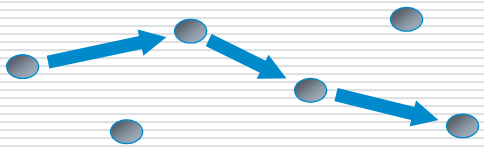
Ad Hoc Networks, Routing and Security

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lectures 20)

Introduction

- Two basic groups of ad-hoc networks
  - Networks of mobile computers
  - Wireless sensor networks
- Basic characteristic
  Ability to establish network communication between hosts without any infrastructure
  - The most significant advance compared to classical fixed systems
  - Reveals a very large scale of new possibilities



Ad-hoc Fundamentals

- Ad hoc networks are autonomous networks operating either in isolation or as "stub networks" connecting to a fixed network
- Do not necessarily rely on existing infrastructure
- No "access point"
- Each node serves as a router and forwards packets for other nodes in the network
- Topology of the network continuously changes

University at Buffalo The State University of New York

Ad-Hoc Fundamentals

- Characteristics
  - Dynamic topology: Nodes are free to move arbitrarily within the network (or leave and join the network) causing random topology changes which can happen rapidly at unpredictable times. Packets are very likely routed over multiple hops
  - Variable capacity links: Significantly lower link capacities compared to traditional hardwired links. High mobility -> low link capacity and vice versa
  - Congestion: More like a rule than exception
  - Energy-constrained mobile nodes: Nodes usually operate on batteries -> all operations must be optimized for energy conservation
  - Weakened physical security: More prone to physical threats than hardwired networks

University at Buffalo The State University of New York

Motivation

- Must support mobility
- Avoids single point of failure typical of centralized systems
- Often unable to rely on existing communications infrastructure
- Desire for a rapidly deployable, self - organizing network
- Multi-hop packet routing used to exchange messages between users who are not within LOS of each other

Why Ad-hoc networks?

- Setting up of fixed access points and backbone infrastructure is not always viable
  - Infrastructure may not be present in a disaster area or war zone
  - Infrastructure may not be practical for short-range radios; Bluetooth (range ~ 10m)
- Ad hoc networks
  - Do not need backbone infrastructure support
  - Are easy to deploy
  - Self-configure
  - Useful when infrastructure is absent, destroyed or impractical

Challenges

Limitations of the Wireless Network

- Packet loss due to transmission errors
- Variable capacity links
- Frequent disconnections/partitions
- Limited communication bandwidth
- Broadcast nature of the communications

Limitations imposed by Mobility

- Dynamically changing topologies/routes
- Lack of mobility awareness by system/applications

Limitations of the Mobile Computer

- Short battery lifetime
- Limited capacities

Applications

- Military
  - Rapidly deployable battle-site networks
  - Sensor fields
  - Unmanned aerial vehicles
- Disaster management
  - Disaster relief teams that cannot rely on existing infrastructure
- Neighborhood area networks (NANs)
  - Shareable Internet access in high density urban settings
- Impromptu communications among groups of people
  - Meetings/conferences
  - Wearable computing
- Automobile communications

Routing in Ad-Hoc Networks

- Why traditional routing protocols cannot be used in mobile ad-hoc networks?
  - MANETs are usually highly dynamic and heterogeneous mobile networks
  - No pre-existing infrastructure
  - No centralized administration
  - Dynamic topologies
  - Variable capacity links
  - Energy-constrained nodes
  - Limited physical security

MANET Protocols

- **Proactive Protocols**
  - Table driven
  - Continuously evaluate routes
  - No latency in route discovery
  - Large network capacity to keep info. current
  - Most routing info. may never be used!
  - Establish routes in advance
  - Example: Optimized Link State Routing Protocol (OLSR)
- **Reactive Protocols**
  - On Demand
  - Route discovery by some global search
  - Bottleneck due to latency of route discovery
  - May not be appropriate for real-time comm.
  - Establish routes as needed
  - Example: Dynamic Source Routing (DSR)
  - Less routing overhead, but higher latency in establishing the path

MANET Protocols

- Hybrid
  - Proactive within a restricted geographic area, reactive if a packet must traverse several of these areas
  - Example: Zone Routing Protocol (ZRP)

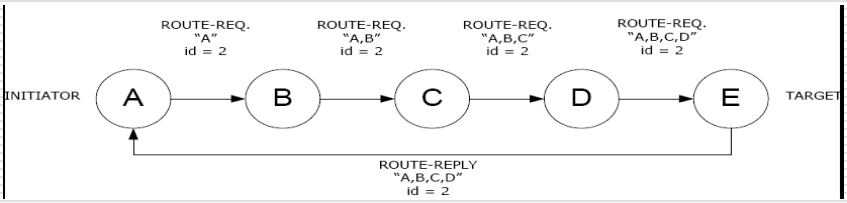
DSR (Dynamic Source Routing)

- DSR is a simple and efficient on-demand source routing protocol designed for multi-hop wireless ad-hoc networks
- DSR doesn't require any existing network infrastructure
- DSR allows network to be completely self-organizing and self configuring
- Two major phases
  - Route discovery
  - Route maintenance
- Route discovery: Used to discover new source routes across multiple network hops to arbitrary destinations in an ad-hoc network
- Route maintenance: Responsible for detecting network topology changes and keeping up-to-date information of already discovered source routes

Overview

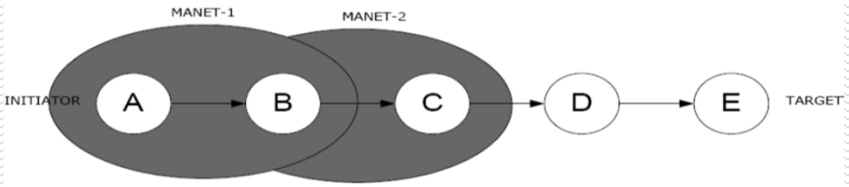
- Route discovery and route maintenance rely on source route caches that are maintained in each node participating in a DSR network
- Each route cache can contain several routes to the same destination node
- Upper levels of software can decide on which criteria source route is selected (throughput, reliability, no. of hops, etc.)
- Designed to work up to 200 nodes
- Use of source routing makes packet routing trivially loop free
- Supports both unidirectional and bidirectional links
- Entirely on-demand based operation -> protocol overhead
- Scales to that needed to react to the topology changes (zero overhead if all nodes stationary and routes have been discovered already)

Route Discovery



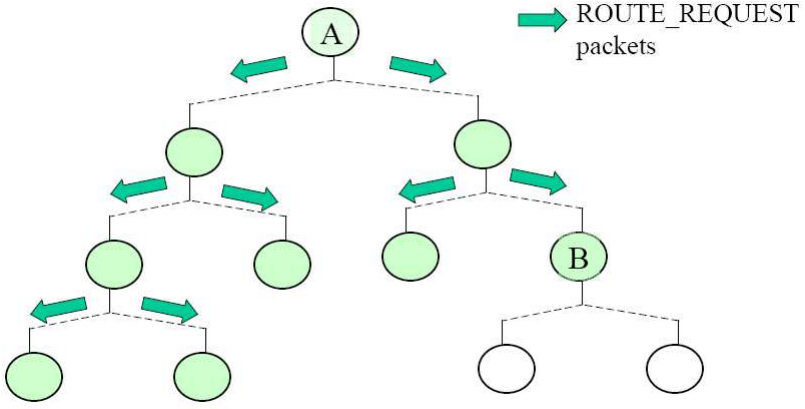
- If source route to the target node is not found in the cache, node A initiates route discovery
- Route-Request packet contains
  - Information about the initiator (A)
  - The target of the Route-Request (E)
  - Unique request identifier (2)
  - List of node addresses through which the particular Route-Request packet has been forwarded

Route Discovery

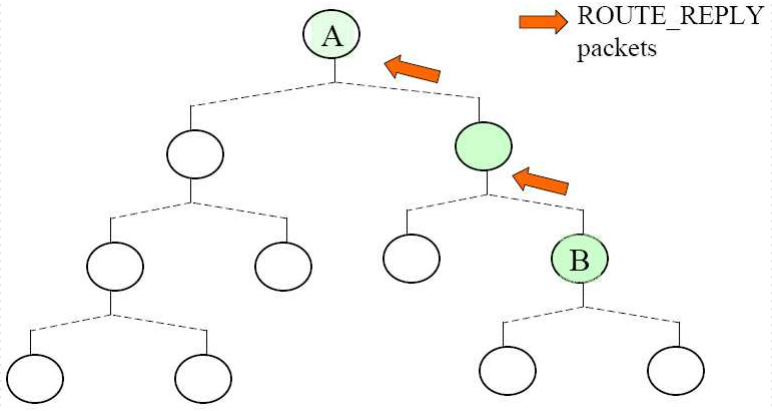


- It is highly possible that some nodes receive the same Route-Request packet more than once -> duplicate packets are discarded
- When returning Route-Reply, node E must take into account that some links in source route might be unidirectional
- If node E doesn't have a route to node A, it must in turn send a Route-Request to the node A. In that case, Route-Reply packet is piggybacked in a Route-Request packet to avoid infinite recursion

DSR Illustration

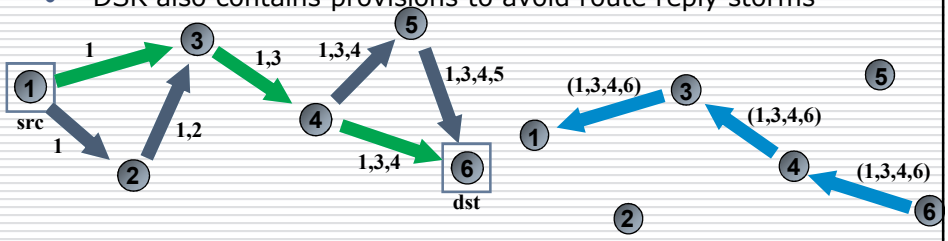


DSR Illustration

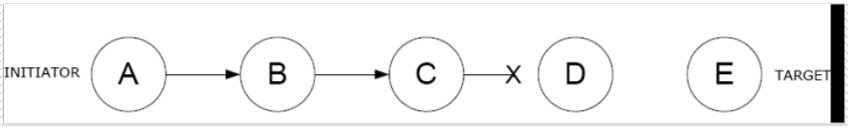


DSR Illustration

- Intermediate nodes may cache accumulated route record contained in the ROUTE_REQUEST packet headers in order to reduce routing overhead
  - Security concerns with this type of snooping
- Confirmation of the receipt of a packet can be done by passive acknowledgement
  - Node overhears a downstream node forwarding the packet
- DSR also contains provisions to avoid route reply storms



Route Maintenance



- Each node is responsible for confirming that the next hop in a source route receives the packet
- The packet is retransmitted up to some maximum number of times until the confirmation is received from the next hop
- Confirmation options: link-level acks, passive acks or software level acks
- If retransmission results in a failure, Route-Error packet is sent to the initiator. Route-Error packet contains information about which link has failed so the initiator can remove that source route from its cache

Summary

- Advantages
  - Ability to work with asymmetric links
  - No periodical routing advertisement
    - Enables bandwidth and energy conservation
    - Overhead does not exist when there are no changes in the network
  - Can be easily improved to become able for providing multiple routes
    - That way, it is not always necessary to initiate new route discovery when some link breaks

Summary

- Disadvantages
  - Large bandwidth overhead
    - Route request packets rapidly grow as they propagate through the network (in their route records they store information about every host over which they passed)
    - That causes potential huge route reply packets
    - Also larger message packets, because addressing demands the whole route to be specified
  - Scalability problems – acceptable size of the network is limited
    - *Diameter* of the network (the largest number of hops needed for communication between any two hosts in the network) directly refers to bandwidth overhead

AODV protocol

- Ad hoc On demand Distance Vector routing protocol
- New route is discovered in a manner that looks similar to route discovery by DSR
  - *Source host* (*src*) broadcasts *route request* (RREQ) to all of its neighbors when it needs to discover route to some *destination host* (*dst*)
  - Then, it waits for *route reply* (RREP)
- But similarity is discontinued at this point

AODV protocol

- Sequence number
  - Number that every host generates for itself
  - It is incremented every time when something is changed in adjacency (e.g., when some link breaks)
  - For every route, *destination sequence number* (DSN) is stored in the *routing table*
  - Last DSN that *src* earlier knew for any route to *dst*, is sent in RREQ, together with current sequence number of *src* and other information needed

    RREQ (src, dst, srcSN, dstDSN, …)

AODV protocol

- RREQ does not contain the route record
  - Does not collect information about hosts through which it propagates
  - Remembers only the number of hops
- Instead, the host through which RREQ propagates adds inverse route (towards *src*) to its routing table
  - Stores, together with other relevant information, the address of the neighbor that sent RREQ to it
  - If that host later receives relevant RREP, it will automatically know that reply should be transferred to the neighbor
  - In that case, it also records the address of the neighbor that sent RREP, thus establishing route towards *dst*

AODV protocol

- Instead of recording the whole route, as with DSR applied, host here keeps only *next hop* (among other relevant information about some destination), i.e., address of its neighbor to which it transfers packets addressed to the destination

Summary

- Advantages
  - Significantly smaller network bandwidth overhead
    - Both control and message packets are smaller
    - The reason is the requirement of only two addresses when routing (*destination* and *next hop*), instead of the whole route as with sequenced routing
    - This is good for scalability, because the size of a packet does not depend on the network diameter
  - Provides support for multicasting

Summary

- Disadvantages
  - Works only with symmetric links
  - Hosts must periodically advertise hello messages
    - Increased bandwidth overhead
    - Reduced possibility of energy conservation by remaining in the sleep mode
  - Does not support *multi path* routing (offers only one route per destination)
    - Every time when some link on the route breaks, new route must be discovered
    - Increased probability of congestion

Security Goals and Challenges

- Availability
  - Survive despite DoS attack
  - Primary concern: Key management service
- Confidentiality
- Integrity
- Authentication
- Non-repudiation

- Challenges
  - Use of wireless links leads ad hoc networks susceptible to link attacks
  - Relatively poor protection, as in battlefields
  - So for high survivability, distributed architecture needed
  - Dynamic network topology: ROUTING
  - Scalable security mechanisms

Security Problems with Existing Ad hoc Routing Protocols

- Attacks against ad hoc routing protocols can be active or passive
- A passive attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic
- An active attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes

Specific Attacks

- Location disclosure: reveals information regarding the location of nodes, or the structure of the network
- Black hole: an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it
- Replay attack: an attacker sends old advertisements to a node causing it to update its routing table with stale routes
- Wormhole: an attacker records packets at one location in the network, and tunnels them to another location

Security Requirements for Ad hoc Routing Protocols

- Certain discovery: if a route between two nodes exists it should always be found
- Isolation: misbehaving nodes should be identified and isolated from routing
- Location privacy: protect information about node location and network structure
- Self-stabilization: the routing protocol should be able to recover from any problem without human intervention
- Byzantine robustness: should be able to function properly even if some participating nodes are disrupting its operation
- Lightweight computations

Routing Security in MANETs

- The External Attack Prevention Model (EAPM) secures the network from external attacks by implementing message authentication code to ensure integrity of route request packets
- The Internal Attack Detection Model (IADM) is used to analyze local data traces gathered by the local data collection module and identify the misbehaving nodes in the network

Possible Solutions

- Black hole - disable the ability to reply in a message of an intermediate node
- IPSec – but complex
- TIARA (Techniques for intrusion resistant ad hoc routing protocols)
- SAR (Security aware ad hoc routing)
- ARAN (Authenticated routing for ad hoc networks)

References

- http://www.cscjournals.org/manuscript/Journals/IJCSS/Volume1/Issue1/IJCSS-6.pdf