Defending Against Wormhole Attacks Using AODV Routing

Andrew Fallgren
ajffk6@mst.edu

Aaron Pope
aaron.pope@mst.edu

George Rush
gdr34b@mst.edu

April 19, 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 [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].

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

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 mali-

cious 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.

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.