Protecting Sensitive Data in VANETs Using Active Data Bundles

Abduljaleel M. Al Hasnawi (Advisor: Prof. Leszek T. Lilien)
Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008

Introduction

- Requirements for Vehicular Ad Hoc Networks (VANETs)
  - Integrate capabilities of the next generation wireless networks into vehicles
  - Share vehicular data over large-scale devices
- Typical VANET Applications
  - Traffic Safety, Traffic Efficiency, Convenience, Connectivity, Mobility
- VANET Communications and Communication Domains
  - V2V - Vehicle-to-Vehicle
  - V2I - Vehicle-to-Infrastructure
  - I2I - Infrastructure-to-Infrastructure
  - I2B - Infrastructure-to-Broadband
  - Domains: In-Vehicle, Ad Hoc, Infrastructure, Broadband

Methods

- Active Data Bundles (ADBs) (Then Othman&Lilien, 2009)
  - Sensitive Data: data to be protected
  - Metadata: specifies ADB policies
  - Operational Policies: control ADB behavior
  - Access Control Policies: control data dissemination and disclosure policies
  - Verification Policies: evaluate trust, check integrity
  - Virtual Machine (VM): executes ADB in order to evaluate and enforce privacy policies
  - Results of policy enforcement:
    - Full Data Disclosure: disclosure of all ADB data
    - Partial Data Disclosure: disclosure of a part of ADB data due to an insufficient trust level of the visited host, followed by the selective data disclosure
    - Apoptosis: complete ADB self-destruction when ADB "feels" threatened with unauthorized disclosure of its data
    - VM is encrypted or obsfuscated
- Mobile Agents (MAs)
  - Software objects able to:
    - Interact with and use capabilities of visited hosts
    - Transport themselves from one host to another
- Java Agent Development (JADE)
  - Software framework fully implemented in the Java language
  - Simplifies implementation of multi-agent systems

Results: The Proposed Solution

- ADB Lifecycle in VANETs
  - ADB Creation
    - VM: Create virtual machine
    - Encrypt data
    - Add metadata
    - Sensitive data
    - Data Owner
  - ADB Dissemination
    - Verification
    - Apoptosis
    - Unauthorized Host
  - ADB Enabling
    - VM: Enforce policies
    - Decrypt data
    - Full or partial Data Disclosure
    - Service Provider

ADB Enabling

- ADB trust verification for Host H
  - If trust value for H less than ADB-TT, then apoptosis
  - Otherwise, full or partial data disclosure
- ADB integrity verification for Host H
  - If hash value for H different than ADB-HV, then apoptosis
- ADB privacy policy enforcement for Host H
  - VM evaluates P for H
  - VM discloses data as indicated by F(C, P)
  - If last host visited by ADB, then VM apoptosizes ADB
  - Otherwise, ADB goes to the next host
- ADB decryption

Proof-of-Concept Scenario

- Pay As You Drive (PAYD) Insurance Application Scenario
  - Insurer requests driving data from an insured vehicle
  - Insurance fees calculated based on sensitive data:
    - Distance driven in a period of time
    - Driving style: speed, acceleration, time of day...

Conclusions and Future Work

- Conclusions
  - Integrating ADB with VANETs in an effective and efficient way should solve most of the privacy issues in VANETs
  - ADB is extensible - allows adding more security and privacy protection mechanisms
  - According to the sensitivity of the carried data
- Future Work
  - Evaluate using ADB in VANETs via simulation
  - Propose ADB routing protocol for VANETs
  - Apply the proposed solution to diverse VANET applications