

Security Topics in Networking and Distributed Systems CS 590D

Lecture 16: Security Issues in Routing Protocols

Department of Computer Sciences
Purdue University

References

- Mitigating routing misbehavior in mobile ad hoc networks. Sergio Marti and T. J. Giuli and Kevin Lai and Mary Baker. MOBICOM 2000.



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**: node establishes what will be the next hop that will get the packet closed to destination
 - **Source routing**: source specifies the full path a packet should take to the destination

Routing in Ad Hoc Wireless Networks

- Most well-known protocols: AODV and 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 shortest recorded path
- Nodes cache discovered routes
- Route maintenance mechanisms
- Standardized by IETF

Dynamic Source Routing (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 (PATH) from RREQ
- RREP reaches source of RREQ, it caches the new route in its Route Cache.

DSR

Route Maintenance

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

Security Issues

- Attacks related to the 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

- Attacks related to 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

- Attacks related to route replies
 - Suppress route replies
 - Send route replies with node as destination
 - Send false route replies, modify replies , false topology
 - Send higher sequence numbers

Security Issues

- Wormhole attack
 - 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 Attack:
 - 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

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?

DSR Extensions to defend Against Misbehavior Nodes

- 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.

Results

- Simulation performed, in a 670 by 670 meter flat space filled with 50 wireless nodes
- Nodes communicate using 10 constant bit rate (CBR) node to node connections and move in straight line towards the destination at uniform speed 0-20 meter/seconds(m/s)
- Pause time as 0 and 60 seconds
- The percentage of the compromised nodes vary from 0% to 40% in 5% increments
- Results: Throughput increased with 17% when 40 % nodes are misbehaving, overhead 9-17%

Summary

- Solution to misbehaving nodes:
 - nodes watch their neighbors to make sure that they forwarded packets
 - reliability metric used to select most reliable path
- Has limitations: colluding attacker, multi-rate, etc

