LIP: A Lightweight Inter-layer Protocol for Network Access Control in Mobile Ad-Hoc Networks

Hungyuan Hsu, Sencun Zhu, and Ali Hurson

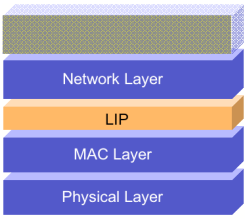
Most ad hoc networks do not implement any ***network access control*** leaving these networks vulnerable to packet injection attacks. To prevent such attacks, it is necessary to employ authentication mechanisms that ensure only authorized nodes may send packets into the network.

Lightweight Inter-Layer Protocol

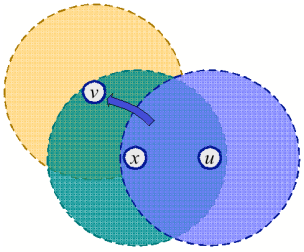
A hop-by-hop authentication protocol in which every node verifies every received packet before forwarding

Features

- Efficiency
- Scalability
- Immediate Authentication
- Transparency
- Independency



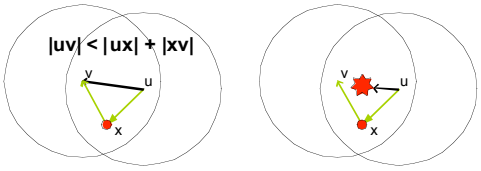
Security Threat



Impersonation Attack

In an ad-hoc network, a node does not have the authenticated knowledge which nodes are within its transmission range; therefore, an adversary can relay messages to commit an impersonate attack as described.

Security Building Blocks



(a) Triangle Inequality (b) Impersonation attack by x

Solutions

- One-way key chain
  - attach a unique traffic key to each packet to prevent replay attacks (based on triangle inequality)
- Probabilistic Neighborship Verification
  - randomly verify the neighborship with a claimed neighbor to prevent more advanced impersonation attacks
- Location-Aware Verification
  - use location information to avoid unnecessarily neighborship validation

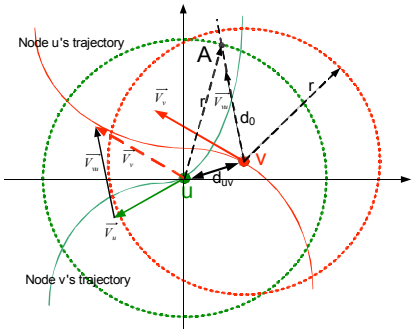
Location-Aware Verification

Radio Effective Duration (RED)

- The estimated time that two nodes stay within the transmission range of each other.

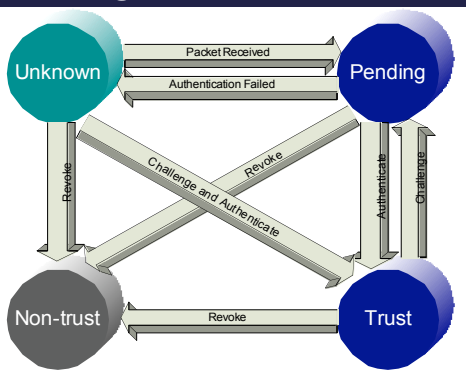
Verification Steps

- If the present time is within RED, forwards the packet to the upper layer.
- If the present time is beyond RED, temporarily buffers the packet and update neighborship with the neighbor node.
- If no response is received from the neighbor, then either drop the packet or challenge again.



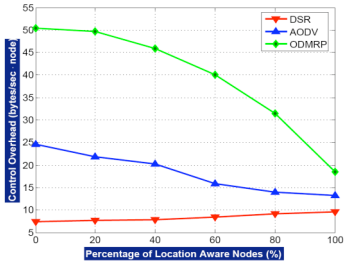
Trust Management

Each neighbor node belongs to one of the four states. In this diagram, every neighbor starts from the unknown state. As a packet received from that neighbor, the state transits to "Pending" and a challenge is sent to that neighbor. If the neighbor responds and is also authenticated, its state will be updated to "Trust" state. Any packet from a revoked node will be dropped immediately.

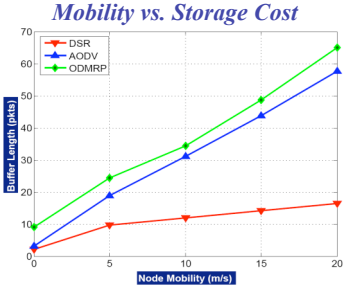


Performance Evaluation

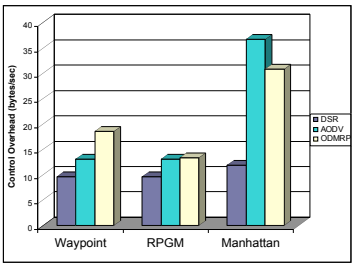
Control Overhead vs. Location Aware



Mobility vs. Storage Cost



Control Overhead vs. Mobility Model



RED vs. Mobility Model