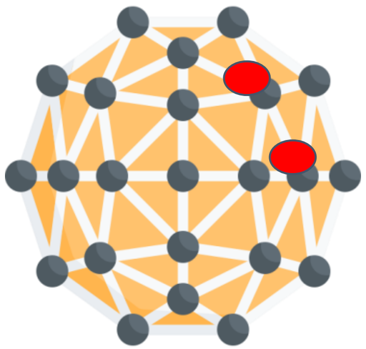
Internet of Things: Protocols and Networks (CSC2106)

Wireless Mesh Network

What is a Wireless Mesh Network

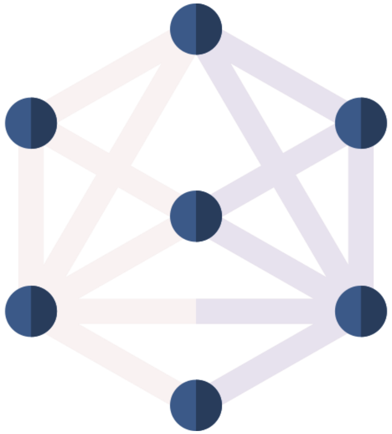
- A wireless mesh network is a decentralized network architecture comprising radio nodes organised in a mesh topology.
- Each node connects directly and dynamically to multiple other nodes without relying on a central router or server.
- Each node in the network can both send and receive data, distributing the network load.
- This setup enhances network reliability, as data can be rerouted through alternative paths if some nodes fail; unlike traditional networks with centralised management
- Widely used in large-scale wireless communications for IoT applications, i.e. smart cities, broadband home networking, and emergency services communications.
- They offer a cost-effective and efficient way to provide robust wireless connectivity across extensive areas, both indoor and outdoor.

Why Mesh?



Failure in 1 Device Won't Break the Network.

No Traffic Problems



New Devices can be Added Easily

Characteristics of Wireless Mesh Network

- **Decentralized Architecture**: Nodes connect directly, dynamically, and non-hierarchically to as many other nodes as possible.
- **Efficient Data Routing**: Nodes cooperate to route data between clients, optimising paths in real-time.
- **Reliability:** Due to the multiple potential paths for data transmission between any two points in the network, wireless mesh networks are highly reliable. Data can be rerouted in case of node failure or path congestion, minimizing the risk of disconnection.
- **Self-forming and Self-healing**: The network automatically establishes and maintains connections among nodes. If any node fails or a path becomes unreliable, the network reroutes data through other nodes to ensure continuous connectivity and coverage.
- **Scalability**: New nodes can be added to the network easily, extending the network's reach and enhancing its capacity without requiring significant changes to the existing infrastructure.
- **Flexibility**: Ideal for IoT, smart homes, and areas where traditional network structures are impractical.

Various Types of Mesh

Distributed

- Nodes in the mesh making connection and routing decisions autonomously

Centralised

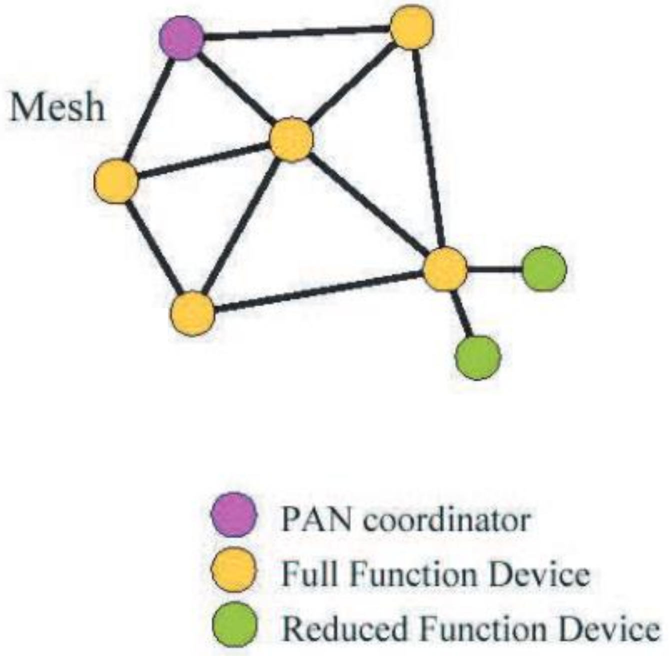
- Central authority assigning roles, routes across the mesh network

Hybrid

- Central authority to establish network topology and nodes autonomously maintain routing

Centralised Mesh

- Characteristics:
  - Nodes rely on a central node to assign them their roles and establish the network topology and routes to node.
  - Resources on nodes such as power are conserved as there is no need to perform discovery of adjacency to send packets
  - Detection of down nodes by central nodes and re-assigning routes t the affected nodes to ensure network stability
- Examples:
  - Zigbee: Mesh Network topology with different device types
    - Network Coordinator acts as central node to form and maintain network
    - End devices purely communicate to routers; does not perform route discovery or maintenance.



Ergen, Sinem Coleri. "ZigBee/IEEE 802.15. 4 Summary." UC Berkeley, September 10.17 (2004): 11.

Distributed Mesh

- Characteristics:
  - Nodes communicate with each other to determine adjacency and routes between each node
  - Uses either reactive or proactive routing protocols to establish routes between nodes and enable multi-hop routing.
  - Detect when nodes are down and work around it by establishing new routes to overcome fault
- Examples:
  - Ad-hoc On-Demand Distance Vector Routing Protocol: Reactive routing algorithm that establishes routes between nodes when there is data that needs to be transmitted
    - Uses hello packets to determine if nodes on the route is still active.
    - If node is down, discovery process is restarted to find route to the destination..

Reference: C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, 1999, pp. 90-100, doi: 10.1109/MCSA.1999.749281

Hybrid Mesh

- Characteristics:
  - Nodes rely on a central node to assign them their roles and establish the network topology.
  - Nodes perform maintenance of routes and adjacencies autonomously using reactive or proactive algorithms
  - Down detection performed by individual nodes and will use routing algorithm to re-establish routes.
- Examples:
  - Hybrid Wireless Mesh Protocol:
    - Network Topology is established using proactive route requests from the root
    - Nodes use RM-AODV for on-demand routing when there is no established route to the destination node, which provides redundancy for when the root is down

Reference: C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, 1999, pp. 90-100, doi: 10.1109/MCSA.1999.749281

Mesh Routing Algorithm

- Wireless ad-hoc and mesh networks are dynamic and mobile, making routing a challenging problem.
- A good routing algorithm should be:
  - Decentralized
  - Self-organizable
  - Self-healing
- Routing should adapt to the bandwidth limitations of the wireless spectrum and exploit multi-hopping for better load balancing.
- Power consumption of the nodes is also essential to provide an energy-efficient solution for wireless networks.

Alotaibi, E. and Mukherjee, B., 2012. A survey on routing algorithms for wireless ad-hoc and mesh networks. Computer networks, 56(2), pp.940-965.

Flooding Mesh Algorithm

What is Mesh Flooding Algorithms

- Nodes are interconnected in a web-like structure, allowing multiple paths for data to travel.
- Data packets are sent to all nodes in the network, allowing them to reach their destination even if the optimal path is unavailable.
- Can lead to network congestion and a high number of redundant transmissions.
  - to address these issues, various techniques such as flooding with control messages or limiting the scope of flooding have been developed.
- Advantages:
  - **Shortest Path:** Useful when many nodes need to keep in sync with each other
  - **Reduced Retransmissions:** Reduce the number of retransmissions that occur during message transmission
  - **Lower Power Consumption:** By reducing the amount of time it takes for a message to be sent, it helps reduce the power consumption

Disadvantages of Mesh Flooding Algo

Resource Utilization

Consumes a significant amount of network resources, including bandwidth and processing power

Security

Vulnerable to malicious attacks, as the messages can be easily intercepted, forged or replicated

Complexity

Complex to manage and troubleshoot, as it requires the coordination of multiple nodes in the network

Scalability

Performance decreases as the network size increases, making it unsuitable for large-scale networks

Overhead

Generates a large amount of control traffic, leading to an increase in network overhead

Latency

Introduces significant latency due to the time necessary for the flooding process to complete

Types of Mesh Flooding Algorithm

01 Simple Flooding

Basic form of Mesh Flooding, where control messages are broadcasted to all nodes in the network without any optimization

02 Reduced Flooding

Reduces the number of control messages by only forwarding them to nodes that have not yet received them

03 Adaptive Flooding

Adjusts the flooding process based on the network conditions and the amount of available resources

04 Selective Flooding

Selectively forwards control messages based on predefined criteria, such as the destination node or the type of information being disseminated

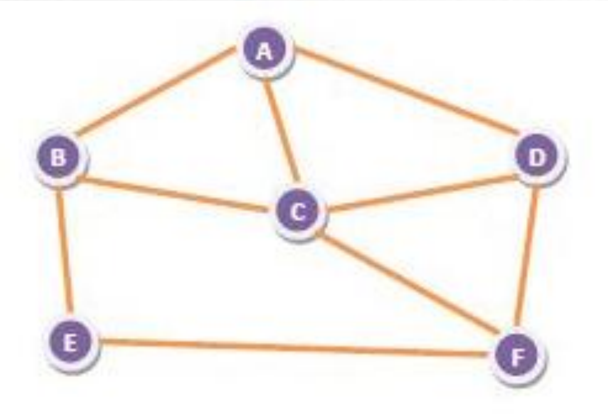
05 Probabilistic Flooding

Uses probability-based techniques to control the forwarding of control messages, reducing the amount of control traffic generated

06 Hybrid Flooding

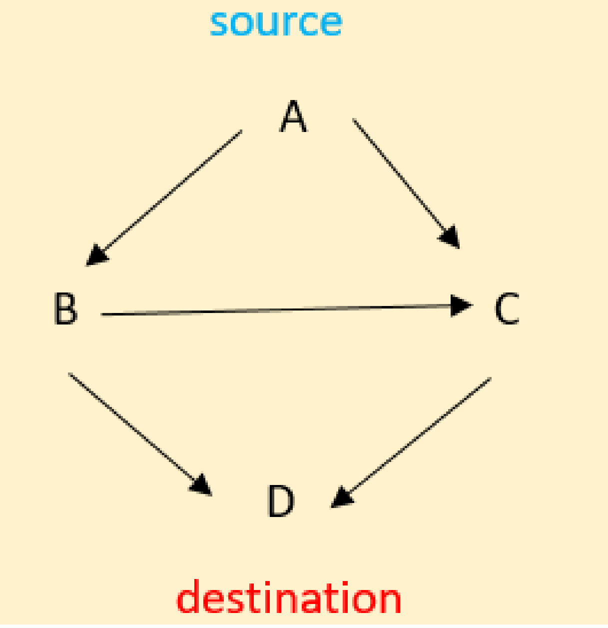
Combines two or more of the above algorithms to optimize the flooding process and improve network performance

01 - Simple Flooding



How It Works

- Dual Role: all nodes act as sender and receiver
- Compare sequence number to determine if data is forwarded to neighbour



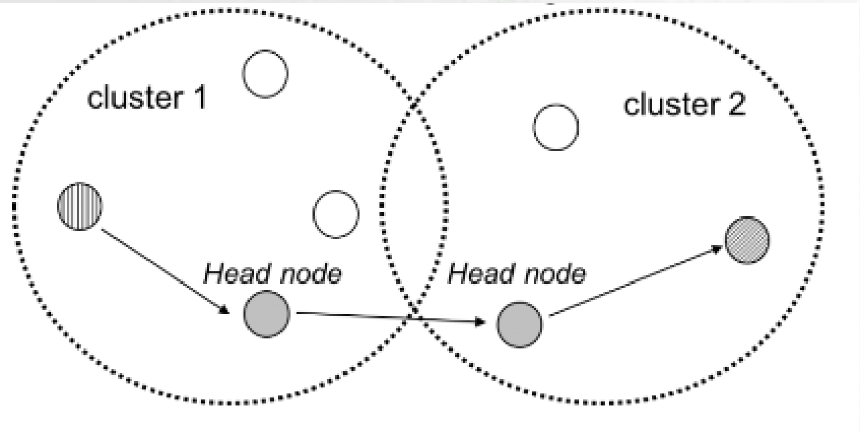
Advantages

- Reliable: multiple paths to send the message if one fails
- Scaleable: easy to add nodes to an existing mesh

Disadvantages

Overhead: more nodes generate more redundant messages
Inefficient: network resources are used by repeated traffic
Latency: data might need multiple hops before reaching destination
Broadcast Storms: packets being forwarded and broadcasted using up all available network
Battery Life: Frequent broadcast messages will drain battery life faster

02 - Reduced Flooding



How It Works

- Hierarchical Reduced Routing Algorithm
  - Divides network into subnets
  - Each subnets has a subnet coordinator (intermediary)
  - Inter-Cluster: Communication between nodes in different clusters
    - coordinators communicate with each other, then forward messages to nodes that have not yet received them
  - Intra-Cluster: Communication between nodes within same cluster
    - nodes within subnet do not talk directly to each other, forwards message to subnet coordinator who will forward to other nodes within subnet or to other coordinators
  - Time to Live (TTL) - a field in the IP header of a packet, indicating how many hops the packet can take before it is discarded, limits distance it can travel, ensures packets not flooded indiscriminately through the network

Source: https://www.comm.upv.es/en/lines-hierarchical-routing/

02 - Reduced Flooding

Advantages

- Reduced network congestion: reduced no. of messages transmitted, improves network performance
- Scalability: division of network allows handling of increasing number of nodes/subnets
- Reduced memory and processing requirements: do not need to store copy of message, only need to store information about nodes that have already received messages

Disadvantages

Complexity: need to keep track which node have received messages and coordination of messages between subnets

Reliability: important control messages may not be transmitted to nodes if one subnet coordinator malfunctions

Latency: messages must pass through subnet coordinators before reaching their destination

03 - Adaptive Flooding

How It Works

- Dynamically adjusts the number of nodes that participate in the flood based on network conditions.
- Nodes monitor the network load and adjust their forwarding behavior accordingly.
- Nodes that observe high network loads reduce their forwarding,
- Nodes that observe low network loads increase their forwarding.

Advantages

<u>Improved scalability:</u> Can scale to large networks by dynamically adjusting the number of nodes participating in the flood.

<u>Reduced network overhead:</u> By reducing the number of nodes participating in the flood when network load is high.

<u>Increased reliability</u>: By adjusting the number of nodes participating in the flood, ensure important messages are transmitted even in presence of high network loads.

03 - Adaptive Flooding

Disadvantages

- Complexity: More complex algorithm compared to traditional mesh flooding algorithms
- Resource requirements: Requires nodes to monitor network load, can increase the resource requirements of nodes in the network.
- Potential for increased latency: In some cases, additional overhead of the Adaptive Flooding algorithm can increase latency and delay the delivery of messages.

04 - Selective Flooding

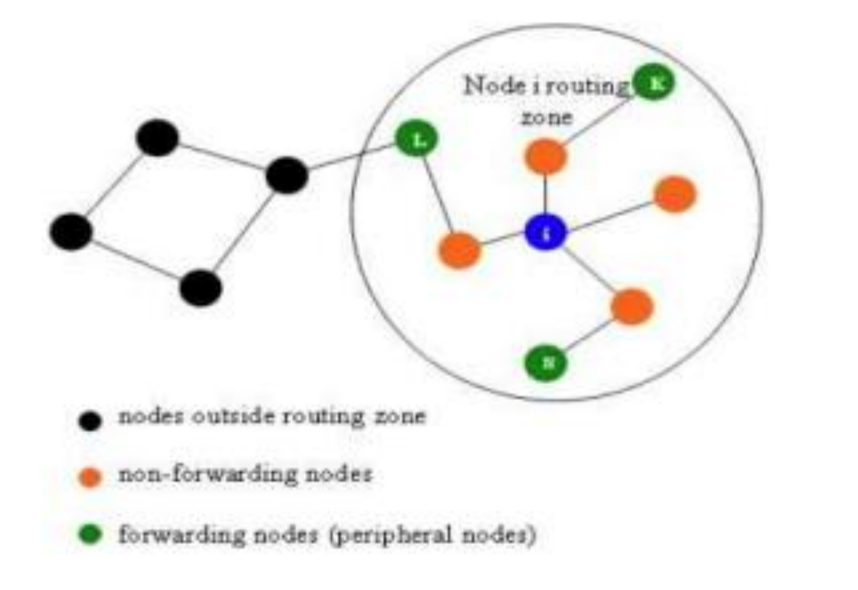
- How It Works
  - Combines the advantages of flooding and selective forwarding.
  - Forwards packet to nodes that are likely to have a route to the destination.
  - Floods packet to neighbours if does not have a route to the destination.
- Advantages
  - <u>Reduced network overhead</u> - Flood only when there is no route to destination.
  - <u>Scalability</u> - Reduce congestion since flooding does not happen all the time.
- Disadvantages
  - <u>Complexity</u> - Algorithm needs to determine which node is likely to have a route to the destination
  - <u>Longer deliver time</u> - May time longer to reach destination since the route selected may not be optimal.

05 - Probabilistic Flooding

- How It Works
  - Uses probabilistic techniques to decide to flood or forward a packet.
  - Probability value assign to each neighbor. The higher the better. Can be calculated with
    - Link quality
    - Number of hops to destination
    - Number of packets previously forwarded
- Advantages
  - Reduced network overhead - Can forward packet to selected neighbours.
  - Scalability - Reduce congestion since flooding does not happen all the time.
- Disadvantages
  - Complexity - Algorithm needs to determine the nodes’ probability value and the threshold to flood or forward a packet.
  - Longer deliver time - May take a longer time to reach destination if threshold is set to too high.

06 - Hybrid Flooding

- How it works
  - Zone based routing protocol (ZRP)
    - Intra zone (IARP)
      - Proactive routing protocol
    - Inter zone (IERP)
      - Reactive routing protocol
- Advantages
  - <u>Overhead</u> - Reduce overhead for longer routes
  - <u>Latency</u> - Periodic flooding of routing information packet
- Disadvantages
  - <u>Routing zone</u> - overlapping of zone on longer routes



Source: https://www.ijcst.org/Volume3/Issue5/p15_3_5.pdf

Comparison of Various Mesh Flooding Algorithm

Flooding Type	Scalability	Latency	Overhead	Complexity	Reliability
Simple	Poor scalability due to high network congestion and bandwidth usage	High latency due to indiscriminate flooding	High overhead due to flooding to all links	Low complexity due to no filtering or control	Low reliability due to lack of filtering
Reduced	Better scalability than simple flooding due to limited scope of flooding	Lower latency than simple flooding due to TTL setting	Moderate overhead due to limited flooding	Slightly higher complexity than simple flooding due to TTL setting	Better reliability than simple flooding due to TTL-based filtering
Adaptive	Good scalability due to dynamic control of flooding scope	Low latency due to adaptive control of flooding	Moderate overhead due to dynamic filtering	Moderate complexity due to dynamic control of flooding scope	Better reliability than reduced flooding due to dynamic control
Selective	Excellent scalability due to targeted flooding	Low latency due to targeted flooding	Low overhead due to targeted filtering	High complexity due to complex routing algorithms	High reliability due to targeted flooding
Probabilistic	Good scalability due to probabilistic filtering	Lower latency than simple flooding due to probabilistic filtering	Low overhead due to probabilistic filtering	Moderate complexity due to probabilistic routing algorithms	Better reliability than simple flooding due to probabilistic filtering
Hybrid	Good scalability due to combination of different flooding types	Low latency due to adaptive control and targeted filtering	Moderate overhead due to dynamic and targeted filtering	High complexity due to multiple routing algorithms and filters	High reliability due to combined filtering mechanisms

Structured Mesh Algorithms

Proactive Mesh Routing Algorithms (Table-Driven):

- **Preemptive Route Maintenance**
- **Lower Latency for Data Transmission** ⬇
- **Increased Overhead** ⬆
- **Examples**:
  - Optimized Link State Routing (OLSR)
  - Destination-Sequenced Distance Vector (DSDV)
  - Wireless Routing Protocol (WRP)
  - Better Approach To Mobile Adhoc Networking (BATMAN).

Reactive Mesh Routing Algorithms (On-Demand)

- **Route Discovery On-Demand**
- **Higher Latency for Data Transmission** ⬆
- **Lower Overhead** ⬇
- **Examples:**
  - Ad hoc On-Demand Distance Vector (AODV)
  - Dynamic Source Routing (DSR)
  - Temporally-Ordered Routing Algorithm (TORA).

Hybrid Routing Algorithms

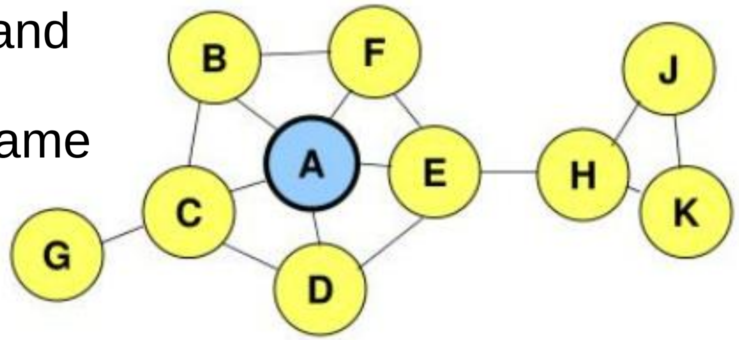
- **Route Maintenance**
- **Network Overhead**
- **Latency**
- **Examples:**
  - Zone Routing Protocol (ZRP)
  - Hybrid Wireless Mesh Protocol (HWMP).

https://ieeexplore.ieee.org/iel7/6287639/6514899/09656902.pdf

Proactive Mesh Routing Algorithm

Optimized Link State Routing (OLSR)

- **Each node** in the network **collects information** about its **direct neighbours**, including their IP addresses and the quality of their links (i.e., the strength of the signal between them). This information is **shared** with **other nodes** in the network through **periodic broadcasts**.
- It uses **multipoint relays (MPRs)** to optimise the transmission of link-state information between nodes. MPRs are nodes that **forward link-state information to other nodes**. They are **selected** based on their **ability to reach many other nodes** in the network with a **minimum** number of **hops**.
- The **best path** is determined based on **factors** such as the **number of hops**, **available bandwidth**, and the **speed of the links** between relays.
- Example: Nodes C and E are multipoint relays of node A. Nodes C and E forward information received from A. Only node E forwards information received from A because C has already forwarded the same information once

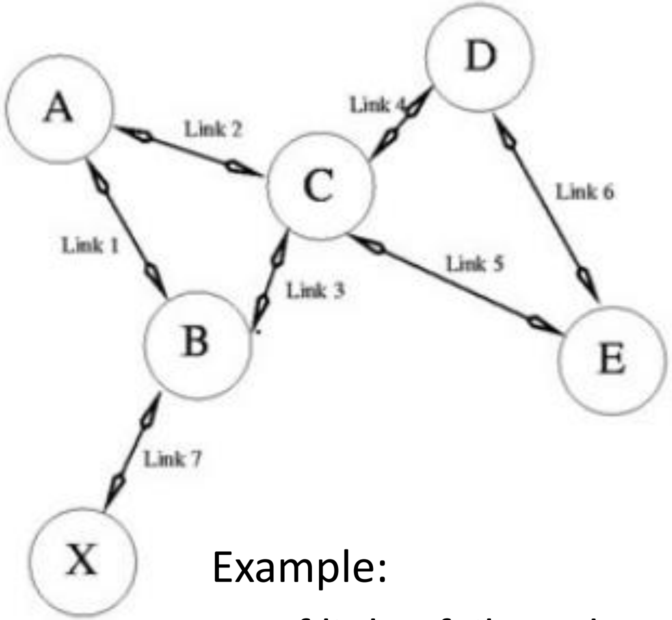


https://www.youtube.com/watch?v=3V19nPxpMp8

Wireless Routing Protocol (WRP)

- Each node maintains four tables:
  - **Distance** table: Contains distance and predecessor node of all destinations as seen by each neighbour
  - **Routing** table: Contains shortest distance to destinations, predecessor node, successor node, and status of the path
  - **Link-cost** table: Contains the number of hops to reach the destination and the number of update periods passed from the last successful update of the link
  - **Message retransmission** list table: Contains counter of each entry
- **Link changes** are propagated using **update messages** sent between **neighbouring nodes**
- **Hello messages** are **periodically** exchanged between neighbours to ensure connectivity
- **Avoids count-to-infinity problem** by forcing each node to **check predecessor information** (by checking for consistency of all its neighbours every time it **detects a change in the link** of any of its neighbours)
- The **goal** is to find the **shortest and most efficient path** for sending data between devices. This is done by **exchanging routing information between devices** and making decisions based on that information. The routing information includes data such as the **distance between devices**, the **quality of the wireless link**, and the **availability of alternative routes**.

Wireless Routing Protocol (WRP)



Dest	Cost	Pred	Succ
A	0	A	A
B	1	A	B
C	2	B	B
D	3	C	B
E	3	C	B
X	2	B	B

→

Dest	Cost	Pred	Succ
A	0	A	A
B	11	C	C
C	10	A	C
D	11	C	C
E	11	C	C
X	12	B	C

Example:

1. If link 1 fail, Node A will notice the failure, considering the single destination which is Node X, Node A will set the “Distance to X” to *infinity* and its predecessor and successor values to *null*.
2. Broadcast that would reach Node C.
3. Node C computes the alternate route to Node A by means of link 2, and then this information is transmitted to Node A.
4. Node A then realised that it could reach other nodes via node C.

Comparing Proactive Mesh Routing Algorithms

	Optimized Link State Routing Protocol (OLSR)	Destination-Sequenced Distance-Vector (DSDV)	Wireless Routing Protocol (WRP)
Network Structure Support	Supports both flat and hierarchical network structures	Supports flat network structures only	Supports hierarchical network structures only
Routing Table Update Frequency	Uses periodic table updates with intervals of a few seconds	Uses triggered updates whenever there is a topology change	Uses triggered updates when there is a change in the network topology
Routing Metric	Uses hop count as the routing metric	Uses hop count as the routing metric	Uses a combination of hop count, bandwidth, and delay as routing metrics
Loop Prevention	Uses Multipoint Relays (MPRs) to prevent loops	Uses sequence numbers to prevent loops	Uses a combination of source routing and sequence numbers to prevent loops
Operation	Uses multipoint relays (MPRs) to minimize flooding and reduce overhead in the network	Table-driven routing protocol that uses sequence numbers to prevent routing loops and maintain consistency in the routing tables	Uses a hierarchical network structure to minimize the routing overhead and improve scalability
Scalability	Can support large-scale networks with a high degree of mobility and traffic	Can support small-scale networks with relatively low mobility and traffic	Can support large-scale networks with moderate to high mobility and traffic

Comparing Proactive Mesh Routing Algorithms

	Optimized Link State Routing Protocol (OLSR)	Destination-Sequenced Distance-Vector (DSDV)	Wireless Routing Protocol (WRP)
Advantages	• Good performance in large, dense networks with a high degree of traffic • Effective use of limited bandwidth and power resources • Resilient to node failures	• Simple to implement and easy to understand • Provides consistent, loop-free routes • Fast convergence time	• Scalable and efficient in large networks with multiple levels of hierarchy • Provides multiple paths and redundancy for better fault tolerance • Supports both unicast and multicast transmissions
Disadvantages	• Can be difficult to set up and configure • High processing and memory requirements • Vulnerable to security attacks	• Requires a lot of overhead traffic to keep the routing tables up-to-date • Not very scalable or suitable for large, dynamic networks • Vulnerable to "counting to infinity" problems	• Hierarchical structure can be complex to implement and manage • Overhead can be high in very large networks • Limited support for dynamic reconfiguration and adaptation
Suitability	large dense networks	large multi-hierarchical networks	small networks, faster to implement

Reactive Mesh Routing Algorithm

Motivation for Reactive over Proactive

Scalability

Reactive routing is considered to be more scalable than proactive routing.

Overhead

Reactive routing requires less overhead traffic compared to proactive routing, making it more efficient in terms of bandwidth usage.

Adaptability

Reactive routing is more suitable for mobile ad-hoc networks where nodes frequently change their position and topology changes frequently.

Alotaibi, E. and Mukherjee, B., 2012. A survey on routing algorithms for wireless ad-hoc and mesh networks. Computer networks, 56(2), pp.940-965.

Dynamic Source Routing (DSR)

Route Discovery

- When a host needs to send a packet to a destination, it first checks its route cache for a pre-existing route
- If no route exists, the host initiates route discovery by broadcasting a route request packet containing the destination's address and a unique identification number
- A route reply is generated when the route request reaches either the destination or an intermediate node that has an unexpired route to the destination in its cache
- The route reply contains a record of the sequence of hops taken

Route Maintenance

- Achieved by using route error packets and acknowledgements
- When a route error packet is received, the hop in error is removed from the node's route cache, and all routes containing the hop are truncated at that point
- Acknowledgements are used to verify the correct operation of route links

P. Sarao, “Comparison of AODV, DSR, and DSDV routing protocols in a wireless network,” Journal of Communications, pp. 175–181, 2018.
https://www.youtube.com/watch?v=GSEvRI6Bptg

Ad-hoc On-Demand Distance Vector (AODV)

SINGAPORE INSTITUTE OF TECHNOLOGY

Route Discovery

- When a host desires to send a message and does not have a valid route to the destination, it initiates a path discovery process to locate the corresponding host
- A route request (RREQ) packet is broadcasted to neighbors, which forwards the request until the destination or an intermediate node with a fresh enough route to the destination is reached
- Intermediate nodes record the address of the neighbor from which they first received the RREQ in their route tables, establishing a reverse path
- The destination or intermediate node with a valid route responds with a unicast route reply (RREP) packet

Route Maintenance

- AODV uses destination sequence numbers to ensure loop-free and up-to-date routes
- Each node maintains its sequence number and a broadcast ID incremented for every RREQ the node initiates
- When a route error is received, the corresponding entry in the route table is invalidated, and the error is forwarded to the source node to initiate a new path discovery process

P. Sarao, “Comparison of AODV, DSR, and DSDV routing protocols in a wireless network,” Journal of Communications, pp. 175–181, 2018.
https://www.youtube.com/watch?v=wlyibjrHhrs

Comparing Reactive Mesh Routing Algorithms

	AODV	DSR
Protocol Type	Hop by Hop Routing	Source Routing
Route Discovery	On Demand	On Demand
Number of Routes	Single route per destination	Multiple route per destination
Route Discovery Frequency	Frequent	Less frequent
Storage Space	Lower storage space	Higher storage space
Utilization	More efficient in networks with high mobility or frequent topology changes	More suitable for networks with lower mobility and fewer topology changes

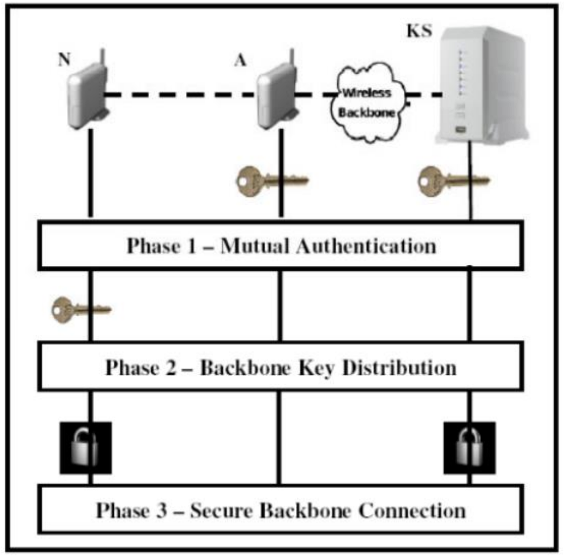
Mesh Security

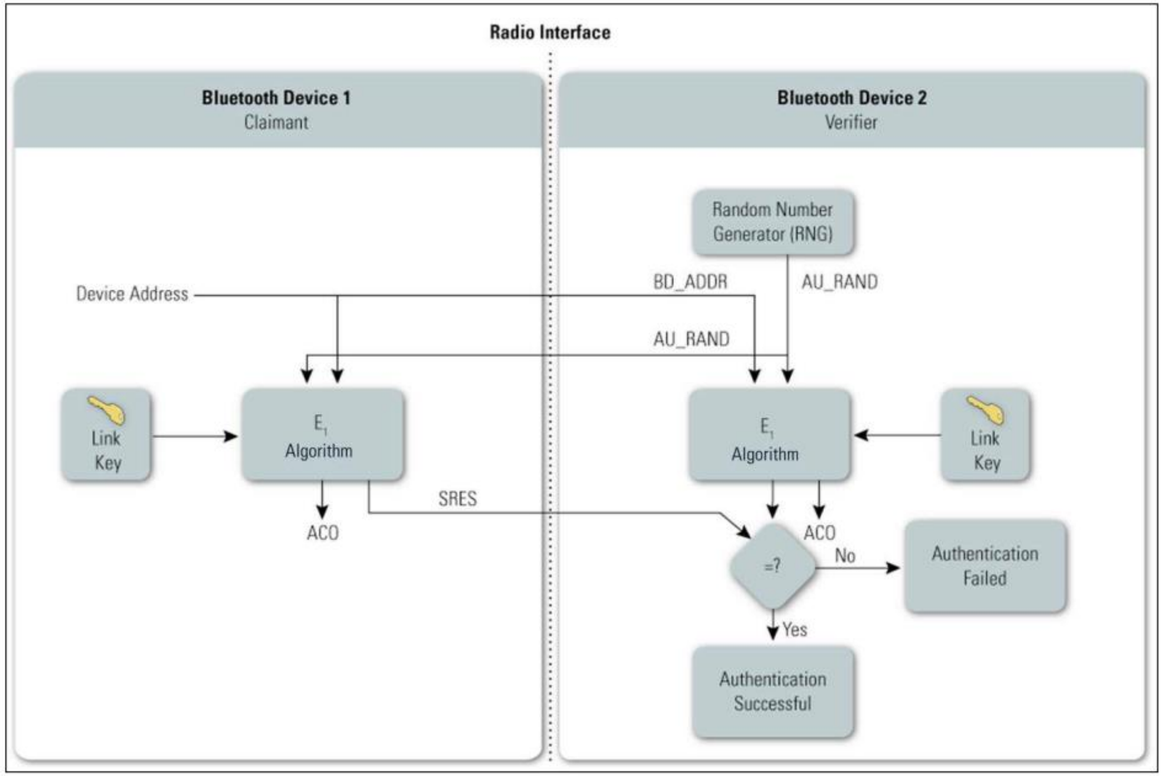
- Malicious nodes joining the network
- Compromised Nodes (Blackhole, sinkhole attacks)
- Man-In-The-Middle (Eavesdropping)
- Flooding (DoS)
- Intentional Collision of Frames

Sen, J. (2013). Security and privacy issues in Wireless Mesh Networks: A survey. *Signals and Communication Technology*, 189–272. https://doi.org/10.1007/978-3-642-36169-2_7

Malicious nodes joining the network

- **Use authentication before allowing devices to join**
- Bluetooth Pairing
  - Challenge-response scheme to allow devices that know the Secret Link Key
  - E1 Algorithm
- Wi-Fi Mesh Networks
  - Key-based authentication

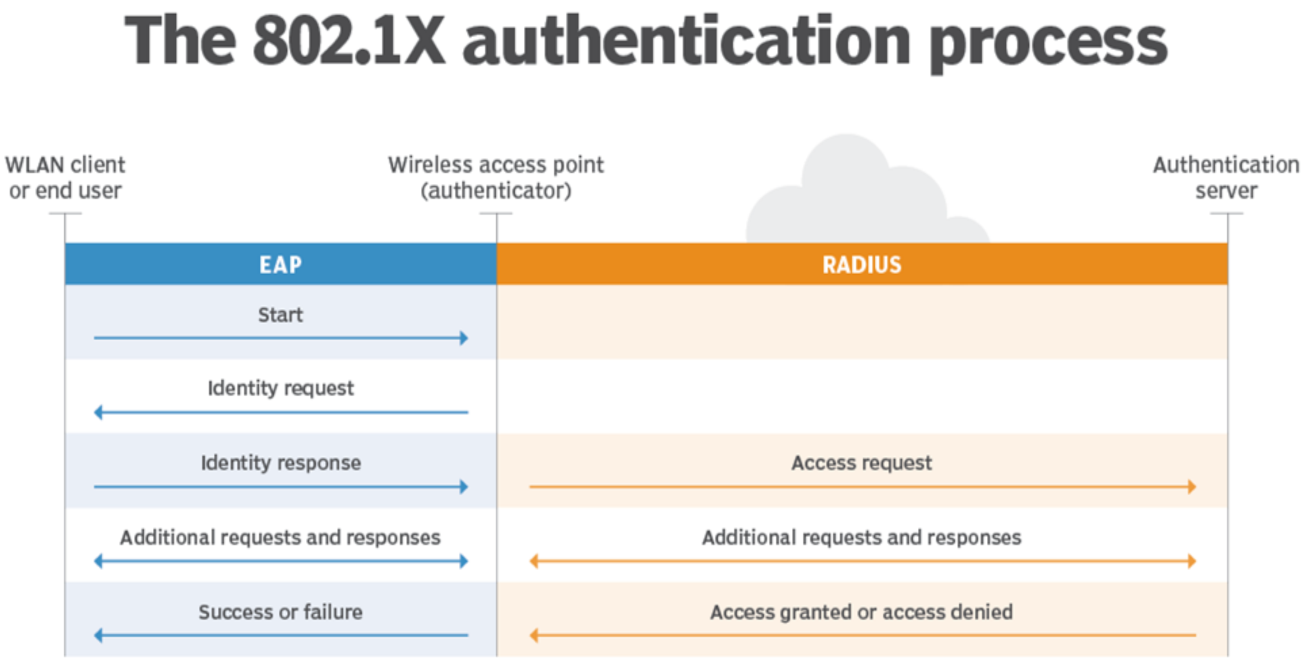




Guide to Bluetooth security. *NIST*. Sen, J. (2013).
Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., & Scarfone, K. (2022).
Security and privacy issues in Wireless Mesh Networks: A survey. Signals and Communication Technology, 189–272. https://doi.org/10.1007/978-3-642-36169-2_7

Compromised nodes

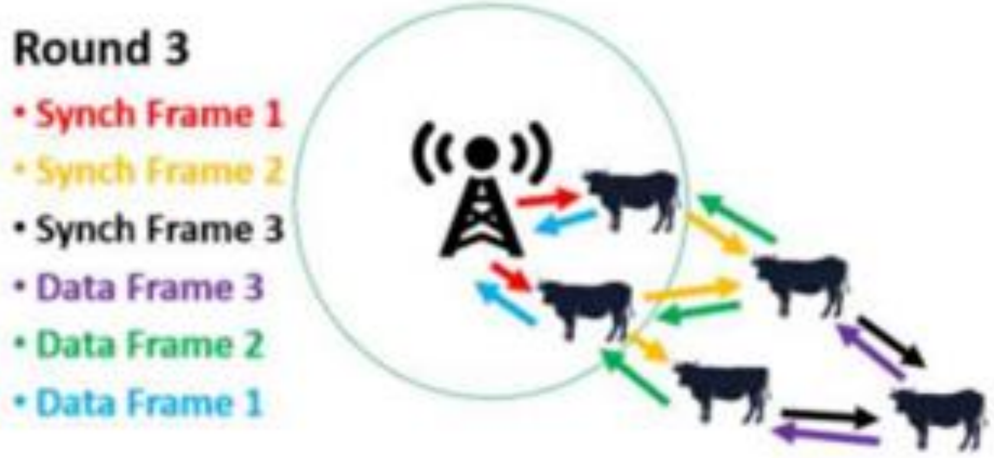
- **Periodic reauthentication to ensure connected nodes are authentic**
- Wi-Fi Mesh Networks
  - Send connection request
  - Provide proof of validity
  - If verified by the authentication server, user remains connected



Agarwal, Shweta & Gupta, Neha. (2012). Authentication and Key Management in Wireless Mesh Network.

Eavesdropping (MITM)

- **Use encryption to keep data private**
- LoRa Mesh
  - AES128, Herd Key & Cattle-specific Key
  - Cattle-specific key to encrypt and decrypt
  - Herd key used to authenticate the packet
  - Herd key updated when new devices join
- Bluetooth Mesh
  - **App Key:** Encrypting/decrypting data for specific applications.
  - **Network Key:** Identify which networks the node belongs to
  - **Device Key:** Identify, provision and configure the node
- Wi-Fi Mesh (not implemented)
  - Spread a stream of packets across different network pathways
  - Different delays for each path; reassembly takes time



Heeger, D., Garigan, M., Tsiropoulou, E. E., & Plusquellic, J. (2020). Secure energy constrained lora mesh network. Ad-Hoc, Mobile, and Wireless Networks, 228–240. https://doi.org/10.1007/978-3-030-61746-2_17

Ren, K., Woolley, M. (2017). Bluetooth Mesh Security Overview. [Online]. Accessible at: https://www.bluetooth.com/blog/bluetooth-mesh-security-overview/

C. Zhou et al., "AMS: Adaptive Multipath Scheduling Mechanism against Eavesdropping Attacks with Programmable Data Planes," 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2021, pp. 2357-2361, doi: 10.1109/IAEAC50856.2021.9390985.

Challenges and Limitations

Timing and Synchronization

- **Issue**: Ensuring that data transmissions are properly timed and that nodes are synchronized can be difficult, especially in environments with variable network delays and node mobility.
- **Impact**: Poor timing and synchronization can lead to collisions, retransmissions, and inefficient use of the communication medium.

Interference and Reliability

- **Issue**: Wireless mesh networks are susceptible to interference from other wireless devices and environmental factors, which can affect signal strength and reliability.
- **Impact**: Interference can lead to increased packet loss, higher retransmission rates, and variable network performance.

Bandwidth Allocation

- **Issue**: Efficiently allocating bandwidth among nodes to ensure fair access and optimal use of the network's capacity is challenging, particularly in high-traffic scenarios or when nodes have differing data transmission needs.
- **Impact**: Poor bandwidth allocation can lead to congestion, increased latency, and degraded quality of service for some or all network participants.

Summary

- What is a Mesh Network
- Flooding Mesh Routing Algorithm
- Proactive Mesh Routing Algorithm
- Reactive Mesh Routing Algorithm
- Mesh Security
- Other Factors