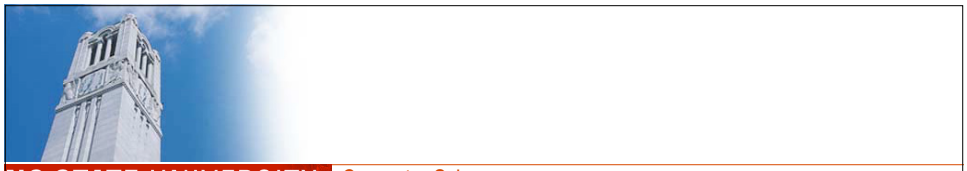


NC STATE UNIVERSITY Computer Science

CSC 774 Network Security

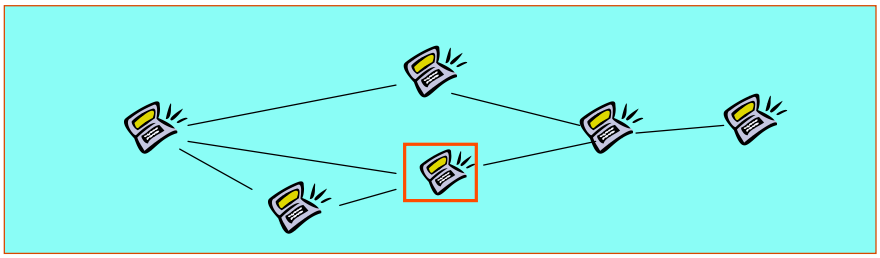
Topic 8.2 Detecting Misbehaving Nodes

Outline

- Misbehaving nodes in MANET
- Watchdog
  - Detect misbehaving nodes
- Pathrater
  - Avoid misbehaving nodes
- Further readings

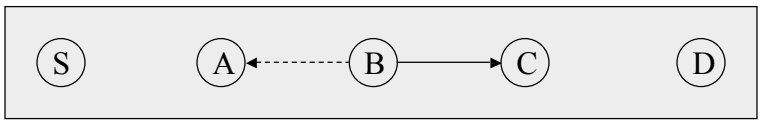
Misbehaving Nodes in MANET

- Misbehaving nodes
  - Use other nodes for routing and forwarding
  - May agree to forward packets for other nodes,
  - But do not do so
    - Drop all
    - Selectively drop



Watchdog

- Basic idea
  - Monitor the forwarding nodes by overhearing their transmission



Observations:

- ✓ When A transmits a packet for B to forward to C
  - A can often tell if B has transmitted the packet.
  - If link encryption is not used, A can also tell if B has tampered with the payload or the header

Watchdog (Cont'd)

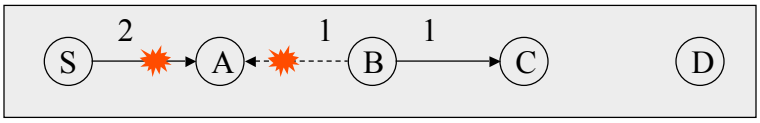
- Method
  - Monitoring
    - Maintain a buffer of recently sent packets
    - Compare each overheard packet with the packets in the buffer
    - If there is a match, remove the matching packet from the buffer
  - Failure detection
    - If a packet remains in the buffer too long, increase a failure tally for the node responsible for forwarding
  - Alert generation
    - If the tally exceeds a threshold, it determines that the forwarding node is misbehaving and notify the source

Watchdog (Cont'd)

- Advantage
  - Can detect misbehaving nodes at forwarding level, not just the link level
- Weaknesses
  - Might not detect a misbehaving node in presence of
    - Ambiguous collisions
    - Receiver collisions
    - Limited transmission power
    - False misbehavior
    - Collusion
    - Partial dropping

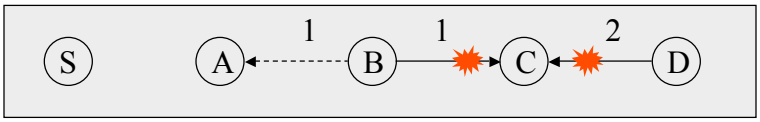
Watchdog (Cont'd)

- Ambiguous collisions
  - A packet collision occurs at the monitoring node



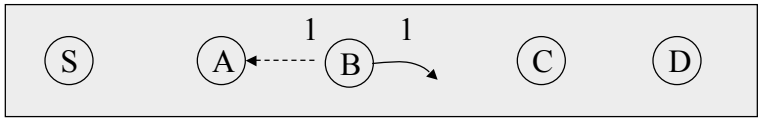
A should continue to monitor B

- Receiver collisions
  - A packet collision occurs at the receiver



Watchdog (Cont'd)

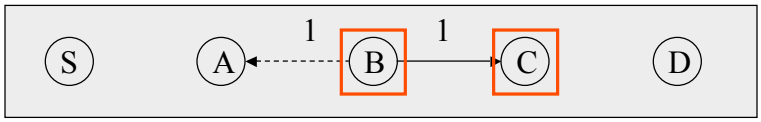
- Control transmission power



- False misbehavior
  - A malicious node claims a normal node to be misbehaving
  - Could be detected

Watchdog (Cont'd)

- Colluding misbehaving nodes



- Partial dropping at a lower rate than the threshold
- Only works for source routing
  - A monitoring node must know the next hop.

Pathrater

- Run by each node in the network
- Picks the route most likely to be reliable by
  - combining the knowledge about misbehaving nodes with link reliability

Pathrater (Cont'd)

- Choosing the path
  - Each node maintains a node rating for every other node
  - It calculates a path metric by averaging the node rating in the path
  - When there are multiple paths, it chooses the path with the highest metric

Pathrater (Cont'd)

- Maintaining the node ratings
  - When a node is known to a pathrater, assign it a neutral rating of 0.5
    - Always assign itself 1.0
  - Increments the ratings of nodes on all actively used paths by 0.01 periodically
    - Actively used path: a path used in the previous period to send packets
    - Maximum rating of a node: 0.8
  - Decrement a node's rating by 0.05 when a link break is detected
  - Assign -100 to nodes suspected of misbehaving
    - Such nodes have their rating slowly increased to a non-negative value

Further Readings

- S. Buchegger and J. L. Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks)," In *Proceedings of The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 226--236, June 2002.
- Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," In *Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000),* pages 275--283, August 2000.