Defending Against Wormhole Attacks Using AODV Routing

Andrew Fallgren
ajffk6@mst.edu

Aaron Pope
aaron.pope@mst.edu

George Rush
gdr34b@mst.edu

April 14, 2015

Introduction

In this work, we suggest using a modified version of the AODV routing protocol to defend against wormhole 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 [2]. In general, AODV will always select the shortest route to its destination for any given network transaction.

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.

Related Work

Defensive techniques have been suggested for man-in-the-middle attacks (MITM) against AODV [3]...

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. Since AODV floods the network when establishing routes, information which may otherwise be spoofed by a wormhole can potentially be discovered through other routes...

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] 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.

[3] 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.