**Group Communications in Wireless Ad Hoc Networks**

**Goal:** Provide resource-efficient secure group communications in wireless Ad Hoc networks.

Multicast communication mode saves network resources by delivering an identical message from one sender to multiple recipients. To restrict access, multicast traffic is encrypted with a Session Encryption Key (SEK) known to the source and all authorized multicast members.

**Multicast in Ad Hoc Networks**

Multicast group in ad hoc networks is dynamic due to:

a) Users join and leave the multicast service

b) Intermitent connectivity

After a membership change the SEK must be updated to preserve forward secrecy (only authorized users can access future communications)

Additional keys called *Key Encryption Keys* (KEKs) are needed to update the SEK to authorized members

**Key Management Problem (KMP)**

Ensure that at any given time only authorized members hold the SEK

**Key Distribution Problem (KDP)**

Develop key distribution schemes, such that at any given time, only authorized members hold the valid SEK

**Proposed Performance Metrics**

- Average energy expended by the network to update the SEK and relevant KEKs
- Average number of messages the network relays to update the SEK and relevant KEKs
- Additional metric: Key storage at each member

**Analysis of Problem Complexity**

We have shown that minimizing the average energy, or network bandwidth are NP-complete problems, by reducing them to a set cover problem

**Challenge:** Balance among all three metrics

**Deletion of a member M<sub>i</sub> from**

- TR<sub>1</sub>: Random key tree
- TR<sub>2</sub>: Location-Aware key tree
- TR<sub>3</sub>: Routing-Aware key tree

Can be shown $E_{TR1} > E_{TR2} > E_{TR3}$

- Routing-Aware Key distribution Algorithm
- Vertex Path Power Proximity Algorithm based on *Network Flows*
- Key Element in Algorithms: *Cross-layer design*, physical, network, application layer interaction

**Selected Publications**

Loukas Lazos and Radha Poovendran, Power-Proximity Based Key Management for Secure Multicast in Ad Hoc Networks, to appear in ACM journal in Wireless Networks


**Contact:** rp3@u.washington.edu