Problem Statement for Vehicle-to-Infrastructure Networking

(draft-jeong-ipwave-v2i-problem-statement-00)

IETF 98, Chicago, US

March 31, 2017

SUNG KYUN KWAN UNIVERSITY(SKKU)

Jaehoon (Paul) Jeong*, and

Tae (Tom) Oh

ROCHESTER INSTITUTE OF TECHNOLOGY R·I·T 1829

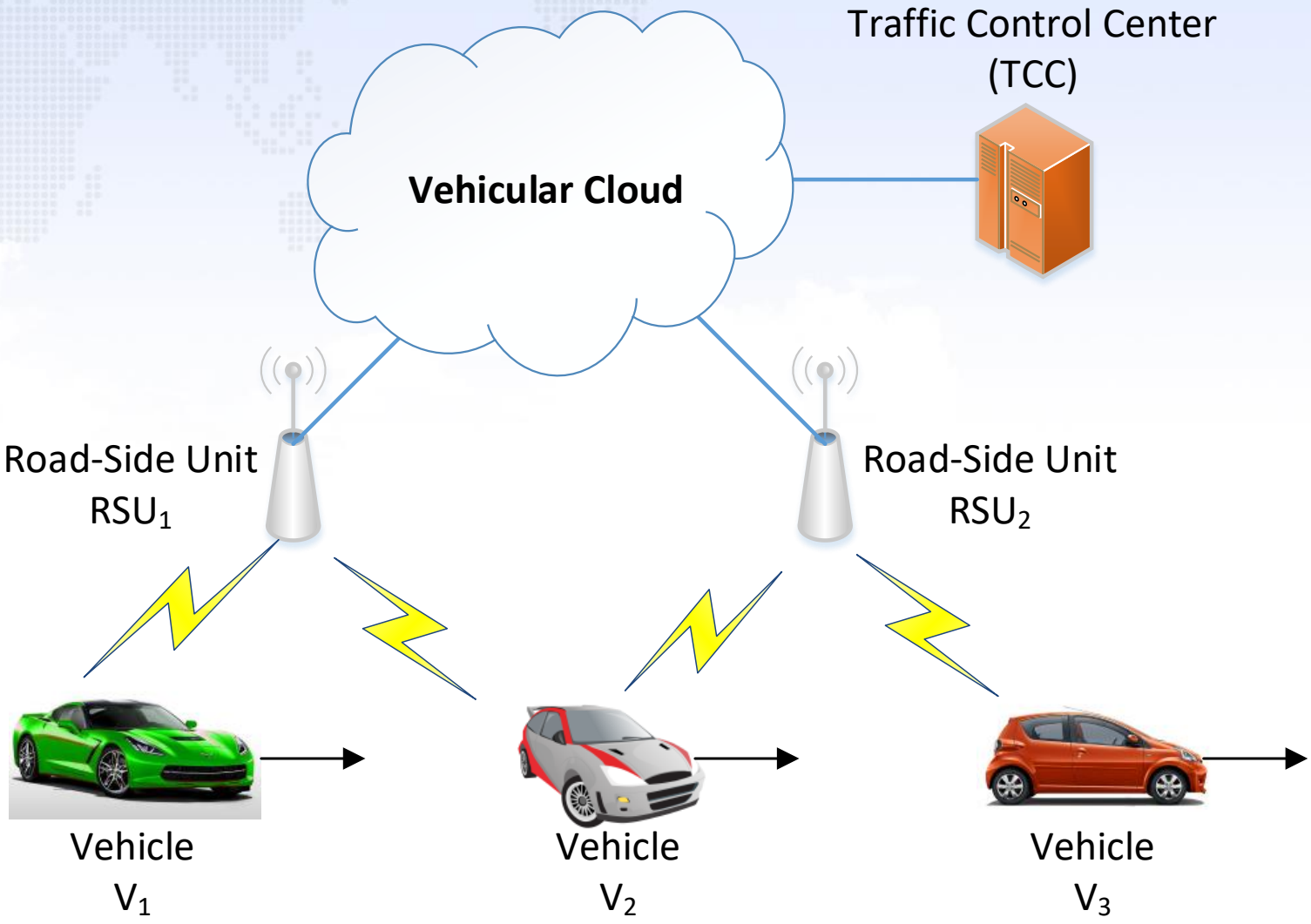
Updates from the Previous Version

- Changes from the previous draft (draft-jeong-its-v2i-problem-statement-02)
  - In Section 12, the considerations on security and privacy are enhanced in terms of:
    - Authentication and Access Control,
    - Periodic Change of MAC and IP Addresses, and
    - Confidential Data Exchange.

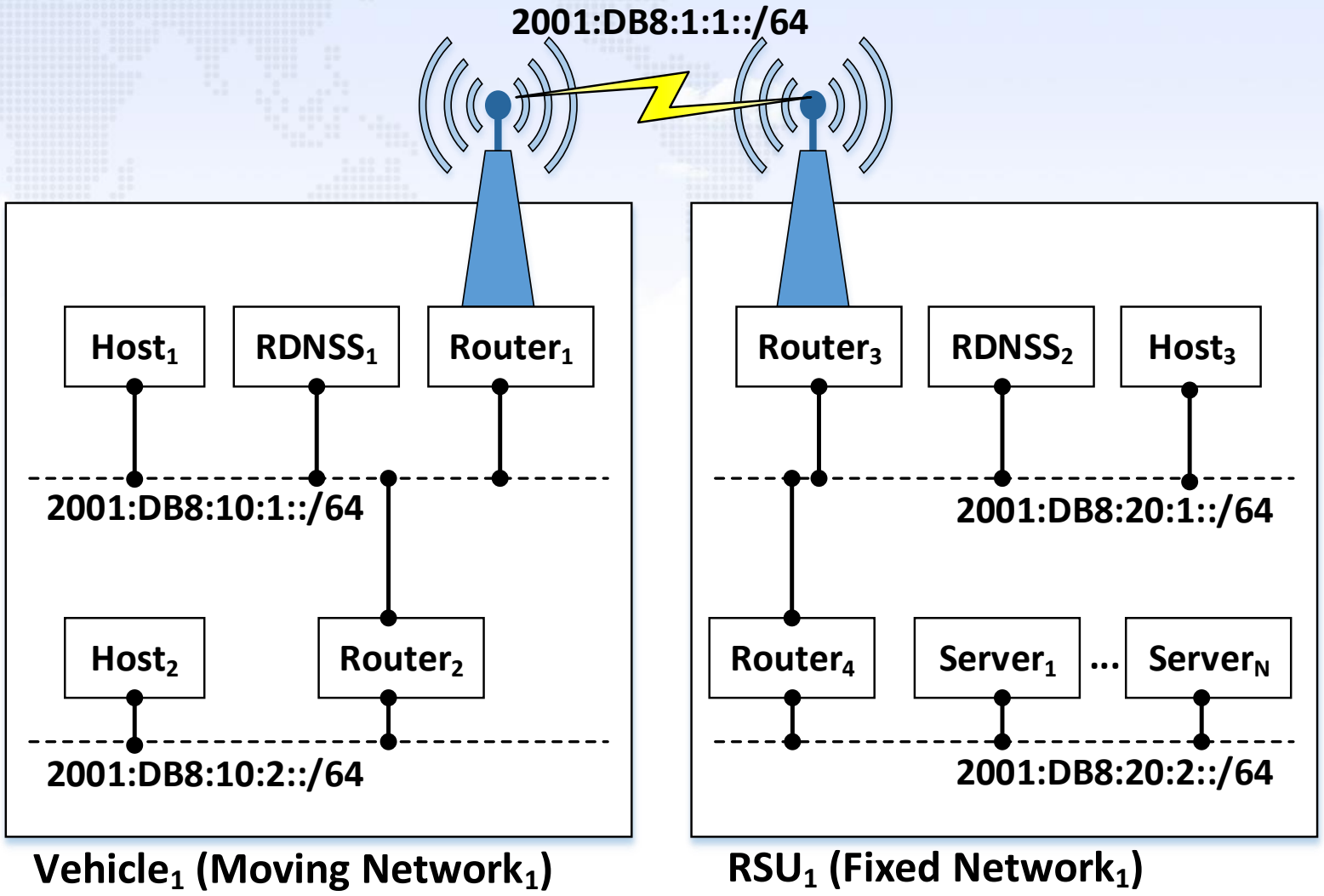
Introduction to V2I Networking

- Objective of this draft
  - To specify the problem statement for IPv6-based Vehicle-to-Infrastructure networking.
- Assumptions for V2I
  - IEEE 802.11p is considered as MAC protocol.
  - IPv6 is considered as Network-layer protocol.
  - Road-Side Unit (RSU) is connected to the Internet as an access point for vehicles.
- Focus of this draft
  - Networking issues in one-hop communications between RSU and vehicles.
  - Internetworking between a vehicle's internal network (i.e., moving network) and an RSU's internal network (i.e., fixed network).

Network Configuration for V2I Networking



Internetworking between Vehicle's Moving Network and RSU's Fixed Network



Security and Privacy for V2I Networking (1/3)

- **Authentication and Access Control**
  - A Vehicle Identification Number (VIN) and a user certificate can be used for authentication.
  - An RSU can be used to give vehicles the connectivity with an authentication server in TCC.
  - TLS certificates can be used for the authentication and access control in secure communications.

Security and Privacy for V2I Networking (2/3)

- **Periodic Change of MAC and IP Addresses**
  - To prevent a vehicle from being tracked by an adversary, the MAC and IP addresses of the vehicle can be changed periodically with randomness.
  - This address update should not interrupt the communications between a vehicle and an RSU
    - In the level of the network layer (i.e., IP) or transport layer (e.g., TCP and UDP).

Security and Privacy for V2I Networking (3/3)

- **Confidential Data Exchange**
  - To protect data packets exchanged between a vehicle and an RSU, they should be encrypted by a cryptography algorithm.
  - This confidentiality can be provided by efficient encryption and decryption algorithms (e.g., IPsec) along with an efficient key management scheme (e.g., IKEv2).

Next Steps

- Merging with the V2V Problem Statement Draft (draft-petrescu-its-problem-03) for a **"Problem Statement" WG draft** in IPWAVE WG.
  - The draft's name will be **draft-jeong-ipwave-problem-statement-00**.

- Terminology Update
  - With draft-ietf-ipwave-ipv6-over-80211ocb-02, ISO 21217 (ITS station/communication architecture) and ISO 21210 (IPv6 networking for ITS)

- We will welcome comments from IPWAVE WG.