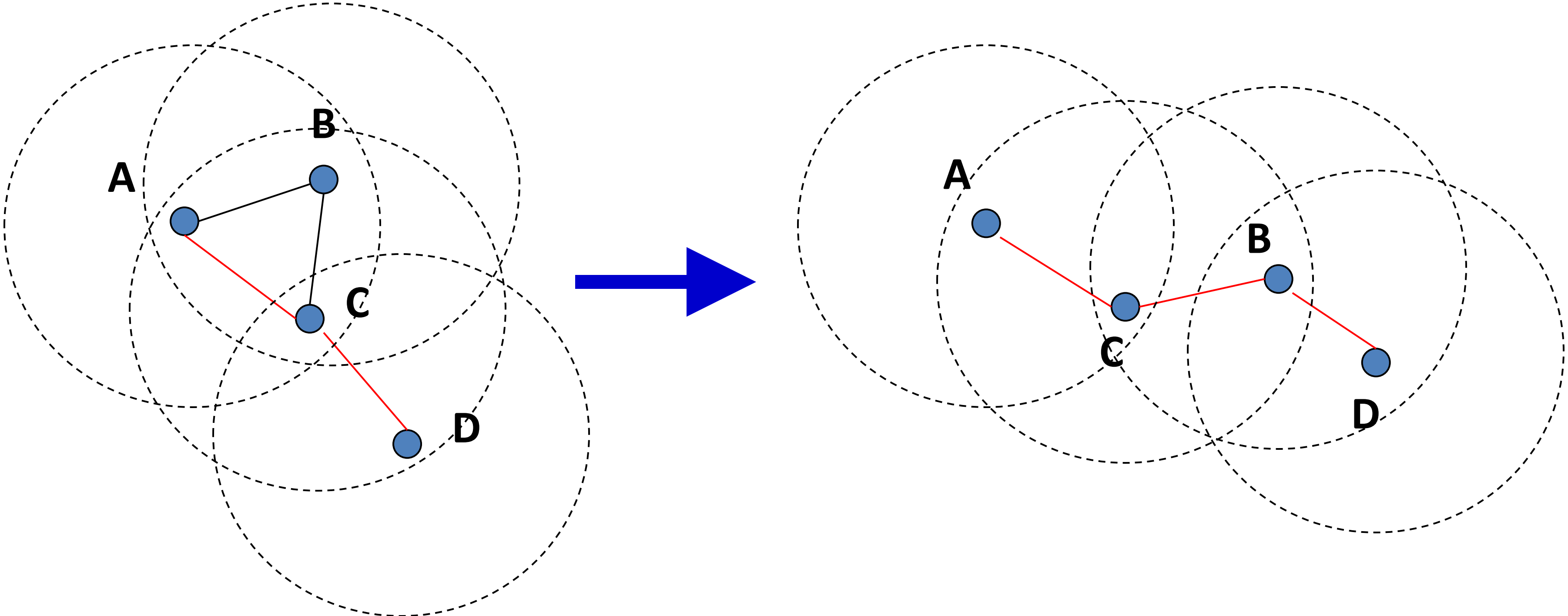
Mobile Ad-hoc Networks

What is a MANET (Mobile Ad Hoc Networks)?

- Formed by wireless hosts which may be mobile
- No pre-existing infrastructure
- Routes between nodes may potentially contain multiple hops
  - Nodes act as routers to forward packets for each other
  - Node mobility may cause the routes change



Why MANET?

- Advantages: low-cost, flexibility
  - Ease & Speed of deployment
  - Decreased dependence on infrastructure
- Applications
  - Military environments
    - soldiers, tanks, planes
  - Civilian environments
    - vehicle networks
    - conferences / stadiums
    - outside activities
  - Emergency operations
    - search-and-rescue / policing and fire fighting

Challenges

- Collaboration
  - Collaborations are necessary to maintain a MANET and its functionality.
  - How to collaborate effectively and efficiently?
  - How to motivate/enforce nodes to collaborate?

- Dynamic topology
  - Nodes mobility
  - Interference in wireless communications

Routing Protocols: Overview

- Proactive protocols
  - Determine routes independent of traffic pattern
  - Traditional link-state and distance-vector routing protocols are proactive
  - Examples:
    - DSDV (Dynamic sequenced distance-vector)
    - OLSR (Optimized Link State Routing)

- Reactive protocols
  - Maintain routes only if needed
  - Examples:
    - DSR (Dynamic source routing)
    - AODV (on-demand distance vector)

- Hybrid protocols
  - Example: Zone Routing Protocol (intra-zone: proactive; inter-zone: on-demand)

Routing Protocols: Tradeoff

- Latency of route discovery
  - Proactive protocols may have lower latency since routes are maintained at all times
  - Reactive protocols may have higher latency because a route from X to Y may be found only when X attempts to send to Y

- Overhead of route discovery/maintenance
  - Reactive protocols may have lower overhead since routes are determined only if needed
  - Proactive protocols can (but not necessarily) result in higher overhead due to continuous route updating

- Which approach achieves a better trade-off depends on the traffic and mobility patterns

Security in Mobile Ad Hoc Networks

Problems

- Hosts may misbehave or try to compromise security at all layers of the protocol stack

- Transport layer: securing end-to-end communication
  - Need to know keys to be used for secure communication
  - May want to anonymize the communication

- Network layer: misbehaving hosts may create many hazards
  - May disrupt route discovery and maintenance: Force use of poor routes (e.g., long routes)
  - Delay, drop, corrupt, misroute packets
  - May degrade performance by making good routes look bad

Security in MANET: Agenda

- Key management
- Securing communications
- Dealing with MAC and Network layer misbehaviors

Key Management

- Challenges
  - In “pure” ad hoc networks, access to infrastructure cannot be assumed
  - Network may also become partitioned

- Solutions
  - Distributed public key infrastructure
    - Self-organized key management
    - Distributed key certification
  - TESLA
  - Others