

Secure Routing in Ad Hoc Networks

Final Project specifications for Class 646 Project

**Submitted by
Mehul Revankar**

Introduction to Ad Hoc Networks:

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure. Each node participating in the network acts both as a host and a router. A number of routing protocols like Dynamic Source Routing (DSR), Ad Hoc On-Demand Distance Vector Routing (AODV), and Destination-Sequenced Distance-Vector (DSDV) have been implemented. Though, these protocols work well in routing the wireless traffic but they are vulnerable to many attacks. Therefore, there is a need of protocol, which not only provides the routing but also the security to the network and user data. In this paper, I explore the working and performance of secure extensions to these protocols.

Project Specification:

1. I am planning to understand, analyze and compare protocols that provide security in Mobile Ad-Hoc networks. Ariadne, SEAD, ARAN.
2. I would like to evaluate to each protocol on the following grounds
 - Basic Underlying Assumptions
 - Conditions assumed for successful operation of protocol.
 - Key Setup assumptions.
 - Efficiency
 - Computational resources required
 - Energy Consumption
 - Average execution time for generation and authentication of keys
 - Security against following attacks
 - Attacks Using Modification
 - Attacks Using Impersonation
 - Attacks Using Fabrication
 - Advanced Attacks
 1. Wormholes
 2. Black holes
 3. Rushing
 4. Gray Hole
 5. Partition of Network
 6. Gratuitous Detour
 - Viability from Implementation point of view

3. I will try to identify the most secure and efficient protocol and try to propose guidelines to implement the same.
4. Format of tentative Final Report
 - Introduction to Ad-hoc Networks
 - Existing Ad-Hoc Protocols
 - Security Objectives
 - Threats and Attacks
 - Secure Routing Protocols
 - Security against Advanced Attacks
 - Analysis of Protocols
 - Conclusion
 - References
5. Time Schedule
 - Oct 7th - Study of all basic Protocols
 - Oct 15th - Review of other protocols that could be considered.
 - Oct 29th - Compare Protocols for security
 - Nov 12th - Comparison of protocols for Performance
 - Dec 3rd - Final Progress Report
6. Possible Changes

I am not sure about the possible changes, but if I am able to implement ARAN I would like to conduct experiments on each protocol evaluate them for different parameters.
7. List of Literature
 - Yih-Chun Hu, Adrian Perrig, David B. Johnson, “[Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks](#)”, MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA
 - Yih-Chun Hu, David B. Johnson, Adrian Perrig, “[SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Routing for Mobile Wireless Ad Hac Networks](#)”, Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002
 - <http://signl.cs.umass.edu/arand/>
 - www.ece.cmu.edu/~adrian/projects/tesla-cryptobytes/tesla-cryptobytes.pdf