Intruder Identification in Mobile Ad Hoc Networks

Bharat Bhargava
CERIAS security Center and
Computer Science Department
Purdue University
West Lafayette
Indiana 47907
bb@cs.purdue.edu
765-494-6013

Intruder identification in ad hoc networks is complementary to intrusion detection. The research challenge is to correctly identify the malicious hosts in a flat infrastructure. We propose a specification of intruder identification and four criteria to evaluate the algorithms. Specifically, we consider intruder identification in the AODV (Ad hoc On-demand Distance Vector) protocol. We study the attacks on AODV that target its security flaws. A protocol called RLR (Reverse Labeling Restriction) is presented to identify and isolate malicious hosts. RLR traces back the propagation paths of false routing information through reverse labeling. The protocol enables the hosts to share the knowledge in a secure way. The knowledge consists of a list of suspicious hosts in the perception of individual hosts and together, it lead towards indicting the intruder. One can assign a level of trust for each suspect. This will allow the discovery and management of a trusted route.

We simulate RLR using ns2. The simulation shows that up to 95% of the normal hosts can successfully reach and accept the identification results in a reasonable amount of time. Isolating the malicious hosts through rejecting the routing information from indicted intruders leads to a 30% increase in the data delivery. Host mobility and the number of independent malicious hosts are input parameters. The observed data includes effectiveness, accuracy, and overhead of RLR in different network environments. The robustness of the protocol is analyzed. It shows that RLR does not introduce any new vulnerabilities. This research can be applied to other ad hoc network routing protocols. This research is leading towards solving the problem of trusted route discovery.

This is joint work with Weichao Wang and Yi Lu and is supported by NSF and CISCO

More information about research in Raid lab is at http://www.cs.purdue.edu/homes/bb.