Overview

- “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, MobiCom 2000
- Introduces two techniques that improve throughput in an ad hoc network in the presence of “misbehaving” nodes.
Outline

• Background
  - Ad-Hoc Networks
  - Routing in Ad-Hoc Networks

• Dynamic Source Routing Extensions
  - Watchdog
  - Pathrater

• Simulation Results
• Related Work
• Future Work and Conclusions

Background: Ad-Hoc Networks

• Collection of wireless mobile devices
• Vulnerabilities
• Misbehaving Nodes
• Solutions
• Routing Issues
Background: Routing in Ad-Hoc

- Two categories:
  - Table Driven
    - Nodes maintain routing tables
    - Broadcast updates
  - On Demand
    - Routes created only when needed
    - Routes expire or removed

Outline

- Background
  - Ad-Hoc Networks
  - Routing in Ad-Hoc Networks
- Dynamic Source Routing Extensions
  - Watchdog
  - Pathrater
- Simulation Results
- Related Work
- Future Work and Conclusions
Dynamic Source Routing

- On Demand routing
- Nodes maintain a route caches
- Route Discovery Phase
  - If not found in cache, broadcast a route request packet
  - Destination sends a route reply
- Route Maintenance Phase
  - Error packets
  - Acknowledgments

Dynamic Source Routing Extensions: Watchdog

- Identifies misbehaving nodes
- Maintains a buffer of transmitted packets
- Monitors next hop node’s transmission

- Increments a failure tally for the nodes
Dynamic Source Routing Extensions: Watchdog cont’d

• Watchdog Weaknesses
  - Ambiguous collisions
  - Receiver collisions
  - False misbehavior reporting
  - Limit transmission power
  - Collusion
  - Partial dropping

Dynamic Source Routing Extensions: Pathrater

• Avoids routing packets through malicious nodes
• Each node maintains a rating for every other node
• A node is assigned as a “neutral” rating of 0.5
• The rating of nodes on all actively used path increase by 0.01 at periodic intervals of 200 ms
• The rating of nodes decrease 0.05 when a link break is detected
• High negative numbers are assigned to nodes suspected of misbehaving nodes by Watchdog
Dynamic Source Routing Extensions: Pathrater cont’d

- It calculates a path metric by averaging the node rating in the path
- If there are multiple paths, the node chooses the path with the highest metric
- It increases the throughput
- It gives a comparison of the overall reliability of different paths
- It increase the ratio of overhead transmissions to data transmission

Outline

- Background
  - Ad-Hoc Networks
  - Routing in Ad-Hoc Networks
- Dynamic Source Routing Extensions
  - Watchdog
  - Pathrater
- Simulation Techniques
- Related Work
- Future Work and Conclusions
Simulation Scenario

• Assumptions
  - Bidirectional communication
  - Wireless interfaces that support promiscuous mode operation

• Setup
  - 50 nodes in various states of mobility
  - Created 4 different extension scenarios (WD, PR, SRR)
  - Varied misbehaving nodes 0% to 40%

Simulation Metrics

• Evaluation done on three metrics:
  - Throughput: % of sent data actually received by the intended destinations
  - Overhead: Ratio of routing-related transmission to data transmissions
  - Watchdog False Positives: The impact when watchdog mistakes a node as misbehaving
Simulation Metrics: Throughput

- Best performance when all three extensions were active
- Pathrater isolated in one test
- Pathrater alone does not affect performance
Simulation Metrics: Overhead

- Increased overhead
- Watchdog isolated in one simulation
- Watchdog alone adds a little overhead
Simulation Metrics: False Detection

• Demonstrated how throughput is effected with the reporting of False Positives
• Throughput does decrease but could result in beneficial side effects:
  - Helps determine unreliable nodes
  - Ambiguous collisions may help increase throughput
  - Nodes maintain a fresher route cache

Outline

• Background
  - Ad-Hoc Networks
  - Routing in Ad-Hoc Networks
• Dynamic Source Routing Extensions
  - Watchdog
  - Pathrater
• Simulation Results
• Related Work
• Future Work and Conclusions
Related Work

- No significant related work before publication date in 2000.
- DSR, AODV, TORA, DSDV, STAR only detect if the receiver's network interface is accepting packets.
- Some recent related work:

Outline

- Background
  - Ad-Hoc Networks
  - Routing in Ad-Hoc Networks
- Dynamic Source Routing Extensions
  - Watchdog
  - Pathrater
- Simulation Results
- Related Work
- Future Work and Conclusions
Future Work

- Expand on how the threshold values could be optimized
- Implementation of a priori trusted relationships
- Detection of multiple node collusion

Conclusions

- Ad hoc networks are vulnerable to nodes that misbehave when routing packets
- Simulation evaluates that the 2 techniques
  - increases throughput by 17% in network with moderate mobility, while increase ratio of overhead to data transmission from 9% to 17%
  - increases throughput by 27% in network with extreme mobility, while increase ratio of overhead to data transmission from 12% to 24%
Thank you.

- Questions...