CS 525M – Mobile and Ubiquitous Computing Seminar

Ted Goodwin

Mitigating Routing Misbehavior in Mobile Ad Hoc Networks

Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker
Department of Computer Science
Stanford University
Stanford, CA 94305 U.S.A

Contents

Introduction

- Ad Hoc Networks
  - Ideal for when network is too transient or infrastructure is destroyed.
  - Maximize throughput by using all nodes for routing and forwarding.
  - Misbehaving nodes cause problems.
    - Overloaded – lacks cpu cycles, buffer space, or network bandwidth to forward packets.
    - Selfish – unwilling to spend battery life, CPU cycles, or network bandwidth.
    - Malicious – drops packets for denial of service attack.
    - Broken – software fault keeps from forwarding packets.

Introduction (cont.)

- Solution to misbehaving nodes
  - Priori trust relationship: separate relationship outside of network
    - Problems:
      - Requires key distribution.
      - Trusted nodes overloaded.
      - Trusted nodes can be compromised.
      - Untrusted nodes may be well behaved.
  - Isolate or forestall misbehaving nodes
    - Problems:
      - Complexity added to well defined protocols.
  - Many existing ad Hoc networks admit misbehavior.

Introduction (cont.)

- Solutions to misbehaving nodes:
  - Priori trust relationship – separate relationship outside of network
    - Problems:
      - Requires key distribution
      - Trusted nodes overloaded
      - Trusted nodes can be compromised
      - Untrusted nodes may be well behaved
  - Isolate or forestall misbehaving nodes
    - Problems:
      - Complexity added to well defined protocols.
  - Many existing ad Hoc networks admit misbehavior.

Introduction (concl.)

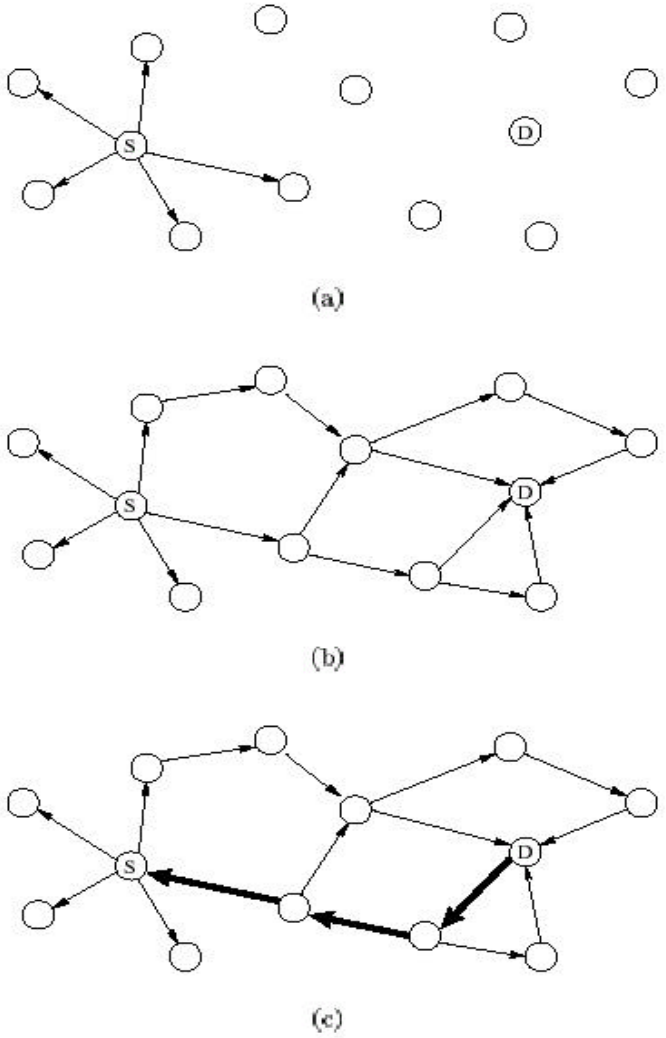
- Paper's solution – Watchdog and Pathrater added to network.
  - Watchdog – identifies misbehaving nodes.
    - Node A sends a packet to Node B.
    - Node A Watchdog listens promiscuously to Node B to ensure it forwards the packet.
    - If Node B does not, Watchdog identifies it as misbehaving.
  - Pathrater – avoids routing packets through misbehaving nodes.

Assumptions and Background

- Definitions
  - neighbor – node within wireless transition of another node
  - neighborhood – all nodes that are within wireless transmission range of a node
- Physical Layer Characteristics
  - Bidirectional links between all nodes (Watchdog relies on bidirectional links).
  - Promiscuous mode supported by all nodes.
- Dynamic Source Routing (DSR) – On-demand source routing protocol
  - Route path – each packet has the addresses of nodes agreed to participate in routing packet.
  - “On demand” – route paths are discovered when there is no path to a destination.

Assumptions and Background (cont.)

- DSR – route discovery
- From S (source) to D (destination)
- S sends Route Request
- Request is forwarded, adding their address building a route.
- D returns Route Reply using a route in a Route Request packet or do its own route discovery back.
- S caches multiple paths from destination for later.

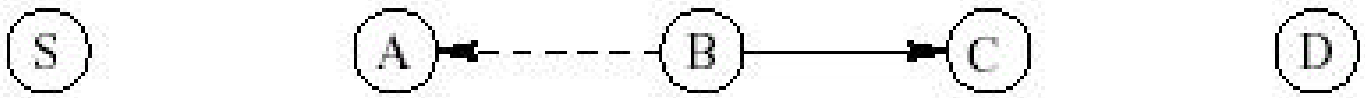


Assumptions and Background (concl.)

- DSR – route maintenance
  - Link breaks – Two nodes are no longer in transmission range of each other.
  - If an intermediate node detects a link break during forwarding, it notifies source.
  - Source either tries another path or does a route discovery.

Watchdog and Pathrater

- Watchdog – checks for misbehaving nodes.
- Below, A sends a packet to B to be forwarded to C.
- A then listens to B to make sure it forwards the packet to C.
- If packets are not encrypted individually, can check for tampering.



Watchdog and Pathrater (cont.)

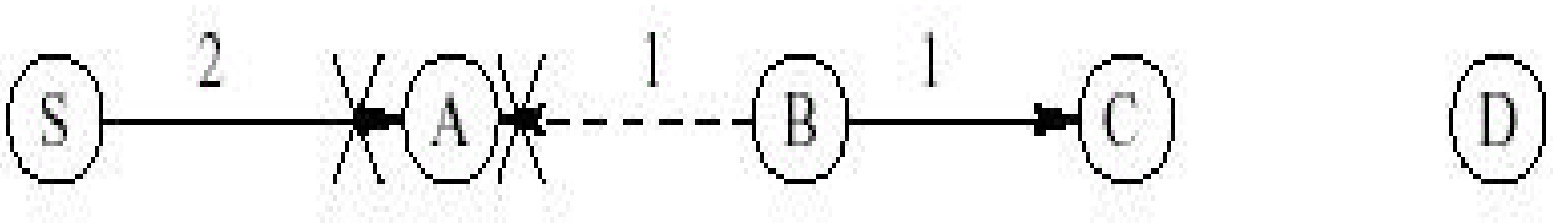
- Watchdog
  - Maintains a buffer of recently sent packets.
  - Compares each overheard packet with the buffer.
  - If overheard packet is in buffer, remove it.
  - If not, wait for a timeout, then increase tally for that node.
  - If that node's tally reaches a certain threshold, mark it as misbehaving.
  - If misbehaving, notify the source of the misbehaving node.

Watchdog and Pathrater (cont.)

- Watchdog (cont.)
  - Advantages:
    - Detects errors at the forwarding level, not just the link level.
  - Disadvantages:
    - May not detect misbehaving nodes when:
      - Ambiguous collisions
      - Receiver collisions
      - Limited Transmission power
      - False misbehavior
      - Collusion
      - Partial dropping

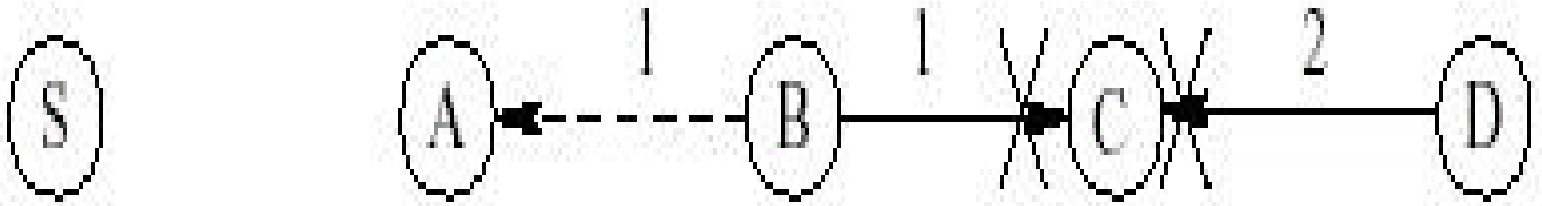
Watchdog and Pathrater (cont.)

- Watchdog – Disadvantages
  - Ambiguous collisions
    - Node A listens for Node B to forward packet 1 to Node C.
    - Packet 1 from Node B and packet 2 from Node S collide at Node A.
    - Node A cannot tell in this instance if B is misbehaving or not.
    - Keep listening to Node B to see if it is misbehaving.



Watchdog and Pathrater (cont.)

- Watchdog – Disadvantages (cont.)
  - Receiver collisions
    - Node A knows Node B forwarded the packet, but does not know if Node C receives it.
    - Node B could refuse to resend the packet to Node C, because it does not want to waste resources to resend.
    - Node B could also wait until Node C is sending to cause a collision. This would be malicious behavior.



Watchdog and Pathrater (cont.)

- Watchdog – Disadvantages (cont.)
  - Falsely misbehaving
    - If nodes falsely accuse the node they forwarded the packet to as misbehaving.
    - Should be caught, because the source will receive packets back from the destination.
    - If the accusing nodes start dropping the return nodes, the accused would inform the destination and it would reroute.

Watchdog and Pathrater (cont.)

- Watchdog – Disadvantages (cont.)
  - Limited transmission power
    - Signal strength is manipulated
      - Previous node can hear forward.
      - Next node can not hear forward.
    - The node must know the signal power to reach the others.
    - (Directional transmission could cause the same problem.)

Watchdog and Pathrater (cont.)

- Watchdog – Disadvantages (cont.)
  - Collusion
    - If two nodes in a row collude, you can fool Watchdog.
      - Node A sends a packet to colluding Node B.
      - Node B forwards the packet to other colluding Node C.
      - Node C drops the packet and Node B does not report it.
    - Do not have two untrusted nodes in a row in a path.
    - This paper assumes nodes act by themselves.

Watchdog and Pathrater (cont.)

- Watchdog – Disadvantages (concl.)
  - Partial droppings
    - Node keeps its tally just below the threshold.
    - Never is labeled as misbehaving.
  - Replay attacks
    - Ineffective dealing with replay attacks.
    - Too much state information at each node.
    - Retransmits could be seen as replay attacks.

Watchdog and Pathrater (cont.)

- Pathrater
  - Run by each node.
  - Misbehaving nodes + link reliability data to pick route.
  - Each node keeps a metric for each node it knows about.
  - Path is chosen by averaging the metric for each node.
  - Highest average metric is chosen.

Watchdog and Pathrater (concl.)

- Pathrater – Assigning Ratings to other nodes
  - Starts with neutral rating (0.5) at discovery.
  - At periodic intervals (200 ms), increment nodes on active paths (0.01).
  - Decrement the rating when link breaks occur.
  - Misbehaving nodes set to -100.
  - If a node on a path misbehaves and there no other paths, sends a Route Request.

Methodology

- The paper used Berkeley's Network Simulator with CMUs Monarch project plugin, and CMU's ad-hockey to visualize the network data.
- The simulation was of 50 wireless nodes in a flat space measuring 670 x 670 meters.

Methodology (cont.)

- Movement and Communication Patterns
  - 10 constant Bit rate connections.
    - 4 nodes source 2 connections.
    - 2 nodes source 1 connection.
    - 8 nodes destination 1 connection.
    - The last is a destination for 2 connections.

Methodology (cont.)

- Movement and Communication Patterns (concl.)
  - Random waypoint model
    - Pick destination and move in straight line.
    - Move at constant rate of 0 or a maximum speed.
  - Pause time of 0 or 60 seconds.
  - Gives 4 mobility scenarios.

Methodology (cont.)

- Misbehaving Nodes
  - Agree to participate in forwarding packets.
  - Drops all data routed through it.
  - Percentage of the network
    - Between 0 and 40 percent by 5 percent increments.
    - Picked pseudo randomly.

Methodology (concl.)

- Metrics
  - Throughput – Percentage of sent data received.
  - Overhead – Ratio of routing related transmissions to data transmissions.
  - Effects of Watchdog false positives on throughput.

Simulation Results

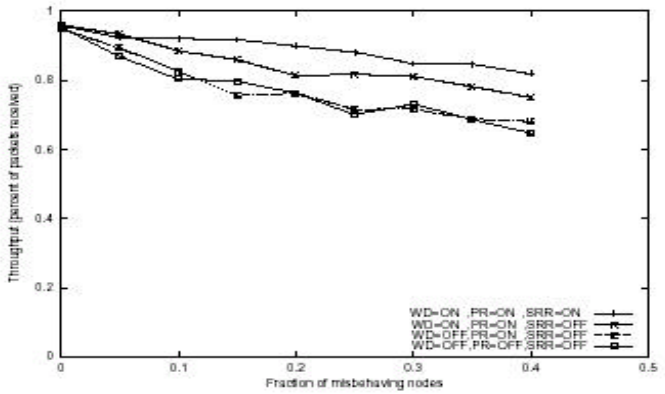
- Network Throughput
  - Watchdog, Pathrater, and SRR enabled.
  - Everything disabled.
  - Watchdog and Pathrater enabled.
  - Only Pathrater enabled.
  - Watchdog and SRR will not work without Pathrater to use the information.

Mitigating Routing Misbehavior in Mobile Ad Hoc Networks

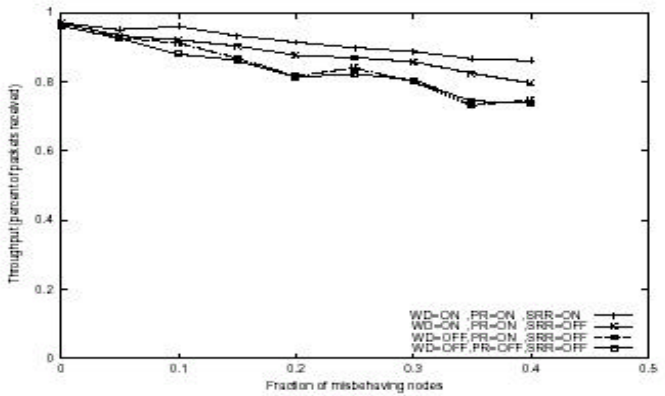
Simulation Results (cont.)

Network Throughput (concl.)

- Fraction of data generated received versus Fraction of misbehaving Nodes.
- 0% Misbehaving all were 95% throughput.
- Up to 27% increase compared to basic protocol.
- Subset of extensions do not improve as much.



(a) 0 second pause time



(b) 60 second pause time

Simulation Results (cont.)

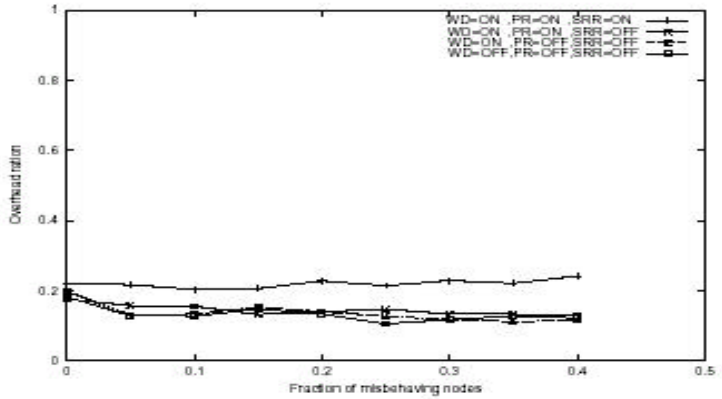
- Routing Overhead
  - Everything enabled.
  - Pathrater and Watchdog enabled.
  - Watchdog enabled.
  - Everything disabled.

Mitigating Routing Misbehavior in Mobile Ad Hoc Networks

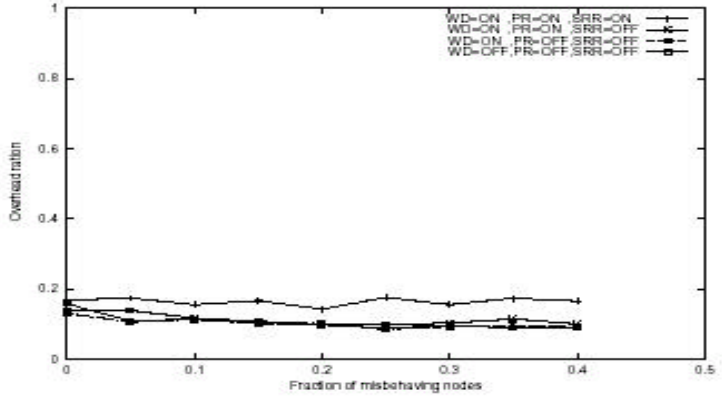
Simulation Results (cont.)

Routing Overhead (concl.)

- Ratio of routing to data packets versus fraction of misbehaving nodes.
- 40% misbehaving overhead rises from12 to 24% with SRR.
- Watchdog has very little overhead.



(a) 0 second pause time

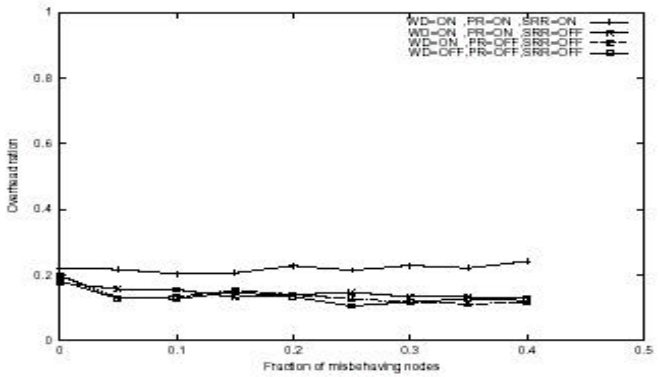


(b) 60 second pause time

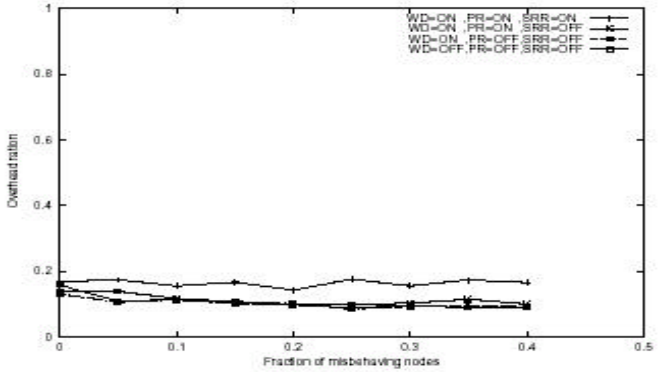
Simulation Results (concl.)

Effects of False Detection

- Network throughput of Regular Watchdog versus a Watchdog no false positives.
- False positives have no effect on throughput.
- Misbehaving nodes could have moved out of range.
- Increased false positives increase suspect nodes, so it evens out.



(a) 0 second pause time



(b) 60 second pause time

Future Work

- Determine optimal value for parameters to extensions (watchdog thresholds and Pathrater's in/decrement amounts).
- Evaluate routing extensions using trusted node lists.
- Replace watchdog with a reliable transport layer.
- Test extensions using reliable data transfer (i.e., ftp transfer).
- Test extensions for latency as opposed to throughput.

Conclusion

- Pathrater and Watchdog extend DST
  - To increase throughput by 17% and overhead from 9% to 17% with moderate mobility.
  - To increase throughput by 27% and overhead from 12% to 24% with extreme mobility.
- Shows we can add routing nodes while minimizing misbehaving nodes' effect.

Questions?