

Authenticated Routing for Ad Hoc Networks

Kimaya Sanzgiri Elizabeth M. Belding-Royer
Department of Computer Science
University of California, Santa Barbara
{kimaya, ebelding}@cs.ucsb.edu

Abstract

Most proposed routing protocols for mobile ad hoc networks are vulnerable to modification, impersonation and fabrication attacks. The proposed secure routing protocol, Authenticated Routing for Ad Hoc Networks, prevents such attacks through message authentication, integrity and non-repudiation. Simulation results show that ARAN maintains good network performance while offering significant security advantages over existing routing protocols.

1 Introduction

Mobile ad hoc networks consist purely of wireless mobile nodes with no wired infrastructure. Most of the proposed routing protocols for ad hoc networks have many security vulnerabilities that may be exploited to launch different types of attacks.

In this analysis, three main categories of attacks are identified. The first of these are Modification attacks, where malicious nodes can make illegitimate modifications to routing messages. The second category is that of Impersonation or Spoofing attacks, where a malicious node can fake its identity by illegally modifying its IP and/or MAC address in outgoing messages. Fabrication attacks form the third category of attacks, where a malicious node could inject false routing messages into the network. These techniques can be used both individually and in various combinations to cause illegal route redirection, route corruption and denial of service.

The proposed protocol, Authenticated Routing for Ad-hoc Networks (ARAN), prevents the above types of attacks through message authentication, integrity and non-repudiation.

2 Protocol Description

The ARAN Protocol uses public key cryptography to guarantee message authentication, integrity and non-repudiation. The protocol is designed for the 'managed-

open' environment, where nodes have an opportunity to obtain a public key certificate from some common certification authority that is trusted by all other nodes in the environment. Typical examples of such an environment are classroom or conference scenarios. The operation of the protocol can be divided into route discovery and route maintenance phases.

The route discovery process is initiated by the source node by flooding a digitally signed Route Discovery packet (RDP) through the network. As message travels through the network, each node verifies the signature of the previous node, and then replaces it with its own signature (the signature of the source node is retained). When the first RDP reaches the destination, the destination node verifies the signature of the source node and then sends a digitally signed Route Reply packet (REP) back to the source. The REP travels along the same path as the RDP, and the same signing procedure is performed by intermediate nodes.

Route maintenance is performed through digitally signed Error messages that are initiated by the node directly upstream of a link failure.

3 Conclusions

ARAN provides both end-to-end and hop-by-hop authentication of route discovery and reply messages, preventing impersonation attacks. The digital signatures guarantee integrity and non-repudiation, preventing illegal message modification and enabling identification of the source of erroneous messages.

Simulation results show that ARAN provides the same throughput as leading ad hoc routing protocols with marginally increased overhead and delay due to the digital signatures.

4 Acknowledgement

The work described in this poster is a joint work with Brian Levine and Bridget Dahill of the University of Massachusetts, Amherst, and Clay Shields of Georgetown University.