Malicious Node Detection in MANET

Sugata Sanyal, Ajith Abraham,
Dhaval Gada, Rajat Gogri, Punit Rathod,
Zalak Dedhia and Nirali Mody

IWDC – 2004, 28th Dec 2004

http://www.it.iitb.ac.in/~punit

Malicious Activities

- Before Route Formation
  - RREQ Flooding
  - Exhaustion of Network Resources
- After Route Formation
  - Dropping of Packets
  - Modification of Packets
  - Routing to incorrect Destination

RREQ Flooding (Before Route Formation)

- More RREQ than allowed
  - Unwanted Routes
  - Many routes
  - More Delay for regular traffic
- RREQ_RATELIMIT
  - Malicious Node may ignore this limit

Distributed Solution to Flooding

- RREQ_ACCEPT_LIMIT
  - Accept from neighbor and process
- RREQ_BLACKLIST_LIMIT
  - Heavy RREQ flood, Blacklist neighbor.
- Even Distribution of Network Resources
- Ensure compliance of RREQ_RATELIMIT

Malicious Activity (After Route Formation)

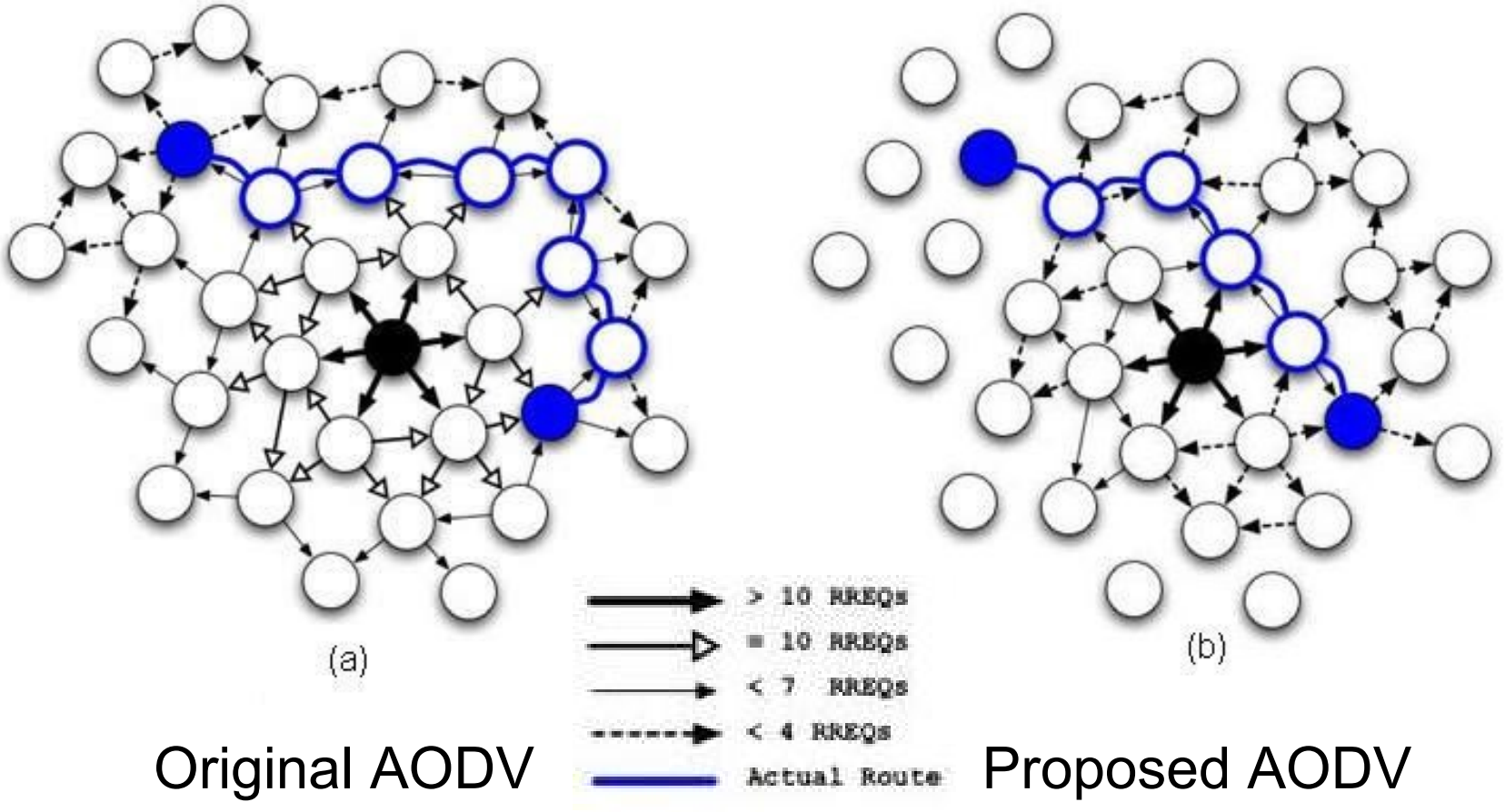
- Dropping Packets
  - Greedy Behavior
- Forwarding to un-intended Destination
  - Eavesdropping
- Modification of Messages
  - Fabrication / Spoofing

Detecting Malicious Nodes

- Extra information about Next-to-Next-Hop

  - D is NTNH of B
- Check correct NTNH in RREP
  - No Modification of Route
- Check correct forwarding of DATA
  - No Malicious Activity

Route Formation in Simulations



Original AODV

Proposed AODV