Trusted Route Discovery in Ad Hoc Networks

Primary Investigator: Bharat Bhargava
CERIAS and Department of Computer Science
Purdue University, West Lafayette, IN 47907-1398, USA
bb@cs.purdue.edu, (765) 494-6013

DESCRIPTION OF RESEARCH AND GOALS

Introduction
In Ad Hoc networks, it is hard to employ static routes, link-state based protocols and complex public-key encryption algorithms. Routing protocols must be dynamic and robust against malicious attacks. One type of attacks targets the route discovery phase. By initiating false route queries and distorting the routing information, an attacker can overwhelm a network with excessive traffic load or partition the network [2]. Second threat occurs in the forwarding phase. An adversary host on the route can intentionally drop packets, obtain the content of the traffic, or analyze the traffic pattern even if the data is encrypted. An appropriate routing protocol will filter erroneous query and routing information and determine a route that only involves trustworthy hosts. We consider the trustworthiness as the metric of a route, which is determined by the trustworthiness of all hosts along it.

Research Goal
We investigate the design and evaluation of a trusted route discovery protocol for Ad Hoc networks. The principle challenges are: (1) Quantifying a host’s trustworthiness and assessing the trustworthiness of the route, (2) Design of an efficient trusted route discovery protocol, and (3) A series of experiments to evaluate the protocol.

We are conducting research on secure mobile and Ad Hoc systems. Our research group is supported by two NSF grants and two CERIAS (Center for Education and Research in Information Assurance and Security) grants [6]. The research integrates the ideas from security and fault-tolerance and makes the system survivable from intentional and unintentional attacks [1][5]. We are investigating the development of computational trust models and automated trust assessment with support from CERIAS. We plan to apply these ideas and techniques to discover trusted routes. We will collaborate with Cisco researchers to investigate integrating their high speed, secure wireless technology with Ad Hoc networks to defend against attacks on route discovery for safe delivery of packets.

Research Tasks
Research consists of three tasks as follows:

• The first task includes the definition of the trust metric of a single host, designing schemes to dynamically update the trust value, and assessing the trustworthiness of a route based on the involved hosts. The host’s behaviors, such as forwarding, dropping, choosing proper routes, etc., are parameters that comprise the metric. Communication principles, such as Kalman filtering [4], can be applied to build the trust model as a multivariable, time-varying state vector that utilizes past information to predict future performance. Using this model, the trust on the hosts in the network can be dynamically updated with each message exchanged. The assessment of trustworthiness will be based on our current research on trust formalization. We plan to investigate how to collect information from trusted neighbors and how trust on hosts affects the trustworthiness of a route with respect to different forwarding schemes (e.g. source routing, hop-to-hop).
The second task is to design an efficient trusted route discovery protocol for Ad Hoc networks. This protocol will be scalable and adaptive, and can operate in on-demand or proactive fashion. The protocol will be capable of identifying trustworthy hosts by using authentication, filtering erroneous query and routing information. We plan to design this protocol using the dynamic programming principle and tailor the logic of authentication [3] to prove its correctness.

The third task is to evaluate the proposed protocol through simulation. The protocol will be tested on OPNET modeler [7] and ns2 (Network Simulator) [8]. We have extended ns2, implemented a hierarchical routing protocol, and simulated attacks on AODV (AdHoc On-demand Distance Vector) routing protocol. We have built supporting tools to analyze the traffic in an Ad Hoc network. We plan to examine the trust metric, the efficiency of route discovery, the overload on control traffic and routing computation, and different cooperation schemes among neighbors. For experimental study, we plan to take the number and density of hosts, the mobility of hosts, traffic load, and the required trustworthiness as input parameters. The protocol load and the delay will be measured and compared with available protocols. We will simulate attacks on routing protocols to estimate the robustness. Based on the results of simulation, we will identify the tradeoff between the protocol load, the delay and the required trustworthiness of a route. Experimental study will give guidelines to improve the protocol.

We plan to organize a workshop with Cisco researchers for potential enhancement in security for Cisco Aironet series wireless products.

Impact of Research

Next-generation wireless applications, such as multimedia, e-commerce, and videoconferencing, require wireless networks to offer more bandwidth, security and quality of service (QoS). The completion of this project will contribute to:

I. Development of secure routing protocols that make wireless networks survivable to external or internal hostile attacks.

II. Development of QoS support in wireless networks. Our research effort will provide a mechanism to measure the trustworthiness of routes and choose the best one based on the measurement. Similar idea can be applied to other metrics of a route, such as bandwidth, delay, etc., so that the proper route can be chosen to fulfill the QoS requirements.

Reference:


