Fraunhofer FOKUS Institute for Open Communication Systems

On Identification and Addressing

SEVECOM Workshop, 1. -2. Feb 2006

matthias.gerlach@fokus.fraunhofer.de

The Network on Wheels Project

Fraunhofer Institute for Open Communication Systems

Mission

- Specification of Car2Car communication protocols and submission to the Car2Car Communication Consortium
- Implementation according to (C2C CC) standardization progress

Major Aspects

- Business models for market introduction
- Active safety and deployment application
- Position based routing (Scalable GeoBroadcast)
- Data security for vehicular ad hoc networks

Partners

DAIMLERCHRYSLER

BMW Group

NEC

carmeq

FOKUS

UNIVERSITÄT KARLSRUHE (TH)

Funded by:
Bundesministerium für Bildung und Forschung

Context - Security Objectives

The Security WG in NoW shall

- “Propose Algorithms providing different levels of Security for Ad Hoc Networks and in particular for the NoW Network.”

Objective: “Trusted Network on Wheels”

- Private Communication and Location Privacy
- Reliable, Secure Communication even in the Face of Malicious Attacks
- Detection of Malicious and Faulty Data

Influence on all aspects of the NoW System

- Communication System
- Applications
- Reference System

What will this talk be about ?

Addressing and Identification

- How do we create addresses
- How do we identify a node
- How do we support Privacy (?)
- Can we integrate addressing an key management ?

Integrity and Authenticity

- Based on some cryptographic algos
- Can it be combined with addressing ?

Authorization of nodes

- “this node is legitimate part of the NoW network”
- Implicit (by possession of a key pair) or explicit (certificates)

Saving Bandwidth and Time

- Minimize security overhead (by combining address and public key, for example)
- Minimize processing time

Identification - What for?

Different Possible Purposes

- Re-recognition (network)
- Reputation assignment (network)
- As a basis for key management (network)
- Addressing of nodes (network)
- Liability issues (legal)
- User Identification / Application identification (out of scope)

We focus on Addresses as the prevalent means of identification

Requirements on Addresses

General Requirements

- World-wide uniqueness
- Immutability and non-migratability
- Verifiability

NOW Specific Requirements

- Suitable for VANETs
- Large Identifier (address) space
- Sporadic, well defined access to security infrastructure
- Privacy support
- Support broadcast authentication
- Use fast algorithms
- Cannot assume static network config (must always include all relevant information for security in the messages)

Pro and Con Addressing

Some say that addressing is unnecessary ...

Depends on

- Communication required (Application)
- Security Measures envisioned

Pro secure addressing

- Can detect malicious/faulty nodes by their communication identifier
- May be basis for authorization to send messages
- Basic functionality (e.g. Routing) based on some sort of identification anyway.

Con secure addressing

- Privacy concerns
- May not be needed, if we only rely on position (or even attributes) for routing.
- Some (802.11p) propose using random MAC addresses anyway.

NoW Assumptions on Addresses/Identification

Fraunhofer FOKUS Institute for Open Communication Systems

NoW Node Identity

- GUID (Globally Unique Identifier)
  - Unambiguous Identifier for NoW OBUs /RSUs
  - Car Manufacturer or other authorized organization assigns
  - Not used for communication
- Pseudonyms for communication (→ Addresses)
  - Shall change according to a defined metric
  - Pseudonyms are unlinkable

Link Layer Addressing

- Link Layer Address is EUI-64, EUI-48 supported for compatibility
- Concurrent use of 48 and 64 bit link layer addresses required
- Unambiguous addressability within a certain scope
- Link layer address should be derived from a NoW pseudonym
- Support multiple link layer addresses sequentially or simultaneously

What did we look at?

Standard Addresses

- Basis for Addressing (EUI 48tm, EUI 64tm)

ID Based Crypto

- Having an Identity implies being authorized,
- no certificate needed

Addresses Derived from Cryptographic Keys

- Binding Address to Public Key saves overhead (?)

Hash Chains

- Efficient broadcast authentication, saves time

Standard Addresses

EUI 48tm / EUI 64tm

- Used in Ethernet, WiFi, common standard
- Two parts:
  - upper 24 bits : Organization Identifier
  - lower 24 / 40 bits: Burned In Address (BIA), Locally Administered Address (LAA)
- EUI 64 fits the need for scalability, EUI 48 would not, in the long run.
- Assume that we cannot use the upper 24 bits.
- Can create IPv6 addresses from EUI addresses
- We will most certainly use these addresses

ID Based Crypto

Properties

- Identifier = public key
- TTP assigns respective private key

Pro

- Elegant way of dealing with authorization
- May save a lot of bandwidth (no public key, no certificate needed)

Con

- Pretty new technique
- How do we revoke identities
- Too slow to be suitable for VANETs
- No non-repudiation property, TTP may know all private keys

Addresses Derived from Cryptographic Keys

Properties

- Create an address from a public key (e.g. by means of a hash function)
- Hash function verifiably binds address to public key

Pro

- Solves address ownership problem (which was not our problem anyway)
- Gives us (statistically) unique addresses for free

Con

- No bandwidth gain, still need authorization certificate, public Key included in a message.

Hash Chain based Solutions

Properties

- Used for efficient broadcast authentication in sensor networks
- Must only authenticate hash chain commitment
- Existing Protocols: TESLA, TIK, ZCK

Pro

- Fast and efficient crypto
- Similar to a public private key scenario (commitment is public key, yet undisclosed key in chain are private keys)

Con

- Probably no significant reduction in overhead, still need a certificate for authorization
- May need to authorize current public key every time

Summary and Future Work

Summary

- We support standard addresses
- Addresses will be bound to a cryptographic key

Future Work

- Look at different algos more closely
- Look at WAVE Security more closely

Thank You

Fraunhofer FOKUS Institute for Open Communication Systems

Do you have any Questions ?