sensor communication
- FANET-VANET communication

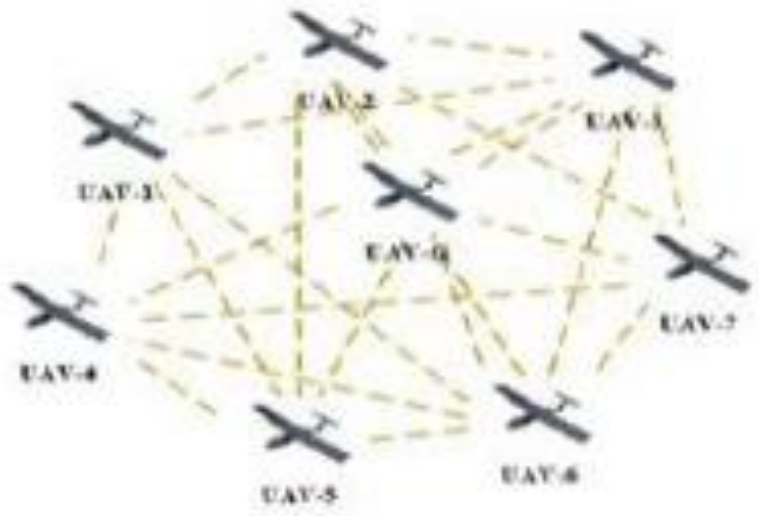


FANET & Ad Hoc Networks



- A2A links for data delivery among UAVs.
- Heterogeneous radio interfaces can be considered in A2A links, such as XBee-PRO (IEEE 802.15.4) and Wi-Fi (IEEE 802.11).
- Ground networks may be stationary WSNs or VANETS or Control stations.
- UAV-WSN link-up may be used for collaborative sensing as well as data-muling.
- UAV-VANETS link-up may be used for visual guidance, data-muling and coverage enhancement.

Distributed Gateway Selection



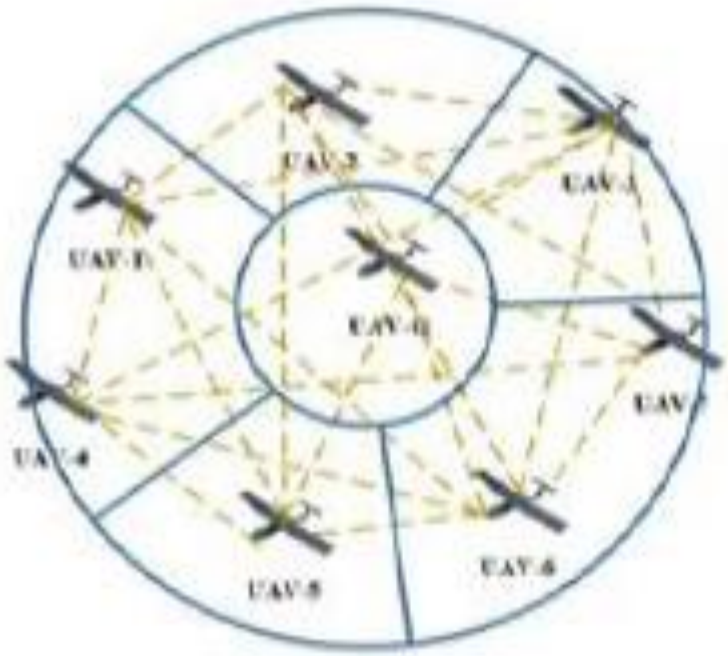
Main communication requirements of UAV networks are:

- Sending back the sensor data.
- Receiving the control commands.
- Cooperative trajectory planning.
- Dynamic task assignments.

Number of UAV-ground remote connections should be controlled to avoid interference.

Reduced nodes in the UAV network should act as gateways, to allow communication between all UAV and the ground

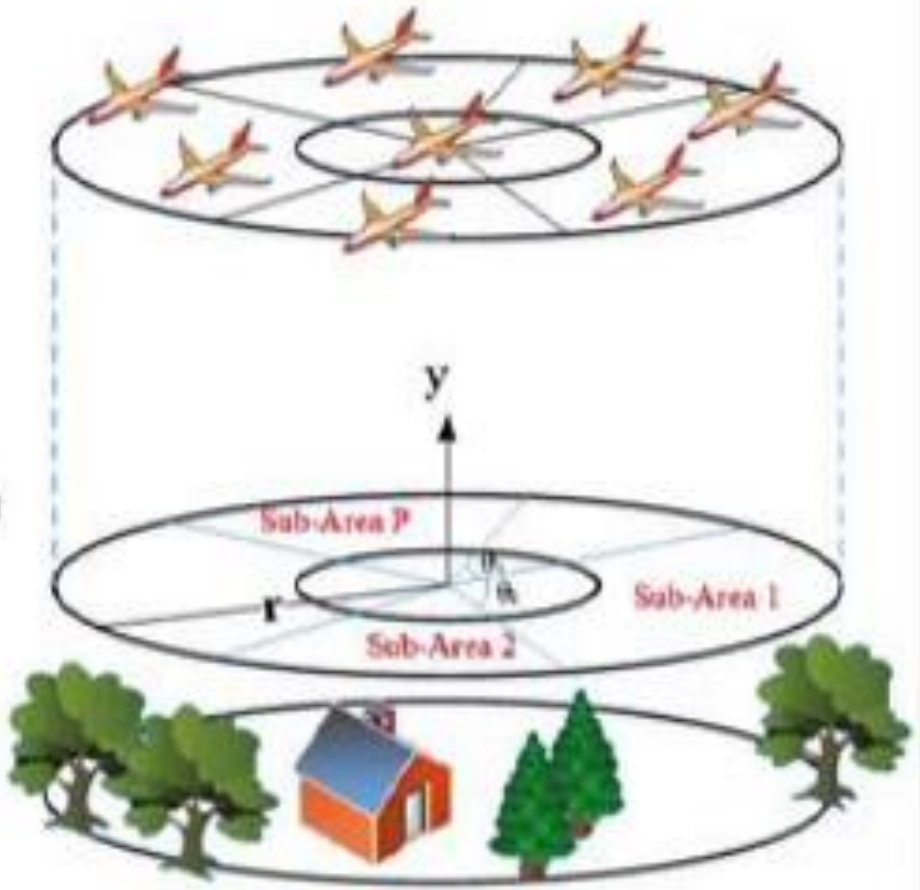
Distributed Gateway Selection



- Entire UAV network coverage area divided into sub-areas.
- Sub-areas collectively cover the entire communication area.
- Size of sub-area to be controlled and adjusted dynamically.
- Adjustments based on UAV-interconnections and derived metrics.
- The derived metrics are optimized for several iterations till optimum state is achieved.

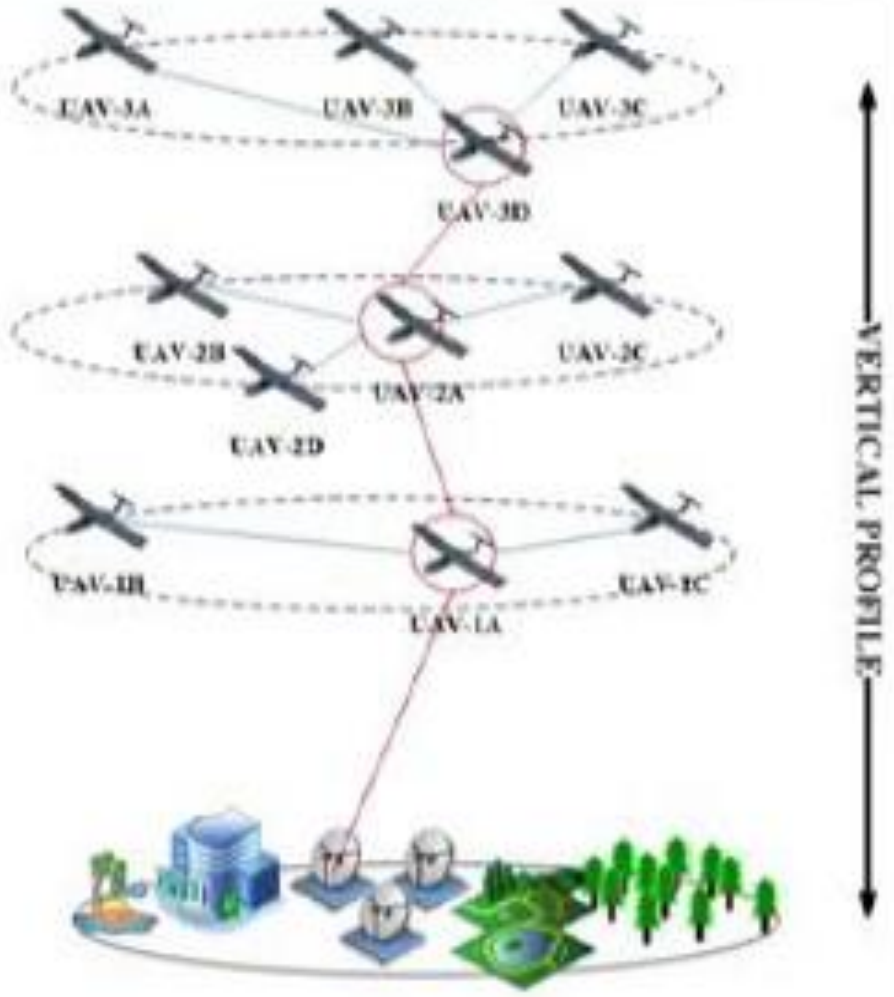
Distributed Gateway Selection

- Gateway selection initiated by selection of the most stable node in the sub-area.
- Consecutively, the partition parameters are optimized according to topology.
- Each UAV acquires the information of all UAVs within its 2 hops.

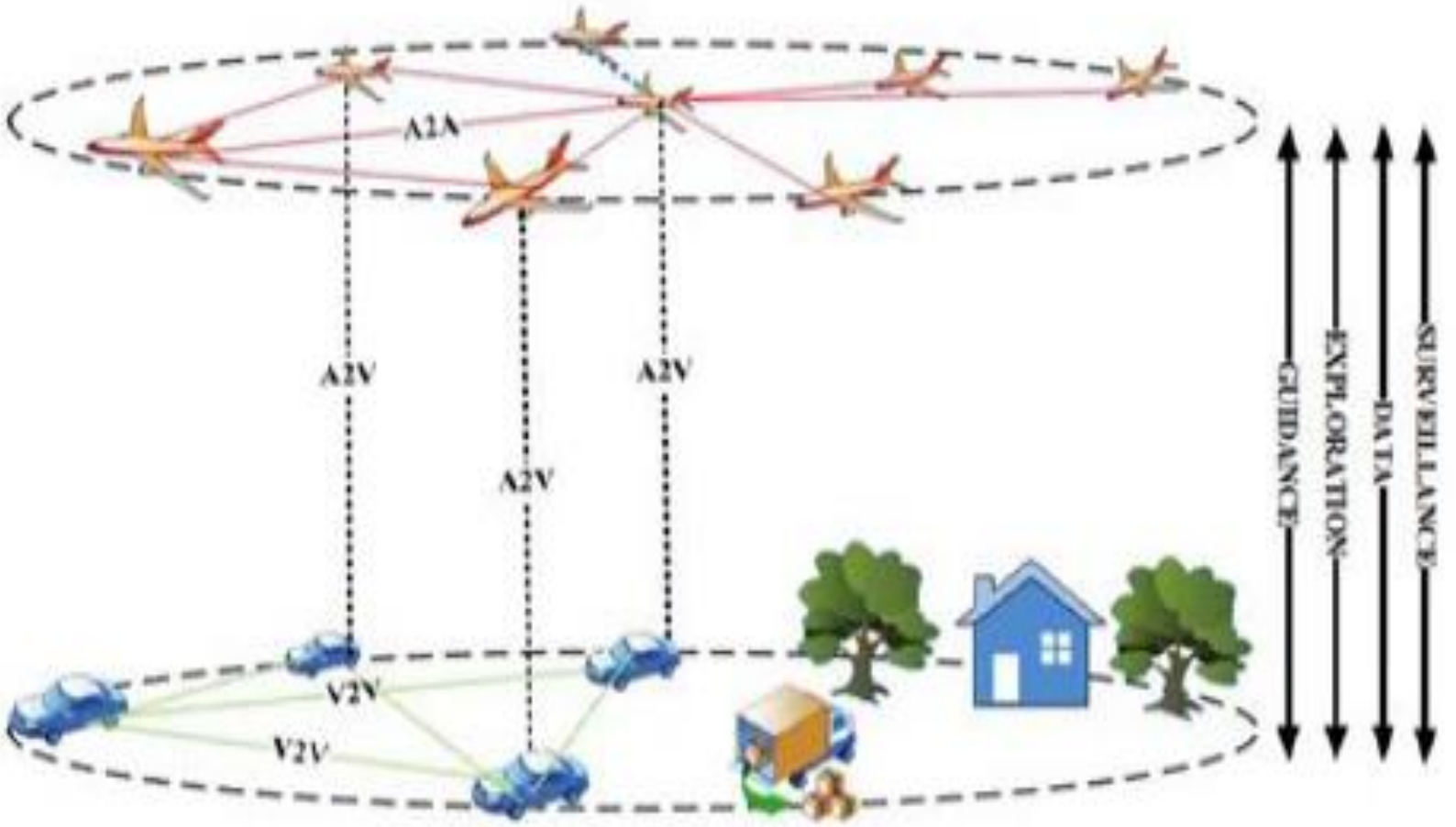


Layered Gateway In FANETs

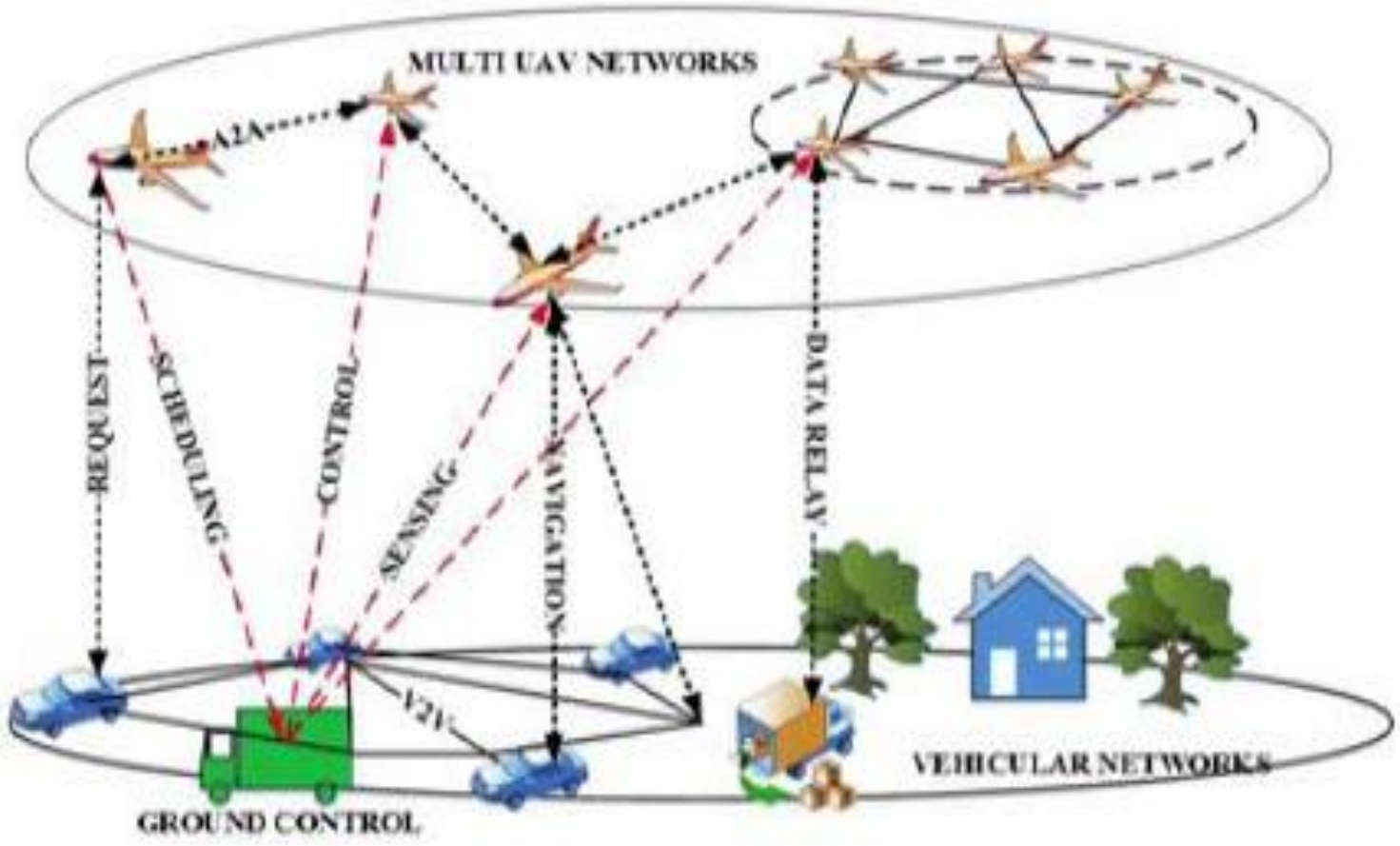
- Multi-layered UAV topologies select one gateway.
- The gateways from each layer communicate to forward information between layers, as well as from ground control.
- Will increase the delay between ground control and higher layers.
- Not suitable for time-critical relaying tasks.



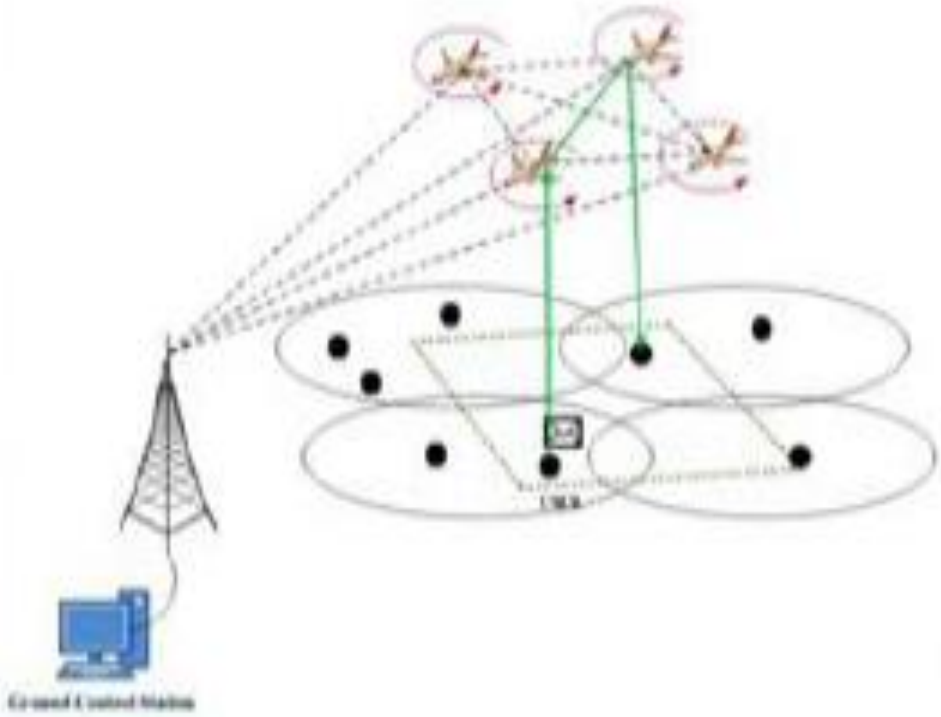
FANETs & VANETs



FANETs & VANETs

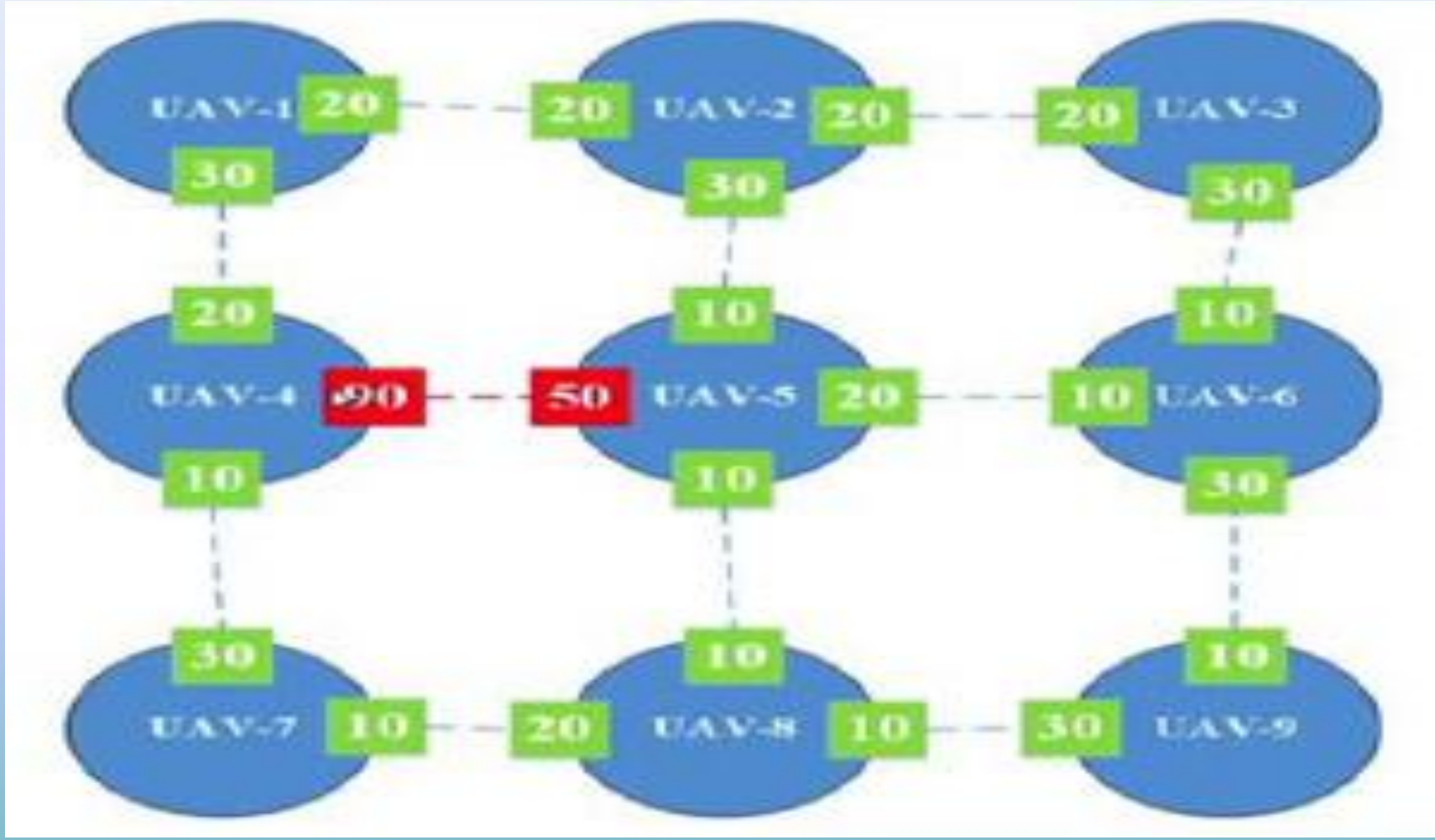


Trajectory Control for Improving Throughput

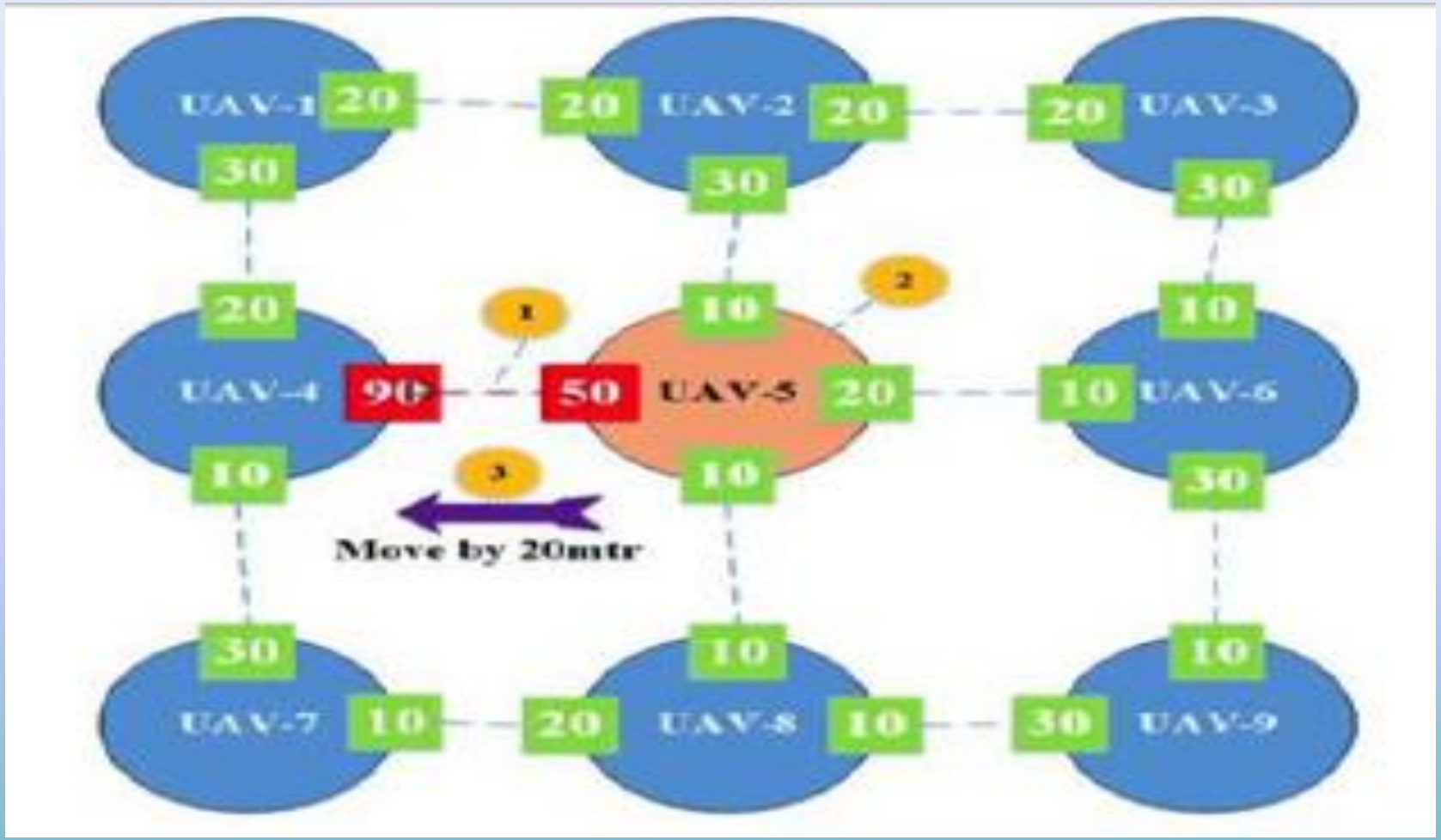


- UAVs with queue occupancy above a threshold experience congestion resulting in communication delay.
- Control station instructs UAVs to change centers of trajectory.
- Command given based on traffic at "busy" communication link.
- To provide enhanced coverage, UAVs may be commanded to change radius of their trajectories.

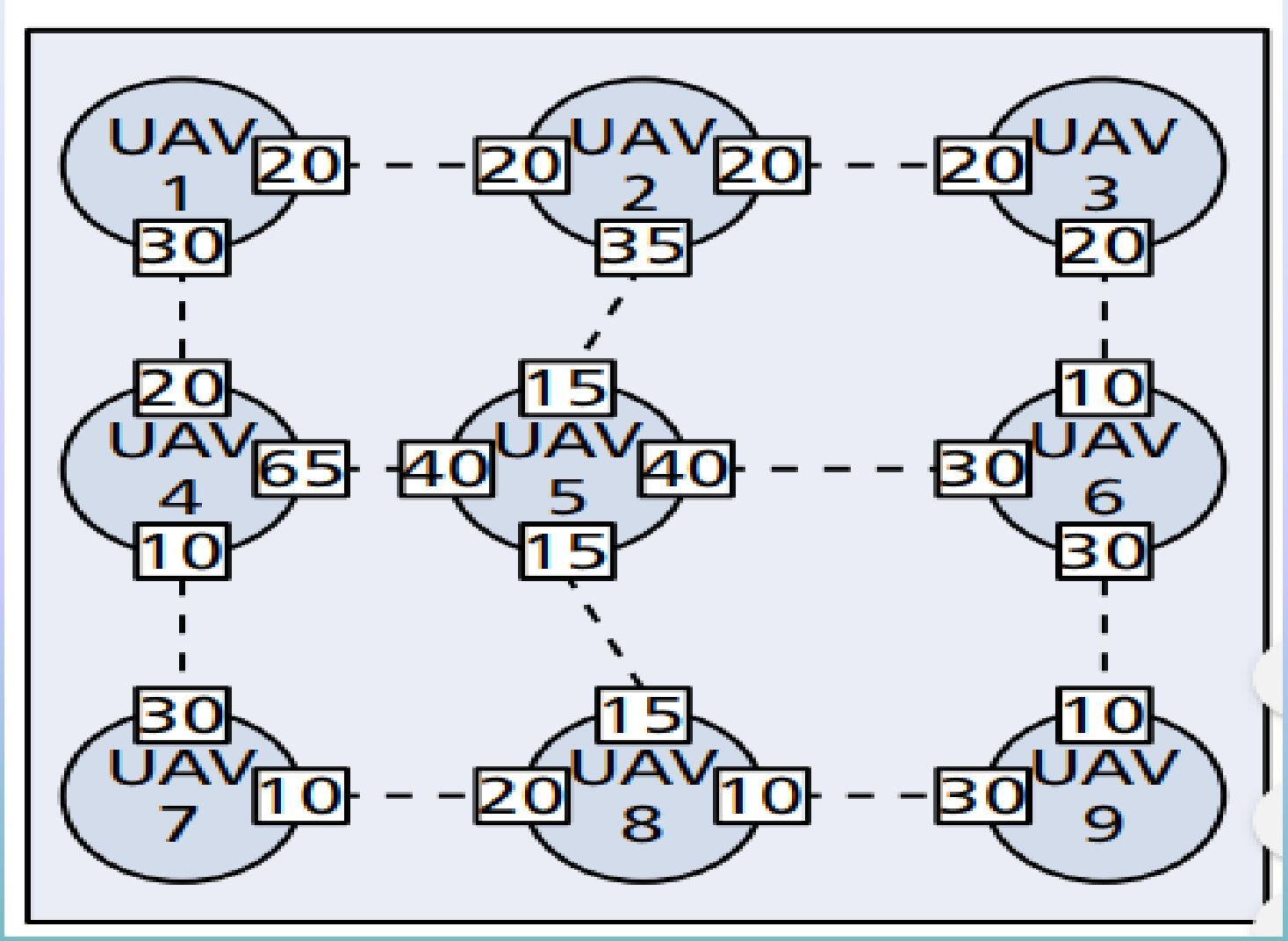
Trajectory Control for Improving Throughput



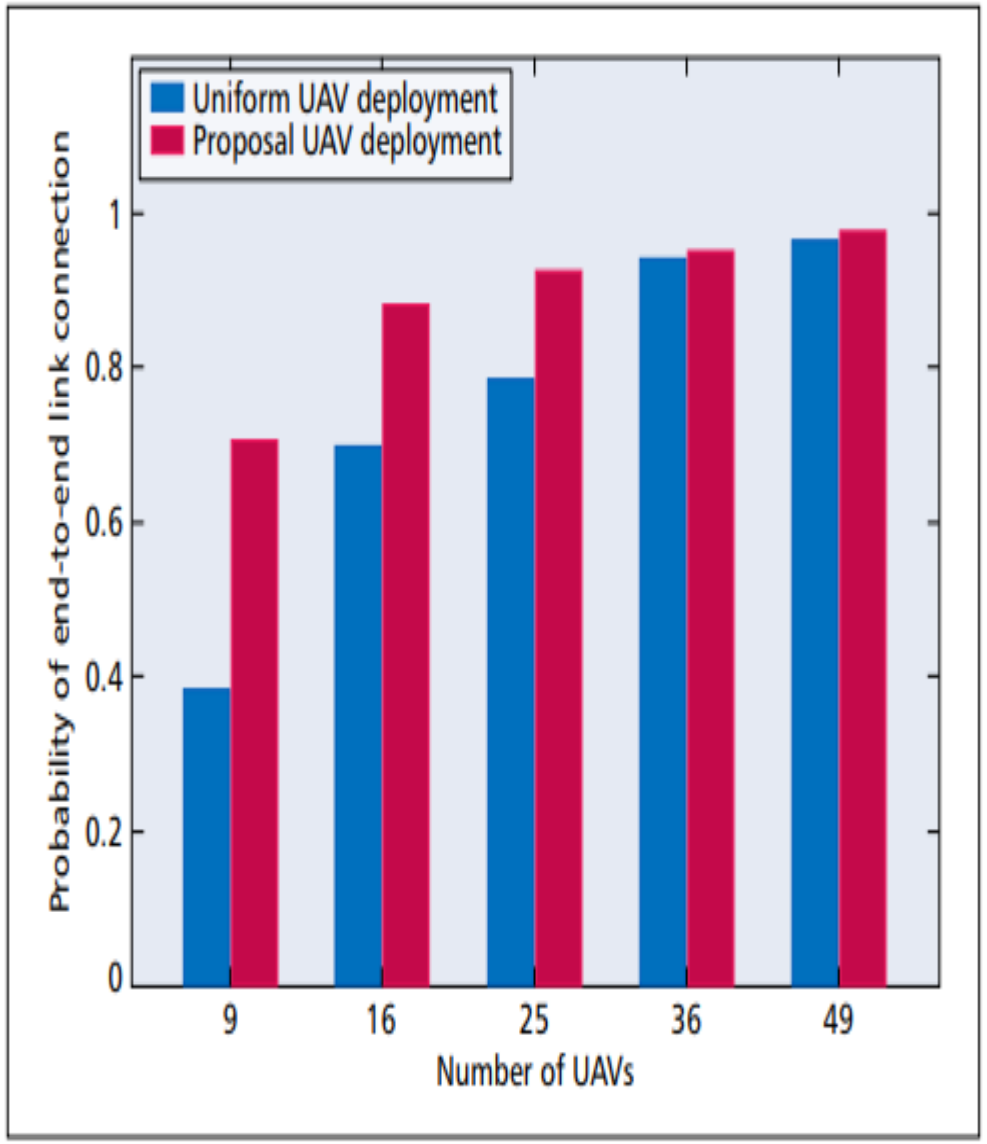
Trajectory Control for Improving Throughput

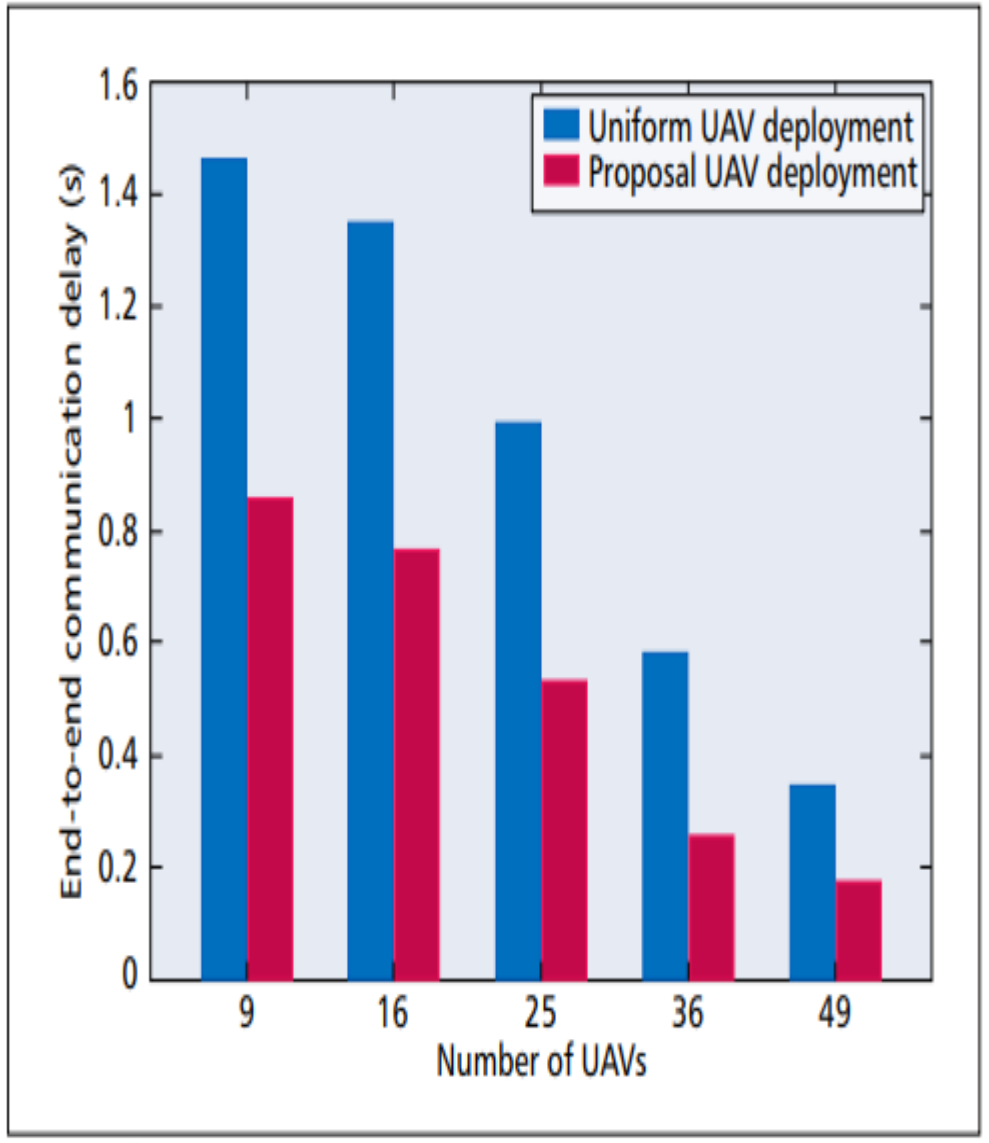


Trajectory Control for Improving Throughput



Trajectory Control for Improving Throughput

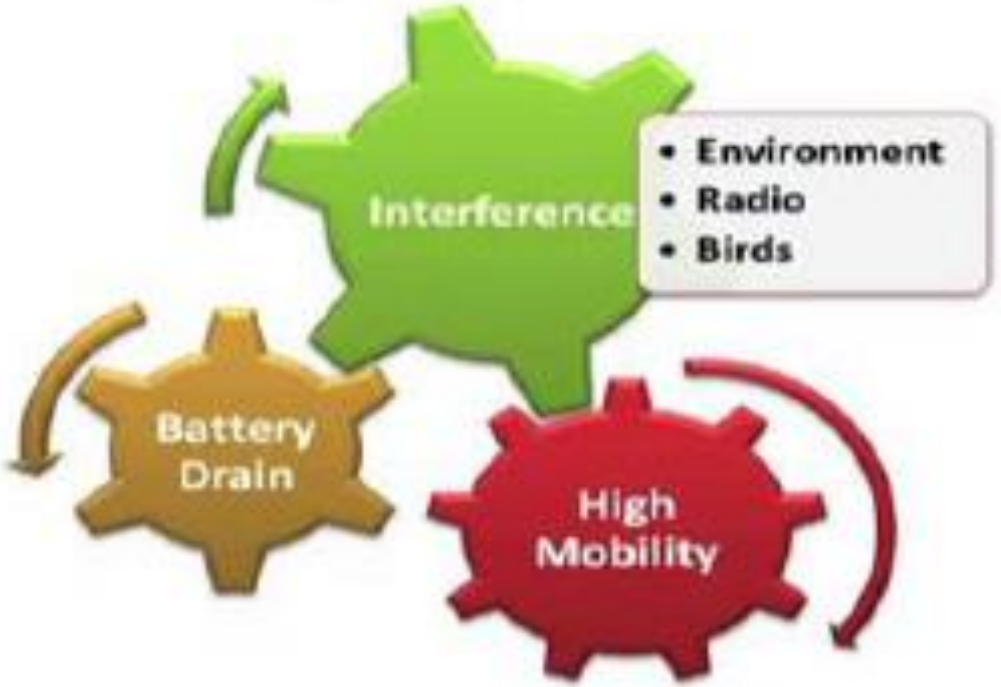




Self-Organization in UAV Networks

- Why ?

Links can be broken frequently because of :

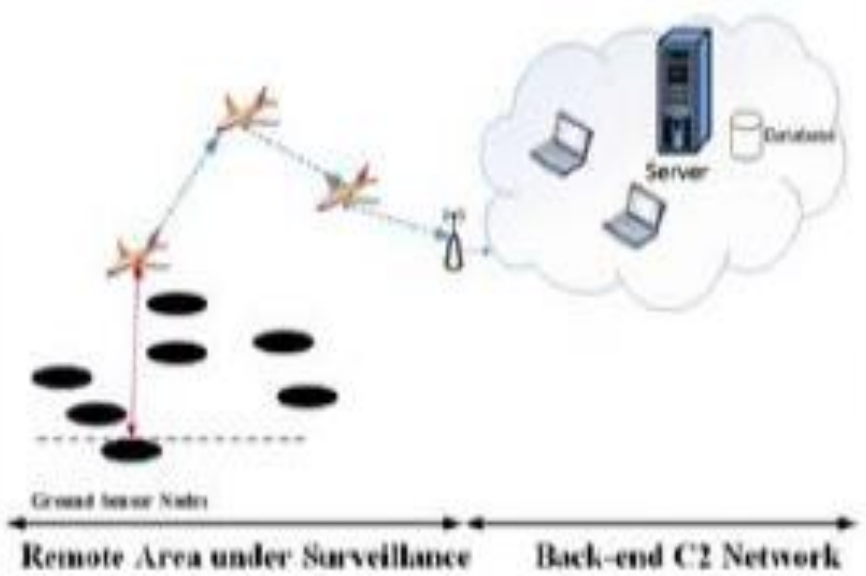


This translates into utilization challenges in planning and allocation of resources.

Self-Organization in UAV Networks

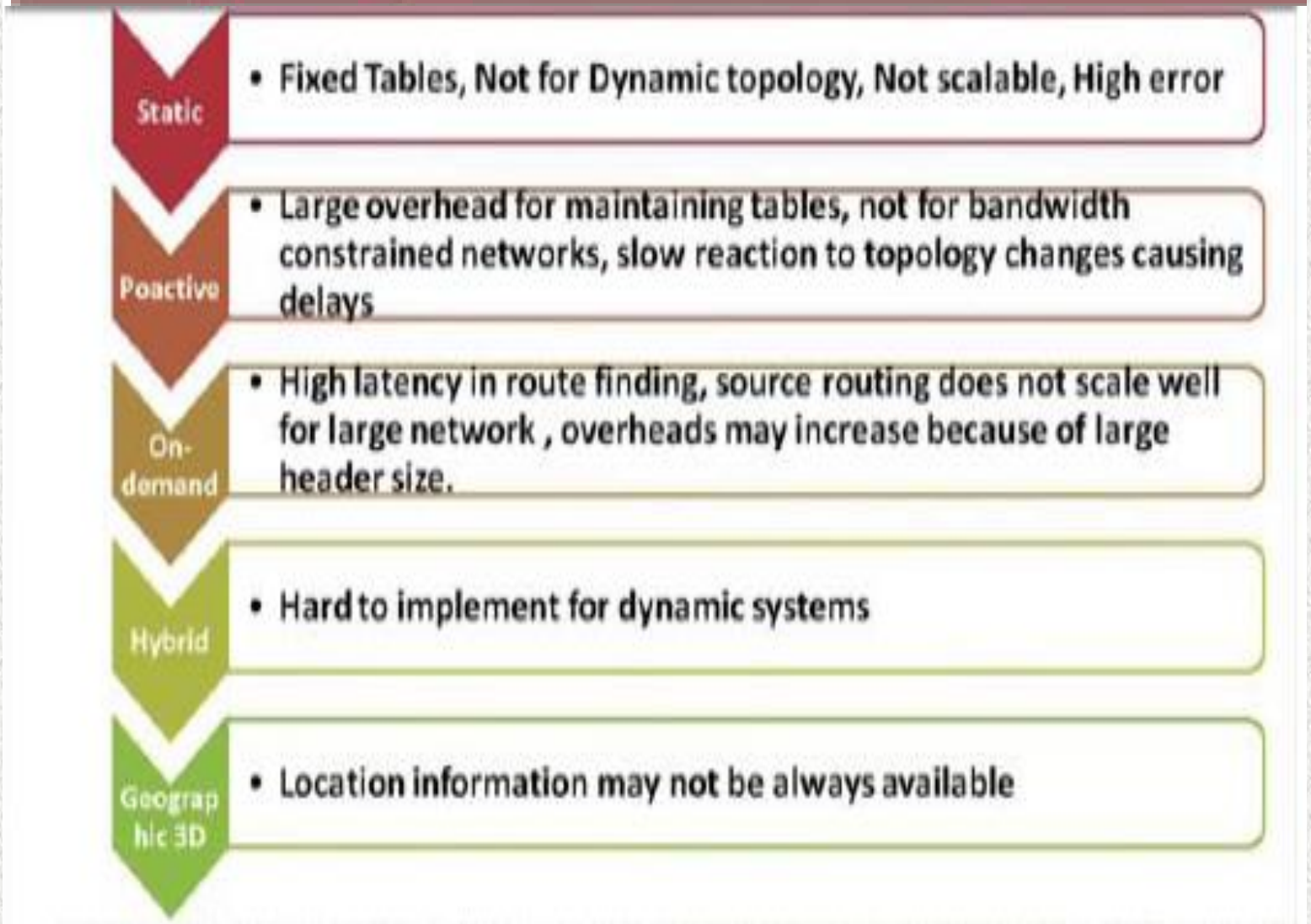
- Steps of Self-organization :

Self Organizing FANETs

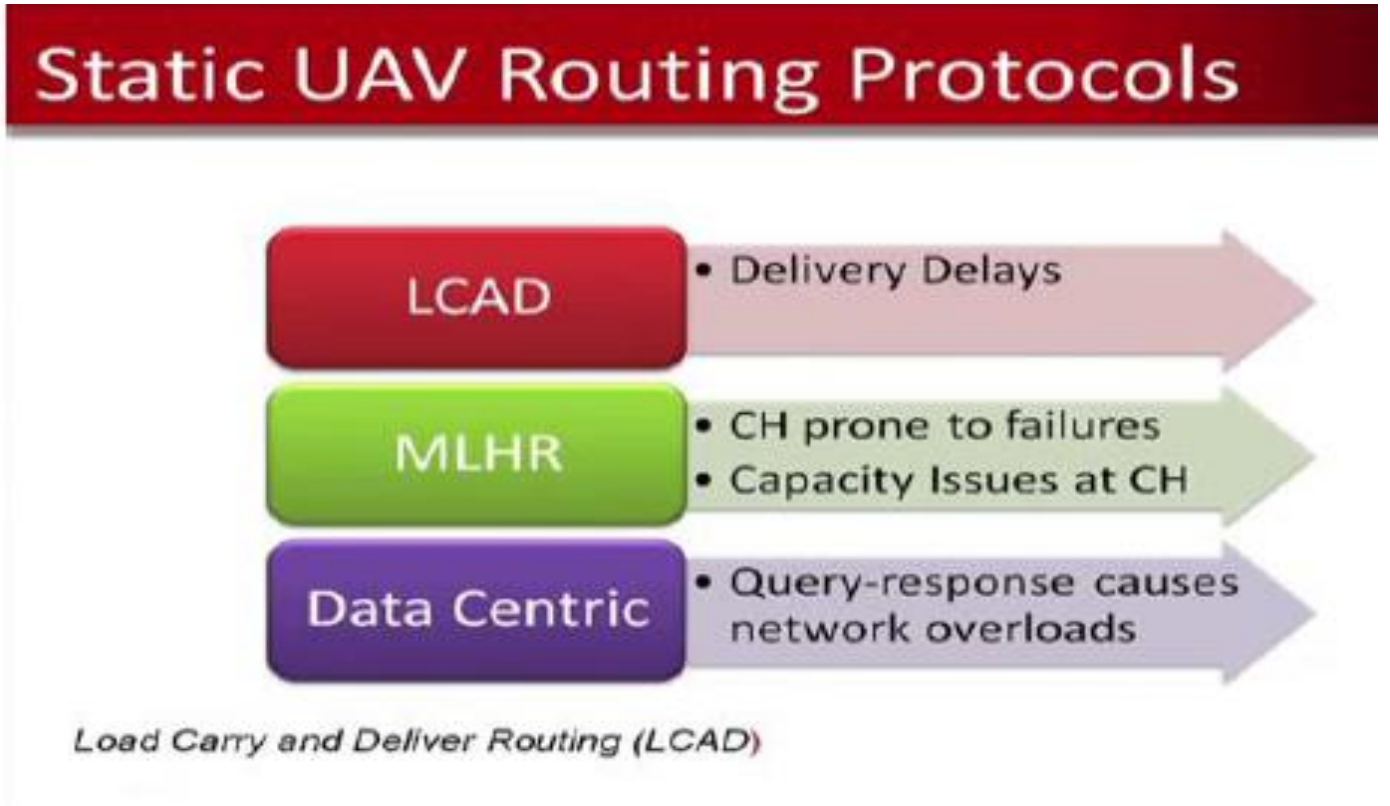


- Unpredictability of motion for military applications can be achieved through:
  - Embedding randomness into the UAVs behavior,
  - Minimizing the number of UAVs needed for a mission, as well as
  - Minimizing the total number of conducted missions by combining them into a single multi-goal mission.

UAV Network Protocols



Static UAV Routing Protocols



Load Carry and Deliver Routing (LCAD)

One of the most popular secure routing protocols. In this model, communication between UAVs does not occur.

This protocol is used to transfer data from a ground base to a ground base using flying UAVs with single hop communication; it is useful to transfer images or videos.

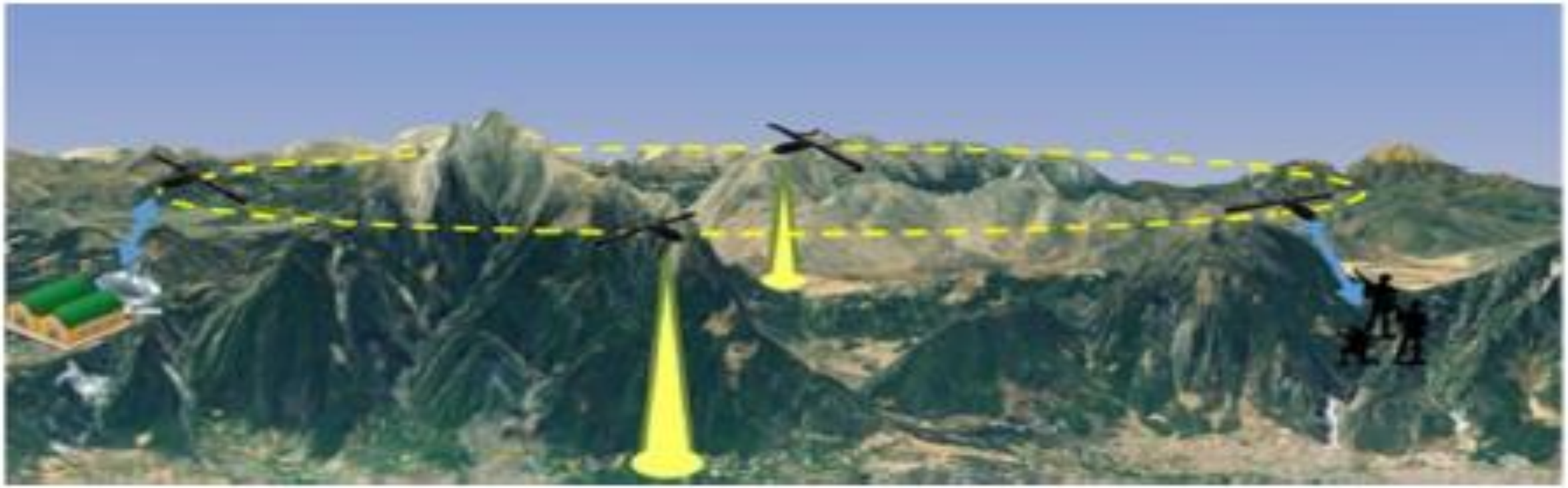
Firstly, the data is loaded from a source access point to the UAV and the UAV moves to the destination access point to deliver the data.

The main objectives of load carry and deliver routing is to maximize throughput and increase the security. In terms of security, this model is secure; because there are no hops during the transfer of data.

The time needed to deliver the data from the source ground base to the destination ground base depends on the speed of UAV and the distance between the source and destination access points.

To decrease the transfer time more than one UAV can be used for the same source and destination, or increase the speed of UAVs, or divide the network into smaller LCAD sub-networks.

Load Carry and Deliver Routing (LCAD)



Multi-Level Hierarchical Routing(MLHR)

Used when UAV networks are organized hierarchically into a number of clusters that need to operate in different mission areas.

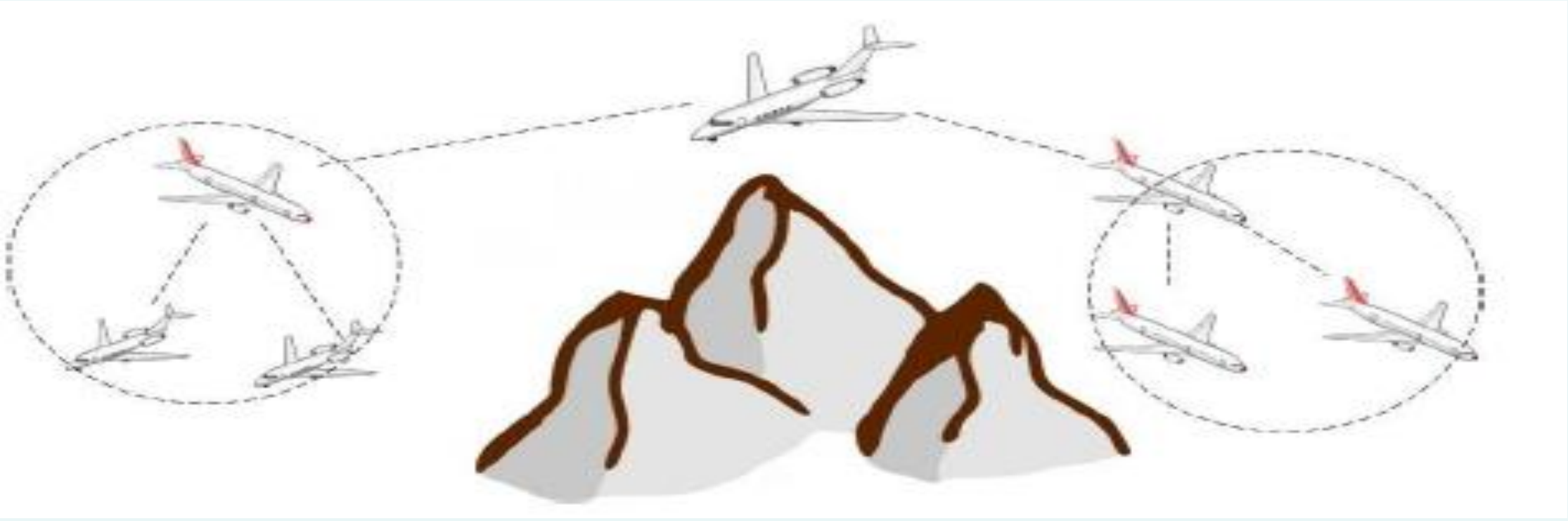
Each cluster has a cluster head (CH), which will represent the whole cluster; this separate cluster can perform different activities.

Each CH is in connection with the upper/lower layers (ground stations, UAVs, satellites, etc.) directly or indirectly.

To broadcast data and control info to other UAVs in the cluster, CH should be in direct communication range of other UAVs in the cluster.

This model is better if UAVs are controlled in changed swarms, the mission area is huge, and several UAVs are used in the network.

Multi-Level Hierarchical Routing(MLHR)



Data-Centric Routing (DCR)

This routing protocol is used when some data is needed by many UAVs in the network, in this case , one-to-many communication is preferred than one to one data transmission.

In this routing protocol, the ID for UAVs is not important; routing is done with respect to the data, not the ID of UAVs that requests it.

UAVs are divided into clusters and work as follows; when a UAV or a ground station needs data such as ,Take a photo for region A if there is more than one tank on the ground, this request will be sent to all UAVs and each one decides if it must collect the data or not, and send the data to other UAVs.

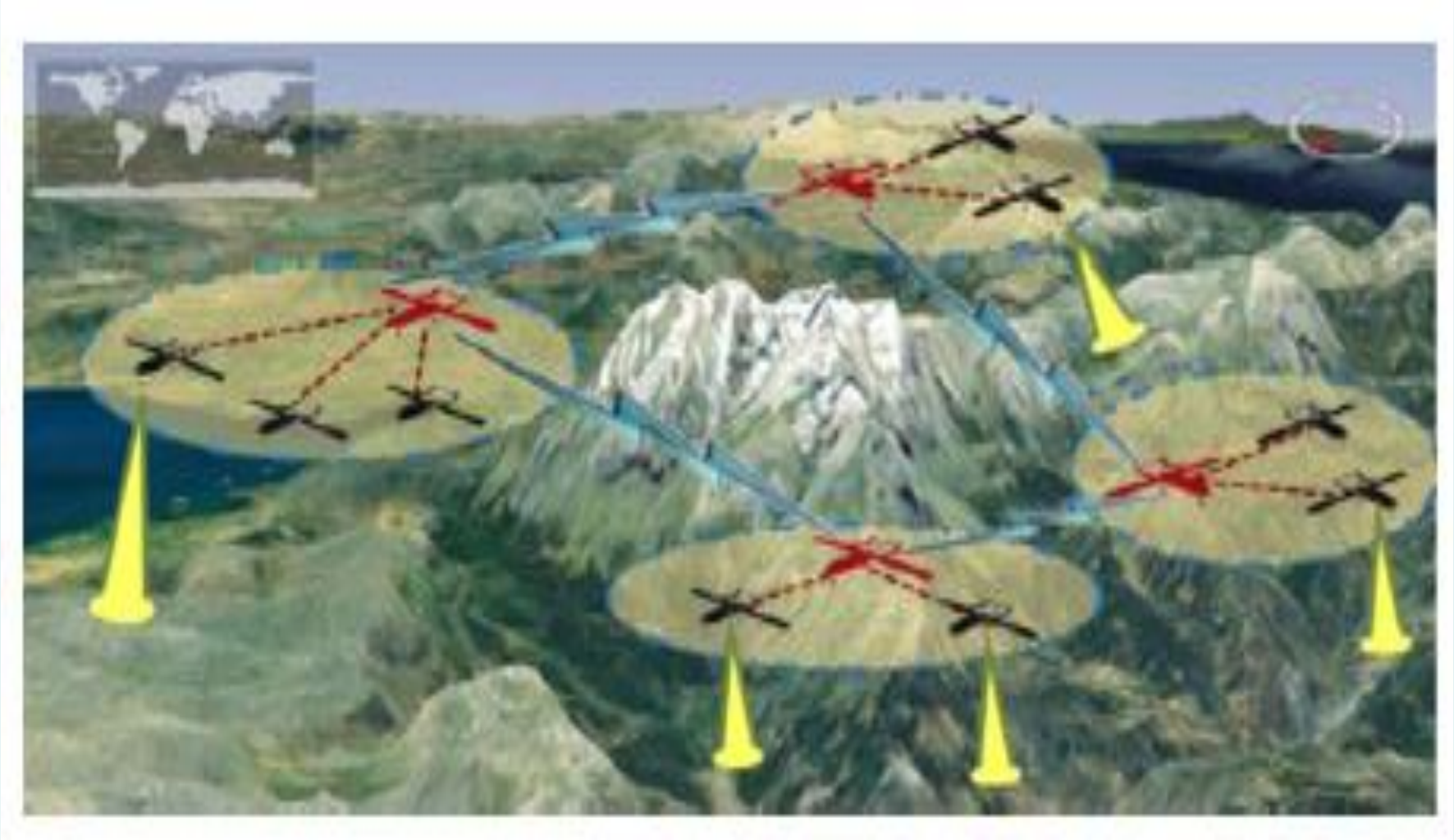
The disadvantage of this technique is the redundant data sent on the network, but there are advantages of this technique like:

 Space decoupling: Communicating UAVs and ground station does not need to know the ID and the location of each other.

 Time decoupling: There is no need for UAVs to be online all the time.

 Flow decoupling: In case there is an interaction in the outside, message sending process is not blocked between UAVs.

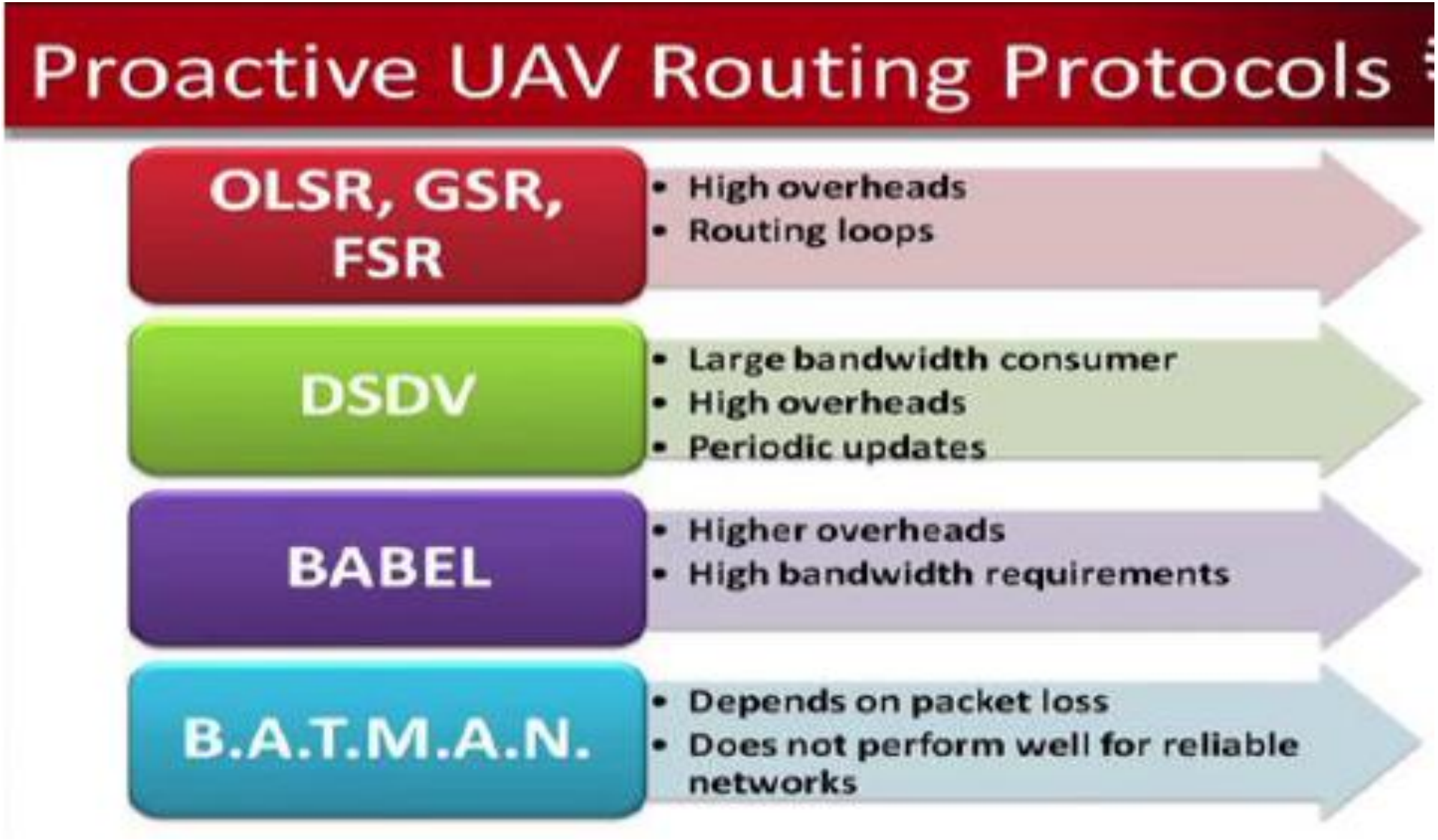
This model can be chosen when the system contains a small number of UAVs on a planned path, which involves minimum assistance.



Proactive Routing Protocols

- Continuously learn the topology of the network by exchanging topological information among the network nodes
- Sometimes called as table-driven routing protocols
- On receiving a request, no need to explore the path, as it proactively maintains the topology information of all nodes
- Periodic update is required

Proactive UAV Routing Protocols



Proactive – OLSR

- OLSR - Optimized Link State Routing protocol
- Inherits the stability of link state algorithm
- Usually in a pure link state protocol, all the links with neighbor nodes are declared and are flooded in the entire network
- OLSR is an optimized version of a pure link state protocol designed for MANET
- Each node in the network uses its most recent information to route a packet
- Hence, even when a node is moving, its packets can be successfully delivered to it, if its speed is such that its movements could at least be followed in its neighborhood

- Link Sate
  - Every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes.
  - Each node then independently calculates the next best logical path from it to every possible destination in the network.
  - The collection of best paths will then form the node's routing table.
- Distance vector
  - A router informs its neighbors of topology changes periodically and, in some cases, when a change is detected in the topology of a network.
  - Compared to link-state protocols, which require a router to inform all the nodes in a network of topology changes, distance-vector routing protocols have less computational complexity.

- It reduces the size of control packets for a particular node by declaring only a subset of links with the node's neighbors who are its multipoint relay selectors, instead of all links in network

- It minimizes flooding of control traffic by using only the selected nodes to disseminate information in the network.

- As only multipoint relays of a node can retransmit its broadcast messages, it significantly reduces the number of retransmissions in a flooding procedure

- Using Hello messages, each node discovers 2-hop neighbor information and performs a distributed election of a set of multipoint relays (MPRs).

- Nodes select MPRs such that there exists a path to each of its 2-hop neighbors via a node selected as an MPR.

  - Each node periodically floods status of its links
  - Each node re-broadcasts link state information received from its neighbors
  - Each node keeps track of link state information received from other nodes
  - Each node uses above information to determine next hop to each destination

24 retransmissions to diffuse a message up to 3 hops

Retransmission node

- Only selected neighbors (MultiPoint Relays, MPRs) retransmit messages
- Select MPRs such that they cover all 2hop neighbors
- 2-hop neighbors taken from neighbors' HELLO messages

11 retransmission to diffuse a message up to 3 hops

Retransmission node - MPR

Global State Routing (GSR)

- Invented by Mario Gerla et al (UCLA).
- Link State Routing (to re-iterate) requires that an update be sent to every node in the network upon the change of the state of a link.
- Flooding may have to be used.
- This is very expensive in a bandwidth starved wireless network.
- GSR is similar to the other link state routing protocols.

GSR Principles

- Attempts to provide the benefits of link-state routing but with the simplicity of distance vector protocols.
- Don't flood the network with link-state updates.
- Instead maintain a link-state table based on up to date information received from neighboring nodes.
- Periodically exchange collected link-state information with its neighbors.
- In some sense this is similar to STAR when optimal routes are required.

Use of Sequence Numbers.

- GSR uses sequence numbers to ensure that the link state table is up to date.
- Entries with older sequence numbers are replaced with updates with later sequence numbers.
- A source rooted minimum cost tree is computed based on the collected link-state and is used to route packets to any destination.

Advantages:

. Can provide loop free paths that are optimal.

· Can be used to support Quality of Service.

Disadvantages

· Most inadequacies of link-state routing protocols remain.

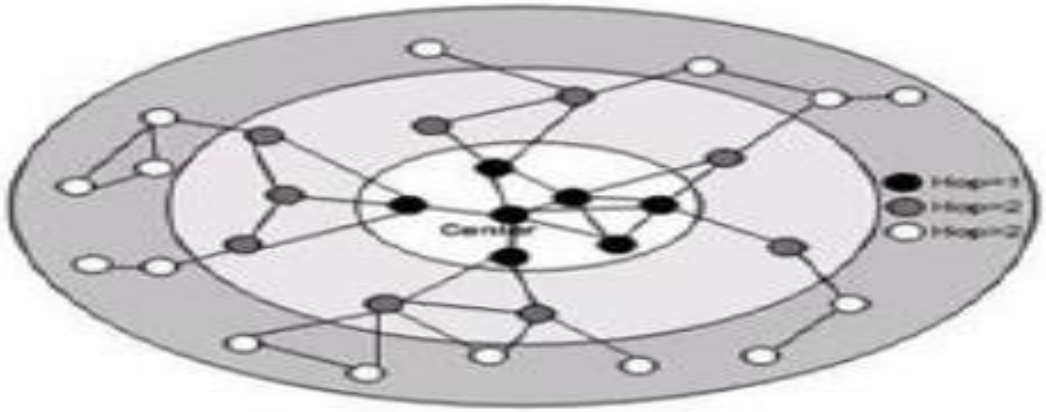
· Link layer reliability is still required.

· If updates are frequent → high overhead, else stale routing info.

· Not very scalable.

Proactive – FSR

- FSR – Fisheye State Routing Protocol
- Uses a special structure of the network called the 'fisheye'
- The basic idea is that, each update message does not contain information about all nodes
- Contains update information about the nearer nodes more frequently than that of the farther nodes
- Each node can have accurate and exact information about its own neighboring nodes



The scope of fisheye is defined as the set of nodes that can be reached within a given number of hops from a particular center node.

Proactive — FSR

FSR routing is made of three tasks:

Neighbor Discovery: Via HELLO messages

Information Dissemination: Link State Announcements messages (LSA)

Route Computation:

LSA messages are generated every Δ seconds using a sequence of distinct Time-To-Live(TTL) values.

Take as an example the sequence 1, 3, 8, 64, the 1-hop neighbours receive the LSA every Δs, so they have the most updated information. 2-hop neighbours receive the LSA with TTL 3, 8, 24. Nodes at a distance from 4 to 8 hops receive only the LSA with TTL 8 and 64. All the others receive only the LSA with TTL 64. As a consequence every node has progressively less updated information on the network topology as the distance increases.

Proactive — FSR

The protocol exploits the fact that when a packet moves from a source to a destination, the nodes encountered on the shortest path have an increasingly precise topology information about the topological position of the destination (as their distance to the destination decreases), so the loss of accuracy in the shortest path computation from the source node is compensated along the path to the destination.

FSR thus decreases the overall quantity of information spread in the network, since LSA are not sent with a fixed maximum TTL.

Drawbacks:

One of the typical issues with link-state protocols is that when a node or link breaks, temporary loops can be created. It introduces areas in the network with potentially different information sets, so it increases the probability of creating temporary loops.

Proactive – DSDV

- DSDV – Dynamic Destination-Sequenced Distance-Vector
- Based on the Bellman-Ford routing algorithm with some modifications
- Each mobile node keeps a routing table.
- Each of the routing table contains the list of all available destinations and the number of hops to each.
- Each table entry is tagged with a sequence number which is originated by the destination node
- Periodic transmissions of updates of the routing tables help maintaining the topology information of the network.

DSDV (Contd.)

- If there is any new significant change for the routing information, the updates are transmitted immediately
- Routing information updates might either be periodic or event-driven
- DSDV requires each mobile node in the network to advertise its own routing table to its current neighbors.
- The advertisement is done either by broadcasting or by multicasting
- By the advertisements, the neighboring nodes can know about any change that has occurred in the network due to the movements of nodes

- The routing updates can be done in two ways:
  - Full dump: the entire routing table is sent to the neighbors
  - Incremental Update: only the entries that require changes are sent
- Full dump is transmitted relatively infrequently when no movement of nodes occur.
- Incremental updates could be more appropriate when the network is relatively stable, so that extra traffic could be avoided.
- When the movements of nodes become frequent, the sizes of the incremental updates become large.
- In such a case, full dump is useful

- Sequence number is used to denote that an update is new or old.
- For updating the routing information in a node, the update packet with the highest sequence number is used
- Each node waits up to certain time interval to transmit the advertisement message to its neighbors, so that the latest information with better route to a destination can be informed to the neighbors

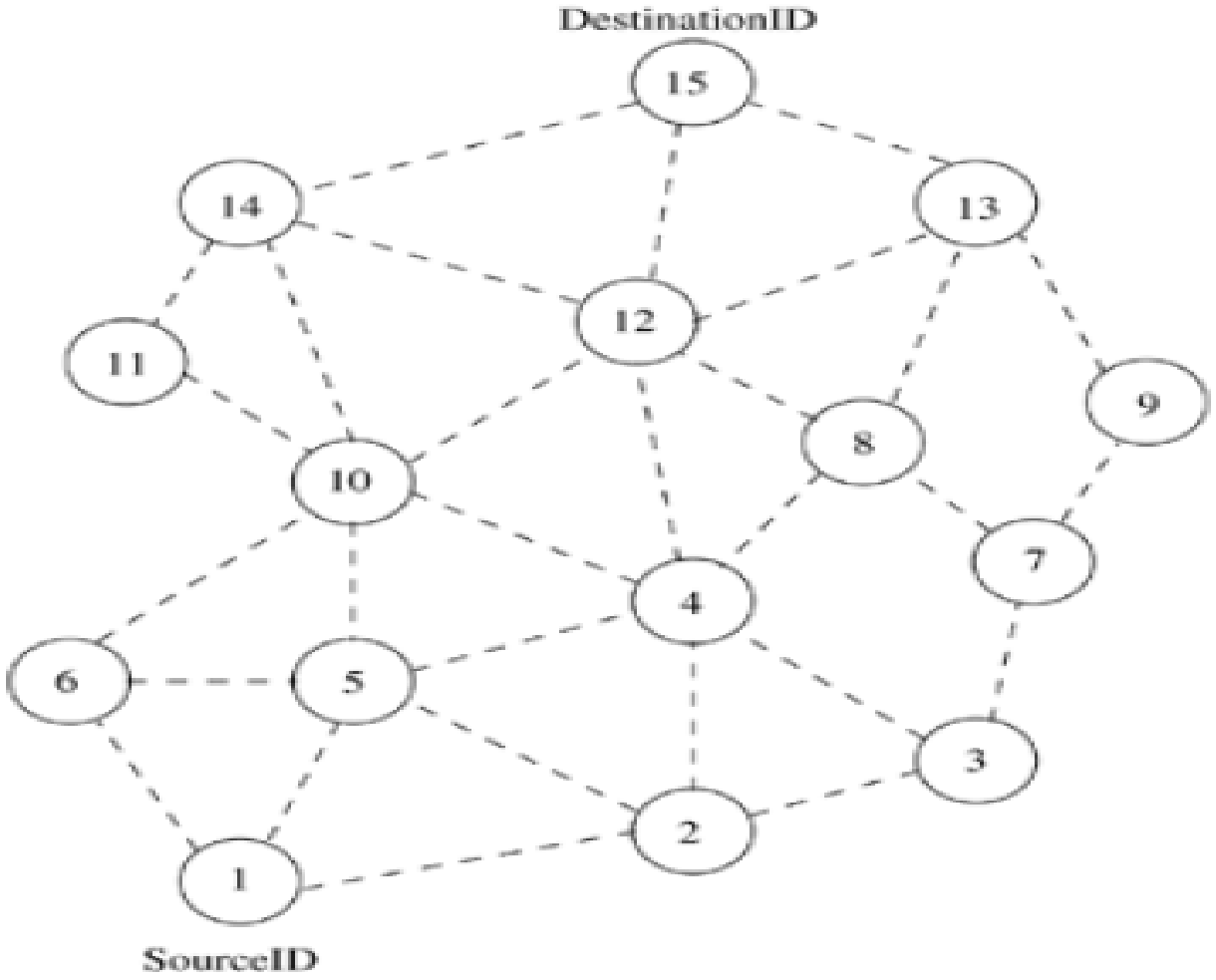
Forwarding Table of Node M2

Destination	Next Hop	Metric	Sequence Number
M1	M1	1	S593_M1
M2	M2	0	S983_M2
M3	M3	1	S193_M3
M4	M4	1	S233_M4
M5	M4	2	S243_M5
M6	M4	2	S053_M6

Advertised Route Table of M2

Destination	Metric	Sequence Number
M1	1	S593_M1
M2	0	S983_M2
M3	1	S193_M3
M4	1	S233_M4
M5	2	S243_M5
M6	2	S053_M6

Route establishment in DSDV.

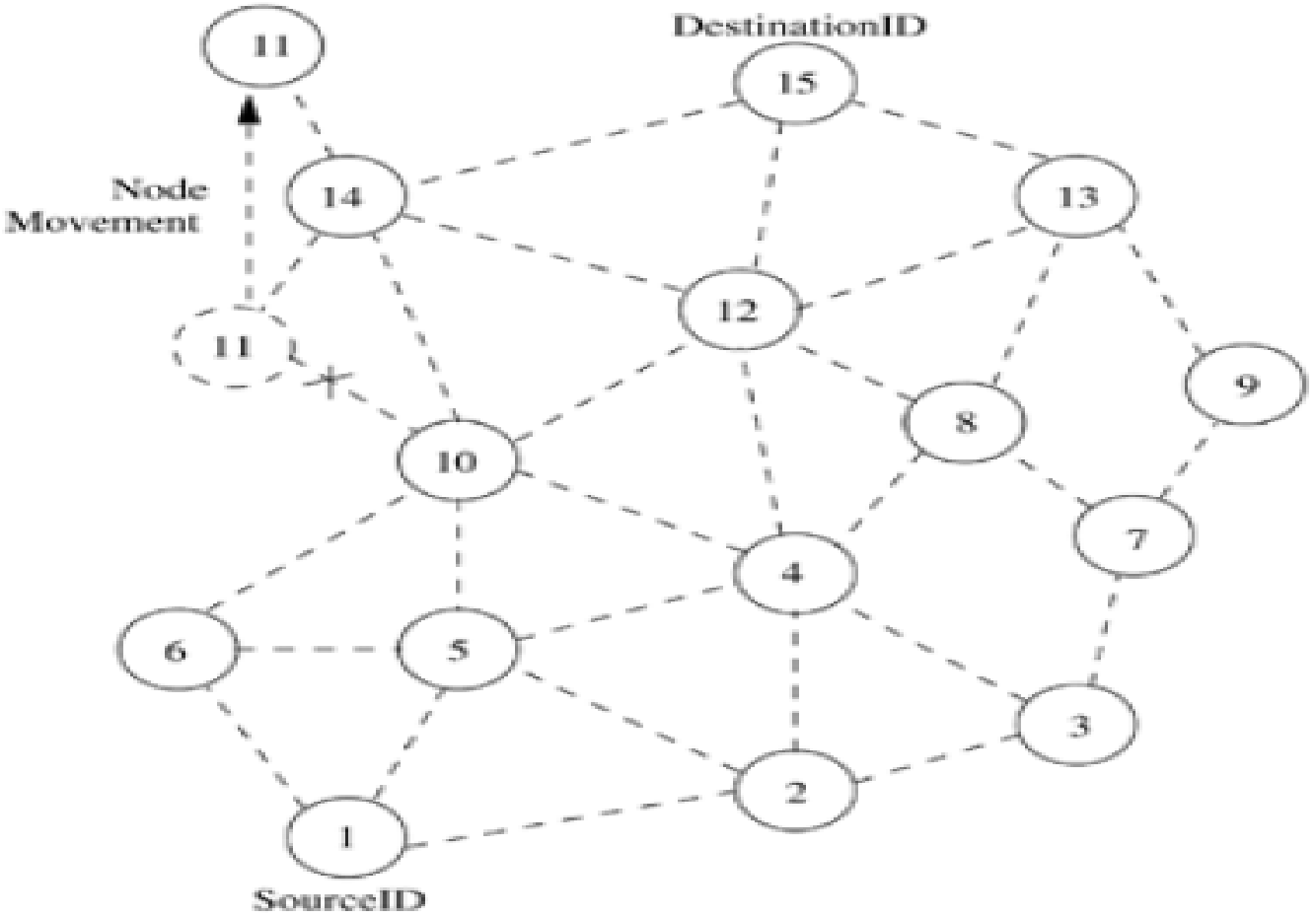


(a) Topology graph of the network

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b) Routing table for Node 1

Route maintenance in DSDV.



(a) Topology graph of the network

Routing Table for Node 1

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b) Routing table for Node 1

- Sequence number
  - Originated from destination. Ensures loop freeness.
  - Generally even if a link is present; otherwise odd
  - Generated by the destination.

- The transmitter needs to send out next update with this sequence number

Disadvantages:

- It suffers from excessive control overhead that is proportional to the number of nodes in the network and hence is not scalable in ad hoc wireless networks, which have limited bandwidth and whose topologies are highly dynamic.

- In order to obtain information about a destination node, a node has to wait for a table update message initiated by the same destination node. This delay could result in stale routing information at nodes.

Advantages:

- The availability of routes to all destinations at all times implies that much less delay is involved in the route setup process.
- The mechanism of incremental updates with sequence number tags makes the existing wired network protocols adaptable to ad hoc wireless networks with fewer modifications.

DSDV - Summary

- Proactive routing protocol
- Each node maintains a routing table
- Sequence number is used to update the topology information
- Update can be done based on event-driven or periodic
- Observations
  - May be energy-expensive due to high mobility of the nodes
  - Delay can be minimized, as path to a destination is already known to all nodes

Proactive - WRP

- WRP – Wireless Routing Protocol
- Belongs to the general class of path-finding algorithms
- Set of distributed shortest-path algorithms that calculate the paths using information regarding the length and second-to-last hop of the shortest path to each destination
- For routing, each node maintains four things
  - Distance Table
  - Routing Table
  - Link Cost Table
  - Message Retransmission List (MRL)

- WRP inherits the properties of the distributed Bellman-Ford algorithm.
- To counter the count-to-infinity problem and to enable faster convergence, it maintains shortest distance to every destination node in the network and the penultimate hop node on the path to every destination node.
- Like DSDV, it maintains an up-to-date view of the network, every node has a readily available route to every destination node in the network.
- It differs from DSDV in table maintenance and in the update procedures.
- While DSDV maintains only one topology table, WRP uses a set of tables to maintain more accurate information.
- The tables that are maintained by a node are the following: distance table (DT), routing table (RT), link cost table (LCT), and a message retransmission list (MRL).

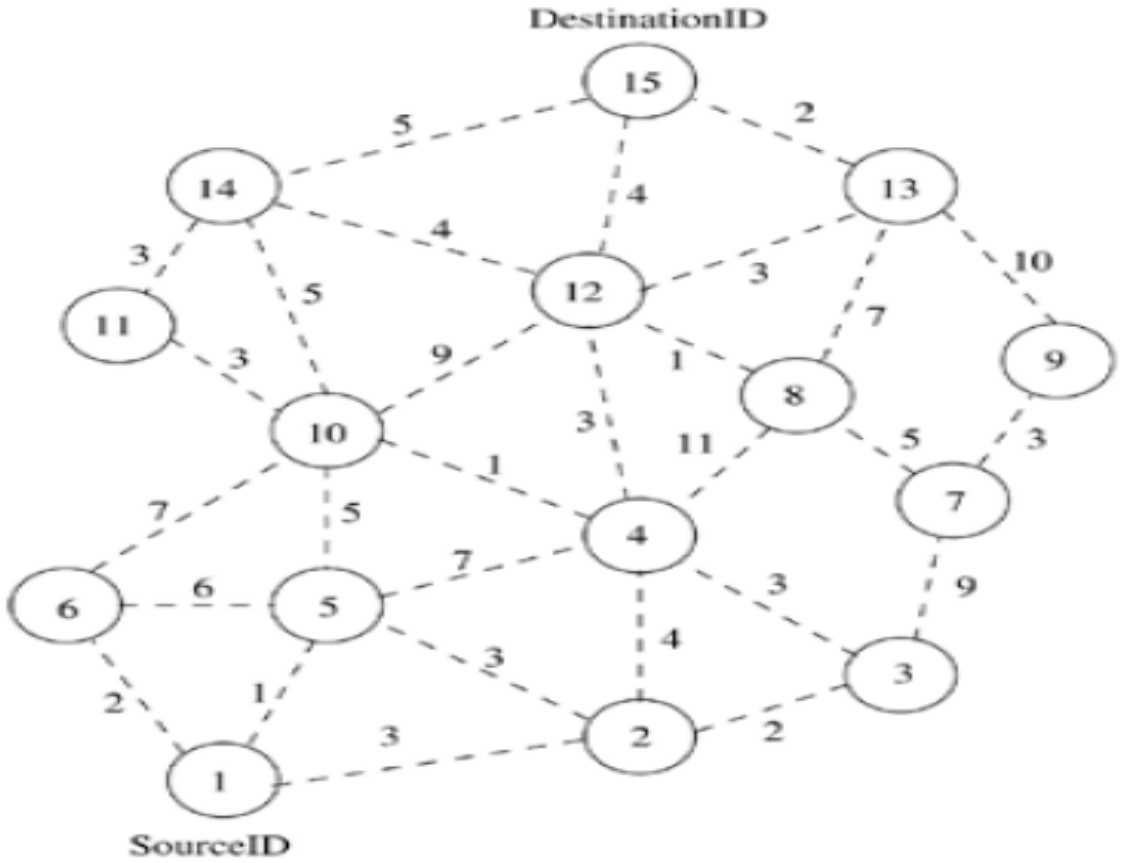
- The DT contains the network view of the neighbors of a node.
- It contains a matrix where each element contains the distance and the penultimate node reported by a neighbor for a particular destination.
- The RT contains the up-to-date view of the network for all known destinations.
- It keeps the shortest distance, the *predecessor* node (penultimate node), the *successor* node (the next node to reach the destination), and a flag indicating the status of the path.
- The path status may be a simple path (correct), or a loop (error), or the destination node not marked (null).
- The LCT contains the cost (*e.g.*,the number of hops to reach the destination) of relaying messages through each link. The cost of a broken link is ∞. It also contains the number of update periods (intervals between two successive periodic updates) passed since the last successful update was received from that link. This is done to detect link breaks.

- The MRL contains an entry for every update message that is to be retransmitted and maintains a counter for each entry. This counter is decremented after every retransmission of an update message.

- Once the counter reaches zero, the entries in the update message for which no acknowledgments have been received are to be retransmitted and the update message is deleted.

- A node detects a link break by the number of update periods missed since the last successful transmission. After receiving an update message, a node not only updates the distance for transmitted neighbors but also checks the other neighbors' distance, hence convergence is much faster than DSDV.

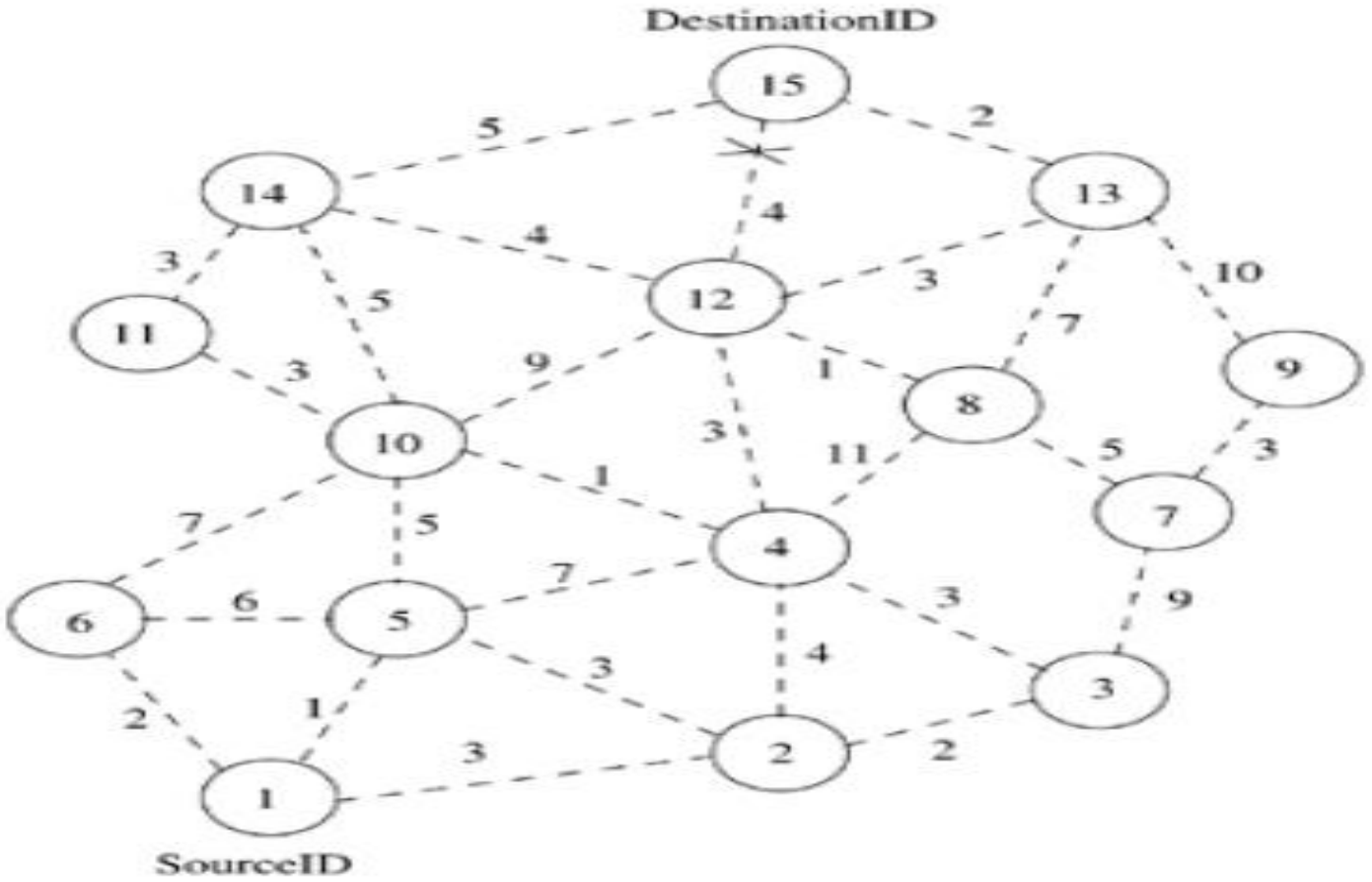
Route establishment in WRP.



Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	12	4
11	14	14	8
10	4	12	8
9	13	13	12
8	12	12	5
7	8	12	10
6	10	12	15
5	10	12	13
4	12	12	10
3	4	12	7
2	4	12	11
1	2	12	14

Route maintenance in WRP.



Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	13	5
11	14	14	8
10	4	13	9
9	13	13	12
8	12	13	6
7	8	13	11
6	10	13	16
5	10	13	14
4	12	13	8
3	4	13	11
2	4	13	12
1	2	13	15

Advantages:

- WRP has the same advantages as that of DSDV. In addition, it has faster convergence and involves fewer table updates.

Disadvantages:

- The complexity of maintenance of multiple tables demands a larger memory and greater processing power from nodes in the ad hoc wireless network.
- At high mobility, the control overhead involved in updating table entries is almost the same as that of DSDV and hence is not suitable for highly dynamic and very large ad hoc wireless networks.

Summary - WRP

- Proactive routing protocol
- Maintains multiple tables – distance table, routing table, link-cost table, message retransmission list
- Overhead may be increased, a node has to maintain multiple tables
- Energy-expensive – require more energy on updating the neighbor list, as the node retransmits multiple times

- The **Babel** routing protocol is a distance-vector routing protocol that is designed to be robust and efficient(Fast Convergence) on both wireless mesh networks and wired networks.

- Babel is based on the ideas in DSDV, AODV, and Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP), but uses different techniques for loop avoidance. However periodic routing table updates creates more traffic.

- Better Approach To Mobile Adhoc Networking (B.A.T.M.A.N.) is a routing protocol that provides decentralization of the knowledge about the best route through the network — no single node has all the data.

- BATMAN eliminates the need to spread information concerning network changes to every node in the network.

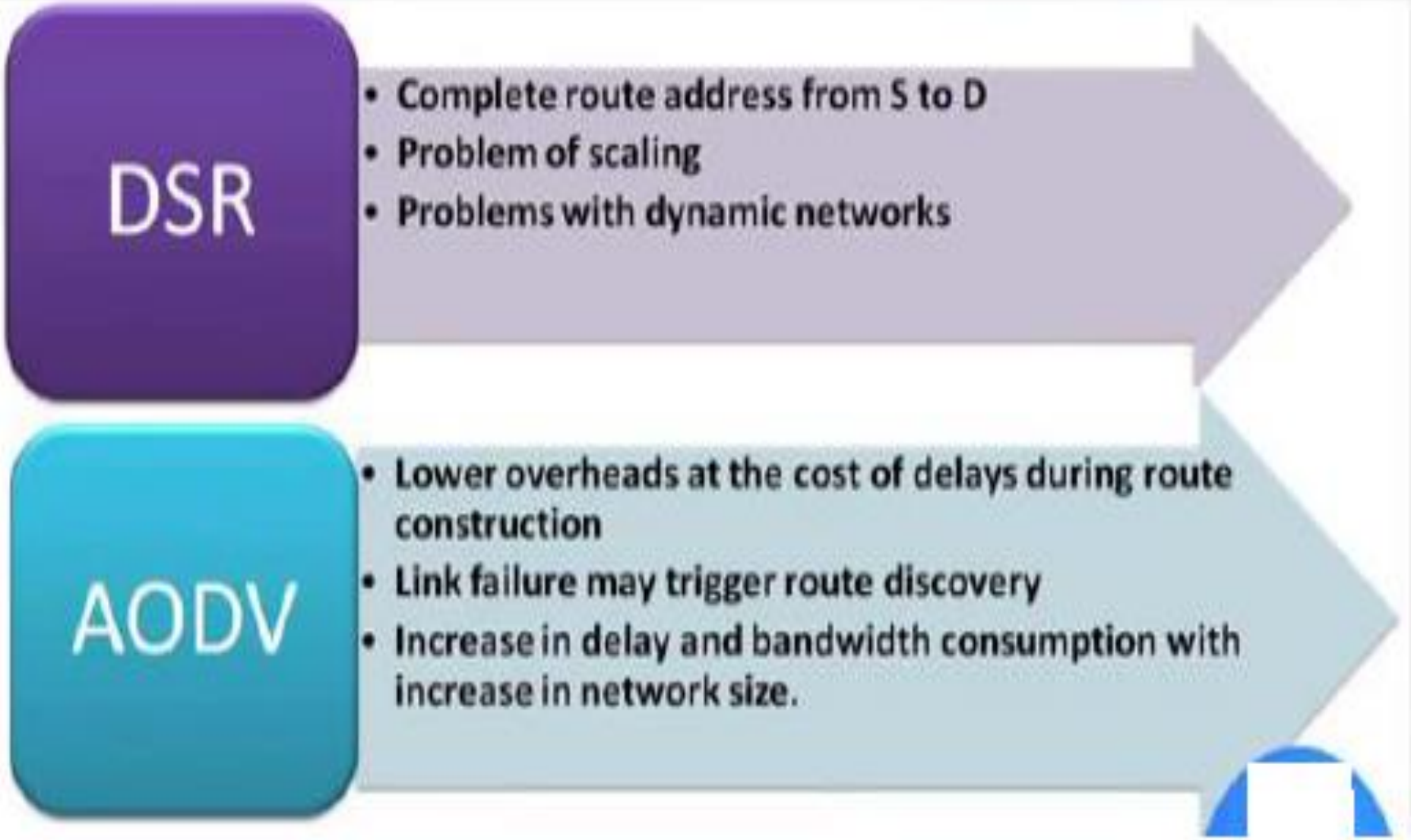
- The individual node only saves information about the "direction" it received data from and sends its data accordingly.

- The data gets passed on from node to node and packets get individual, dynamically created routes. A network of collective intelligence is created.

Reactive Routing Protocols

- Based on some sort of *query-reply dialog*
- On receiving a request, it explores the possible routing paths for establishing route (s) to the destination
- Do not need periodic transmission of topological information of the network
- Primarily seem to be resource conserving protocols
- Reactive protocols are also known as on-demand routing protocols

On-Demand UAV Routing Protocols



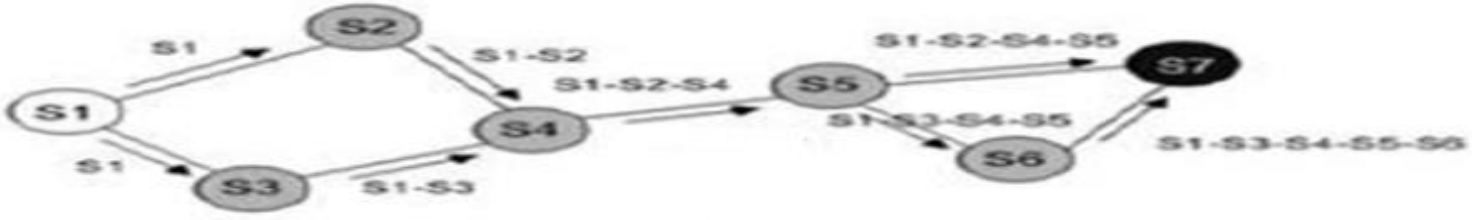
Reactive – DSR

- DSR — Dynamic Source Routing
- Allows nodes in the MANET to dynamically discover a source route across multiple network hops to any destination
- The mobile nodes are required to maintain route caches of the known routes.
- The route cache is updated when any new route is known for a particular entry in the route cache
- Routing in DSR is done using two phases
  - route discovery
  - route maintenance

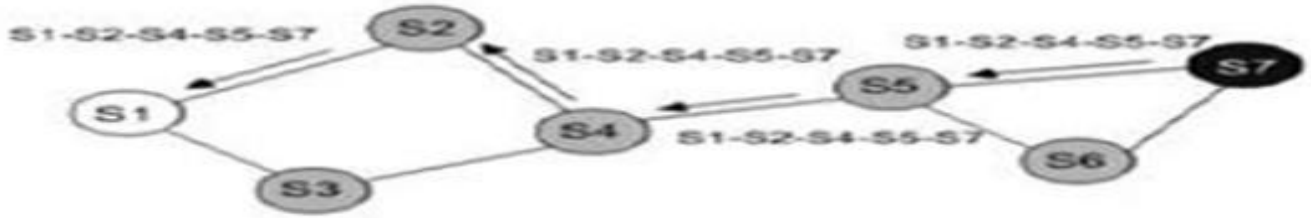
- Need to send a packet to destination
  - First consults its route cache to determine whether it already knows about any route to the destination or not.
  - If already there is an entry for that destination, the source uses that to send the packet. If not, it initiates a route request broadcast
- The request packet includes followings:
  - Destination address
  - Source address
  - Unique identification number
- Each intermediate node checks and forwards the packet and eventually this reaches the destination.

- Mechanism
  - Route discovery
  - Route maintenance
  - Mechanisms "on-demand"
    - No periodic routing advertisement
    - No link status sensing
    - No neighbor detection packets
  - Routes caching

- Route Discovery
  - A node processes the route request packet only if it has not previously processed the packet and its address is not present in the route record of the packet.
  - A route reply is generated by the destination or by any of the intermediate nodes when it knows about how to reach the destination.



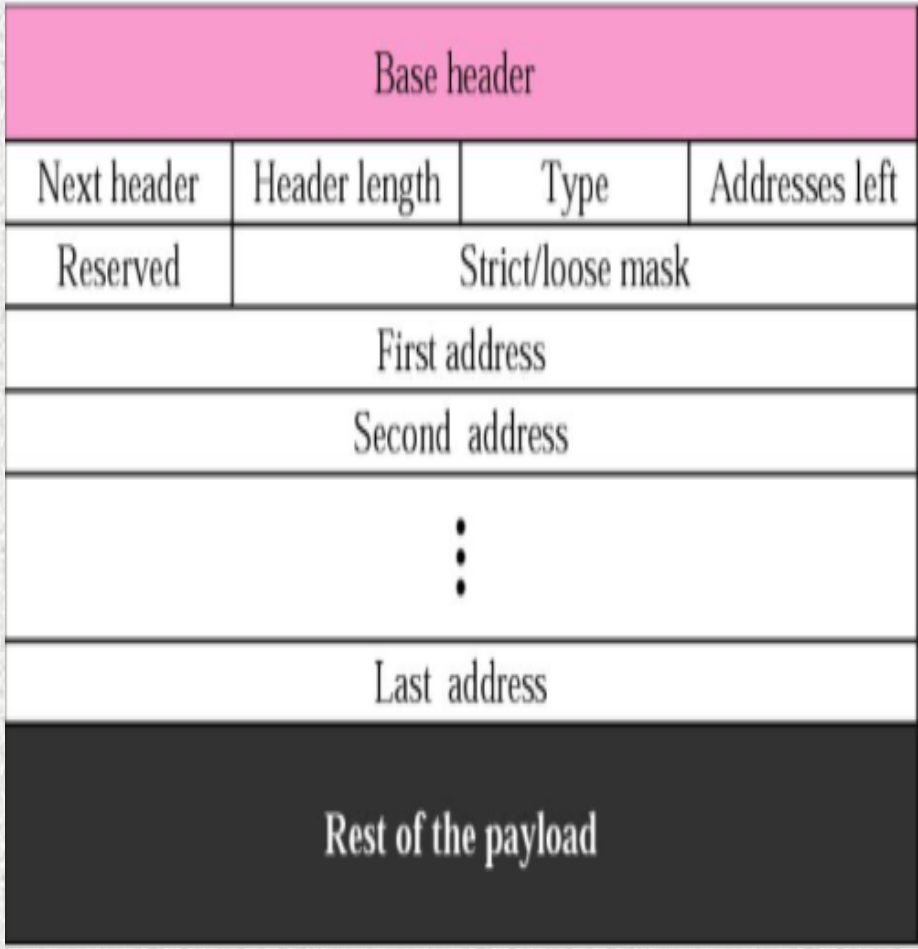
Route discovery



Using route records to send the route reply

- After getting the path to destination (from reply packet), source node sends data packet.

- Route Maintenance
  - Each node maintains a list in its cache to other nodes.
  - If another source node requests path to the same destination, the intermediate node can reply immediately.
  - If there is any change in the path, it updates its cache for the destination
- Route cache
  - Each node maintains a cache to store path information to other nodes



Source Routing Header

Optimizations:

Route Cache, Exponential Backoff Algorithm, Piggy backing of Data

Advantages:

- It eliminates the need to periodically flood the network with table update messages.
- A route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approach is eliminated.
- The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.

Disadvantages:

- The route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase.
- The connection setup delay is higher than in table-driven protocols.
- Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility.
- Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.

DSR - Summary

- Reactive routing protocol
- Consists two phases – route discovery and route maintenance
- Route cache can be updated periodically, so that use of obsolete information can be avoided

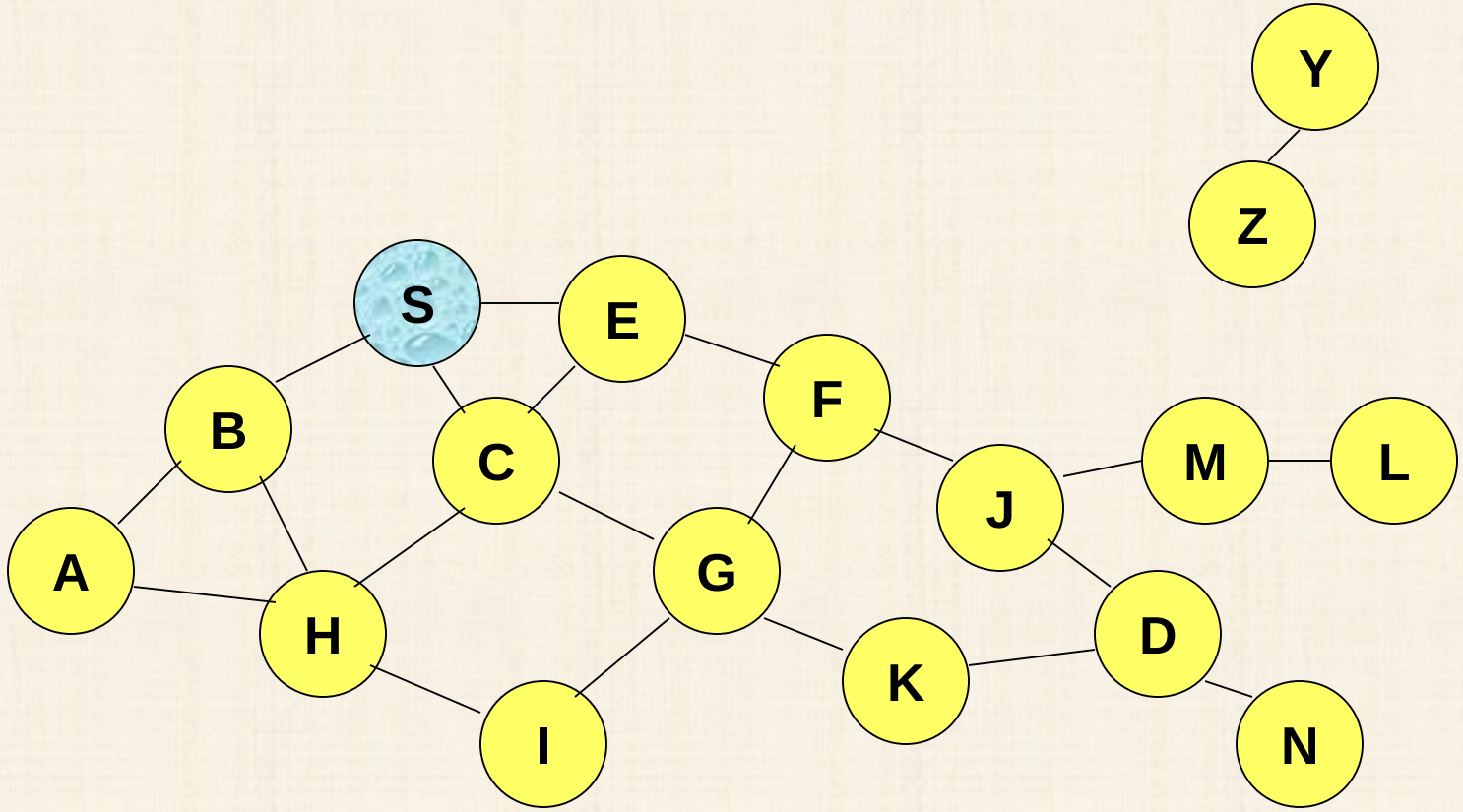
Ad Hoc On-Demand Distance Vector Routing (AODV)

- DSR includes source routes in packet headers
- Resulting large headers can sometimes degrade performance
  - particularly when data contents of a packet are small
- AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes
- AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate

AODV

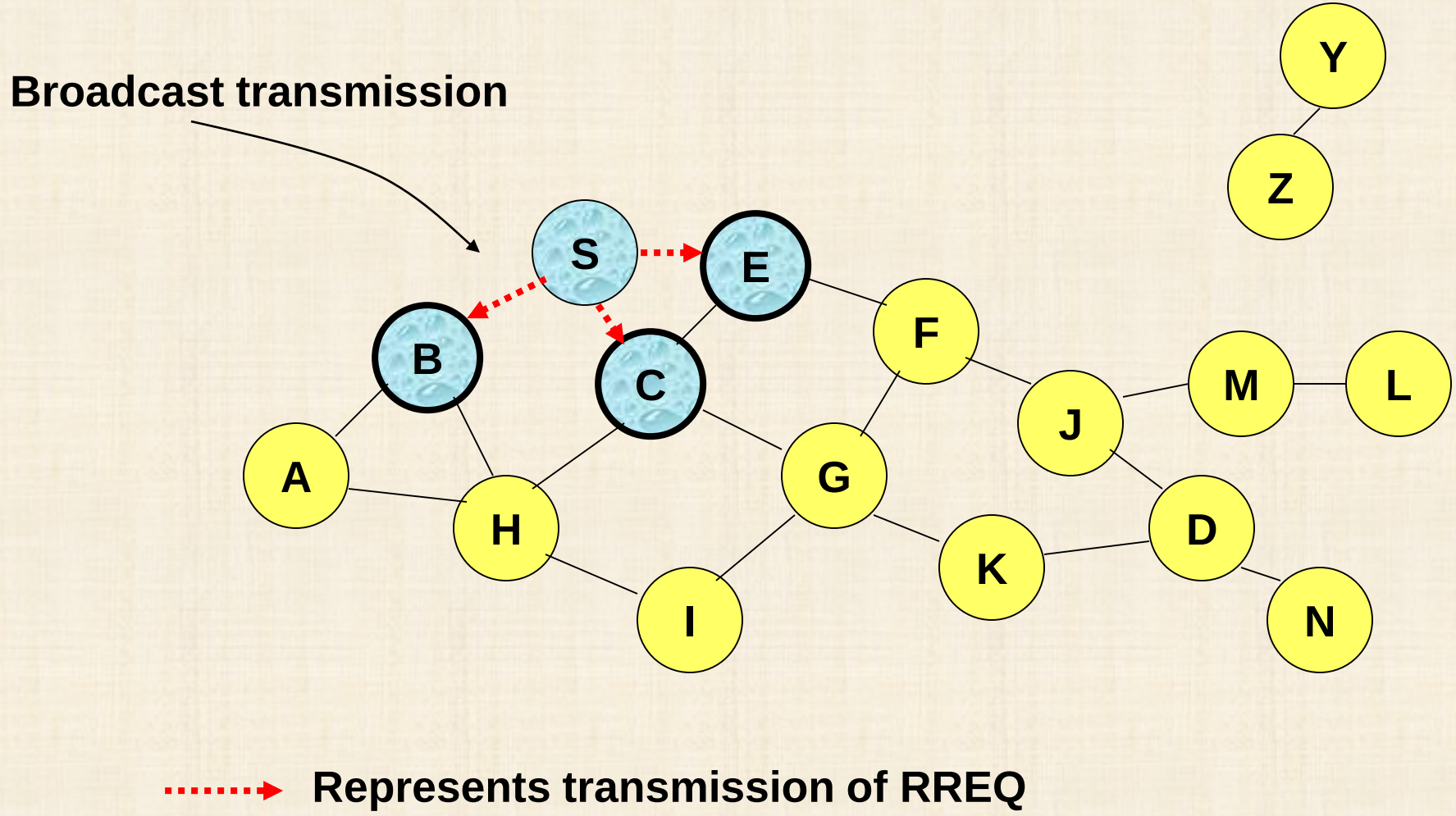
- Route Requests (RREQ) are forwarded in a manner similar to DSR
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
  - AODV assumes symmetric (bi-directional) links
- When the intended destination receives a Route Request, it replies by sending a Route Reply
- Route Reply travels along the reverse path set-up when Route Request is forwarded

Route Requests in AODV

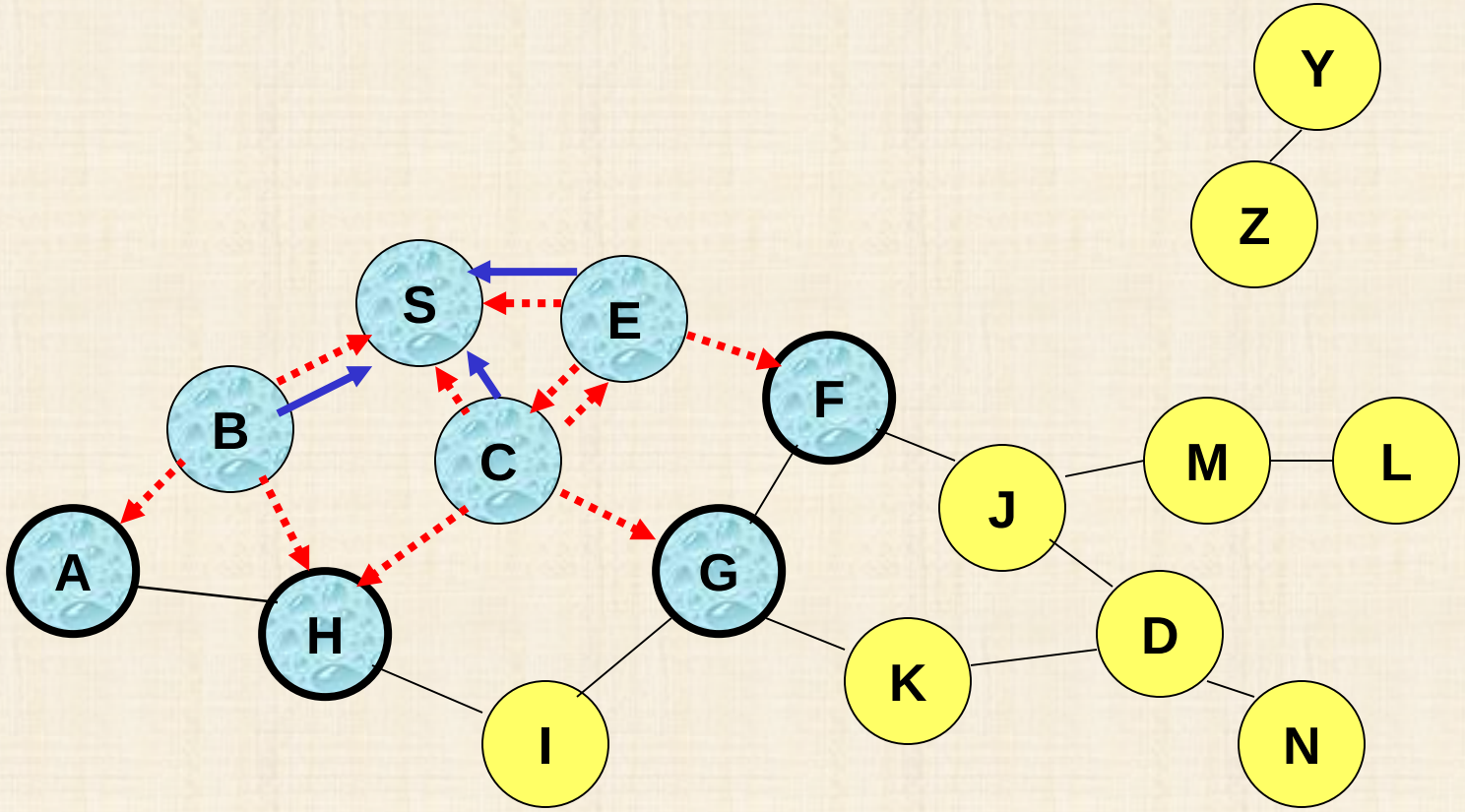


Represents a node that has received RREQ for D from S

Route Requests in AODV

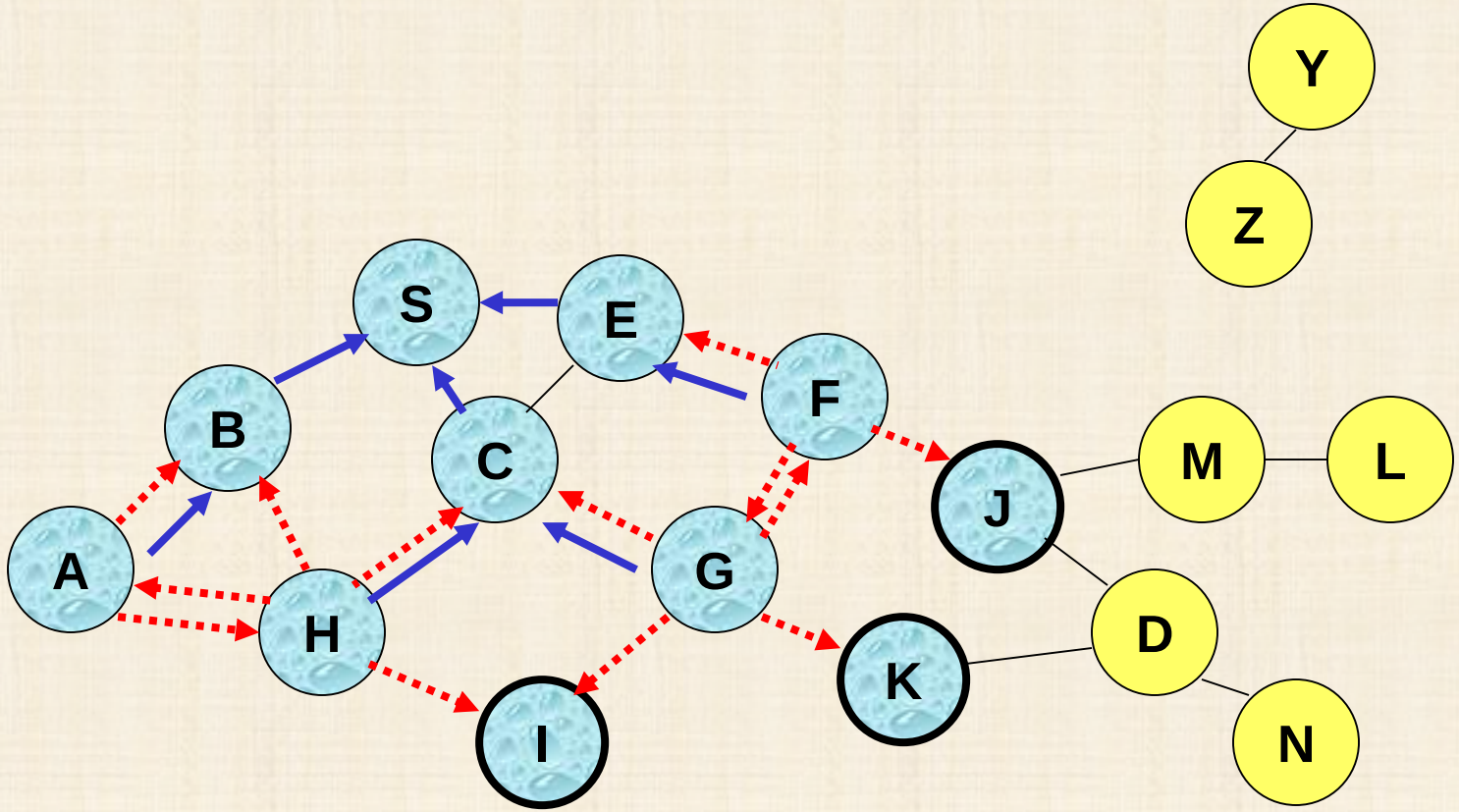


Route Requests in AODV



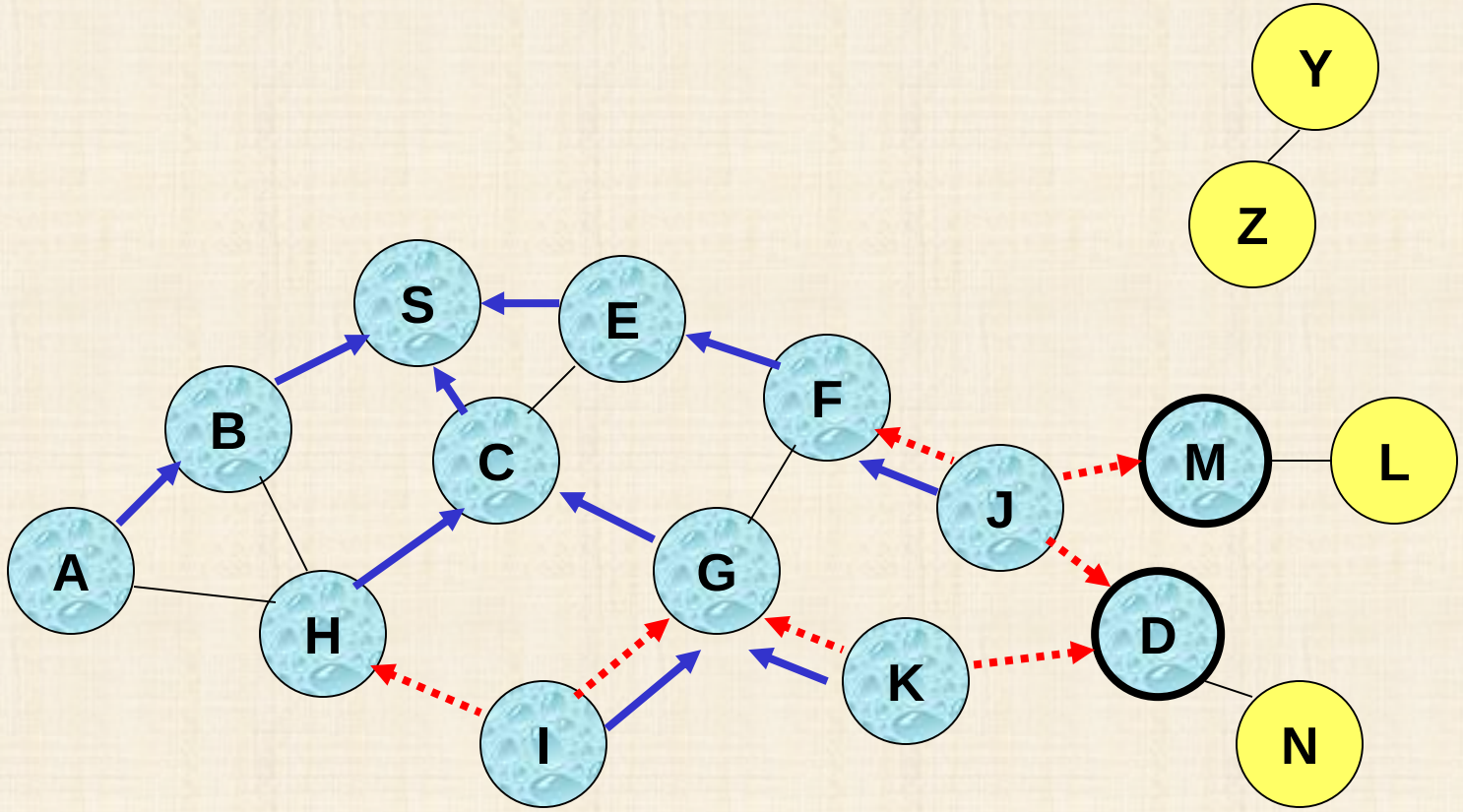
Represents links on Reverse Path

Reverse Path Setup in AODV

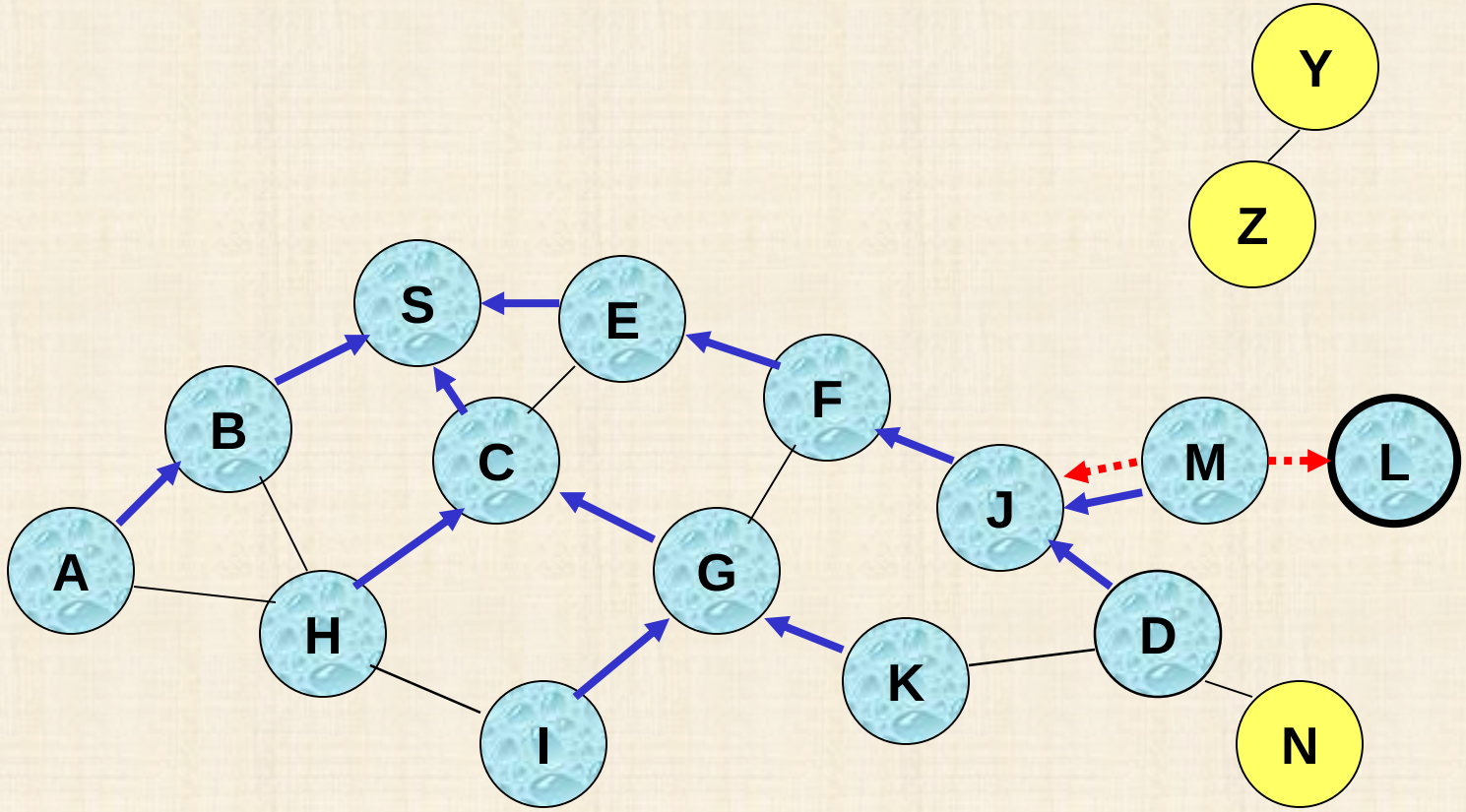


- **Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once**

Reverse Path Setup in AODV

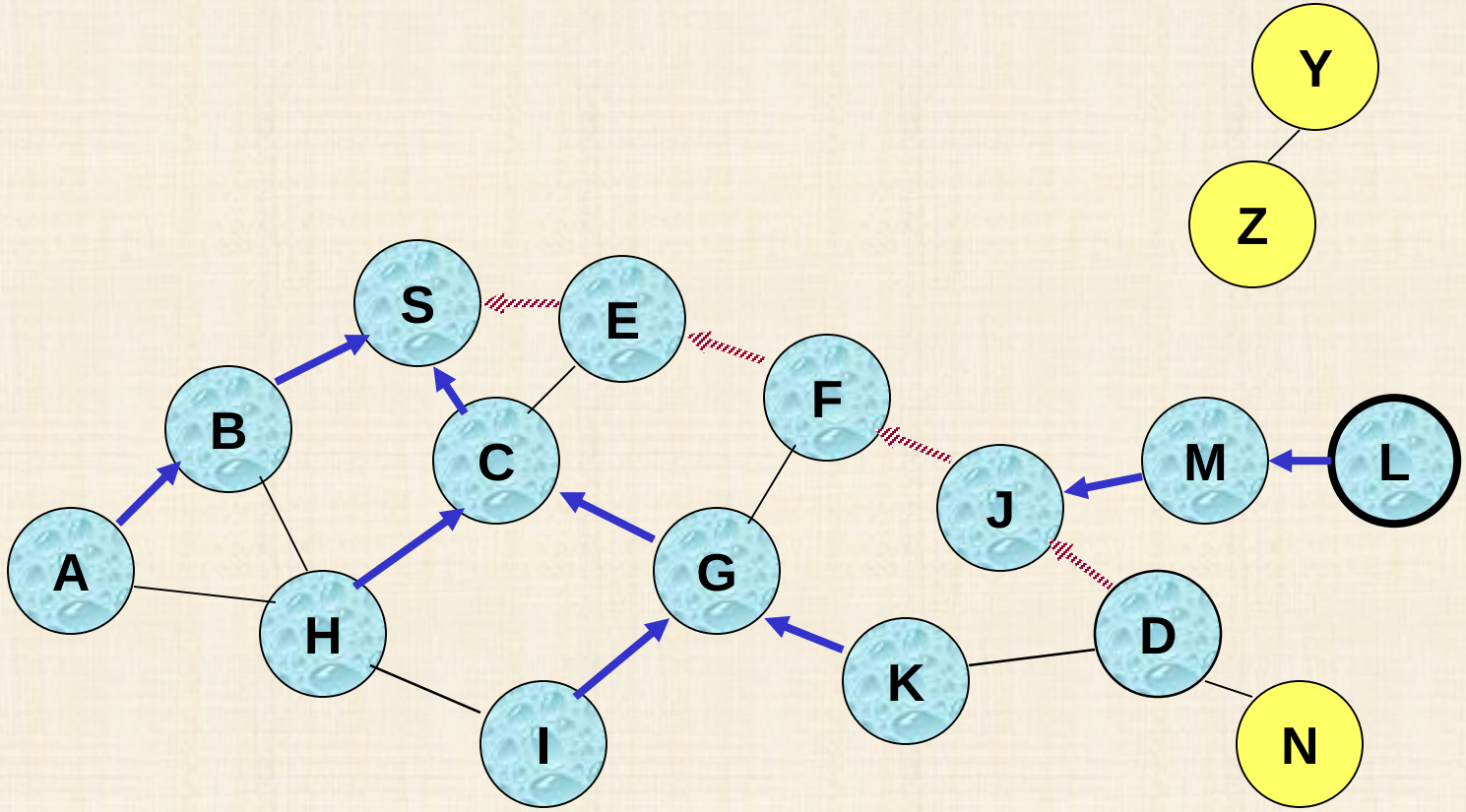


Reverse Path Setup in AODV



- **Node D does not forward RREQ, because node D is the intended target of the RREQ**

Route Reply in AODV

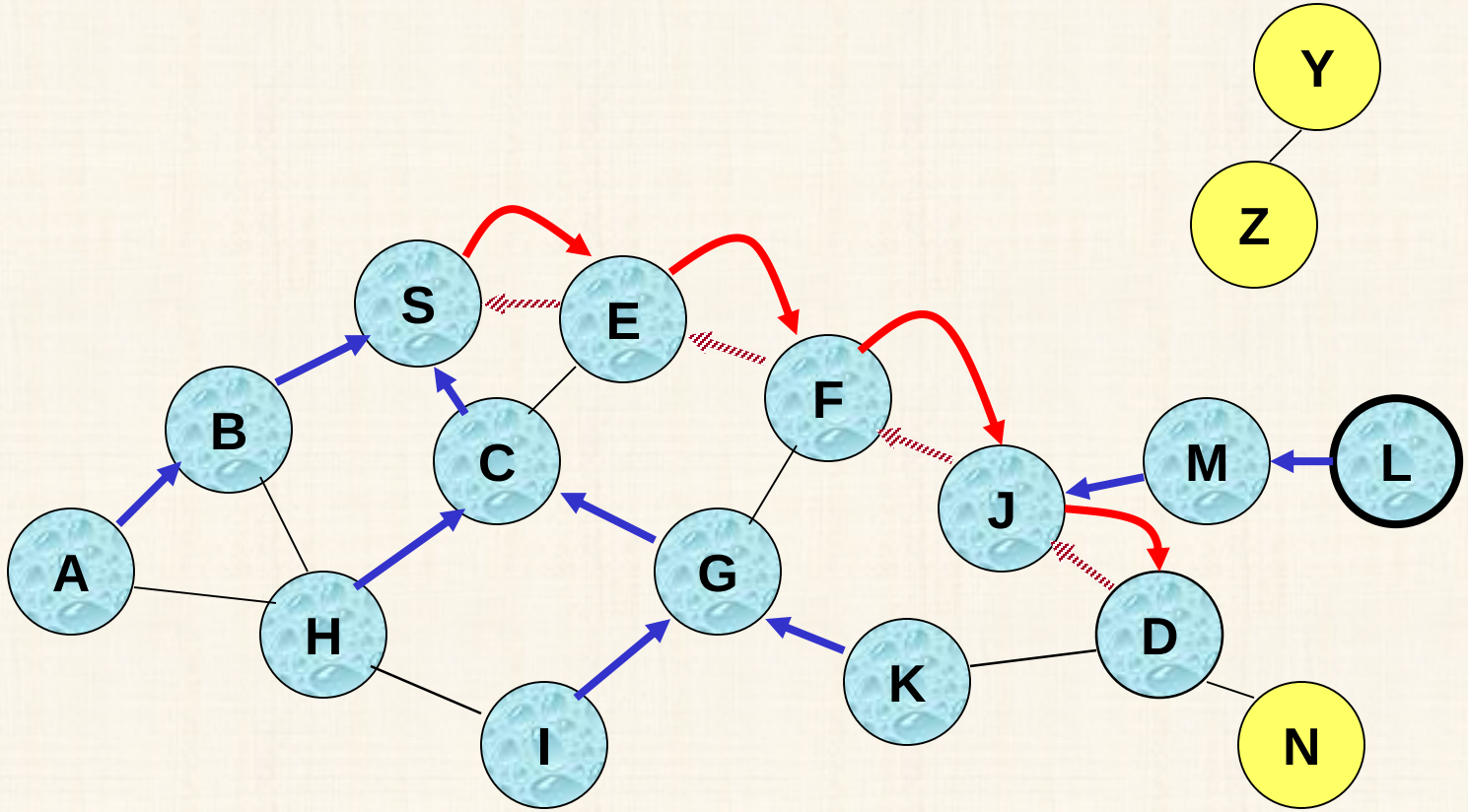


Represents links on path taken by RREP

Route Reply in AODV

- An intermediate node (not the destination) may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender S
- To determine whether the path known to an intermediate node is more recent, *destination sequence numbers* are used
- The likelihood that an intermediate node will send a Route Reply when using AODV is not as high as DSR
  - A new Route Request by node S for a destination is assigned a higher destination sequence number. An intermediate node which knows a route, but with a smaller sequence number, cannot send Route Reply

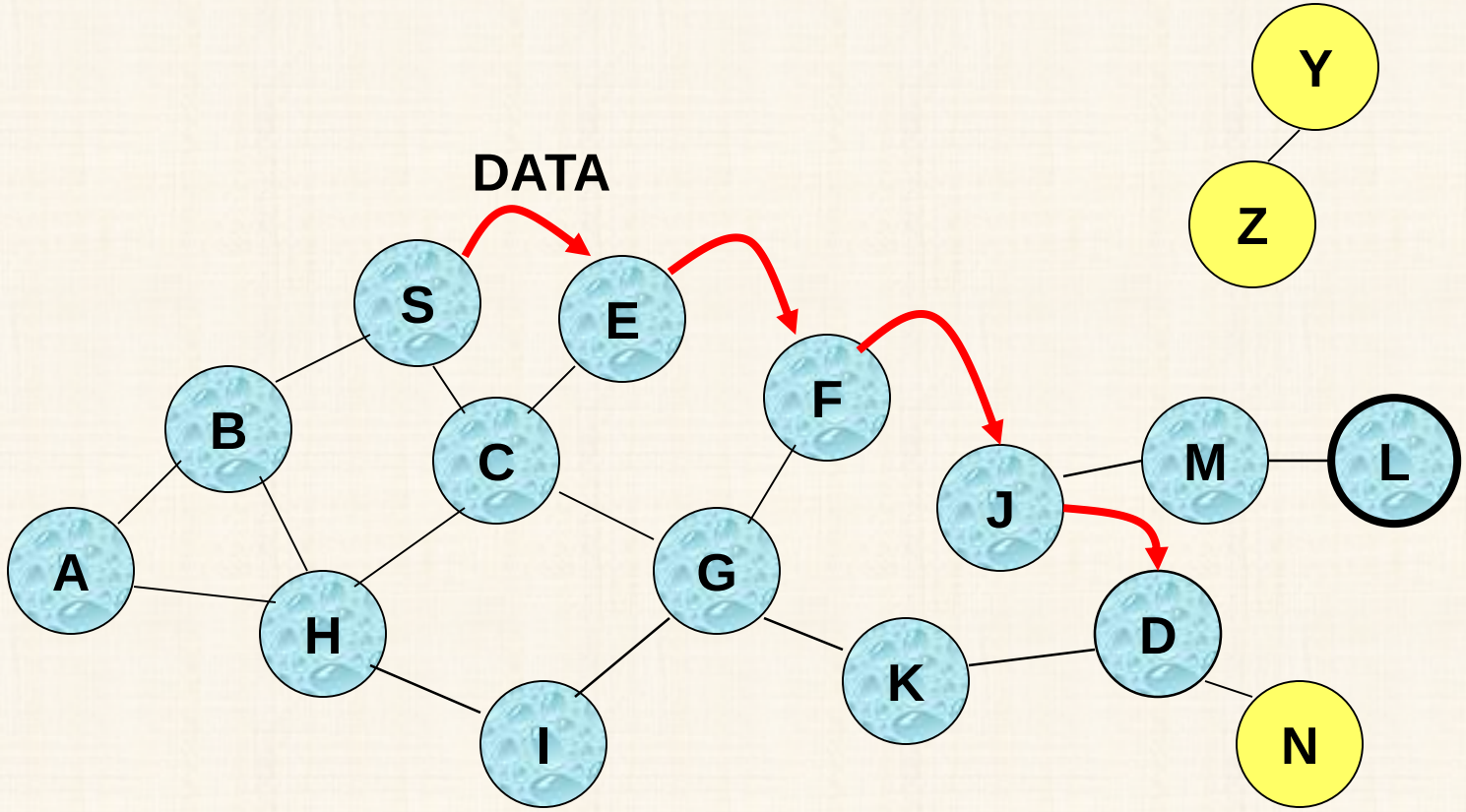
Forward Path Setup in AODV



Forward links are setup when RREP travels along the reverse path

Represents a link on the forward path

Data Delivery in AODV



Routing table entries used to forward data packet.

Route is *not* included in packet header.

Timeouts

- A routing table entry maintaining a reverse path is purged after a timeout interval
  - timeout should be long enough to allow RREP to come back
- A routing table entry maintaining a forward path is purged if *not used* for a *active_route_timeout* interval
  - if no data is being sent using a particular routing table entry, that entry will be deleted from the routing table (even if the route may actually still be valid)

Link Failure Reporting

- A neighbor of node X is considered active for a routing table entry if the neighbor sent a packet within *active_route_timeout* interval which was forwarded using that entry
- When the next hop link in a routing table entry breaks, all active neighbors are informed
- Link failures are propagated by means of Route Error messages, which also update destination sequence numbers

Route Error

- When node X is unable to forward packet P (from node S to node D) on link (X,Y), it generates a RERR message
- Node X increments the destination sequence number for D cached at node X
- The incremented sequence number *N* is included in the RERR
- When node S receives the RERR, it initiates a new route discovery for D using destination sequence number at least as large as *N*

Destination Sequence Number

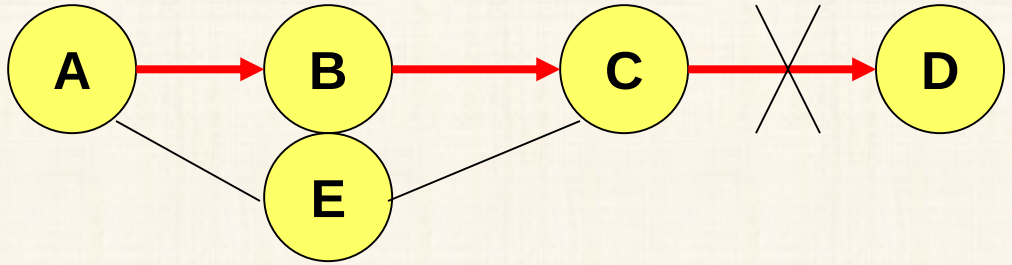
- When node D receives the route request with destination sequence number N, node D will set its sequence number to N, unless it is already larger than N

Link Failure Detection

- *Hello* messages: Neighboring nodes periodically exchange hello message
- Absence of hello message is used as an indication of link failure
- Alternatively, failure to receive several MAC-level acknowledgement may be used as an indication of link failure

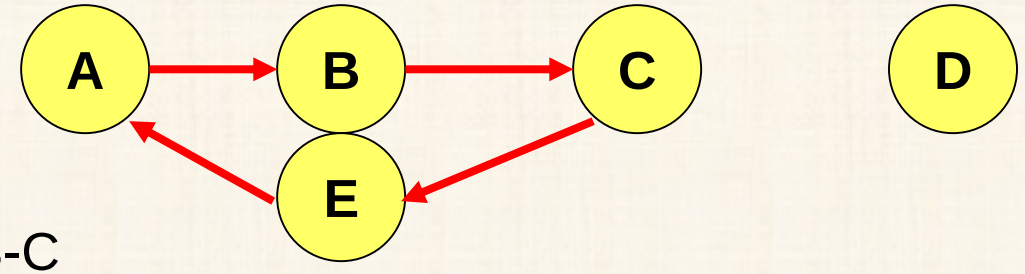
Why Sequence Numbers in AODV

- To avoid using old/broken routes
  - To determine which route is newer
- To prevent formation of loops



  - Assume that A does not know about failure of link C-D because RERR sent by C is lost
  - Now C performs a route discovery for D. Node A receives the RREQ (say, via path C-E-A)
  - Node A will reply since A knows a route to D via node B
  - Results in a loop (for instance, C-E-A-B-C)

Why Sequence Numbers in AODV

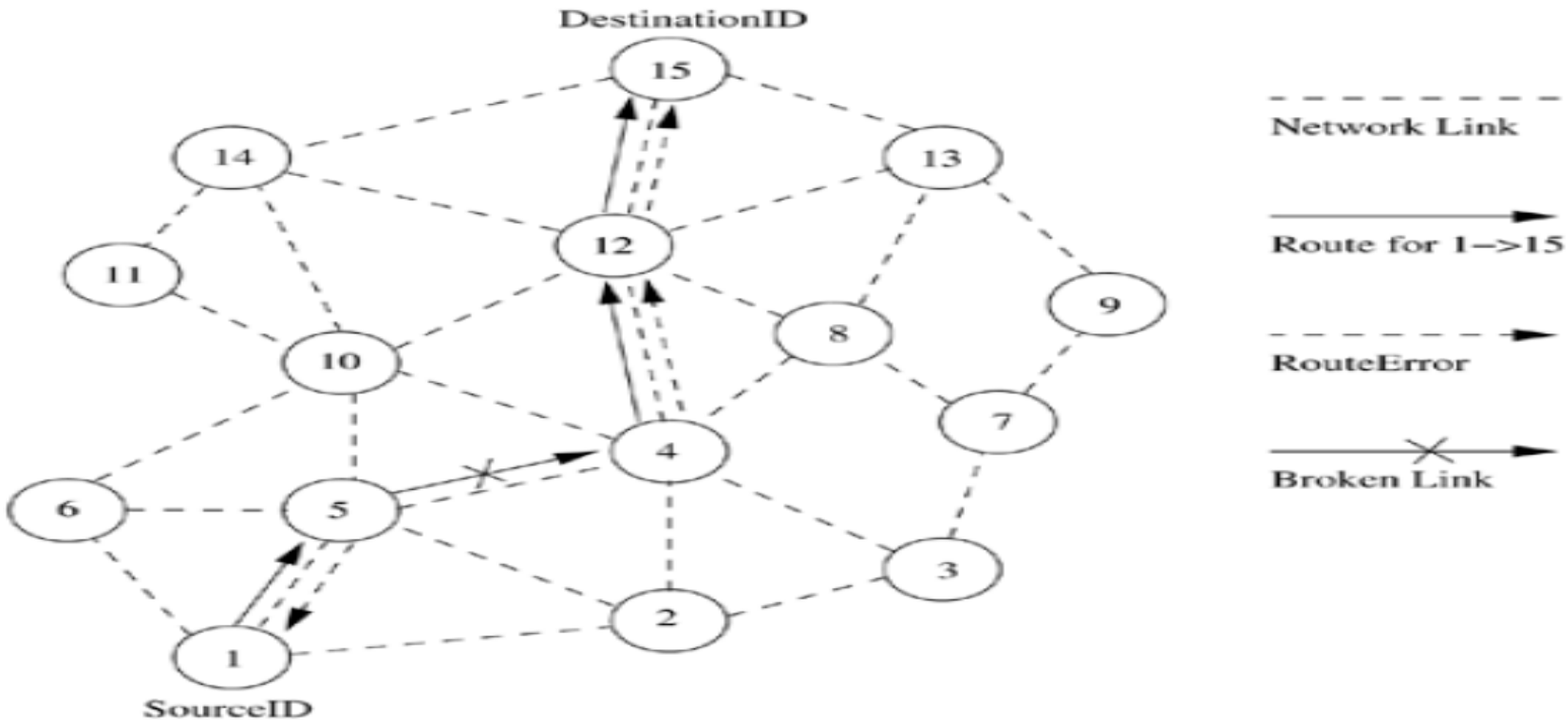


- Loop C-E-A-B-C

Optimization: Expanding Ring Search

- Route Requests are initially sent with small Time-to-Live (TTL) field, to limit their propagation
- If no Route Reply is received, then larger TTL tried

Route maintenance in AODV



When a path breaks, for example, between nodes 4 and 5, both the nodes initiate *RouteError* messages to inform their end nodes about the link break.

The end nodes delete the corresponding entries from their tables. The source node reinitiates the pathfinding process with the new BcastID and the previous destination sequence number.

Advantages:

- Routes are established on demand and destination sequence numbers are used to find the latest route to the destination.
- The connection setup delay is less.

Disadvantages:

- The intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries.
- Multiple *RouteReply* packets in response to a single *RouteRequest* packet can lead to heavy control overhead.
- Periodic *beacon*ing leads to unnecessary bandwidth consumption.

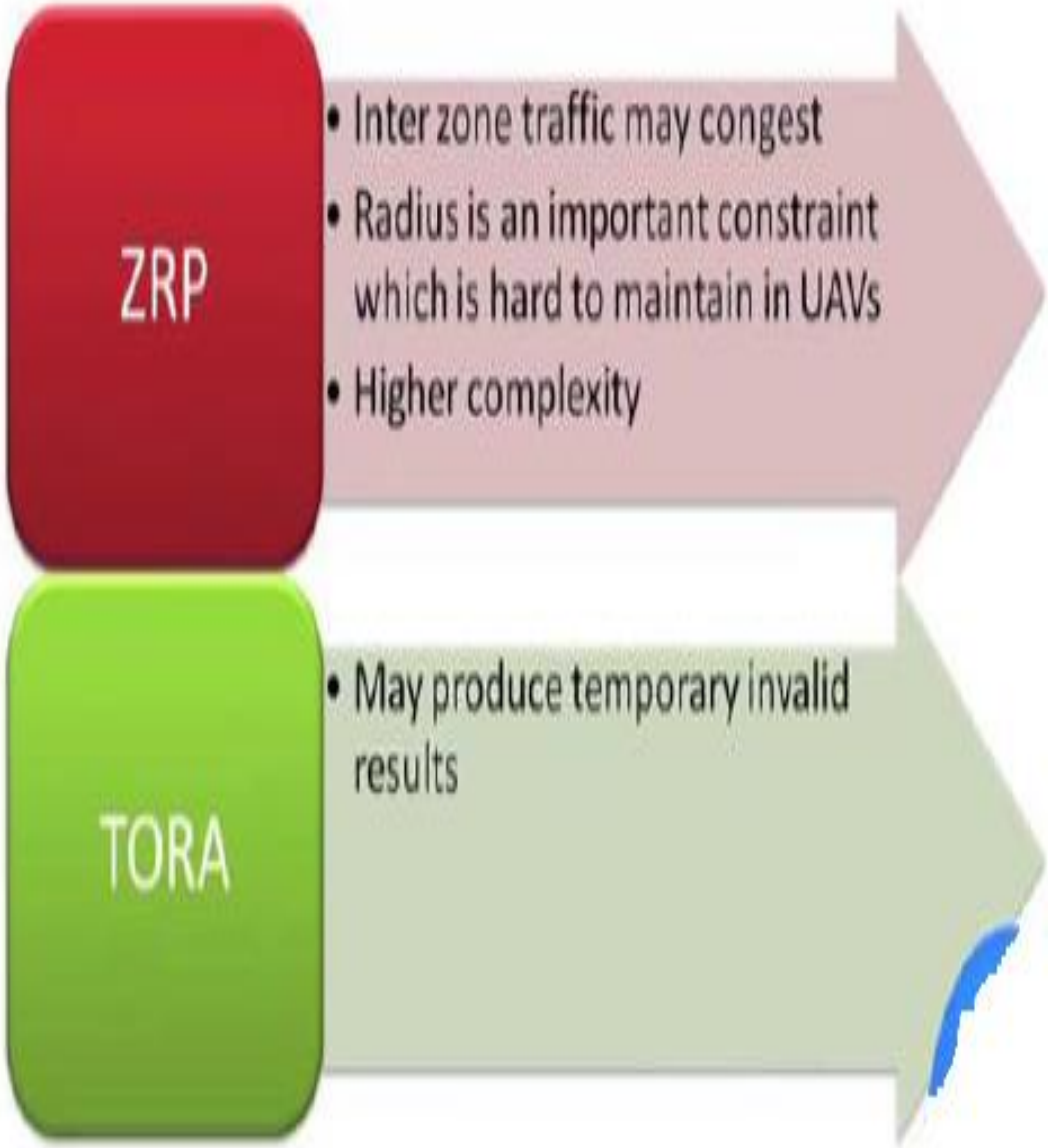
Summary: AODV

- Routes need not be included in packet headers
- Nodes maintain routing tables containing entries only for routes that are in active use
- At most one next-hop per destination maintained at each node
- Unused routes expire even if topology does not change

Hybrid Routing Protocols

- Often reactive or proactive feature of a particular routing protocol might not be enough
- Instead a mixture might yield better solution. Hence, in the recent days, several hybrid protocols are also proposed
- The hybrid protocols include some of the characteristics of proactive protocols and some of the characteristics of reactive protocols

Hybrid UAV Routing Protocols



Zone Routing Protocol (ZRP)

- Zone Routing Protocol (ZRP) is based on the concept of zones.
- In this protocol, each node has a different zone. The zone is defined as the set of nodes whose minimum distance is predefined radius R. So, the zones of neighboring nodes intersect.
- The routing inside the zone is called as intra-zone routing, and it uses proactive method. If the source and destination nodes are in the same zone, the source node can start data communication instantly.
- When the data packets have to be sent outside the zone the inter-zone routing is used and reactive method is applied.

Zone routing protocol combines

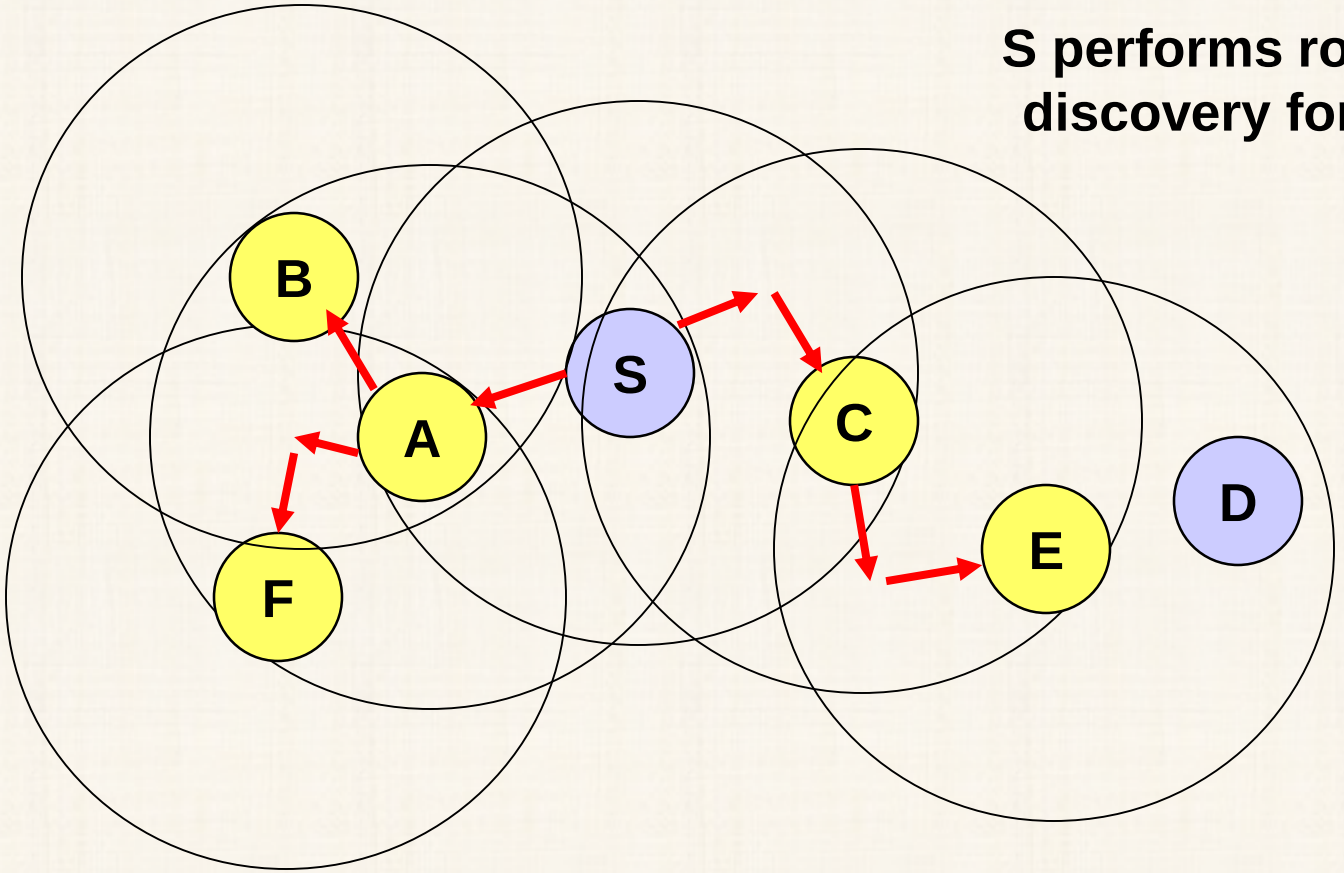
- Proactive protocol: which pro-actively updates network state and maintains route regardless of whether any data traffic exists or not

- Reactive protocol: which only determines route to a destination if there is some data is to be sent to the destination

ZRP

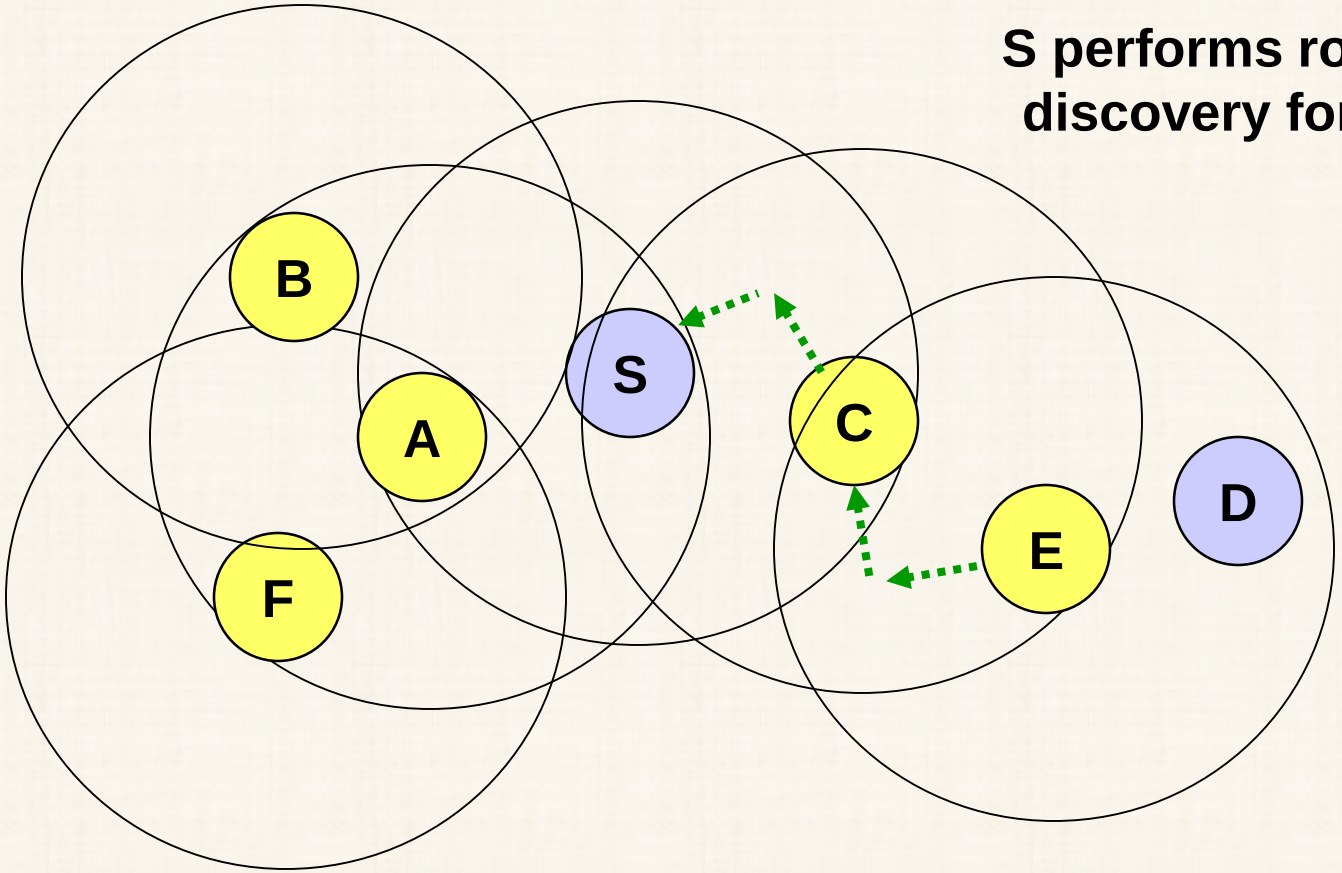
- All nodes within hop distance at most *d* from a node X are said to be in the routing zone of node X
- All nodes at hop distance exactly *d* are said to be peripheral nodes of node X's routing zone
- Intra-zone routing: Pro-actively maintain state information for links within a short distance from any given node
  - Routes to nodes within short distance are thus maintained proactively (using, say, link state or distance vector protocol)
- Inter-zone routing: Use a route discovery protocol for determining routes to far away nodes. Route discovery is similar to DSR with the exception that route requests are propagated via peripheral nodes.

ZRP: Example with Zone Radius = *r= 1*

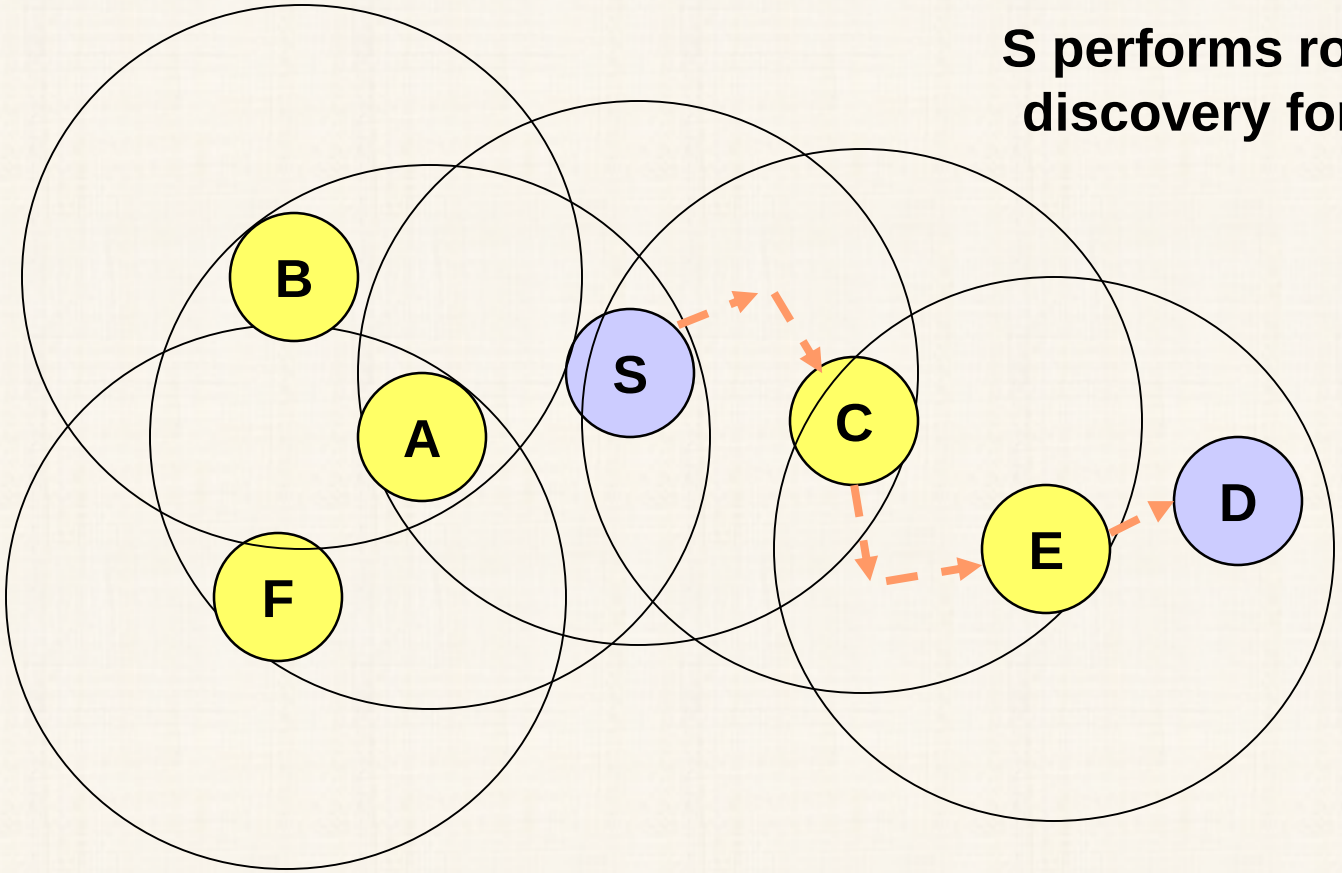


Denotes route request

ZRP: Example with *d* = *2*



ZRP: Example with *d* = *2*

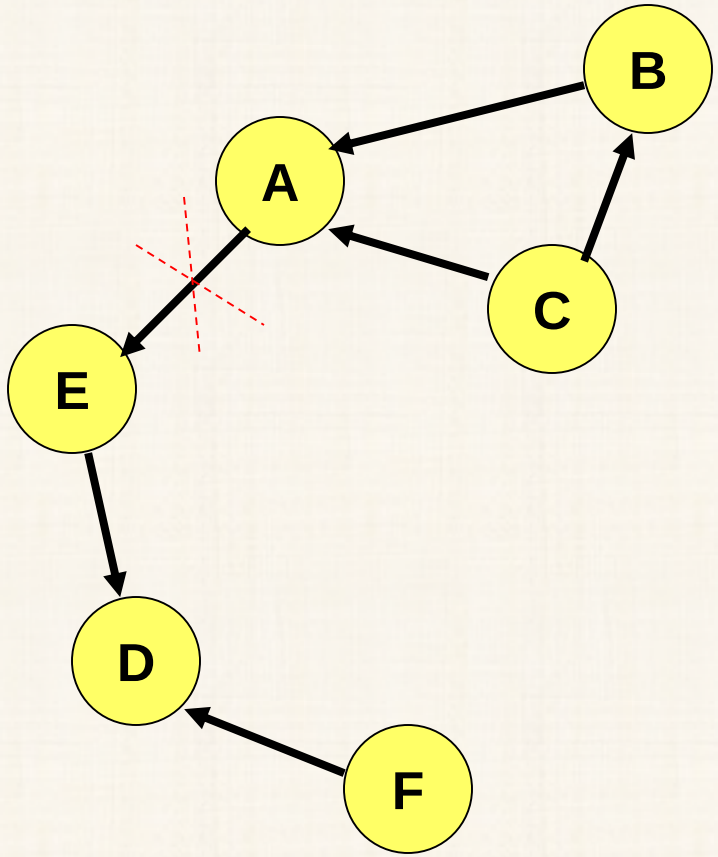


Denotes route taken by Data

Temporally-Ordered Routing Algorithm (TORA)

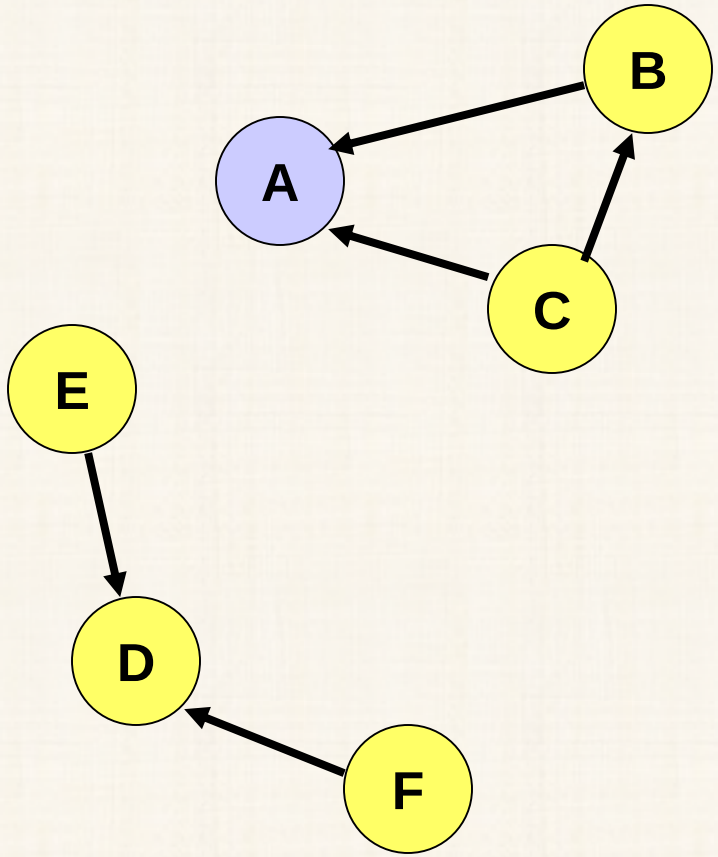
- In Temporarily Ordered Routing Algorithm (TORA) routers only preserve information about adjacent routers. TORA not only uses a reactive routing protocol but it also uses a proactive protocol.
- It constructs and preserves a Directed Acyclic Graph (DAG) from the source node to the destination.
- TORA does not use a shortest path solution always, sometimes longer routes are used to reduce the network overhead. Each node has a parameter value termed as ”height” in DAG, which is unique for each node.
- Data flows as a fluid from the higher nodes to lower. It is structurally loop-free because data cannot flow to the node that has a higher value.
- TORA modifies the partial link reversal method to be able to detect partitions.
- When a partition is detected, all nodes in the partition are informed, and link reversals in that partition cease.

Partition Detection in TORA



DAG for destination D

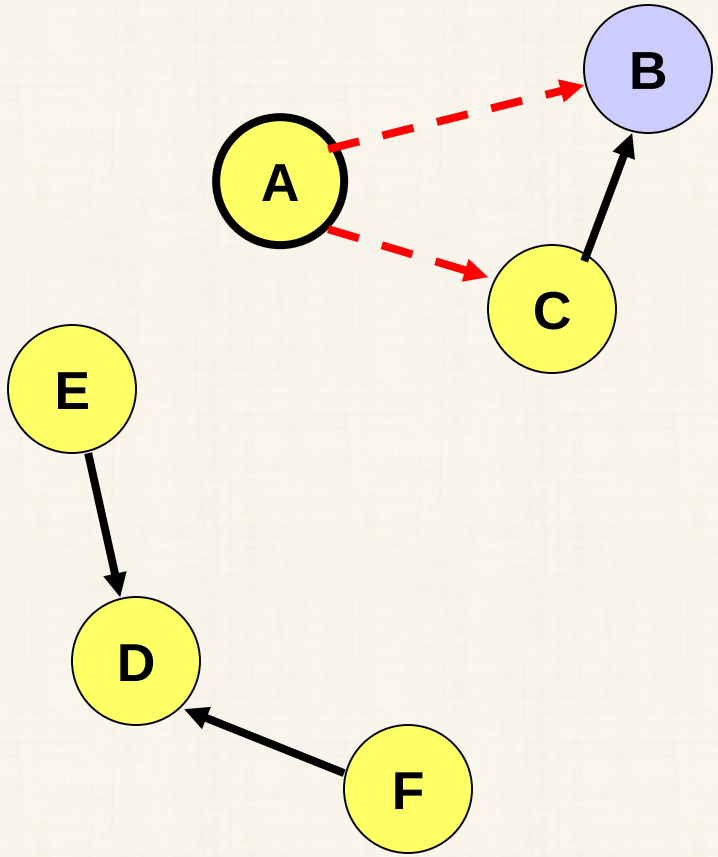
Partition Detection in TORA



TORA uses a modified partial reversal method

Node A has no outgoing links

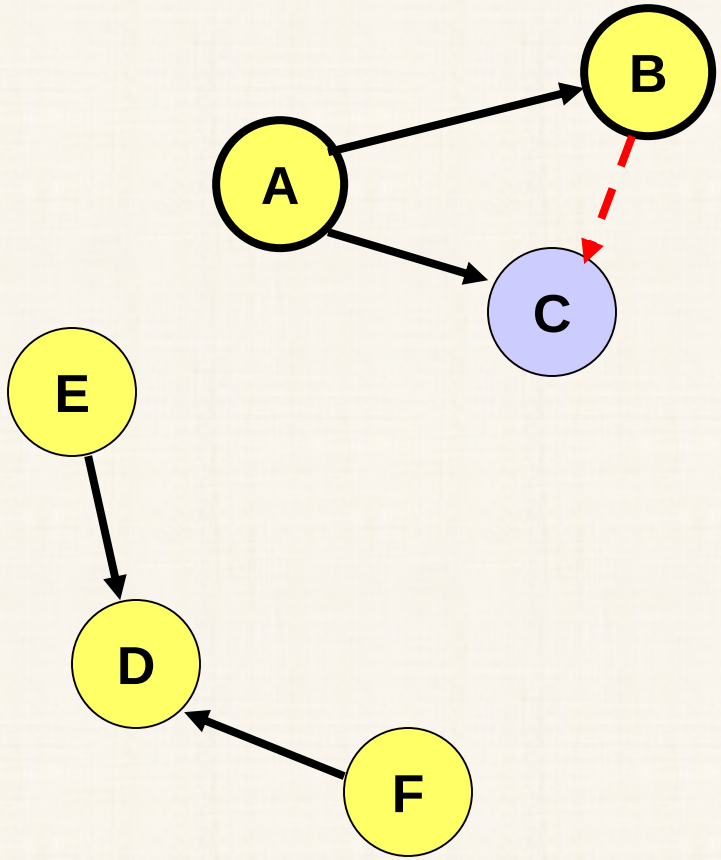
Partition Detection in TORA



TORA uses a modified partial reversal method

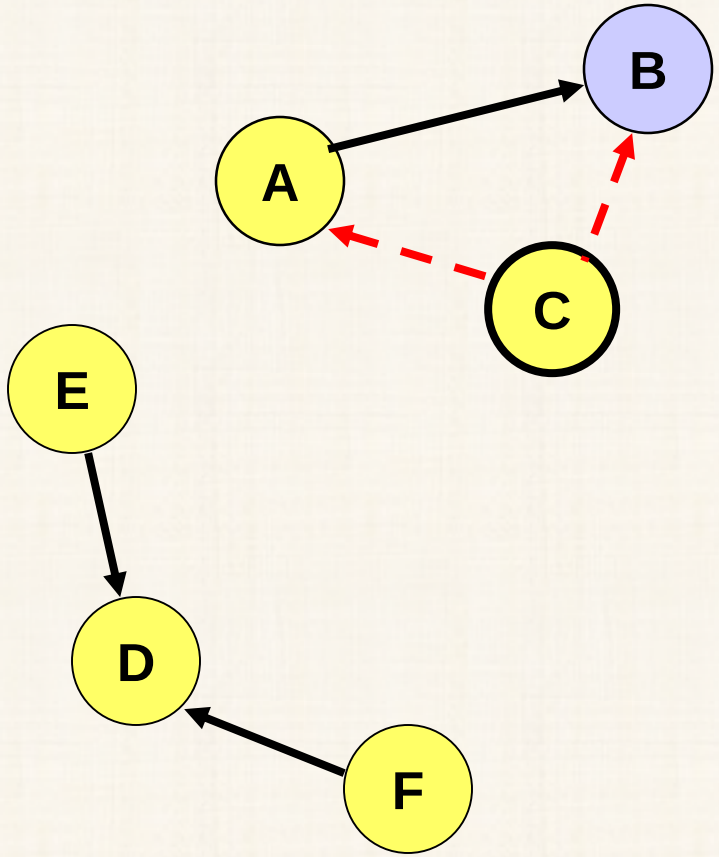
Node B has no outgoing links

Partition Detection in TORA



Node C has no outgoing links -- all its neighbor have reversed links previously.

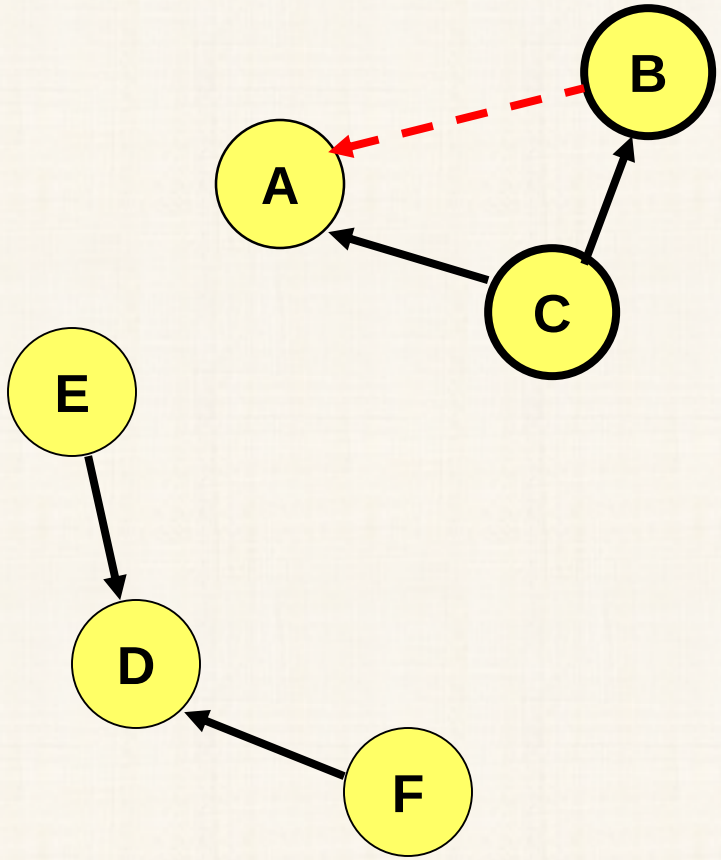
Partition Detection in TORA



Nodes A and B receive the reflection from node C

Node B now has no outgoing link

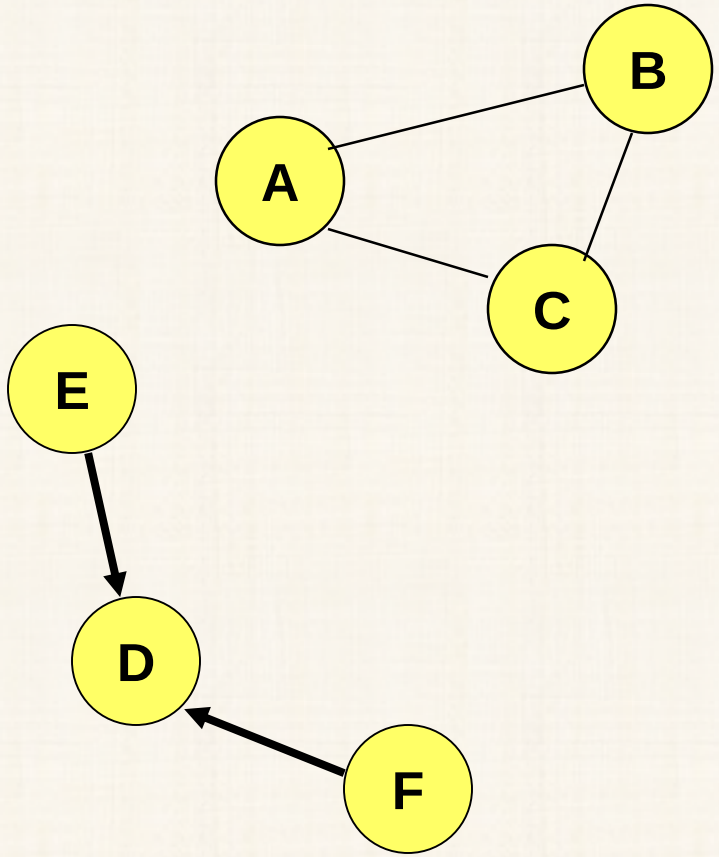
Partition Detection in TORA



Node B propagates the reflection to node A

Node A has received the reflection from all its neighbors.
Node A determines that it is partitioned from destination D.

Partition Detection in TORA



On detecting a partition, node A sends a clear (CLR) message that purges all directed links in that partition

TORA

- Improves on the partial link reversal method by detecting partitions and stopping non-productive link reversals
- Paths may not be shortest
- The DAG provides many hosts the ability to send packets to a given destination
  - Beneficial when many hosts want to communicate with a single destination

TORA Design Decision

- TORA performs link reversals.
- However, when a link breaks, it looses its direction

- When a link is repaired, it may not be assigned a direction, unless some node has performed a route discovery after the link broke
  - if no one wants to send packets to D anymore, eventually, the DAG for destination D may disappear

- TORA makes effort to maintain the DAG for D only if someone needs route to D
  - Reactive behavior

Illustration of temporal ordering in TORA

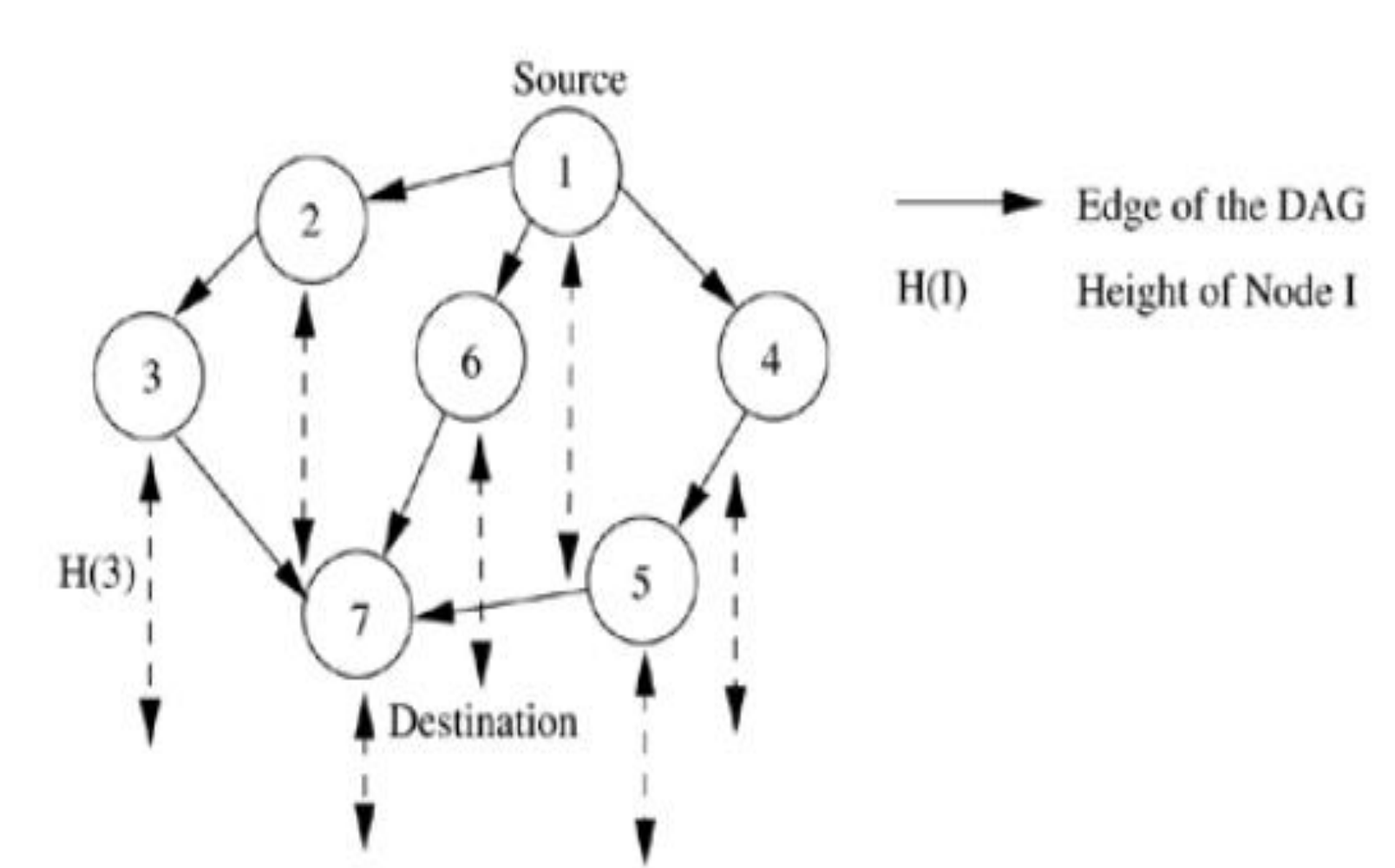
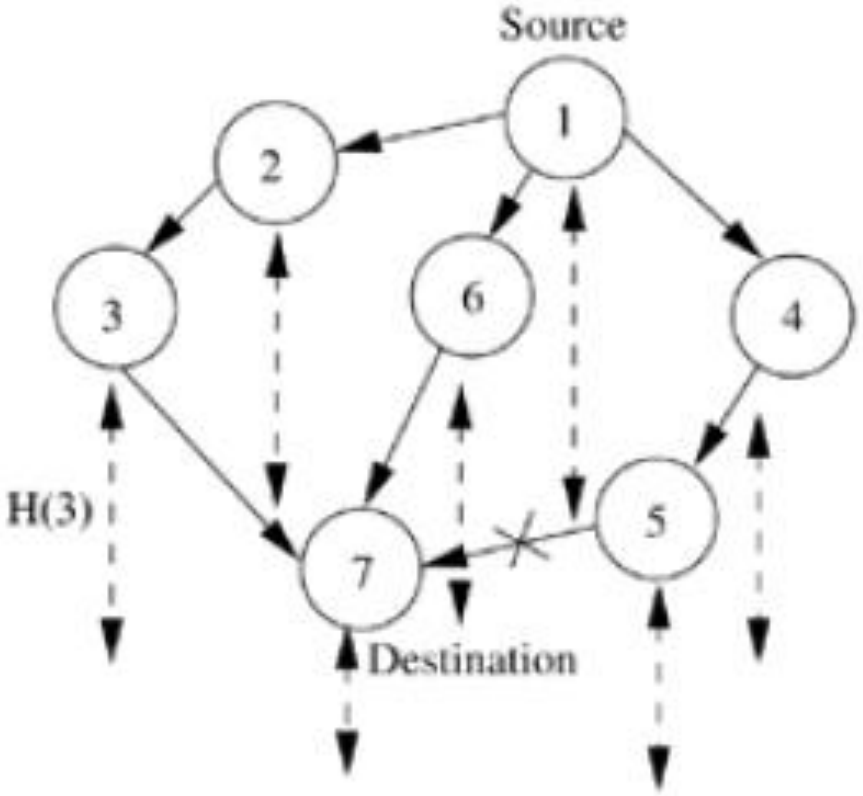
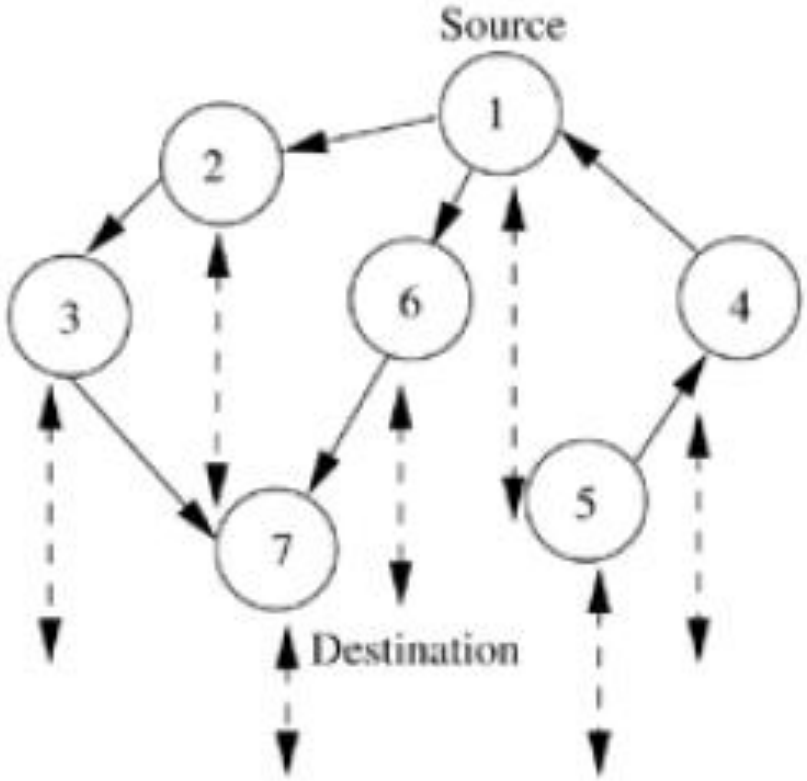


Illustration of route maintenance in TORA



Link break beween Nodes 5 and 7



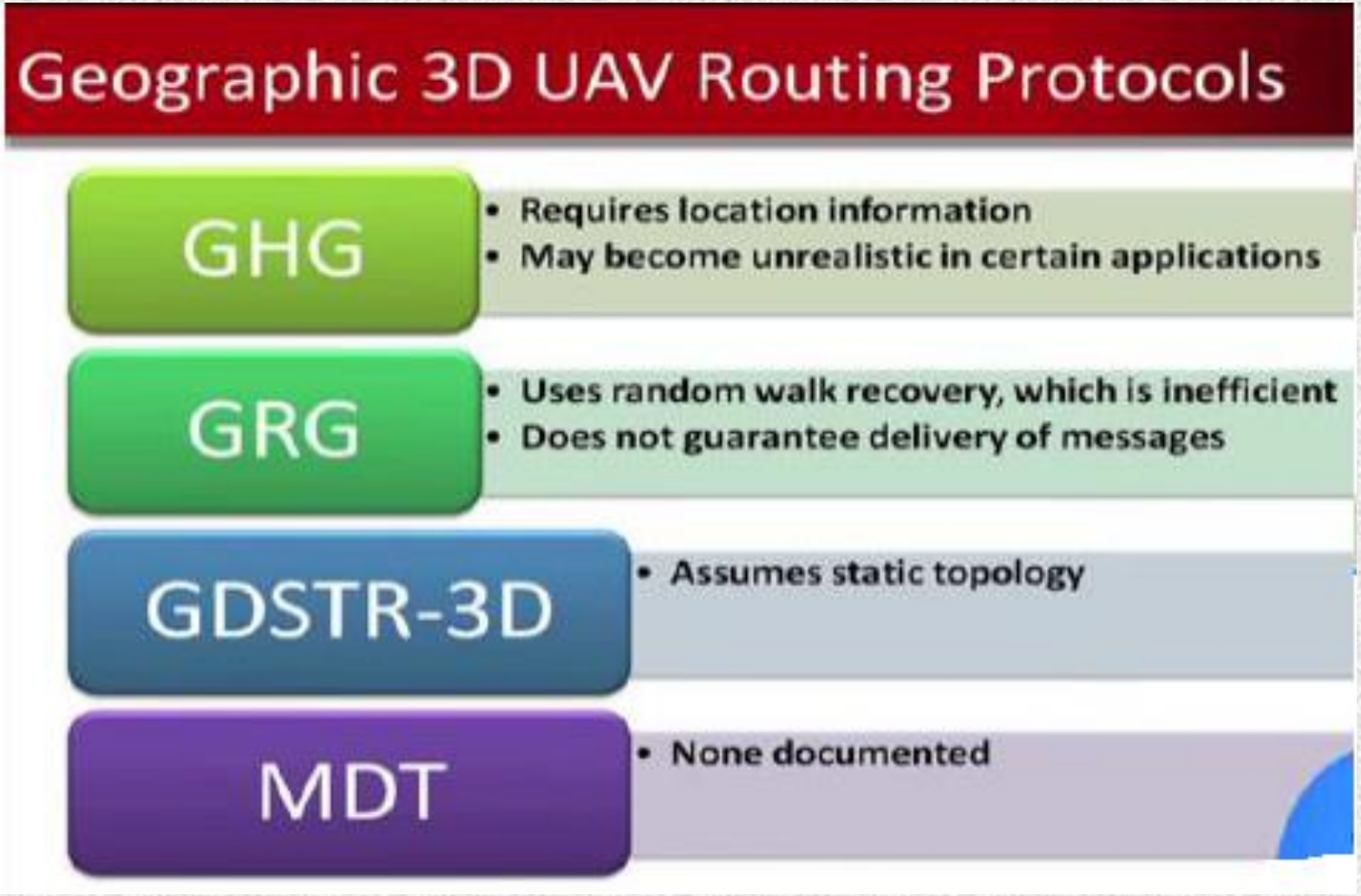
Nodes 4 and 5 reverse their links
in order to update the path

Advantages:

- By limiting the control packets for route reconfigurations to a small region, TORA incurs less control overhead.

Disadvantages:

- Concurrent detection of partitions and subsequent deletion of routes could result in temporary oscillations and transient loops.
- The local reconfiguration of paths results in non-optimal routes.


Geographic 3D UAV Routing Protocols
GHG
• Requires location information
• May become unrealistic in certain applications
GRG
• Uses random walk recovery, which is inefficient
• Does not guarantee delivery of messages
GDSTR-3D
• Assumes static topology
MDT
• None documented

Position-based or geographic routing approaches were introduced to eliminate some of the limitations of the topology-based protocols.

These routing protocols rely on having one piece of information and that is the nodes' physical location information. Thus, it is necessary for nodes to obtain their coordinates either by using a location service such as GPS or other types of positioning services.

By employing position information, geographic routing protocols do not need to establish and maintain routes, thereby eliminating routing table construction and maintenance.

The forwarding strategy in these protocols is based on location information of the destination as well as the one hop neighbours.

It is probable that the forwarding scheme fails if there is no one-hop neighbour whose location is closer to the destination than that of the forwarding node.

In such cases, recovery strategies are introduced to deal with such failures.

They use greedy approach for routing a packet to the destination which is as follows:

- A packet at an intermediate node is forwarded to the neighbor who is the closest to the destination.

- Each intermediate node applies this greedy principle until the destination is reached.

Geographic routing protocols scale better for ad hoc networks mainly for two reasons:

1) There is no necessity to keep routing tables up-to-date and
2) There is no need to have a global view of the network topology and its changes.

Greedy Hull Greedy (GUG) Routing Protocol: Uses both greedy forwarding and hull routing.

- The **Greedy-Random-Greedy (GRG)** algorithm uses Greedy forwarding as the primary stage and a randomized algorithm as a recovery strategy. i.e., when caught in local minimum pick up one of the neighbors at random and try to forward the packet.

- It tries to make the random walk efficient.

- It is found that GRG incurs message overhead greater than flooding for sparse networks between 2,000 and 5,000 nodes in size.

- The **Greedy Distributed Spanning Tree Routing (GDSTR)** algorithm uses greedy routing followed by spanning tree routing when caught in local minimum.

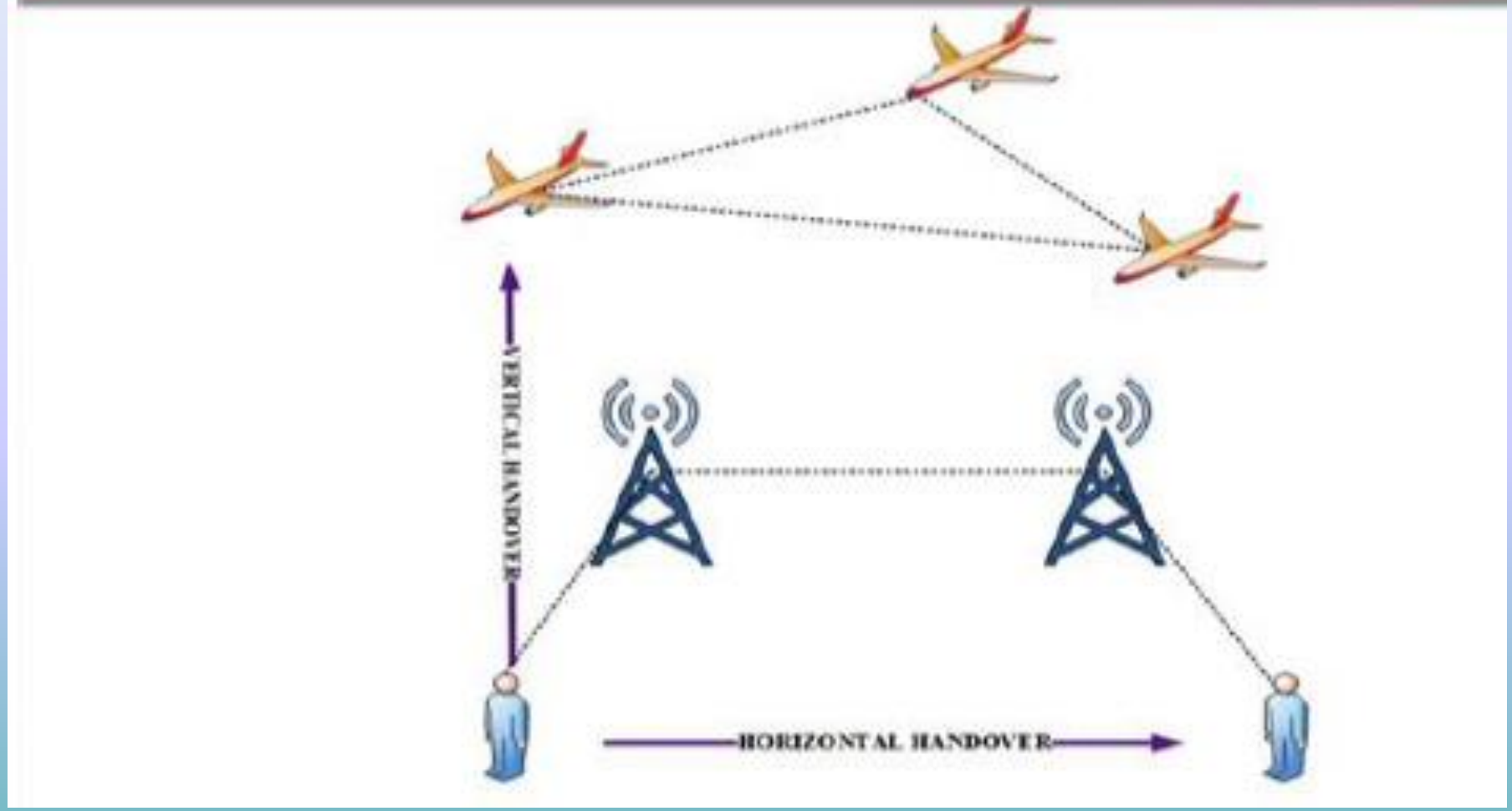
- It uses 2 spanning trees. Each spanning tree has one of the neighbors as the root of the tree and one of the nodes as the destination node.

- Among the two trees it picks up the one with a better path towards the destination.

The **Multi-hop Delaunay Triangulation (MDT)** algorithm uses a greedy forwarding until caught it local minimum at which point it forwards the packet via a virtual link to a multi-hop Delaunay neighbor closest to the destination.

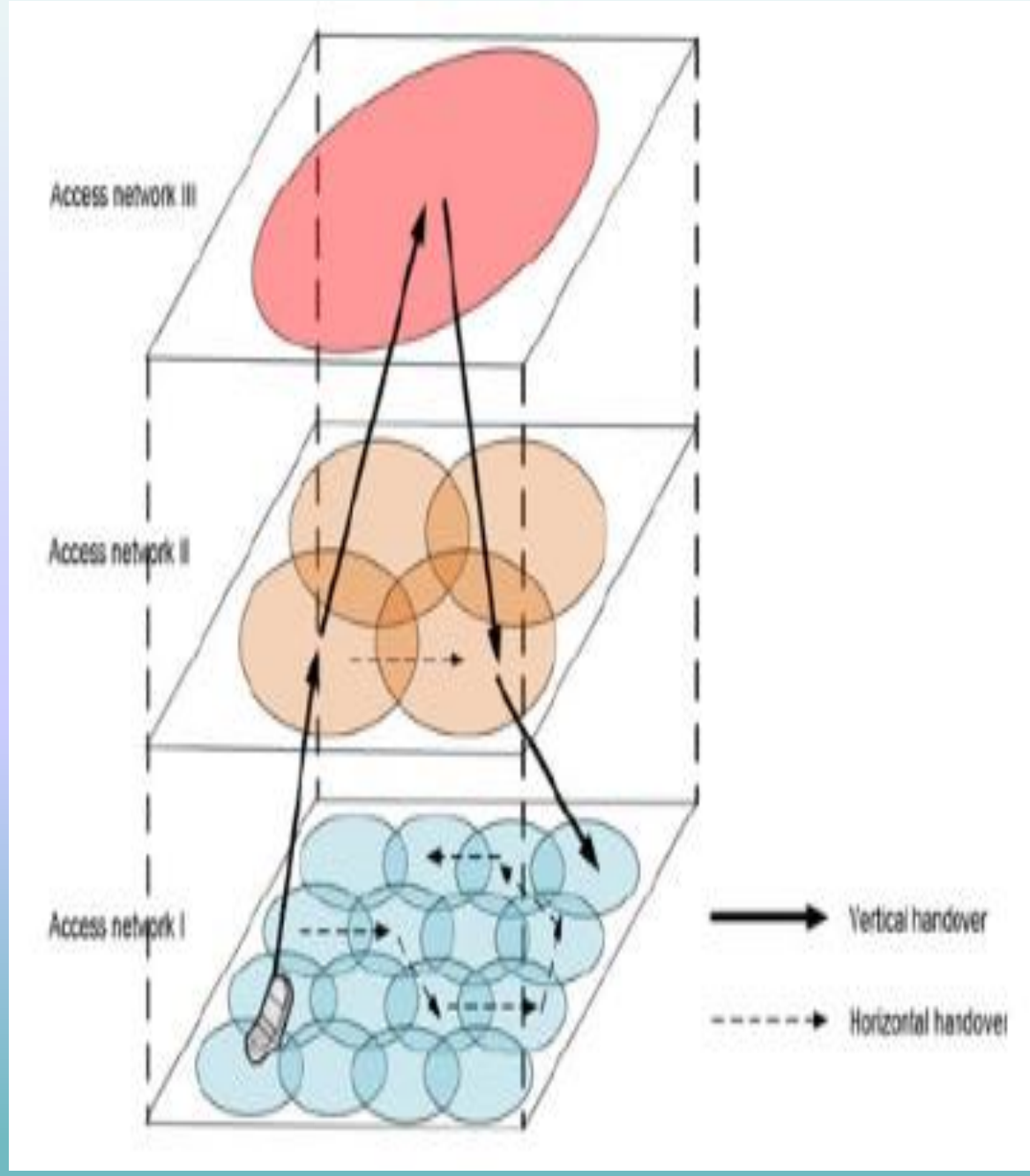
It is required that each node has the ability to construct and maintain the multi-hop Delaunay triangulation.

Handover Types : Horizontal And Vertical

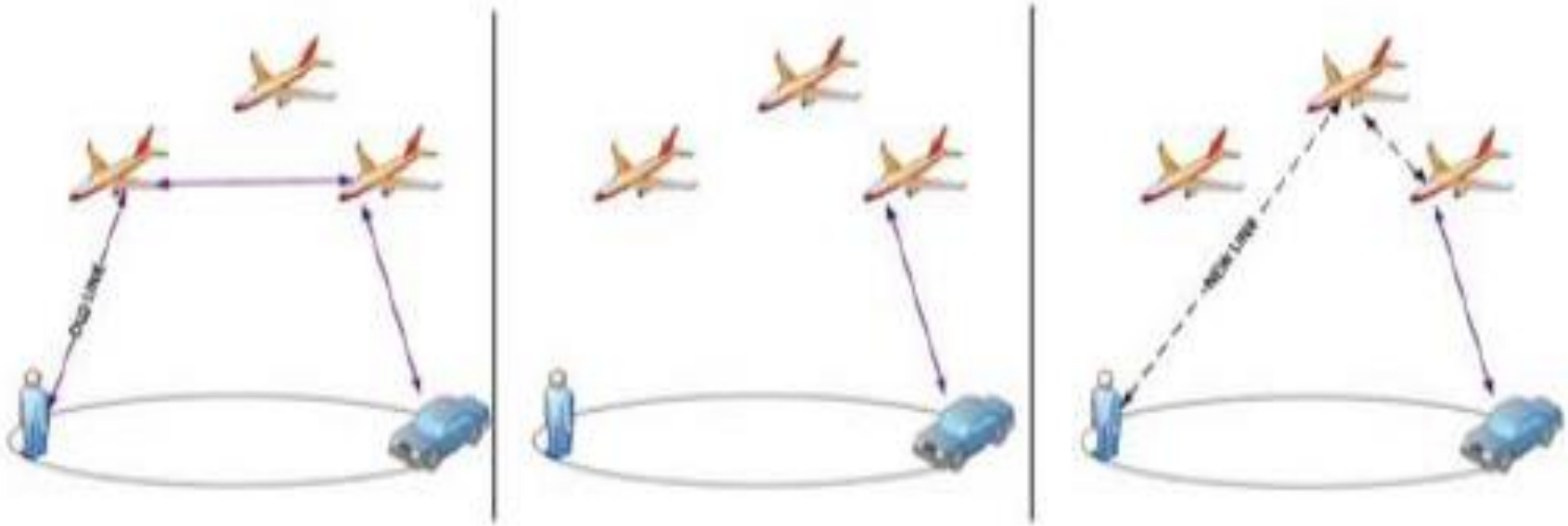


- Handover within same access networks (e.g., WLAN-to-WLAN) is referred to as horizontal handover or intra-domain handover, while handover across heterogeneous access networks (e.g., GSM-to-WiMAX) is referred to as the vertical or Inter-domain handover.

- Vertical handover occurs when a network node changes the type of connectivity it is using to access a supporting infrastructure usually to assist node mobility.

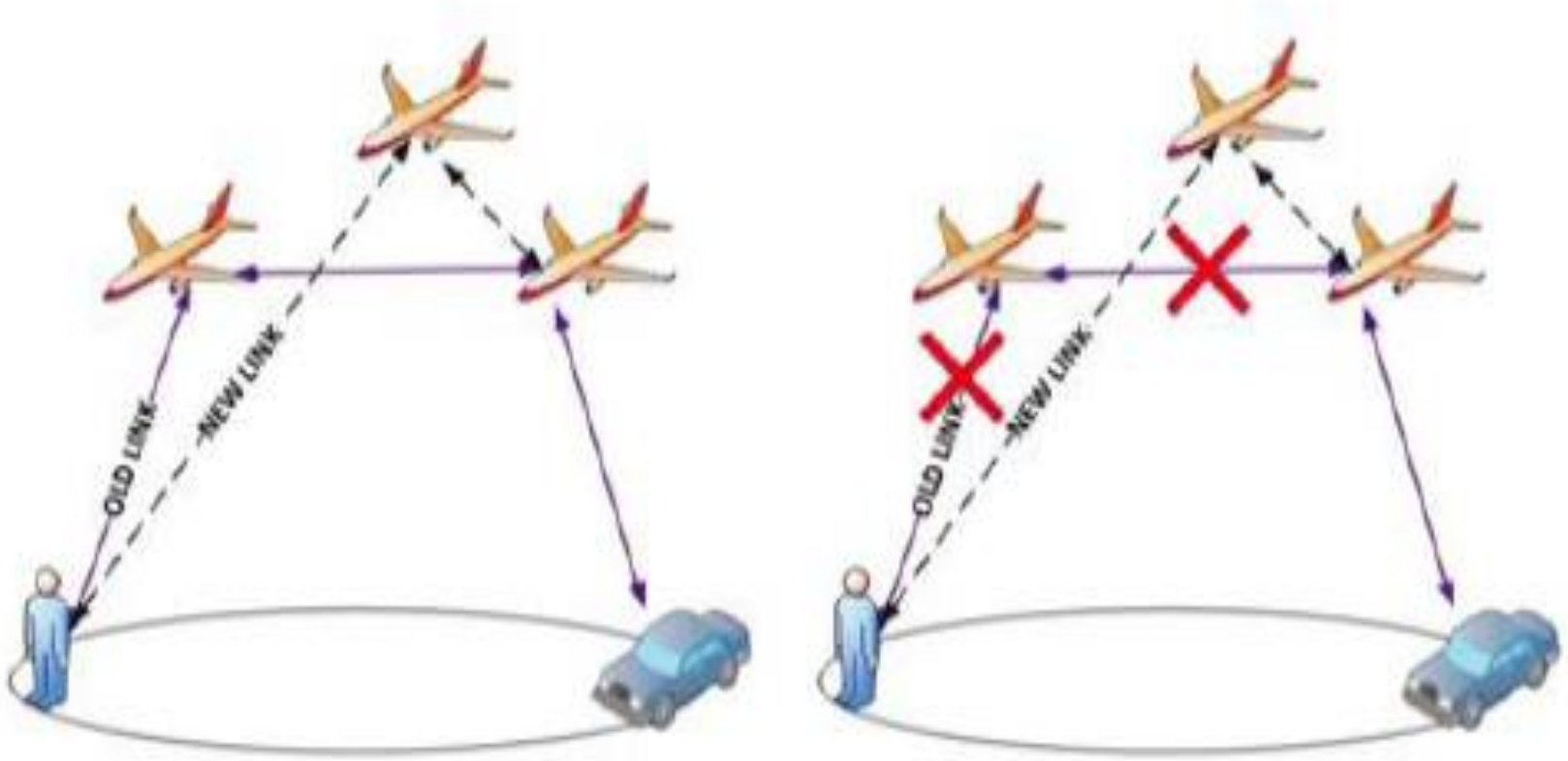


Handover Types : Hard



The links are broken to establish new ones in hard-handover.
The old links are completely deleted, before establishment of new links.

Handover Types : Soft



The old link is temporarily maintained during new link formation.
The old link is deleted only after the new link has been established.

Handover Protocols for UAV Networks

Protocol	Issues
MIPv4 Mobile IPV4	• IP address shortage • Weak security mechanism
MIPv6	• Has high handover latency due to signaling packet loss • Not scalable • Not efficient
PMIPv4 Proxy MIPV4	• Improves latency but does not ensure seamless handover • Better performance than MIPv6 with IEEE 802.11p • Signaling overheads lesser than MIPv4
HMIPv6 Hierarchical MIPV6	• Reduced signaling between nodes and other equipment • Reduces handover latency due to smaller signaling and shorter path.
FMIPv6 Fast MIPV6	• Relies on predictive method with reduced accuracies for mobile networks. • Not suitable for real-time services in fast moving vehicles.

Thank You