

Mitigating Routing Misbehavior in Mobile Ad Hoc Networks

S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *The 6th ACM International Conference on Mobile Computing and Networking*, August 2000.

Student Lecture by
Ragavendra Ananthapadmanabhan
EECS 800 Survivable Networking

Department of Electrical Engineering and Computer Science
University of Kansas

OUTLINE

- Introduction
 - Ad hoc networks
 - Routing in ad hoc networks
 - Types of nodes in ad hoc network
 - Misbehaving nodes and their solution
 - Assumptions and DSR
 - Techniques followed to mitigate the misbehavior
 - Methodology and metrics
 - Simulation results
 - Conclusion and future work – Satisfying “R”s in Survivability
 - References
-

Introduction

- Ad hoc networks
- Routing in ad hoc networks
 - Maximize throughput by routing through all available nodes
 - More participating nodes, more aggregate bandwidth
 - Shorter the routing path, smaller the network partition
- Types of nodes in the network
 - Overloaded -- lacks CPU cycles, buffer space, available BW
 - Selfish -- unwilling to spend CPU cycles, battery life
 - Malicious -- drops packets
 - Broken -- software fault preventing forwarding

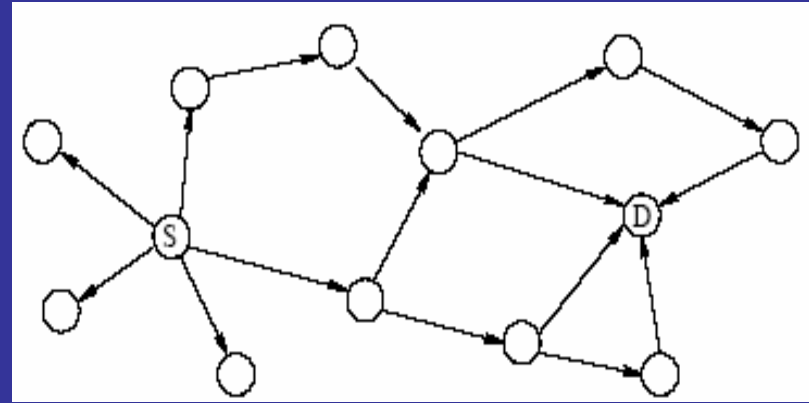
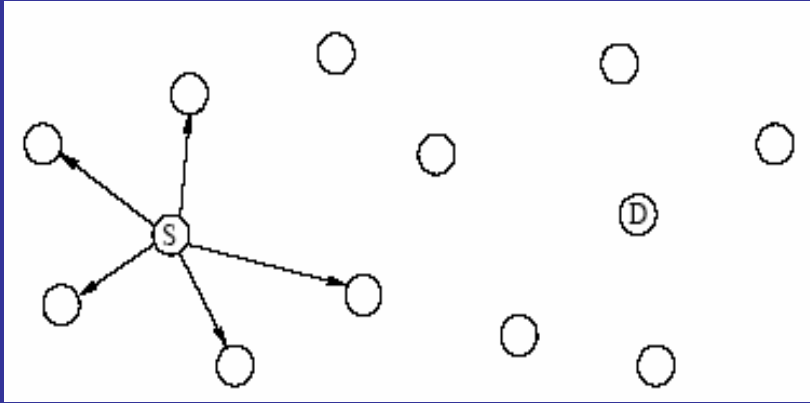
Misbehaving nodes and their solutions

- Decrease in throughput if 10%-40% of nodes misbehave
- Degradation of 16%-32% in throughput
- Solutions
 - a-priori trust relationships
 - Trust relationships built outside of the context of the network
 - Problems can happen due to authentication
 - Another solution is to isolate these misbehaving nodes
 - But this adds significant complexity to the routing protocol
- Techniques
 - Watchdog -- identifies misbehaving nodes
 - Path rater -- avoids routing through these nodes

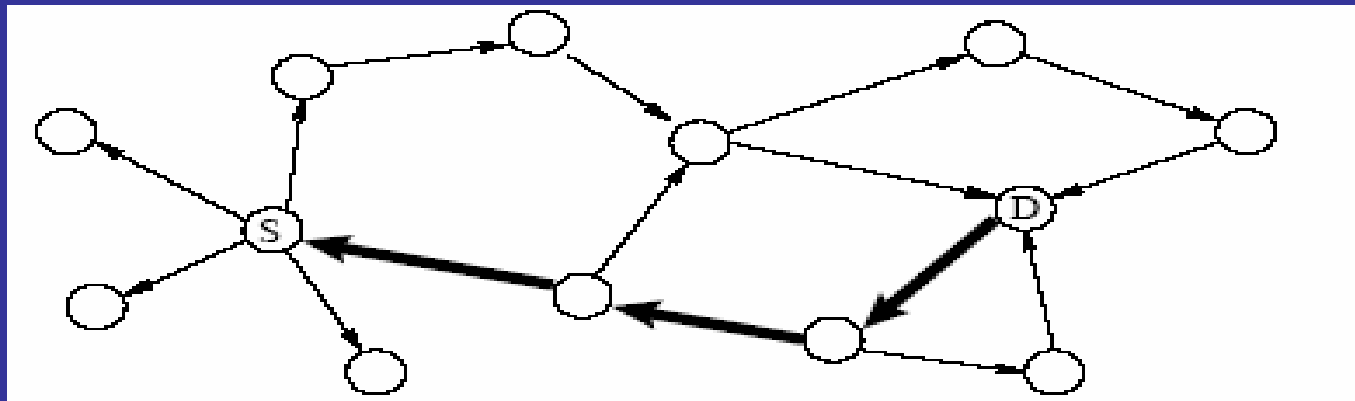
Assumptions and DSR

- Physical layer characteristics
 - Bi-directional links between the nodes
 - In accordance with the 802.11 and MACAW
 - Interfaces supports *promiscuous* mode of operation
 - Lucent Technologies' WaveLAN have this capacity
- DSR (Dynamic Source Routing Protocol)
 - On-Demand source routing protocol
 - Route Discovery through ROUTE REQUEST packet
 - Route Maintenance through ROUTE ERROR packet

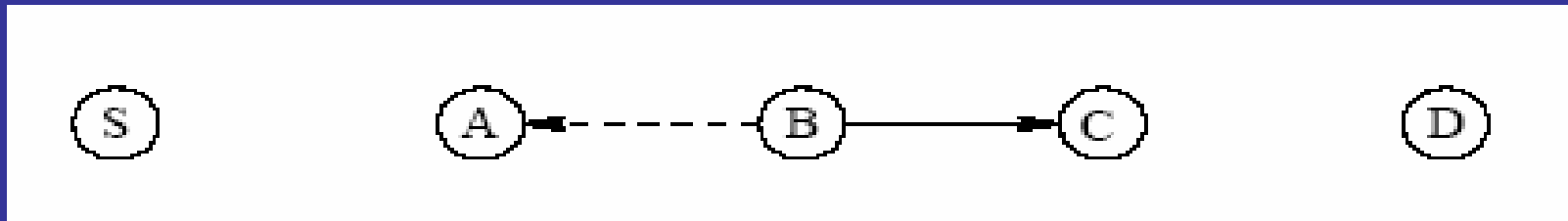
DSR Mechanism



Route discovery mechanism



Techniques followed to mitigate the misbehavior



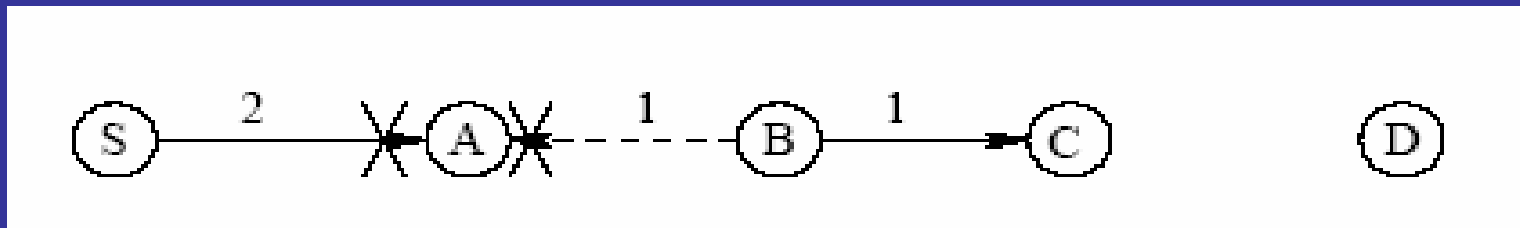
- Watchdog implementation
 - A can overhear B and tell whether B has forwarded the packet
 - Buffer is maintained for recently sent packets
 - The overheard packet is compared with the sent packet
 - If there is a match, discard the packet.
 - If the packet stays till a timeout, increment the failure tally for the node
 - If tally exceeds a threshold, declare the node as misbehaving

Techniques followed to mitigate the misbehavior

- Weaknesses for Watchdog
 - This will not detect the misbehaving node during:
 - Ambiguous collisions
 - Collusion
 - Receiver collisions
 - False misbehavior

Techniques followed to mitigate the misbehavior

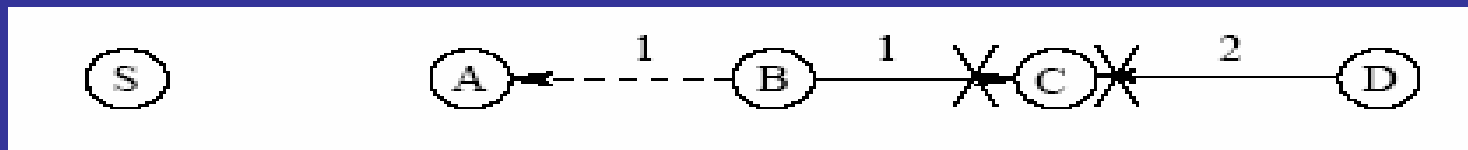
- Ambiguous collisions



- A packet collision can occur at “A” while listening to “B”
 - “A” does not know whether “B” has forwarded the packet
 - Due to this uncertainty, “A” should not immediately accuse “B”
 - Instead watch “B” over a period of time and decide later.
- Collusion
 - Multiple nodes can collude and present sophisticated attack
 - Problem currently studied in CMU

Techniques followed to mitigate the misbehavior

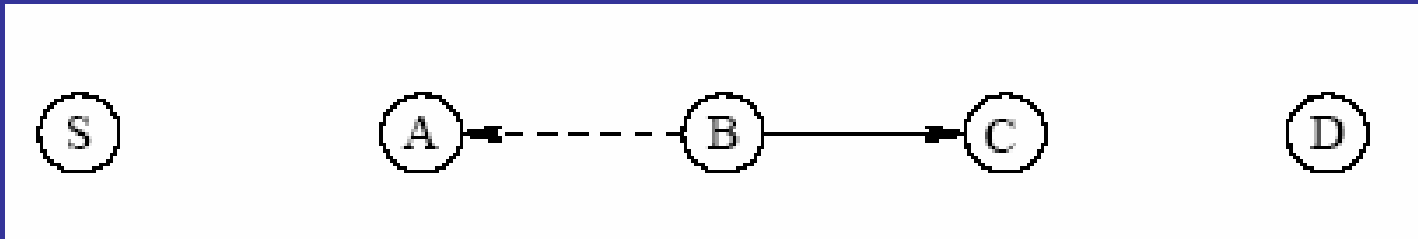
- Receiver collision



- Node “A” cannot tell whether “C” receives the packet
- If collision occurs at “C”, “A” cannot detect the collision.
- “B” can leave “A” none the wiser – doesn’t retransmit – selfishness
- “B” can wait to make a collision – Misbehaving node
- Not an Overloaded or selfish node

Techniques followed to mitigate the misbehavior

- False misbehavior
 - Nodes falsely report other nodes as misbehaving
 - Node “A” can report “B” as misbehaving when “A” is the culprit
 - This will be detected
 - “S” receives ACKs from “D” through “B” and “A”
 - “S” wonders why it receives ACKs if “B” drops the packets
 - If “A” drops ACKs to hide from “S”, “B” detects this and informs “D”



Techniques followed to mitigate the misbehavior

- Pathrater
 - Combines knowledge of misbehaving nodes to pick the route
 - Each node maintains a rating for every other node
 - Calculate a path metric by averaging the node ratings
 - This gives a comparison of overall reliability of different paths
- Ratings Algorithm
 - A neutral rating of “0.5” is assigned to a node discovered
 - Source rates itself with “1.0” to ensure shortest path
 - Increment the rating of nodes in active path by 0.01 every 200ms
 - Decrement the rating by 0.05 in case of broken link
 - Assign “-100” for misbehaving node
 - When calculating metric, negative value indicates misbehaving path
 - Increase the negative rating to non-negative value after long timeout

Methodology and metrics

- NS 2 simulator, 670 x 670 m, 50 wireless nodes
- Movement patterns include random waypoint model
- Communication pattern includes CBR flow
- 10% to 40% misbehaving nodes were included
- Metrics
 - Throughput
 - Overhead due to RREQ, RREP, RERR
 - Watchdog “false positives”

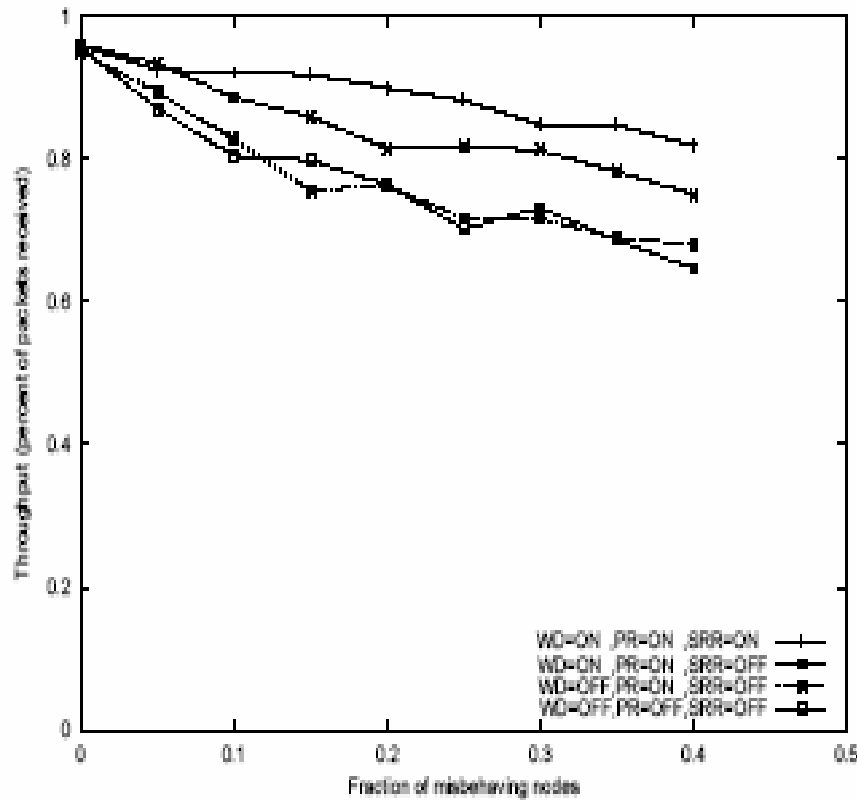
Simulation results

- WD, PR, SRR- everything on and everything off
- Network Throughput – 0 and 60 sec pause time

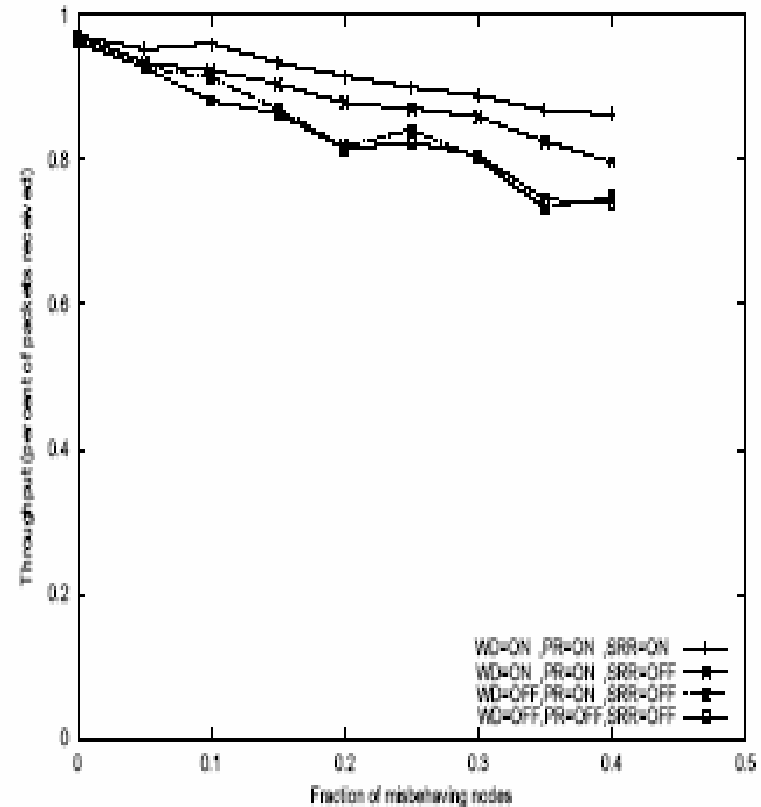
	Maximum	Minimum
0 second pause time	88.6%	75.2%
60 second pause time	95.0%	73.9%

- Same at 0% misbehaving nodes and diverges later
- Throughput increase of 27% in both scenarios
- Interdependency between WD, and PR
- PD cannot function with no WD
- If either WD/PD are off, then it becomes a normal network

Simulation results



0 sec pause time



60 sec pause time

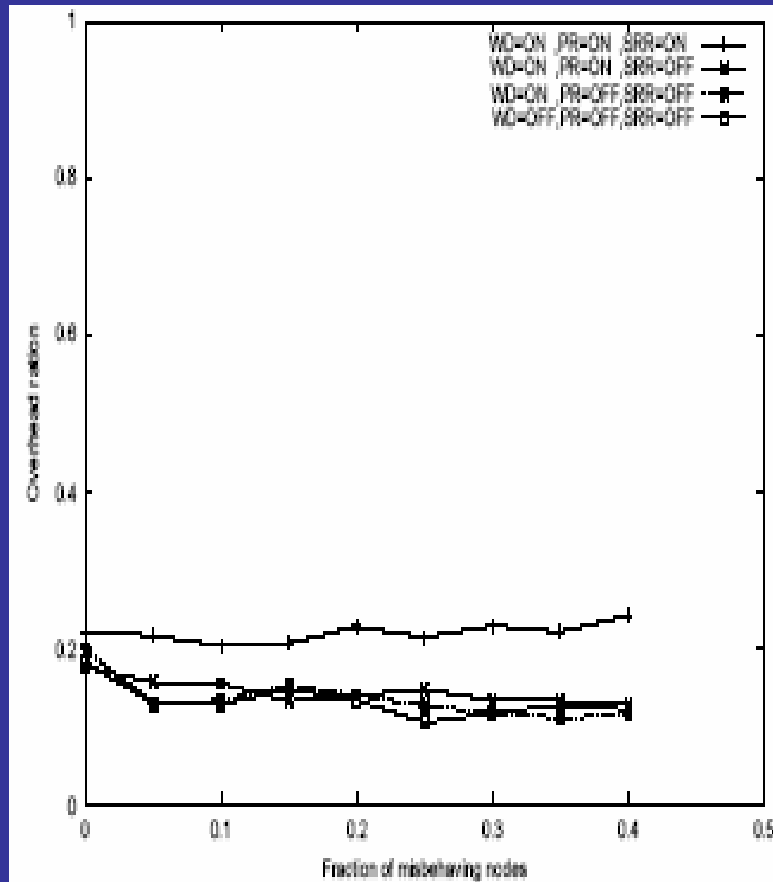
Simulation results

- Routing Overhead – again everything on and off
 - Graph WD only curve to study the overhead due to notifications

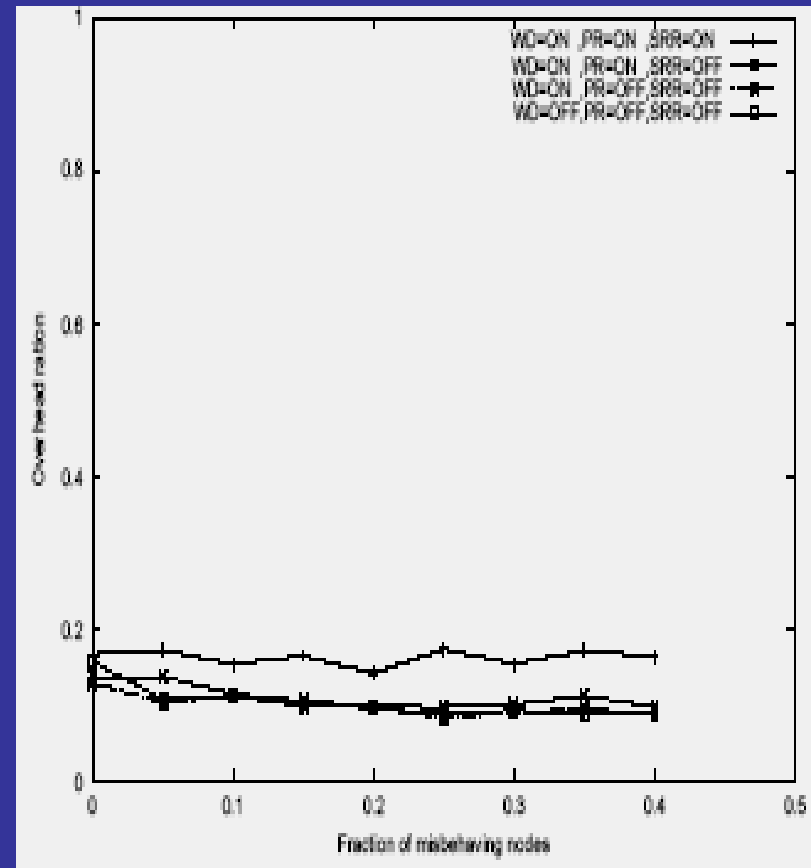
	Maximum	Minimum
0 second pause time	31.3%	18.9%
60 second pause time	23.5%	11.0%

- Greatest effect only when SRR is on
- Overhead increase of 12% when SRR is activated on PR
- WD incurs very small overhead
- This behavior is not affected even by adding misbehaving nodes
- Overhead generally corresponds to battery usage in PDAs
- But net increase of throughput helps the network

Simulation results



0 sec pause time



60 sec pause time

Related Work

- Work proposed only for DSDV till now.
- Zhou and Haas on Cryptographic measures
- Stajano and Anderson on DDOS by nodes

Conclusion and Future work

- Satisfying two “R”s in survivability requirement
 - Resistance to attack
 - Recovery from attack
- Effective increase in net throughput by 27%
- Done with no “a priori” trust relationships

- Working on different thresholds of WD
- Make PR to work with ACKs from upper layer
- TCP and FTP flows along with CBR flows

References

- [1] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in The 6th ACM International Conference on Mobile Computing and Networking, August 2000.
- [2] D. Johnson, D. A. Maltz, and J. Broch. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (Internet-Draft) Mobile Ad-hoc Network (MANET) Working Group, IETF, October 1999.