Defending Against Black Hole Attacks on AODV Routing

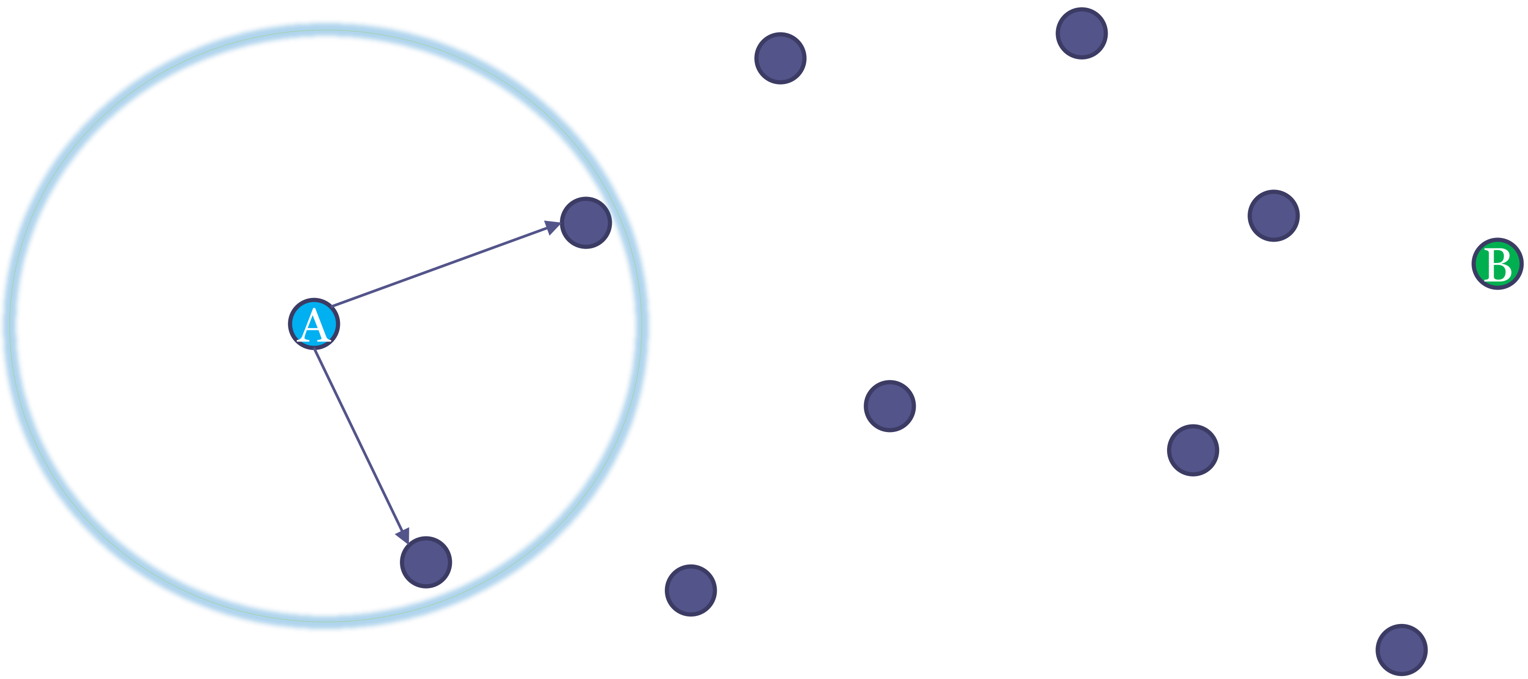
Andrew Fallgren
Aaron Pope
George Rush

What is AODV Routing?

- Ad-hoc On Demand Distance Vector Routing (AODV)
- This is the routing protocol used in ZigBee, a popular standard for wireless mesh networks.
- A mesh network is a topology in which each node relays data for the network.

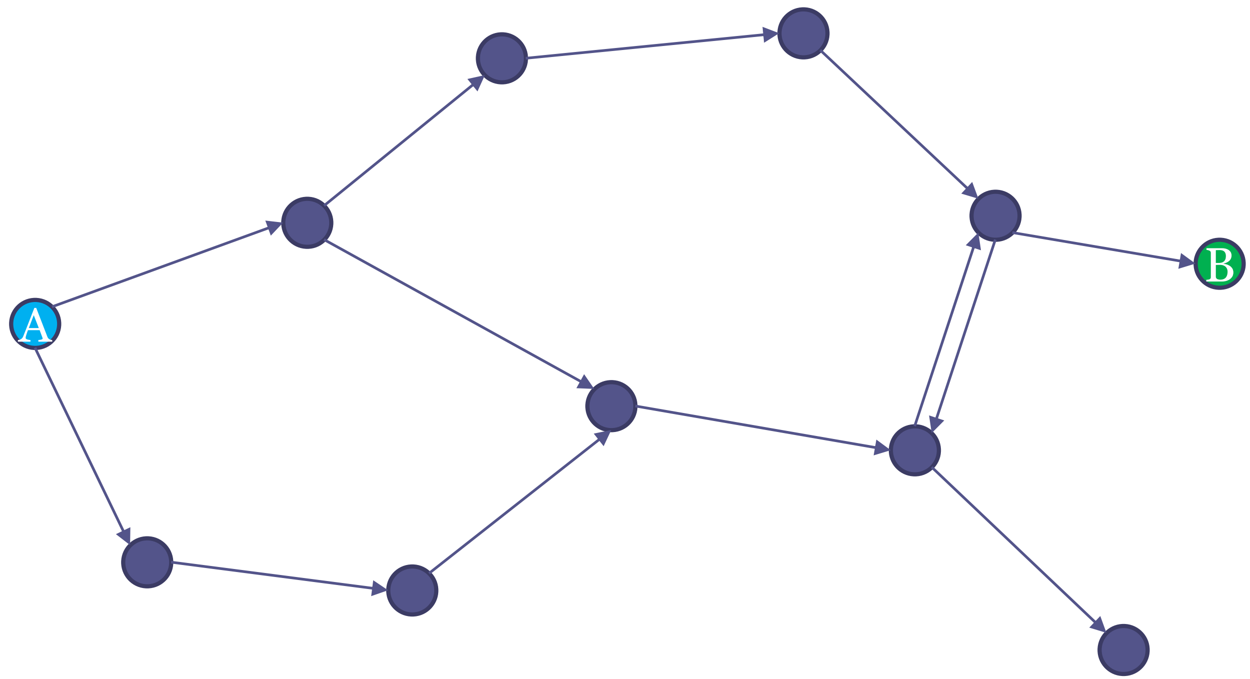
How does AODV work?

- Original sender broadcasts Route Request (RREQ).



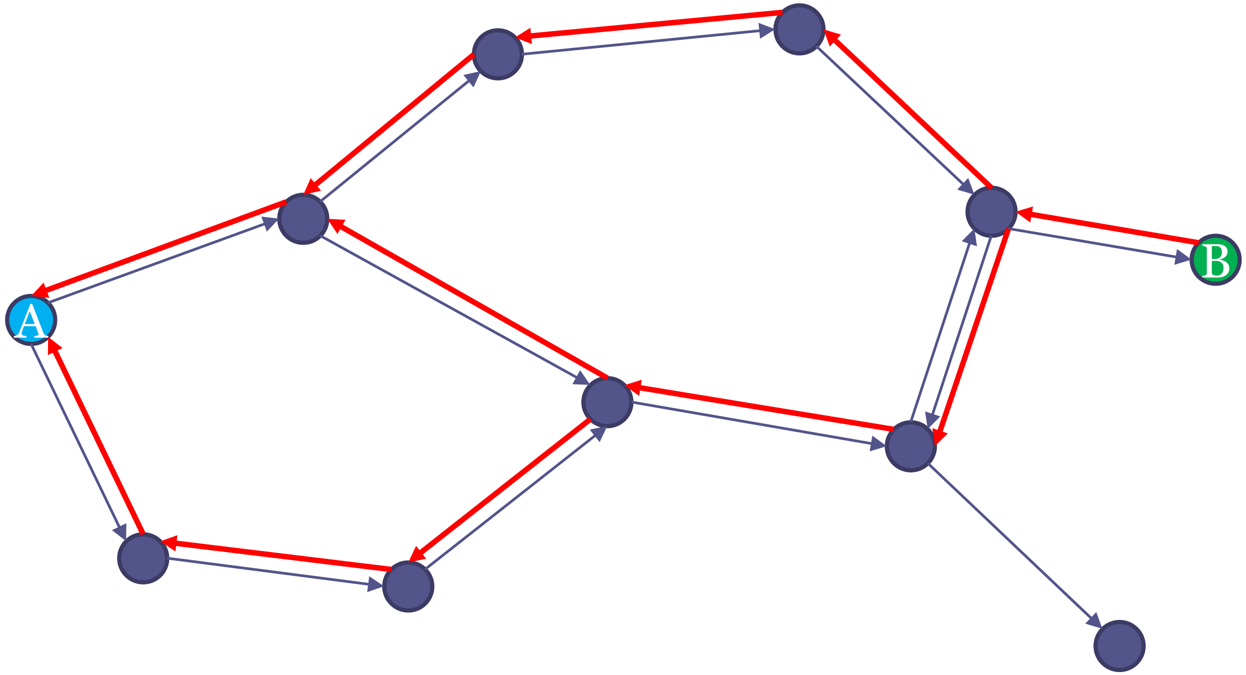
How does AODV work?

- Intermediate nodes propagate RREQ.



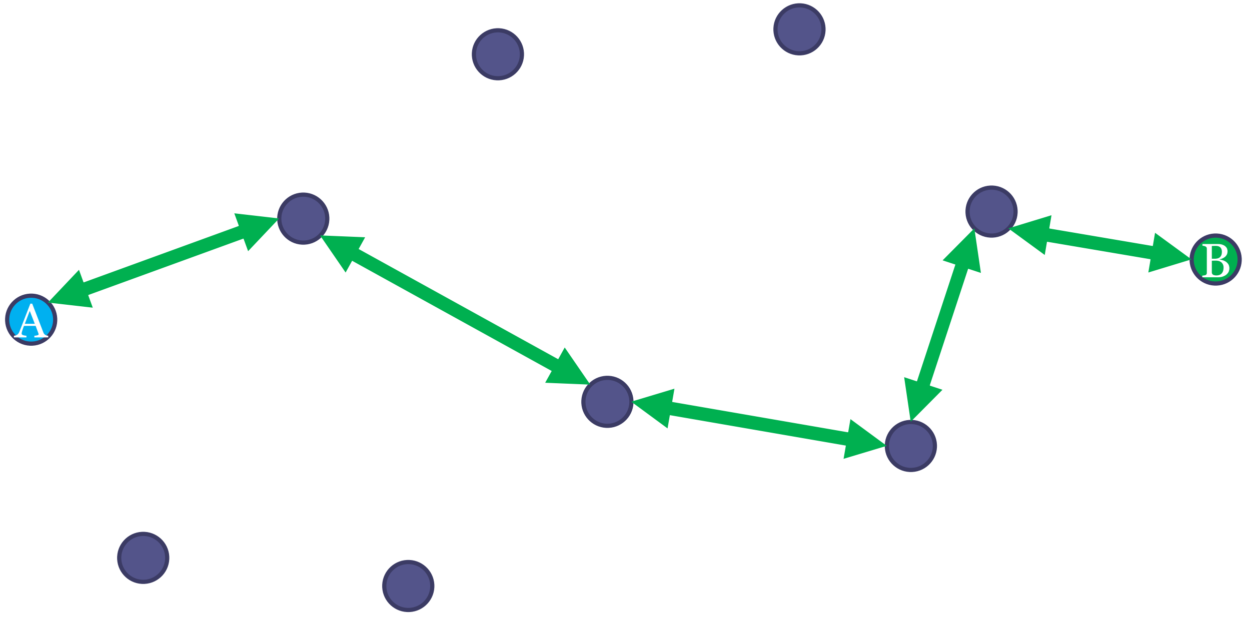
How does AODV work?

- Destination node sends Request Reply (RREP) back to sender for each RREQ.



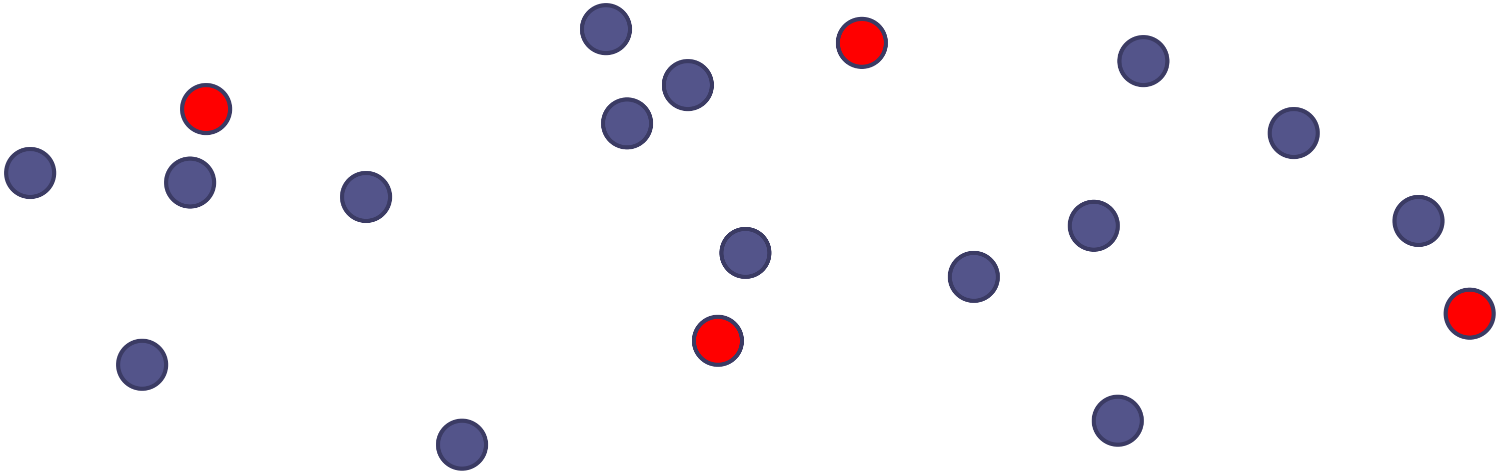
How does AODV work?

- Sender uses lowest hop-count route to communicate with destination.



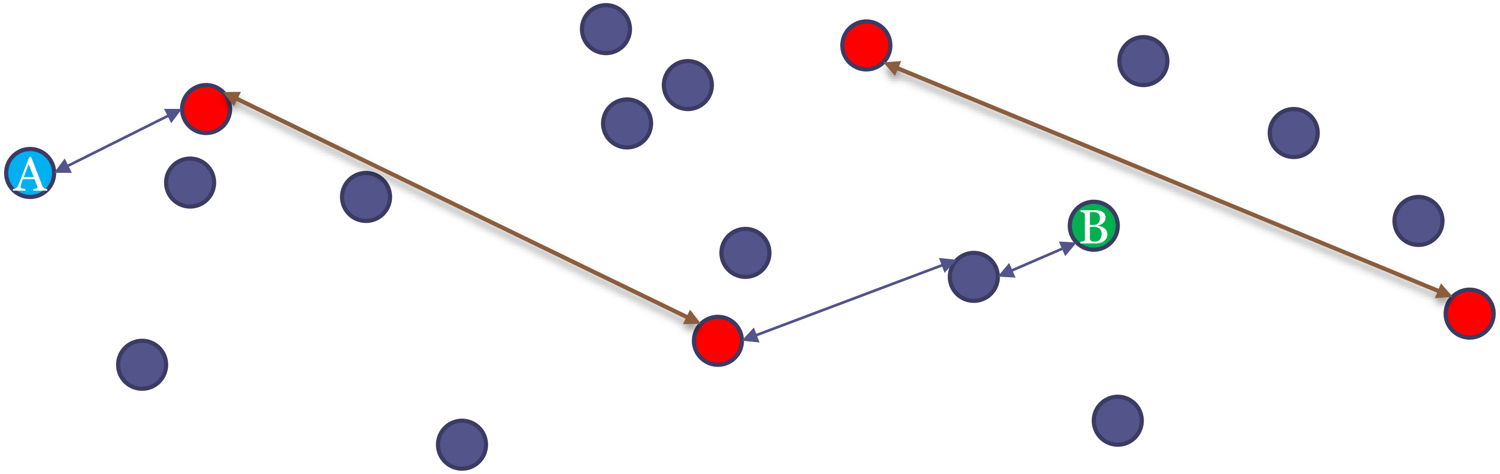
Wormhole Attack (Initial Conditions)

- Two or more nodes are deployed or captured by an adversary. *Capture is unnecessary*.



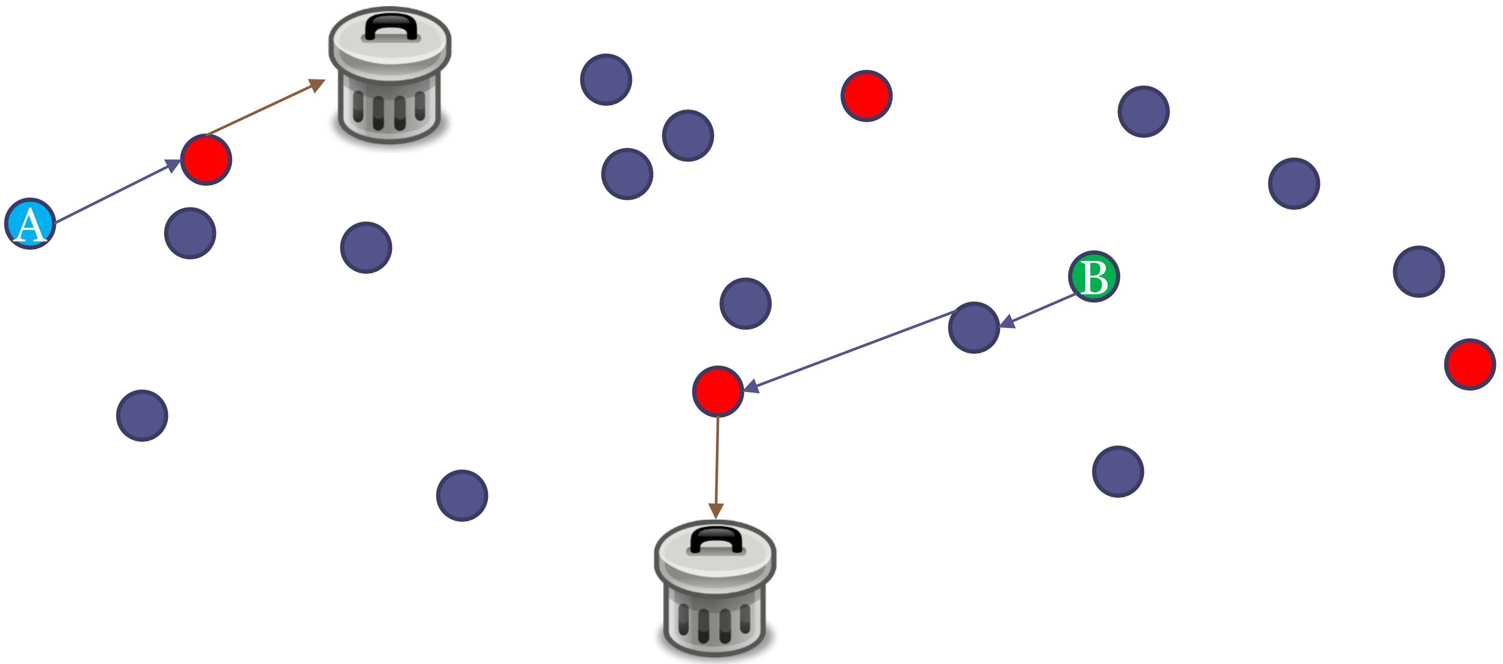
Wormhole Attack (Getting Selected)

- Each pair of enemy nodes creates a tunnel using long-range directional antennas (to offer the shortest path for many routes).



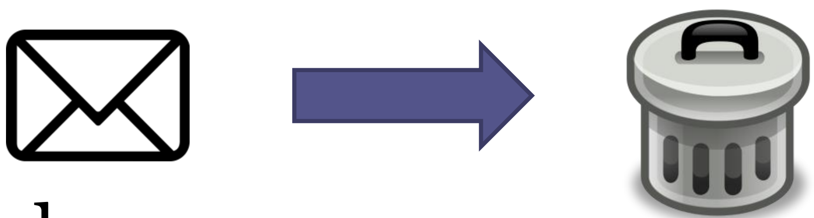
Black Hole Attack (Exploitation)

- The enemy nodes drop all packets rather than forwarding them.

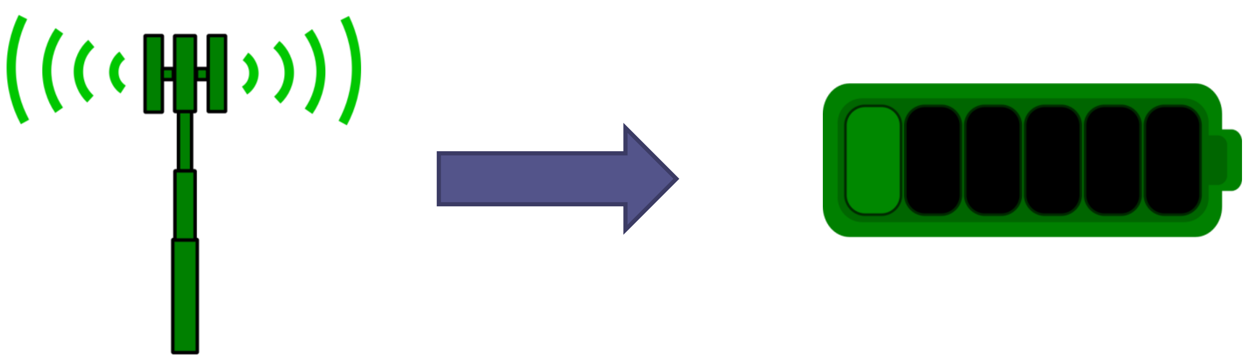


Attack Model (Results)

- Data loss
  - Packets never reach their destination.



- Energy loss
  - Nodes waste energy on radio communication.



Related Work

- Authentication based solutions:
  - Examples: Adriane, ARAN
  - Add encryption to message passing.
  - Allows for very secure communication.
  - Increases computational overhead on participating nodes.
  - Some methods also require centralized authentication.

Related Work

- Statistical intrusion detection systems:
  - Monitor normal packet loss due to network congestion.
  - Differentiates between normal loss and malicious packet dropping.
  - Requires consistent, heavy traffic which might not be present in a lightweight ad hoc network.

Related Work

- Intrusion detection systems via network monitoring devices:
  - Strategically placed devices observe network traffic to identify abnormal behavior.
  - Nodes identified as abnormal are communicated to legitimate nodes and avoided.
  - This can work well for static networks where security is extremely important.
  - Not suited for truly dynamic ad hoc networks.

Defensive Goals

- Primary Objective
  - Detect whether or not packets reach their destination. Pick a new route if too many packets are being dropped.
- Secondary Objective
  - Minimize message complexity in order to reduce network transmissions.

Our Approach

- Routes in AODV must be periodically refreshed.
- Source knows the number of data packets sent, and Destination knows the number received.
  - Exchange # of packets sent/received when refreshing routes.
- AODV floods the network when establishing routes.
  - A polling of the neighbors can be used to detect deception by enemy nodes. Once detected, pick a new route.

Advantages

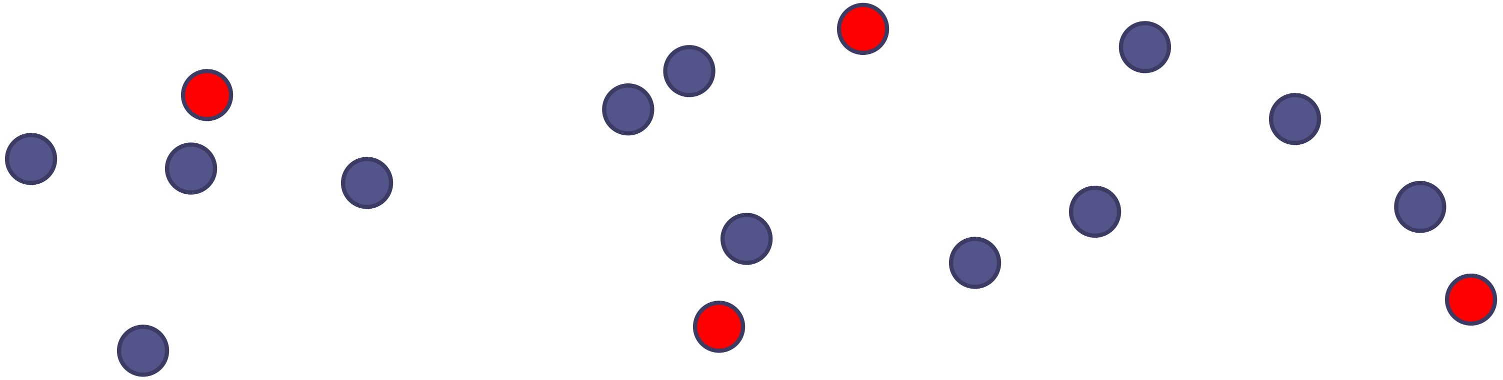
- Minimal changes to AODV.
  - Two new integer data fields.

- Zero encryption required.
  - Not computationally intensive.

- Does not increase message complexity.
  - Better battery life.

Evaluation

- We need to compare our solution to other techniques for preventing or countering black hole attacks.
- Suggested approach: Build a network simulation and test various attack scenarios.



Network Simulation

- Network is represented as a graph.
  - Edges connect nodes in communication range.
- Random nodes are chosen to form routes using AODV.
  - Dummy messages are sent one or both ways to simulate data transactions.
- Attackers attempt to execute black hole attacks per various scenarios.
- Simulation ends after a fixed period of time or fixed number of messages.

Attack Scenarios

- No black holes occur.
  - This would help test how proposed solutions affect normal network operation.
- A single black hole is formed.
  - This would show how proposed solutions work under ideal conditions.
- Multiple black holes are formed.
  - This would test what happens when the enemy has greater capabilities and can further disrupt the network.

Evaluation Metric

- Two main concerns:
  - Number of lost messages (L)
  - Message complexity of proposed solution (M)
- Minimizing L increases availability.
- Minimizing M decreases power usage.
- The end user can prioritize either one if we view this as a multi-objective problem.
  - This means the user can decide the relative weight of both metrics.

Sources

- Y.-C. Hu, A. Perrig, and D. Johnson. Wormhole attacks in wireless networks. Selected Areas in Communications, IEEE Journal on, 24(2):370–380, Feb 2006.
- Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. Wirel. Netw., 11(1-2):21–38, Jan. 2005.
- P. Ning and K. Sun. How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols. Ad Hoc Networks, 3(6):795 – 819, 2005.
- C. Perkins and E. Royer. Ad-hoc on-demand distance vector routing. In Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, pages 90–100, Feb 1999.

Sources

- R. Rao and G. Kesidis. Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited. In Global Telecommunications Conference, 2003. GLOBECOM ’03. IEEE, volume 5, pages 2957–2961 vol.5, Dec 2003.
- K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer. A secure routing protocol for ad hoc networks. In Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, pages 78– 87, Nov 2002.
- C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A Specification-based Intrusion Detection System for AODV. In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN ’03, pages 125–134, New York, NY, USA, 2003. ACM.
- L. Zhou and Z. Haas. Securing ad hoc networks. Network, IEEE, 13(6):24–30, Nov 1999.

Sources

- Images from openclipart.org
  - Including the adorable trash cans.