SAT: Situation Aware Trust Architecture for Vehicular Networks

Xiaoyan Hong, Univ of Alabama
Dijiang Huang, Arizona State Univ
Mario Gerla, UCLA (presenter)
Zhen Cao, UCLA

MobiArch'08, ACM SIGCOMM workshop, Seattle, WA. August 22, 2008
Vehicular Networking Apps

- **Safe navigation:**
  - Forward collision warning
  - Advisories to other vehicles: ice on bridge, congestion ahead, etc

- **Non safety applications**
  - Traffic monitoring (with navigator)
  - Pollution probing
  - Pavement conditions (e.g., potholes)
  - Content distribution
  - Urban surveillance

- **Primary security goals:**
  - Message **integrity, secrecy and authentication**
  - Detect misuse by naïve or malicious drivers.
  - Guarantee message sender **privacy**
Existing Trust in Vehicle Nets

Entity Trust

- Hey buddy, traffic ahead
- Are you serious?
  - origin integrity
  - data integrity

Data Trust

- Hey buddy, traffic ahead
- Are you serious?
  - data evaluation
  - decision on event

- Not adaptive to *situation changes*
- Not effective for group secure comms
- Mostly a reactive approach
- Can we be more proactive??
Situation Aware security approach

Attribute based Trust
- Situation elements are encoded into attributes
- Static attributes (affiliation)
- Dynamic attributes (time and place)

Dynamic attributes can be predicted

Social Trust
- Bootstrap initial trust
- Transitive trust relations

Proactive Trust
- predict dyn attributes based on mobility and location service
- establish trust in advance

An attribute based situation example:
Yellow Cab AND Taxi AND Seattle Street AND 10-11pm 08/22/08
A driver wants to alert all taxicabs of companyA on Washington Street between 10-11am that there was an accident somewhere nearby.

**Attribute (companyA AND taxi AND Washington St. AND 10-11am)**

**Extended ABE Module**

Ciphertext, Signature

Receivers who satisfy those encoded attributes (have the corresponding private key) can decrypt the message.
Attribute-Based Encryption (ABE)

- Encrypt Data with descriptive “Attributes”
- Users' Private Keys reflect Attributes and Decryption Policies
- Based on Identity-based Encryption and Secret Sharing; no need for “published key” (as in PKI) as long as the “attribute-based policy” is known

Authority is offline

sender

Encrypt w/attributes

receiver

CA/PKG

master-key
Access Control via Situation-aware Policy Tree

MSK = Master Secret Key

Authority Sandra the sender

$SK_{Sarah}$: "companyA" “10:30am” “Washington St.”

$SK_{Kevin}$: "companyA" “10: 20 am” “Westwood”

AND

companyA

AND

10-11 am Washington St.
SAT Architecture: supporting situation awareness

**SAT layer**

- **Perception**: communicate & sense environments
- **Comprehension**: extract & aggregate situations
- **Projection**: predict & create action profiles
- **Assessment**: evaluate and adjust trust situations

**Supporting and trust layer (STL)**

- Security primitive
- Comm. primitive
- Portal manage

---

**Situation-Awareness Trust (SAT) Layer**

- **Comprehension** of current situation
- **Projection** of future status
- **Perception** of objects, networks and events
- **Performance assessment**
- **Decision maker**
- **SAT status**
- **Communication model**
- **Vehicular networking & service related actions**
- **Security layer**
- **Policy group and key management**

Supporting and Trust Layer (STL)
Social Trust to overcome failures

How are you? People like to socialize => Social trust

- Suppose infrastructure fails, e.g., Road Side Unit is attacked/destroyed

- Social network helps maintain trust
  - People gang up into communities
  - Mobile users are situation aware
  - Social relations into SAT: social network => dynamic/static attributes
  - ABE based Authenticate and encrypt
Summary

• Situation Aware Trust Architecture
  ◦ Handles dynamic attribute tree based on situation assessment

• SAT architecture components
  ◦ Attribute based trust
  ◦ Proactive trust
  ◦ Social trust
  ◦ Architecture enabling the model.

• Contributions to VANET: mobile, proactive, low latency security for trustworthy communications!

• Future work: Performance Evaluation of the proposed schemes via simulation and testbed experiments
Thanks for your attention

- Do NOT hire a cab without SAT