# Defending Against Black Hole Attacks Using AODV Routing

Andrew Fallgren
ajffk6@mst.edu

Aaron Pope
aaron.pope@mst.edu

George Rush
gdr34b@mst.edu

May 4, 2015

# Contents

# Problem Statement

In this work, we suggest using a modified version of the AODV routing protocol to defend against black hole attacks in ad-hoc wireless networks. Ad-hoc On-Demand Distance Vector Routing (AODV) is a routing algorithm for ad-hoc networks in which routes are obtained only as needed. The algorithm's primary objectives are to broadcast discovery packets only when necessary, to distinguish between neighborhood detection and general topology maintenance, and to disseminate information about changes in local connectivity to those neighbors that are likely to need the information [4]. In general, AODV will always select the shortest route to its destination for any given network transaction, but routing packets can be misused to enable a variety of attacks such as route disruption, node isolation or resource consumption [3].

To understand black hole attacks, it is necessary to first define wormhole attacks. In a wormhole attack, an attacker sniffs packets at one point in the network, tunnels them elsewhere in the network, and replays them. By using a long-range directional antenna, an attacker can make certain nodes appear to have a shorter hop distance to other parts of the network than any of their neighbors. As such, this type of attack is especially effective against AODV since an attacker can easily become part of the shortest route between two points in the network [1]. Furthermore, because it is unnecessary to compromise nodes in the network, all nodes continue to respond as expected by the protocol. This makes attack detection a difficult task.

A black hole attack is an extension on the wormhole attack. To execute it, a wormhole is used to establish routes between nodes, and then all data packets on those routes are silently dropped. In this way, an attacker can launch a permanent denial-of-service attack. Our goal is to detect when data packets are not reaching their destination while simultaneously minimizing the message complexity required to do so. This allows a defender to pick a new route in order to work around the black hole attack.

## Assumptions

Several assumptions are made about the attacker and defender:

- The attacker can obtain at least two nodes compatible with the defender's network.
- The attacker can deploy nodes anywhere at any time in the defender's network.

- Once placed, nodes cannot move elsewhere in the network.
- Nodes have limited energy and computational power, making asymmetric encryption impractical.

## Challenges

A number of issues occur under this setup:

- Attackers can create a wormhole which follows network protocol. It is only when a black hole is formed that unusual behavior occurs, which makes detection more difficult.
- Authentication techniques cannot be used to verify a node's identity since they greatly increase computational complexity for nodes.
- Most distributed IDSs require communication between nodes, increasing message complexity. As such, they are not lightweight enough for our approach.
- Additional hardware for monitoring the network is unavailable.

## Related Work

A variety of methods have been used to improve the overall security of networks employing AODV routing. Some techniques introduce authentication to the message passing within the network [2, 6, 8]. While this approach is very powerful, it can dramatically increase the computational load on participating nodes and in the case of asymmetric encryption, can require a centralized source for public keys which may not be feasible for some wireless network applications.

Alternative approaches use intrusion detection systems to discover malicious node behavior. Statistical methods can be used to distinguish malicious packet dropping from packet dropping that occurs as a result of network congestion [5]. The requirement for predicting congestion limits the usefulness of this approach when dealing with networks which exhibit sporadic and bursty traffic. Other attempts at constructing intrusion detection systems for ad-hoc networks rely on the strategic placement of additional hardware to monitor network traffic for malicious behavior [7]. While the additional hardware requirements might be feasible for some applications where security is of the utmost importance, this approach is impractical for most lightweight ad-hoc networks.

## Our Approach

In our technique, we consider that source and destination nodes can exchange the number of sent and received data packets when establishing routes through the packets sent out in the AODV protocol. Since AODV floods the network when establishing routes, a polling of the neighbors can be used to detect cases where a node is silently dropping packets or if the shortest is not a reliable route. It could then be possible for alternative routes of similar length to be chosen instead. This general purpose approach requires a minimal alteration to the AODV protocol and does not require computationally expensive encryption, a centralized authentication source or any additional monitoring hardware.

# Evaluation

In order to compare our solution to other techniques for preventing or countering black hole attacks, we propose building a network simulation and testing various attack scenarios. That simulation, relevant scenarios, and the evaluation metric are discussed below.

## Network Simulation

The network would be represented as a graph, with edges connecting nodes in communication range. Random nodes would be chosen to form routes using the AODV protocol, and dummy messages would then be sent one or both ways to simulate data transactions. Periodically, routes would be refreshed as per AODV's rules. Attackers attempting to execute black hole attacks would do so depending on scenarios defined in the next section. The simulation would end either after a fixed period of time or when a fixed number of messages had been sent across the network.

## Attack Scenarios

Several scenarios would be beneficial for comparison:

- 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.

Which scenarios are most relevant depends heavily on the enemy's capabilities and the type of network being deployed. Each run of the simulation would return the evaluation metric covered in the next section.

## Evaluation Metric

Regarding black hole attacks, we take into account two main concerns for a network operator: the number of lost messages and the message complexity of any proposed solution. Suppose we denote the number of

lost messages as $L$ and the message complexity as $M$. Minimizing $L$ increases availability, and minimizing $M$ decreases power usage. However, depending on the purpose of any given network and the capabilities of its nodes, one may prioritize either availability or power usage. Rather than choosing specific weights for the end user, we would choose instead to view this as a multi-objective problem. This would allow the end user to decide the relative weight of the two metrics themselves, adapting the evaluation to their particular needs.

## Future Work

Our next steps would include actually implementing the suggested network simulation, measuring the performance of our solution against other solutions, and testing several attack scenarios. Besides that, it would be useful to see if the time to detect black holes could be reduced without sacrificing message complexity. Our current method can only detect lost messages when refreshing routes, which may be an issue depending on how often that occurs. It would be interesting to see if message dropping could be detected more effectively either with a separate message stream or a higher route refresh rate, as well as which one would be better for battery power.

# Bibliography


[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] L. Zhou and Z. Haas. Securing ad hoc networks. *Network, IEEE*, 13(6):24–30, Nov 1999.