VANET PKI-based vs Id-based Scheme

Mr.Sam Banani

Computer Science Program
School of Information and Communication Technology
Sirindhorn International Institute of Technology
Thammasat University

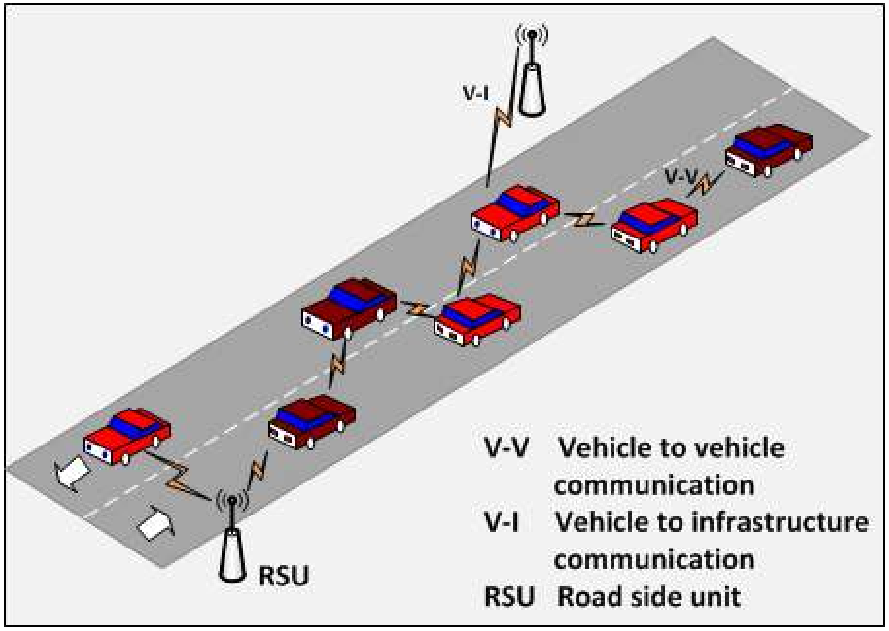
Outline:

- VANET Overview
  - Characteristics
  - Requirement of securing VANET
  - Attacks that threat to authentication
  - secure VANET
- Network model
  - PKI-based scheme
  - Id-based scheme
- Summary

VANET Overview

- VANETs is a network which use wireless communication between vehicles or between vehicles and road side unit.
  - Dedicated Short-Range Communications (DSRCs).
    - Data rate up to 27 Mbps.
    - Range of transmission up to 1 Km.
    - Send message 100-300 ms

- The goals of VANET are to increase road safety and transportation efficiency.


V-I
V-V
RSU
V-V Vehicle to vehicle communication
V-I Vehicle to infrastructure communication
RSU Road side unit

Characteristics of VANETs

- Nature of communication
  - Short range communication
  - The connection is not strong
- Dynamic and mobility
  - High speed
- Frequent information exchange
- Real-time process

Requirements for securing VANET

- Authentication
  - Entity authentication
  - Message integrity
- Non-repudiation
  - No entity can deny the message generated by itself.
- Availability
  - Provide network availability under jamming attacks
- Privacy
  - Provide message unlinkability and prevent driver's tracking
- Efficiency
  - Require low computation and communication overheads due to constraints on time

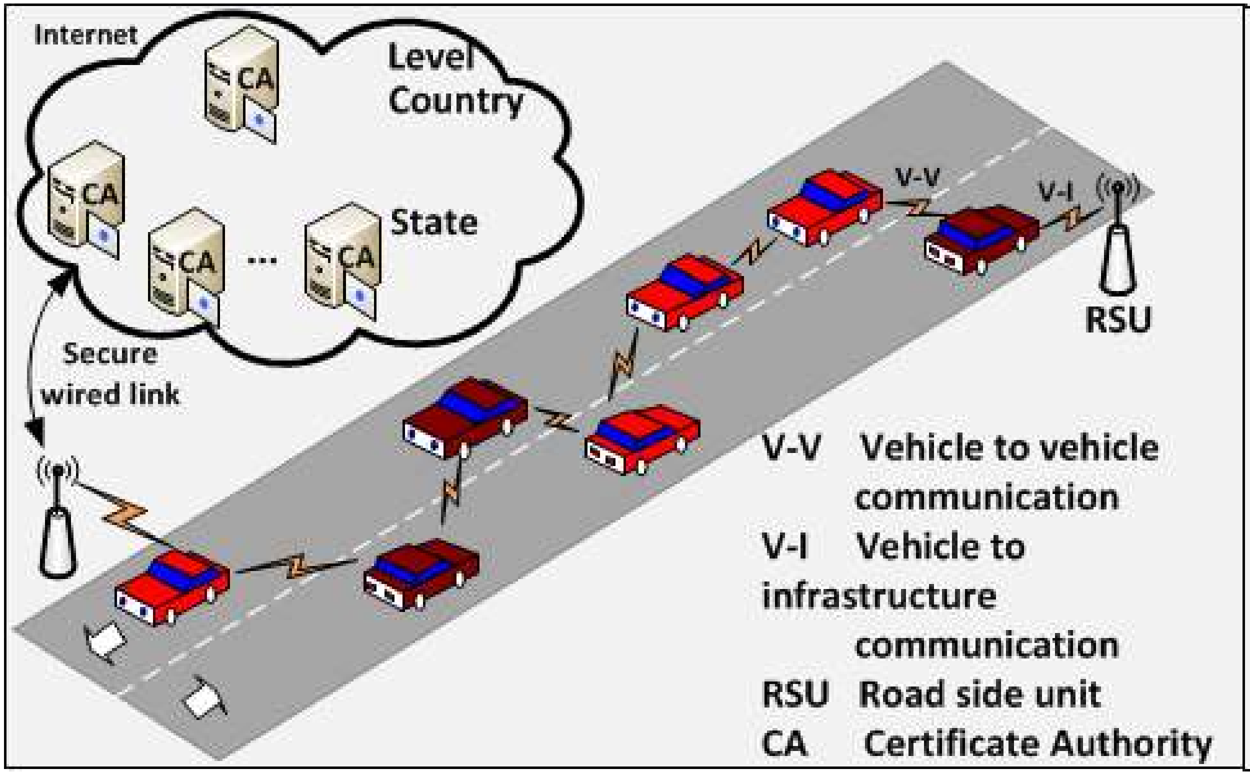
Attacks that threat to Authentication

- Masquerading
  - The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives.
- Message tempering
  - Any node acting as a relay can disrupt communications of other nodes. It can drop or corrupt messages, or meaningfully modify messages.
- GPS spoofing
  - An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices
- Sybil attack
  - Sending multiple message with different identity from one node
- Id disclosure
  - This attack discloses the identity of other nodes in the network and tracks the current location of the target node.

Secure VANETs

- There are mainly two categories of cryptography based algorithms is used for security:
  - PKI-based scheme
    - Pseudonyms-based
    - Group signature-based
  - Non-fully PKI-based scheme.
    - Identity-based scheme

VANETs General model



V-V Vehicle to vehicle communication

V-I Vehicle to infrastructure communication

RSU Road side unit

CA Certificate Authority

Vehicular PKI
Hierarchy of CA's

CA actions

- Register vehicle
- Issue public/private key pair in digital certificate
- Renew digital certificate
- Certificate revocation

Component of node

- Secure computing platform
- Tamper proof hardware
- Event data recorder
- Sensors
- Processing unit

PKI-based examples:

- Procedure of at sending message V_1
  1) V_1: $M'=(M||t)$
  2) V_1 : $Sign_{V1}= E(M',PR_{V1})$
  3) V_1 : $EP= E(Sign_{V1},PU_{CA})$
  4) V_1 : $M''=(M'||EP)$
  5) V_1 : $Sign_{W1}= E(M'',PR_{W1})$
  6) $V_1 \longrightarrow * : (M''||Sign_{W1})$
- Procedure of Verifying message at receiver V_2:
  1) V_2 : $(M''||Sign_{W1})$ separate to M''_1, $Sign_{W1}$
  2) V_2 : $M''_2= D(Sign_{W1}, PU_{W1})$
  3) V_2 : If $(M''_1 == M''_2)$ then successfully message authenticate and integrity is verified.

PKI-based:

- Multiple Certificates Per OBU (Raya & Hubaux, 2007…)
  - Each OBU owns a set of certified public/private key pairs
  - A large set of keys needs to periodically renewed (during regular vehicle maintenance visits)
  - OBUs contact trust authorities through RSUs and send the created pseudonym and public key. Authorities send the built certificates back
  - Each key is used for a short period of time

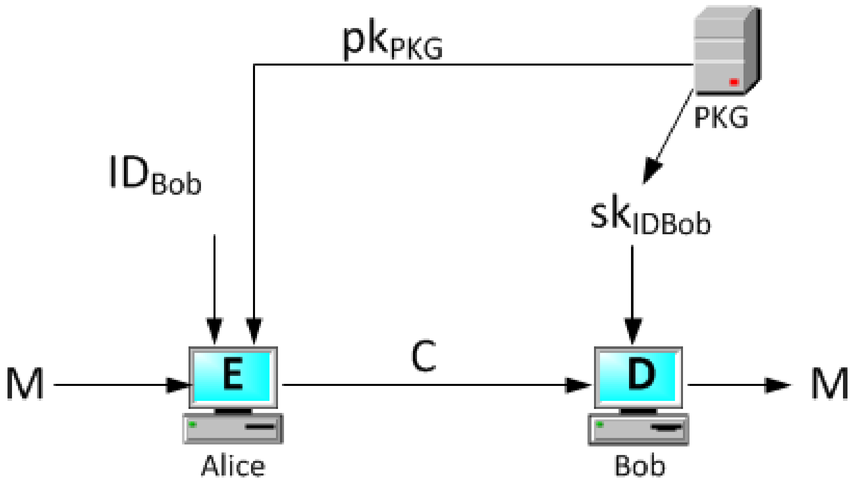
- Suffering from a Sybil attack
  - A malicious OBU can pose as multiple vehicles
- Large overhead to revoke a OBU

PKI-based Group signature:

- Group Signatures (Lin et al., 2007…)
  - Group signature guarantees the unlinkability of the messages since group member can anonymously sign on behalf of the group
  - OBU uses a group signature to sign a message to prove that the signer is a valid OBU (not which OBU)
  - Group manager can trace the identity of a signer from the group signature and revoke the group member

Reduce the storage cost of multiple public/ private key pairs and the bandwidth consumption

ID-based Encryption (IBE)

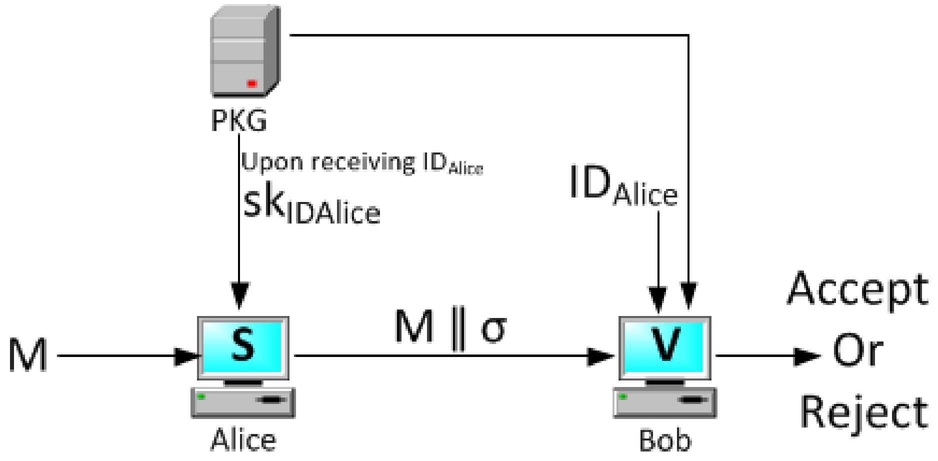


IBE scheme

- Setup
- Private Key Extraction
- Encryption
- Decryption

- Procedure of at sending message at node A
  1) A :T= E(M,$PU_{ID\text{-}B}$)
  2) A → B : T
- Verifying procedure at node B
  1) B: Authenticate itself to PKG , get Private Key
  2) B: M= D(T, $PR_{ID\text{-}B}$)

Id-based signature scheme (IBS)



IBS scheme

- Setup
- Private Key Extraction
- Signature Generation
- Signature Verification

- Procedure of at sending message at node A
  1) A : $\boldsymbol{\sigma} = E(M,PR_A)$
  2) A ⟶ B : $(\boldsymbol{\sigma} \| M)$
- Verifying procedure at node B
  1) B: Authenticate itself to PKG , get Private Key
  2) B: $M_1 = D(\boldsymbol{\sigma}, PU_{ID\text{-}A})$
  3) B: If $(M_1 = M_2)$ then successfully message authenticate and integrity is verified.

Summary:

- Id-based system, for verifying entity dose not require to store, fetch and verify the public key certificates of message signer from a third-party trusted authority.
- Id-based system reduces the system complexity and the cost for establishing and managing the public key.
- In id-based system can save on storage, communication bandwidth , and time.

Literature Review: