

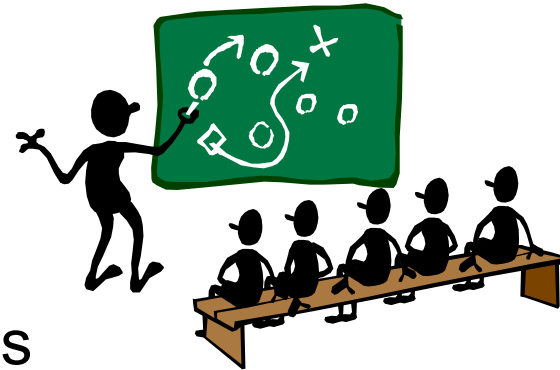
Wireless Revolution

Security Issues in Routing Protocols in Ad Hoc Wireless Networks

Department of Computer Sciences
Purdue University

Outline

- The routing problem
- DSR
- Attacks on routing protocols
- Need for authentication
- Defending against misbehaving nodes



A Word About Routing

- Proactive (table driven) vs on-demand
 - **Proactive**: maintain routes, periodically all nodes send updates, consumes bandwidth independent of the fact that there is data or not to route
 - **On-demand**: a nodes starts looking for a route to the destination when needs to send data, routes are cached, also route maintenance mechanisms
- Hop by hop vs. source routing
 - **Hop-by-hop**: each intermediate node establishes what will be the next hop that will get the packet to destination
 - **Source routing**: source specifies the full path a packet should take to the destination

Routing in Ad Hoc Wireless Networks

- Most well-know protocols: Ad Hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR)
- General mechanism: flood to find a path to the destination, then use reverse path to inform the source about the path
- Both are on-demand protocols, **AODV uses a hop count**, while **DSR uses the shorted path**
- Nodes cache discovered routes
- Route maintenance mechanisms reports broken links
- Standardized by IETF

DSR: Route Discovery

- Source broadcasts **ROUTE REQUEST (RREQ)** packet specifying the destination; RREQ carry unique identifiers
- Intermediary node receiving RREQ, checks to see if he has seen it before: Yes:discard, No, appends its address to a list in the RREQ and rebroadcasts it
- Destination receives RREQ, it sends **ROUTE REPLY (RREP)** back to source of RREQ with a copy of the accumulated address list from RREQ
- RREP reaches source of RREQ, it caches the new route in its route cache.

DSR: Route Maintenance

- If a node on the path does not get an ack after a limited number of local retransmissions it generates a **ROUTE ERROR (RERR)** back to the source identifying the broken link
- Source removes path containing broken link from cache
- Source will use an alternate route to destination (if one exists in cache) or will initiate a new route discovery

Security Issues: RREQ

- Drop the route request
- Change the path on the packet and forward it
- Generate false route request messages to burden the network
- Spoof IP address and send requests
- Result: Nodes can add to a path and make it less probable that the “shortest path” is through them, or can shorten paths to make it more likely they are on paths
- Later, use this to either avoid forwarding traffic, or for traffic analysis, dropping packets

Security Issues: RERR

- Generate false route error messages
- Drop route error messages
- Spoof IP address and send error message for a valid route
- Attacker can continually tear down routes with false error messages, or by not reporting the error, packets will be lost.

Security Issues: RREP

- Suppress route replies
- Send route replies with node as destination
- Send false route replies, modify replies , false topology
- Send higher sequence numbers
- Result: path is not discovered, or make routing path to contain a specific node, possibility for black holes or traffic analysis

Security Issues: Wormhole

- Nodes act in collusion to inject false information
- Take a message and tunnel it to the colluding node in its payload
- Attacker records a packet at one location in the network, tunnels the packet to another location, and replays it there.

Security Issues: Flood Rushing

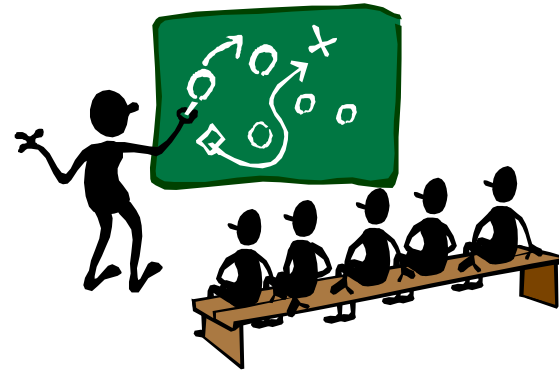
- On-demand routing protocols use duplicate suppression at each node: first RREQ that reaches a node is considered legitimate, next are discarded (all have the same identifier, higher identifiers denote new requests)
- Attacker disseminates RREQ quickly throughout the network suppressing any later legitimate RREQ
- Results: nodes can use flood rushing to make sure that they will be selected on certain routing paths.

Security Issues: Misbehaving Nodes

- Ad hoc networks maximize total network throughput by using all available nodes for routing and forwarding.
- A node may misbehave by agreeing to forward the packet and then failing to do so because it is **selfish, malicious or errors**
- How do you distinguish between the above 3 types?
- What about if nodes collude?

Outline

- Routing
- DSR
- Attacks
- Authentication
- Defense against misbehaving nodes



The Need for Authentication

- Many of the attacks previously presented are possible because of lack of authentication and integrity
- End-to-end authentication vs hop-by-hop:
 - **End-to-end**: the destination is the one verifying the origin, no verification that the packet traveled indeed on the shortest path
 - **Hop-by-hop**: the destination and the intermediate nodes verify any previous sender, as well as origin

Providing Authentication

- Digital Signatures: requires PKI, expensive, provides also non-repudiation
- HMAC: requires a shared key, fast, does not provide non-repudiation
- Hash Chains; fast, requires additional storage, the anchor of the chain must be distributed in an authenticated manner (requires PKI)

Key Management

- Authentication requires some form of key management
- Use Key Distribution Centers (KDC) to distribute symmetric keys
- Use short-lived certificates which require the presence of a Certificate Authority (CA) and revocation mechanisms
- How appropriate are the above solutions for ad hoc wireless networks?
- Other solutions: distributed CA, PGP-like public key infrastructure

Distributed CA

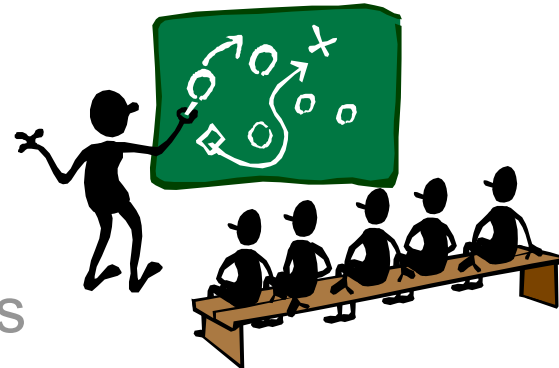
- Centralized CA model not appropriate for ad hoc wireless networks: revocation requires on-line PKI, single point of failure, vulnerability to node compromise
- Distributed CA Model, tolerates t faulty nodes
- Threshold signatures: signing needs coalition of $t+1$ correct nodes, while secret sharing prevents t malicious nodes from reconstructing CA private key

PGP Web of Trust

- Nodes issue certificates as in PGP
- Each node stores the certificates that it issued (**out-bound** certificates) and the certificates that other nodes issued for it (**in-bound** certificates)
- Each node builds up its own **out-bound** and **in-bound** subgraphs
- To establish secure communication, two nodes merge their subgraphs and check if they intersect

Outline

- Routing
- DSR
- Attacks of routing protocols
- Providing authentication
- Defense against misbehaving nodes



DSR Extensions to defend Against Misbehavior Nodes

- Defends against selfish nodes and unreliable links
- Two extensions to DSR - “Watchdog” and “Pathrater”
- Watchdog: identifies misbehaving nodes by overhearing transmissions
- Pathrater: avoids routing packets through these nodes

Watchdog

- Uses promiscuous modes that allows a node A to overhear his neighbors forwarding packets for other nodes
- Each node maintains a buffer of recently sent packets and a failure rating for each node
- By overhearing, tampering of payload or header can also be detected (if packet is not encrypted)

Watchdog (contd.)

- Each node compares each overheard packet with packets in the buffer
- In case of a match, the packet in the buffer is removed
- By overhearing, tampering of payload or header can also be detected
- If the packet has remained in the buffer for longer than a certain timeout: watchdog
 - increases the failure rating for the node responsible for forwarding on the packet
 - If the tally exceeds the threshold value, it determines that the node is misbehaving

Limitations

- **Ambiguous Collisions:** prevents node A from overhearing transmissions from B
- **Receiver Collisions:** node A can only tell this whether node B sends the packet to node C, but it cannot tell if C receives it
- **Limited transmission power:** misbehaving node can control its transmission power to circumvent the watchdog
- **Partial dropping:** a node can circumvent the watchdog by dropping packets at a lower rate than the watchdog's configured minimum misbehavior threshold

Limitations (contd.)

- **False misbehavior**: nodes falsely report other nodes as misbehaving
- **Collusion**: multiple nodes in collusion can mount a more sophisticated attack and circumvent watchdog
- **Multi-rate**: The transmission rate is selected dynamically based on the current channel conditions when a node transmits, such that each frame shall be transmitted at the highest available rate.

Pathrater

- Combines knowledge of misbehaving nodes with link reliability data to select most reliable path
- Each nodes maintain a rating for every other node it knows about in the network
- If there are multiple paths to the same destination, the path with the highest metric is chosen
- Relevant metrics to evaluate the protocol: throughput, overhead, false positives.

Summary

- Many attacks in wireless network can be prevented by providing authentication, integrity and non-repudiation
- Requires some form of key management
- Wormholes and flood rushing can not be addressed by authentication only
- Detecting malicious nodes is very challenging

