Empowered by Innovation NEC

C2C-C Requirements for Usage of NEMO in VANETs

draft-baldessari-c2ccc-nemo-req-00.txt

Roberto Baldessari
NEC Europe Ltd. Heidelberg

Andreas Festag
NEC Deutschland GmbH Heidelberg

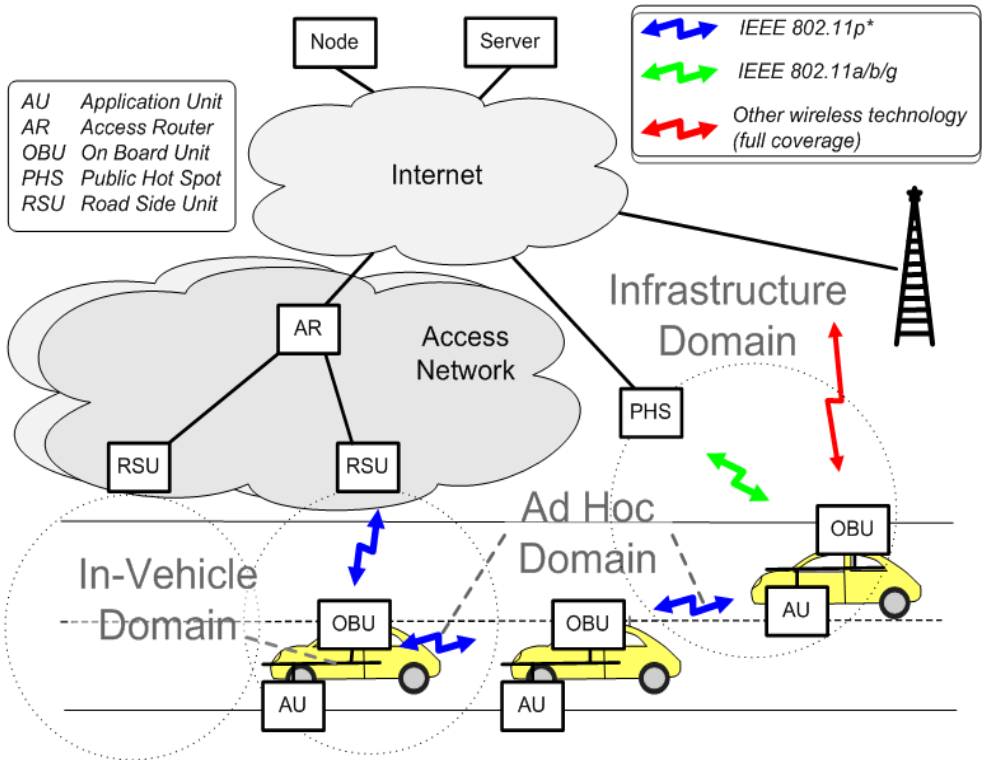
Massimiliano Lenardi
Hitachi Europe SAS Sophia Antipolis

Outline

- **VANET Scenario**
- **Overview of C2C-CC**
- **C2C-CC Technical Approach: A *MANET-centric* view**
- **Requirements for NEMO**
  - Routing
  - Privacy
  - Security
- **Conclusions**

VANETs Scenario

- Special kinds of MANETs, supporting both **safety** and non-safety applications
- Single, short-range dedicated technology (802.11p draft) in basic systems
- Additional technologies (especially 802.11) in extended systems
- Peculiarities:
  - High **mobility**
  - **High number** of nodes
  - Costs restrictions to allow for high **deployability**
- **Internet**-based applications
  - Beneficial for safety purposes
  - Fundamental for non-safety purposes

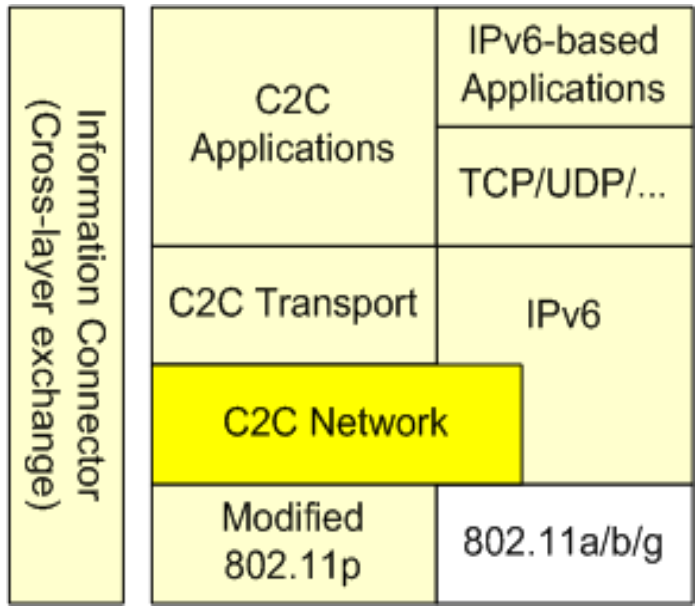


Overview of C2C-C Consortium

- Industrial consortium (mostly) comprised of car manufacturers and electronics suppliers operating in Europe
- Primary goal: Defining a European standard for vehicular communication
- Aims at harmonizing with other bodies (e.g. ISO) to build an European infrastructure for ITS applications
- C2C-CC Handbook to be published by mid-2007

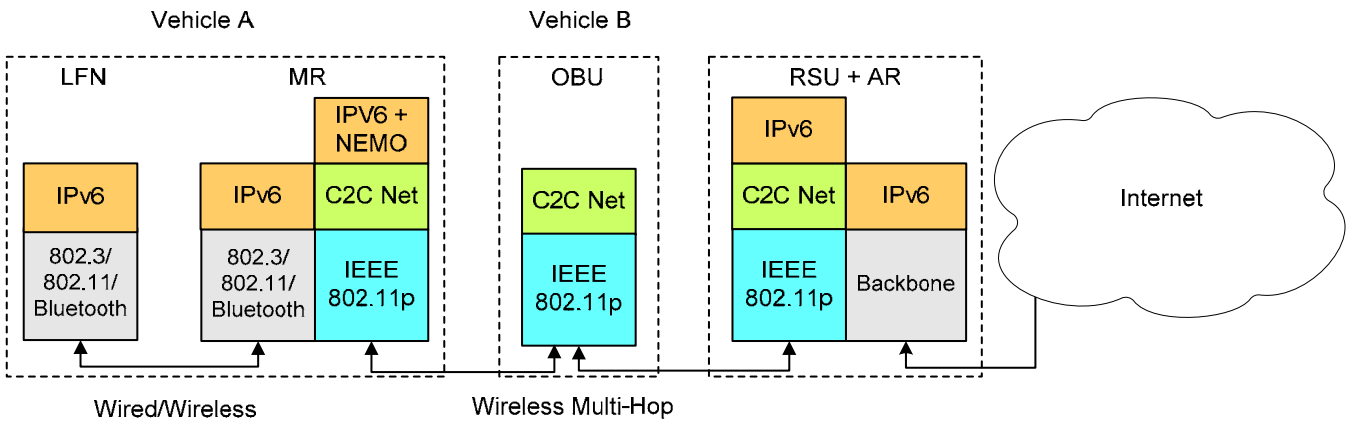
C2C-CC Technical Approach (1/2)

- Based on a slightly modified 802.11p
- Safety requirements have lead to a specific protocol stack offering:
  - Geographic packet distribution (Geocast)
  - Information-centric forwarding (data aggregation)
  - Cross-layer congestion control
  - Specific security/privacy features
- C2C Network Layer: Implements a **position-based** ad hoc routing protocol using GPS position (semi-reactive, on the fly forwarding)
- IPv6 layer on top of C2C Network Layer resulting in:
  - 2.5 layer providing ad hoc routing
  - IPv6 layer not aware of ad hoc routing (single logical link)



C2C-CC Technical Approach (2/2)

- **NEMO** to be used for **non-critical** safety applications and for **infotainment**. Main use cases:
  - Notification Services (traffic, weather, news)
  - Peer-to-peer applications (messaging, VoIP, file transfer)
  - Upload/Download services (maps, travel info, software updates, Internet)
- NEMO not supported by every car
- NEMO runs on top of the C2C Network Layer and is not aware of the ad hoc network
  - Advantages: Clean **separation of roles** reduces design complexity and requirements
  - Drawbacks: Additional C2C header increases **overhead** (European 802.11p frame TBD)
  - Performance and scalability proven by simulation and tests with **prototypes**. Measurements in Field Operation Tests (FoT) already planned

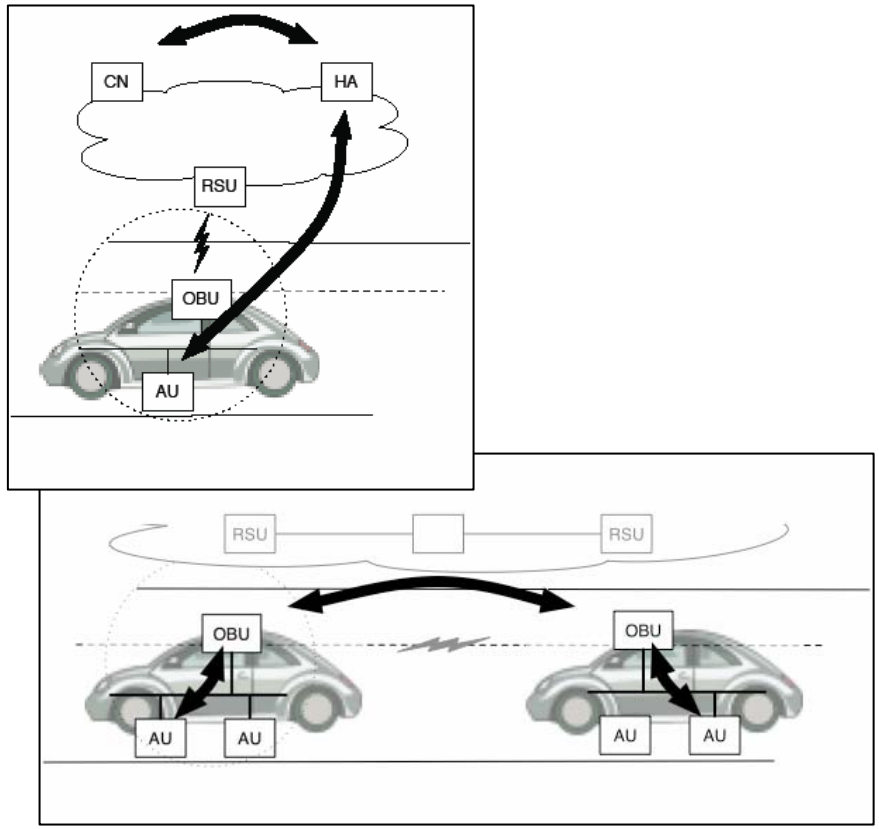


Requirements for NEMO: Routing

- Intermittent, **rare connectivity** requires a broader concept of Route Optimization: MRs should use MNP also independently of the Home Agent

- **Vehicle-to-Infrastructure** (Infrastructure available)
  - "Classic" (MIPv6-like) Route Optimization with Correspondent Entity is required
  - Highest priority for **MR-to-CN** (MR-to-CE)
  - Low priority for Visiting Mobile Node
  - Nested Mobile Networks not considered

- **Vehicle-to-Vehicle** (Infrastructure available or not)
  - **MR-to-MR** enabled by exposing MNP to egress interface
  - Issues: Route consistency, service provider control on MNP, privacy



Requirements for NEMO: Privacy

- Vehicular networks can potentially introduce new methods to invade user privacy (tracking)
- Unlike traditional Internet scenario, privacy issues concern the **ad hoc domain**
- Common approach in VANET is adopting **pseudonyms**
  - Temporary identifiers at different layers (MAC/NET), assigned by authority
  - Real identity is revealed only to trusted nodes
  - A pseudonym change requires updating the Binding at the Home Agent in order to keep sessions alive
- NEMO signaling and data exchange should not allow for **linking** of pseudonyms
  - HoA/MNP always encrypted in BU/BA
  - Outer header reveals Home Agent address...(!)
- Exposing the MNP on the egress interface should be subject to policies (only to trusted nodes)

Requirements for NEMO: Security

- For **safety** applications, data security is fundamental
  - Mandatory features: Integrity, authentication, non-repudiation
  - The routing protocol itself must include security features
- Currently considered approach:
  - Relying on a dedicated PKI
  - Using signature for safety payloads calculated including protocol header fields
- At this moment, very precise requirements cannot be provided
- Identified principles:
  - Security against already studied attacks (MIPv6) must be provided (IPsec to protect signaling and tunnel MR-HA, RO security)
  - NEMO must not introduce new security leaks for the C2C-CC applications nor render their security measures ineffective

Conclusions

- C2C-C Network layer provides 2.5 efficient and scalable ad hoc routing to IPv6 layer
- NEMO does not have to deal with ad hoc routing (in fact, it's not designed for ;-)
- High priority requirements for NEMO
  - Route Optimization with Correspondent Node (Entity) in the Infrastructure
  - Direct MR-to-MR without infrastructure:
    - ***Is it in the scope of NEMO WG?***
    - ***Should it be standardized as a NEMO extension or provided by the ad hoc routing protocol by injecting routes?***
  - Privacy:
    - ***Encryption of constant identifiers (MNP, HoA)***
    - ***Outer header impact to be analyzed***
- Security:
  - IPsec for signaling
  - Too early to define more precise requirements

Empowered by Innovation