



Vehicular Communications Security

Christine Laurendeau

Kevin Nelson

Michel Barbeau

School of Computer Science

Carleton University

Outline

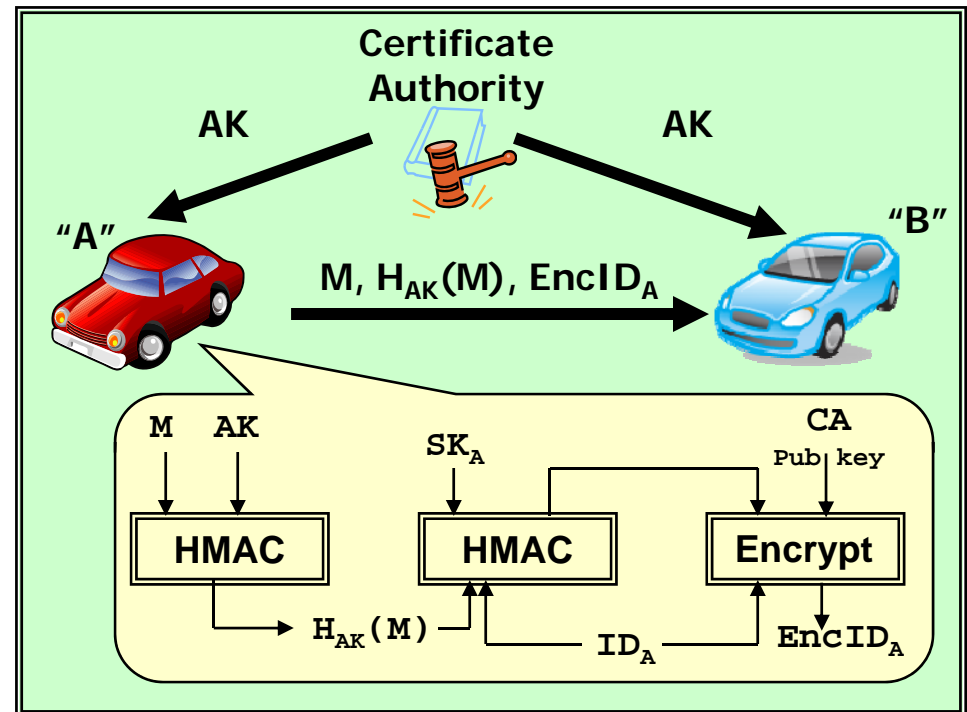
- Detection of Anomalous Position Reports
- Secure Anonymous Broadcasting in Vehicular Networks
- Rogue Attribution Using Signal Strength Based Location Estimation

Detection of Anomalous Position Reports

- Objective is to calculate a tight area bounding a vehicle's future location, given its present speed, direction, and acceleration
- Three models:
 - Semi-circle boundary using speed
 - Semi-circle boundary using speed and acceleration
 - Cardioid boundary using speed and acceleration

Secure Anonymous Broadcasting

- DSRC/WAVE uses broad-spectrum PKI
 - All devices:
 - Digital signatures
 - ➔ Vulnerable to location tracking
- SAB uses Hybrid Key Infrastructure
 - Trusted devices:
 - Ambulances, fire trucks, police
 - Asymmetric mechanism
 - PKI digital signatures
 - Anonymous devices:
 - Private & commercial vehicles
 - Symmetric mechanism
 - Shared authorization key (AK) for authorized devices only
 - Unique sender id encrypted for CA



SAB/HKI Performance Analysis

- Security: Authorization, Integrity, Non-repudiation
 - Equivalent to DSRC/WAVE
- Privacy
 - Non-existent in DSRC/WAVE; introduced in SAB/HKI
- Cryptographic Operation Performance
 - Transmit: 100% slower than DSRC/WAVE
 - Receive: Orders of magnitude faster than DSRC/WAVE
 - **But** for every message sent, N messages received (where N=#neighbors)
- Reference
 - C. Laurendeau and M. Barbeau, "Secure Anonymous Broadcasting in Vehicular Networks," in First IEEE LCN Workshop on User Mobility and Vehicular Networks (ON-MOVE), 2007.



URL: www.scs.carleton.ca/~barbeau/Publications/2007/ONMOVE_2007.pdf

Rogue Attribution Using Signal Strength Based Location Estimation

- Rogue insider exploits its valid identity to transmit false messages
- Goal is to attribute an attack message to its originator by locating the physical source of the transmission
- Our scheme uses relative signal strength received by neighboring nodes
- Signal strength differences between pairs of receivers define an area bounded by max and min distance hyperbolas
- Intersection of multiple hyperbola pairs pinpoints location of rogue