IPWAVE WG Side Meeting

IETF 106, Singapore

Nov 21, 2019

Organizer: Jaehoon (Paul) Jeong

Agenda

- IPWAVE Hackathon Project (Yiwen Chris Shen, 5 min)
- IPWAVE Problem Statement Draft (Jaehoon Paul Jeong, 5 min)
- Individual I.D.s:
  - Vehicular Neighbor Discovery Draft (Yiwen Chris Shen, 5 min)
  - Vehicular Mobility Management Draft (Yiwen Chris Shen, 5 min)
  - Security and Privacy Draft (Jaehoon Paul Jeong, 5 min)
  - Context-Aware Navigator Draft (Yiwen Chris Shen, 5 min)
  - Neighbor and Service Discovery Draft (Zhiwei Yan, 5 min)
- Open Discussion: Possible Work Items for IPWAVE (25 min)

IETF Hackathon Report

IETF 106, Singapore

Nov 21, 2019

Yiwen (Chris) Shen

SKKU

Hackathon Project

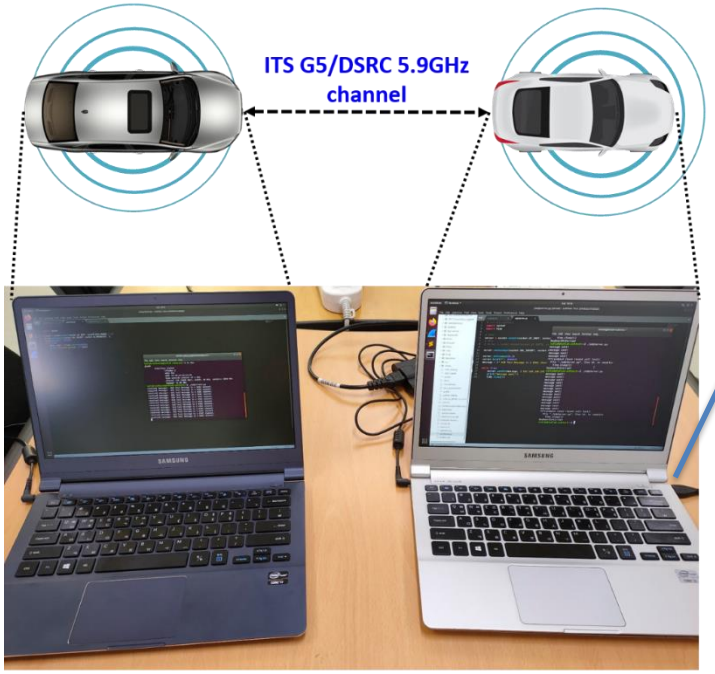
- IPv6 Packet Transmission over two OCB-enabled WiFi modules in vehicular networks
  - How to enable a commercial WiFi module to work on 5.9GHz band?
  - How would IPv6 ND work in IEEE OCB mode?
  - How to enable webcam (dashcam) streaming by IPv6 over 802.11 OCB mode?

- Related IPWAVE Drafts:
  - https://datatracker.ietf.org/doc/draft-ietf-ipwave-ipv6-over-80211ocb/
  - https://datatracker.ietf.org/doc/draft-ietf-ipwave-vehicular-networking/

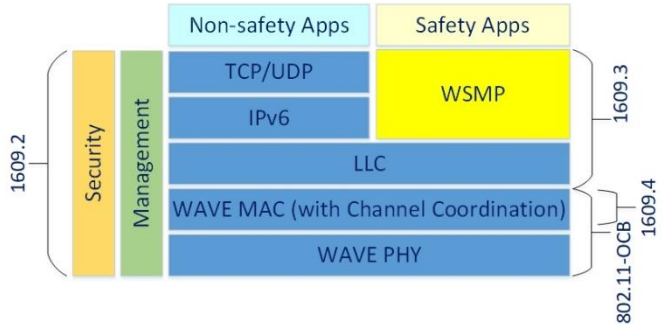
What got done

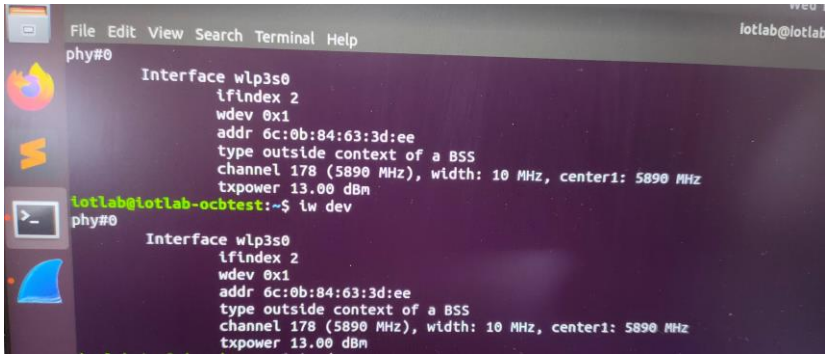
- Compiling Linux Kernel for OCB mode (Kernel version 4.4).
  - Modify Makefile to remove possible errors
  - Menuconfig for OCB mode
    - Enable ITS G5/DSRC band
    - Atheros 802.11 ath9k wireless card driver
    - Enable webcam driver
- IPv6 packet transmission by two OCB-enabled WiFi modules.
  - IPv6 address configuration
  - UDP packets transmission
  - Webcam streaming

Setup Environment



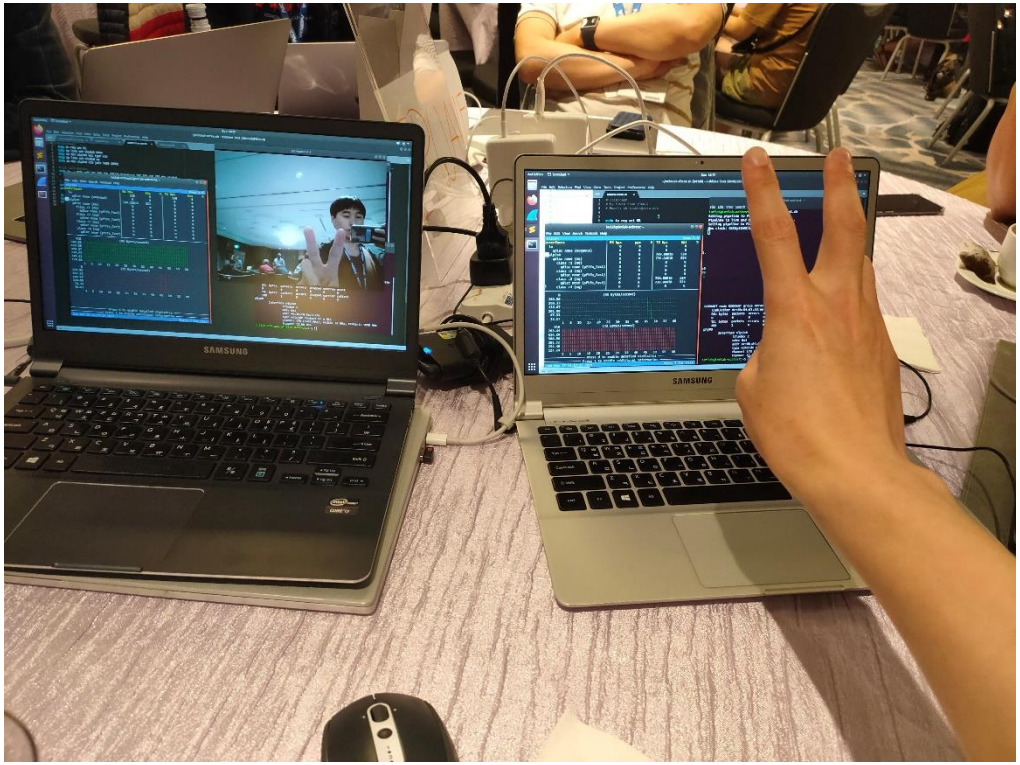
Environment Setup





Experiment

- Successfully str eam webcam ov er two OCB-ena bled laptops.



What We Learned

- Compiling error can happen due to Makefile setting.
  - Updated Makefile to remove the error
  - Updated Makefile of Central Regulatory Domain Agent (CRDA) to remove a compiling flag, -*Werror*, that shows compiling errors when variables are not used.
  - Made a new manual for running OCB mode

- IPv6 ND is not automatically running on the interface.
  - No Carrier shown on the interface
  - Need to manually configure IPv6 address and neighbors

Wrap Up

Team members:

Champions:

- Jaehoon Paul Jeong (SKKU)
- Younghan Kim (SSU)

Students:

- Yiwen Chris Shen (SKKU)
- Zhong Xiang (SKKU)
- Bien Aime Mugabarigira (SKKU)
- Kyoungjae Sun (SSU)

First timers @ IETF/Hackathon:

Hyojoon Han (Dongguk Univ.)

Video clip demo: https://youtu.be/gQxOLU740b4

Where to get code (manual):

https://github.com/ipwave-hackathon-ietf/ipwave-hackathon-ietf-106

Original contributors:

Czech Technical University and Volkswagen:

https://ctu-iig.github.io/802.11p-linux/

IPWAVE-Problem Statement and Use Cases

(draft-ietf-ipwave-vehicular-networking-12)

IETF 106, Singapore

Nov 21, 2019

Jaehoon (Paul) Jeong [Editor], Nabil Benamar, Sandra Cespedes, Jerome Haerri, Dapeng Liu, Tae (Tom) Oh, Charles E. Perkins, Alexandre Petrescu, Yiwen (Chris) Shen, and Michelle Wetterwald

Introduction

- Use cases using V2V, V2I, and V2X networking.
- Problem statement, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy.
- This document specifies requirements in IP-based vehicular networking, and suggests the direction of solutions satisfying those requirements.

Update from -11 version

Comments from C. Perkins

Update from -11 version

- Comments from C. Perkins
  - Section 5: Problem Statement
    - A new and identifiable problem statement

In order to specify protocols using the abovementioned architecture for VANETs, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a time relatively small compared to the lifetime of a link between a vehicle and an RSU, or between two vehicles. This has a major impact on IPv6 neighbor discovery. Mobility management is also vulnerable to disconnections that occur before the completion of identify verification and tunnel management. This is especially true given the unreliable nature of wireless communications. Finally, and perhaps most importantly, proper authorization for vehicular protocol messages must be assured in order to prevent false reports of accidents or other mishaps on the road, which would cause horrific misery in modern urban environments. This section presents key topics such as neighbor discovery and mobility management.

Update from -11 version

- Comments from C. Perkins
  - Section 1: Introduction
    - Remove geographic routing description since it's not related to IPWAVE's use cases

Along with these WAVE standards, IPv6 [RFC8200] and Mobile IP protocols (e.g., MIPv4 [RFC5944], MIPv6 [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213][RFC5844]) can be applied to vehicular networks. ~~In Europe, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. GN protocols are useful to route an event or notification message to vehicles around a geographic position, such as an accident area in a roadway.~~ In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].

Update from -11 version

- Comments from C. Perkins
  - Section 2: Terminology
    - Add description of OCB, Context-Awareness, Platooning

OCB: "Outside the Context of a Basic Service Set". It is differentiated from the Basic Service Set (BSS) mode in IEEE 802.11 standard. A node in OCB mode can directly transmit packets to other nodes in its wireless range without the authentication or association process defined in BSS mode.

Context-Awareness: A vehicle can be aware of spatial-temporal mobility information (e.g., position, speed, direction, and acceleration/deceleration) of surrounding vehicles for both safety and non-safety uses through sensing or communication [CASD].

Class-Based safety Plan: A vehicle can make safety plan by classifying the surrounding vehicles into different groups for safety purposes according to the geometrical relation ship among them. The vehicle groups can be classified as Line-of-Sight Unsafe, Non-Lin e-of-Sight Unsafe, and Safe groups [CASD].

Update from -11 version

- Comments from C. Perkins
  - Section 4.1:
    - Update the Fig. 1 and its description

A single subnet prefix can span multiple vehicles in VANET. For example, in Figure 1, for Prefix 1, three vehicles (i.e., Vehicle1, Vehicle2, and Vehicle5) can construct a connected VANET. Also, for Prefix 2, two vehicles (i.e., Vehicle3 and Vehicle6) can construct another connected VANET, and for Prefix 3, two vehicles (i.e., Vehicle4 and Vehicle7) can construct another connected VANET.

Update from -11 version

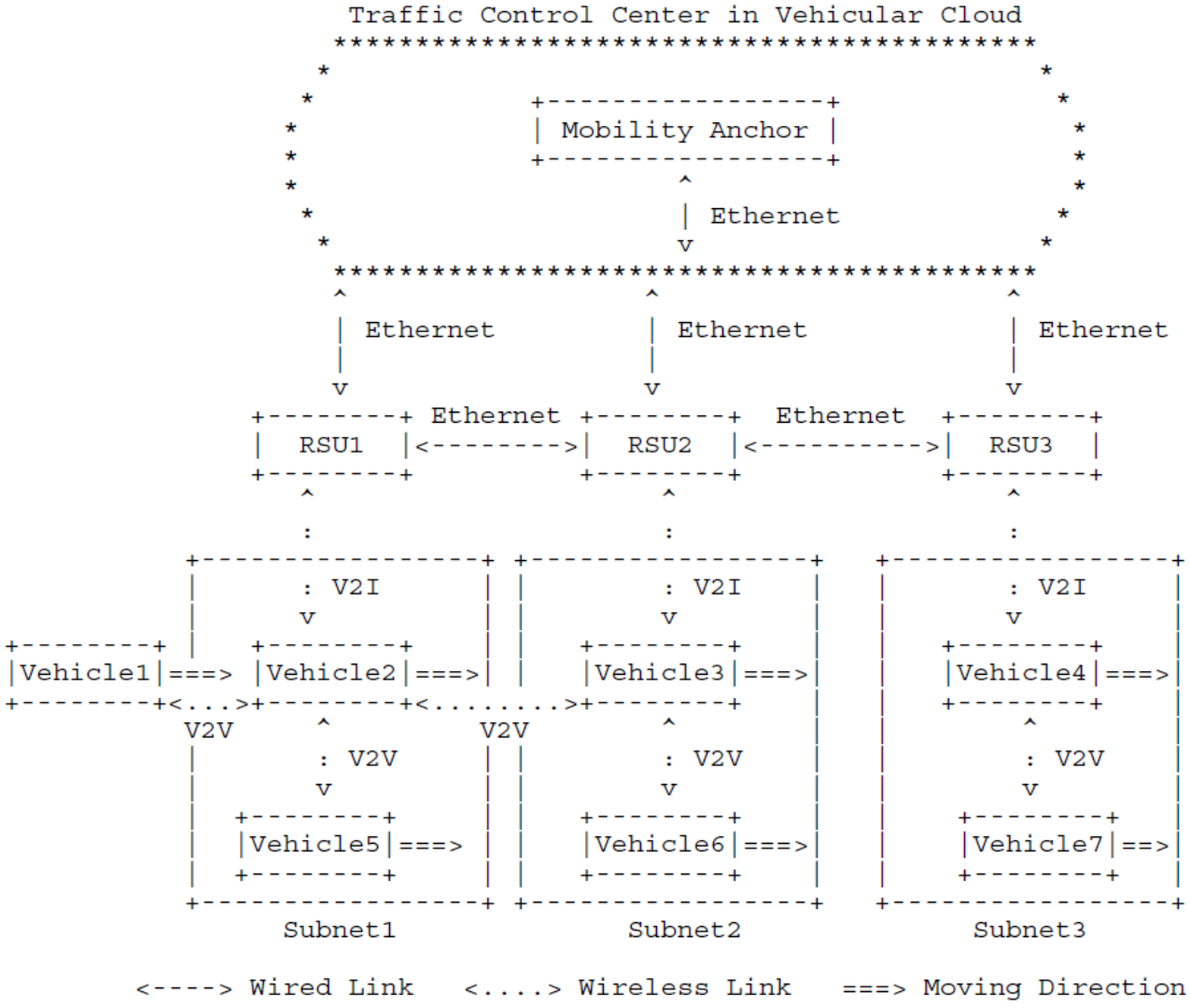


Figure 1: A Vehicular Network Architecture for V2I and V2V Networking

Update from -11 version

- Comments from C. Perkins
  - Section 5.1.1: Link Model
    - The vehicular link model for vehicular networks is clarified, considering “on-link” and “off-link” in subnet operation as follows.

A VANET can have multiple links between pairs of vehicles within wireless communication range, as shown in Figure 4.

……

When these two VANETs are converged into one VANET, the two vehicles can communicate with each other in a multihop fashion. A vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility. Therefore, the vehicular link model uses on-link prefix and off-link prefix according to the one-hop reachability among the vehicles. If the vehicles with the same prefix are reachable with each other in one hop, the prefix should be on-link. On the other hand, if some of the vehicles with the same prefix are not reachable with each other in one hop due to the multi-hop topology in the VANET, the prefix should be off-link.

Update from -11 version

- Comments from C. Perkins
  - Section 5.1: Neighbor Discovery
    - The merging and partitioning of VANETs.

The legacy DAD assumes that a node with an IPv6 address can reach any other node with the scope of its address at the time it claims its address, and can hear any future claim for that address by another party within the scope of its address for the duration of the address ownership. However, the partitioning and merging of VANETs makes this assumption frequently invalid in vehicular networks. The merging and partitioning of VANETs occurs frequently in vehicular networks. This merging and partitioning should be considered for the IPv6 Neighbor Discovery (e.g., SLAAC). Due to the merging of VANETs, two IPv6 addresses may conflict with each other though they were unique before the merging. Also, the partitioning of a VANET may make vehicles with the same prefix be physically unreachable. Also, SLAAC should be extended to prevent IPv6 address duplication due to the merging of VANETs. According to the merging and partitioning, a destination vehicle (as an IP host) should be distinguished as either an on-link host or off-link host even though the source vehicle uses the same prefix with the destination vehicle.

Update from -11 version

- Comments from C. Perkins
  - Section 5.1.1: MAC-Address-Pseudonym
    - A citation for Scrambler-Attack is added.

For the protection of drivers' privacy, a pseudonym of a MAC address of a vehicle's network interface should be used, so that the MAC address can be changed periodically. However, although such a pseudonym of a MAC address can protect some extent of privacy of a vehicle, it may not be able to resist attacks on vehicle identification by other fingerprint information, for example, the scrambler seed embedded in IEEE 802.11-OCB frames [Scrambler-Attack]. The pseudonym of a MAC address affects an IPv6 address based on the MAC address, and a transport-layer (e.g., TCP) session with an IPv6 address pair. However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.

Update from -11 version

- Comments from C. Perkins
  - Section 5.1.3: Prefix Dissemination/Exchange
    - removed Section 5.1.3 since this section discusses a solution.

Update from -11 version

- Comments from C. Perkins
  - **In section 5.1.4, it was not clear to me about why Neighbor Discovery really needs to be extended into being a routing protocol.**
  - Section 5.1.4: Routing
    - The motivation of merging the IPv6 Neighbor Discovery and a VANET routing protocol is the efficient wireless channel utilization described as follows.

Update from -11 version

- Comments from C. Perkins
  - **In section 5.1.4, it was not clear to me about why Neighbor Discovery really needs to be extended into being a routing protocol.**

The merging of the IPv6 Neighbor Discovery and a VANET routing protocol is the efficient wireless channel utilization. A routing protocol for VANET may cause redundant wireless frames in the air to check the neighborhood of each vehicle and compute the routing information in VANET with a dynamic network topology if the IPv6 ND is used to check the neighborhood of each vehicle, and can be extended to compute each vehicle's routing table in VANET.

Update from -11 version

- Comments from C. Perkins
  - **It seems to me that section 5.3 really belongs in section 6.**
  - The contents of Section 5.3 are moved to Section 6.

Update from -11 version

- Comments from C. Perkins
  - **Also, even a perfectly authorized and legitimate vehicle might be persuaded somehow to run malicious applications. I think that this point is not sufficiently covered in the current text.**

- This compromise of a perfectly authorized and legitimate vehicle is described as a security problem.

Update from -11 version

- Comments from Sandra Cespedes
  - I revised the definition of an RSU in Section 2 so that it can accommodate multiple routers (or switches) and servers (including DNS serv er and edge computing server) as an edge co mputing system because the RSU is regularly a router or switch as follows.

An RSU can accommodate multiple routers (or switches) and servers(e.g., D NS server and edge computing server) in its internal network as an edge co mputing system.

Update from -12 version

Comments from Carlos

Update from -12 version

- Comments from Carlos
  - **I think the title (and the text in many parts of the document) should be changed to refer to IPv6, instead of IP, as the document (and the WG) is IPv6 specific. Another example: we should not mention Mobile IPv4 in the document (as done currently in page 2).**

The title IP is changed into IPv6

Update from -12 version

- Comments from Carlos
  - **Page 4 (but also later in different parts of the doc): Mobility Anchor (MA): is this term coined somewhere you can reference? It is mentioned as a component of a vehicular architecture, but it is not discussed why, not even why an IPv6 mobility solution is needed in a vehicular scenario. It might seem like straightforward, but you need to present that need.**

Mobility Anchor (MA) is a new term even though it has mobility management functions like a Local Mobility Anchor (LMA) in Proxy Mobile IPv6.

Update from -12 version

- Comments from Carlos
  - **Page 4: the terms OBU and RSU should be aligned with what the basic OCB draft uses (IP-OBU and IP-RSU) and probably refer to that document. Besides I understand OBU and RSUs as single IP devices, not set of nodes as the document currently defines.**

IP-OBU and IP-RSU will replace OBU and RSU, respectively, according to the term definitions in the basic OCB draft.

Update from -12 version

- Comments from Carlos
  - **Page 5: V2I2P and V2I2V deserve additional explanation.**

The definitions of V2I2P and V2I2V will be clarified with additional explanation

Other Comments and Responses

- Refer to our revision letter to see Carlos' other comments and our responses.

- Welcome your feedback on our revision.

Next Steps

- **Enhancement of the Draft**
  - We will revise the PS document with Carlos' comments.
  - We will ask 5 reviewers to review the revised PS document before WGLC.

IPv6 Neighbor Discovery for IP-Based Vehicular Networks

(draft-jeong-ipwave-vehicular-neighbor-discovery-08)

IETF 106, Singapore

Nov 21, 2019

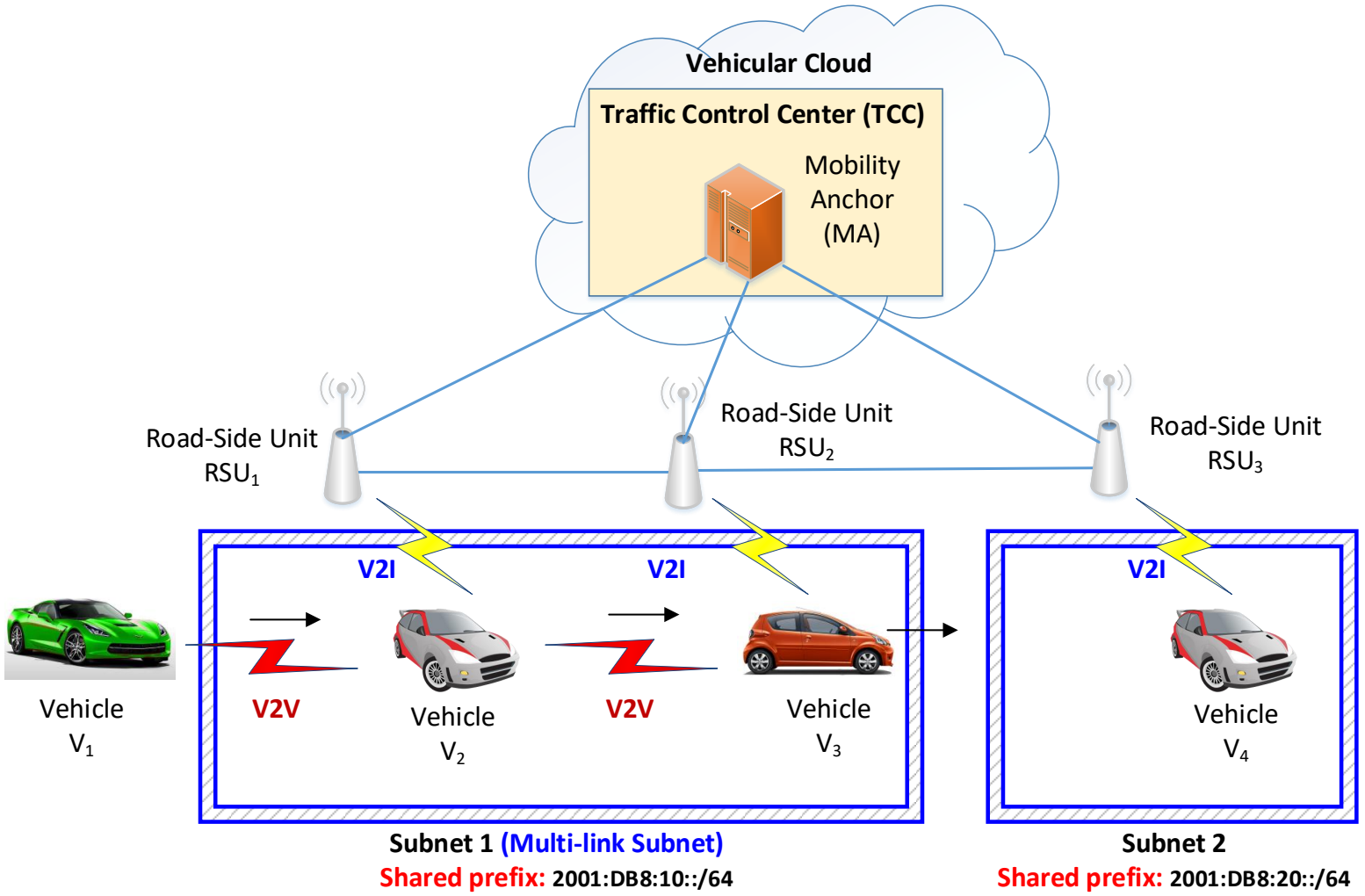
Jaehoon Paul Jeong, Yiwen Chris Shen [Presenter], and Zhong Xiang

Sungkyunkwan University

Introduction

- Motivation of Vehicular Neighbor Discovery (VND)
  - This is a candidate for IPv6 ND in IP-based vehicular networks according to IPWAVE Problem Statement Document [draft-ietf-ipwave-vehicular-networking-12]
- Subjects of This Draft
  - Definition of Link Model for Vehicular Wireless Link
  - ND Optimization with Multihop DAD
  - Multihop DAD and UDP/TCP Transmission via Intermediate Vehicles
  - MAC Address Pseudonym Handing with VND

Vehicular Network Architecture



Vehicular Network Architecture
for V2I and V2V Networking

Vehicular Neighbor Discovery (1/2)

- Infrastructure-Based Address Registration
  - It avoids multicast storm for energy and wireless channel conservation.
  - Vehicles create their Neighbor Cache Entry in a serving RSU to maintain registration.

- Multihop Duplicate Address Detection
  - It eliminates redundant address configuration when vehicles pass by RSUs belonging to the same multi-link subnet.
  - Neighbor Cache and DAD Table are maintained by each RSU and an MA, respectively.

Vehicular Neighbor Discovery (2/2)

- Prefix Discovery
  - It rapidly finds the prefix information of an internal network in a vehicle or an RSU.
  - Two nodes in two different internal networks can communicate with each other.

- Service Discovery
  - It rapidly finds the service information of an internal network in a vehicle or an RSU.
  - A client in an internal network can contact a required server in another internal network.

Update from -06, -07 Version

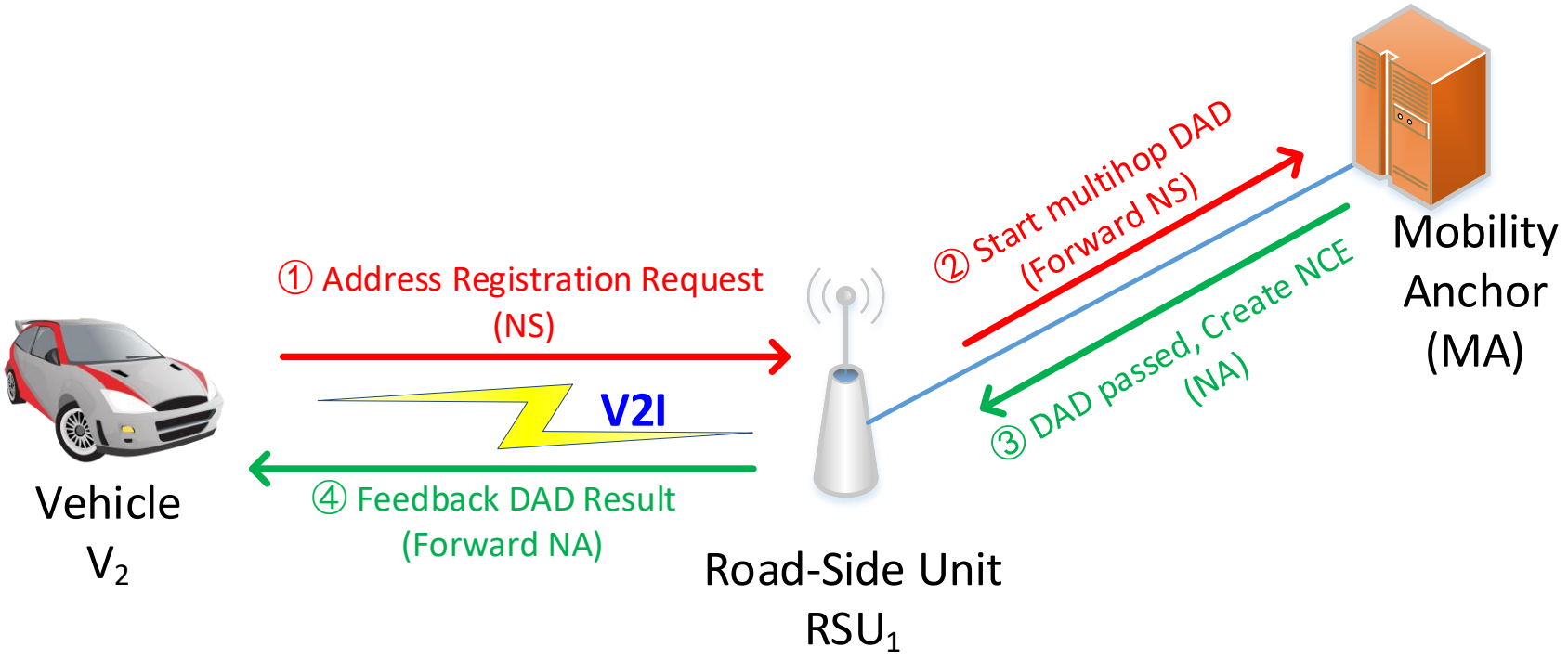
- Major Changes from -06, -07
  - The Mobility Management Section is removed and moved to draft-jeong-ipwave-vehicular-mobility-management-02.
  - Simplified message flows of DAD by removing the two new ICMPv6 message types such as Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC).
  - The V2I internetworking and V2V internetworking is removed from this version.
  - In Section 7.3, an arbitrary number of intermediate vehicles can be used between source vehicles and RSUs for the Address Registration along with multihop DAD.

Update from -06, -07 Version

- Major Changes from -06, -07:
  - In Section 7.3.2, a new waiting mechanism is defined to guarantee vehicles to find a neighbor vehicle (as a relay node) closest to an RSU in order to connect to the RSU.
  - In Section 7.3.3, a new routing mechanism is proposed to extend the IPv6 neighbor discovery protocol for routing among vehicles and RSUs. An example of Neighbor Routing Table is specialized to explain the routing service.

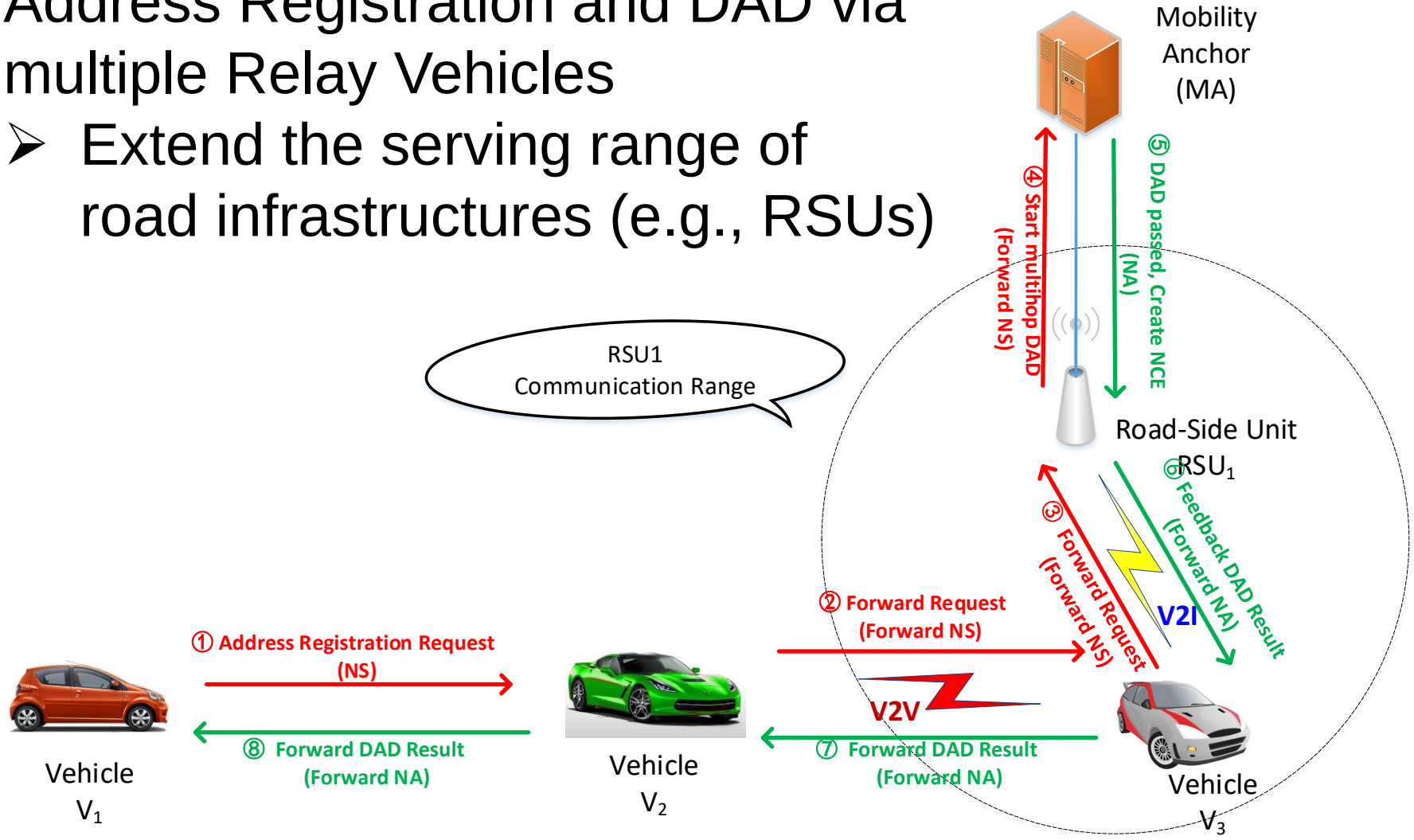
Extended Vehicular ND (1/3)

- Multihop DAD with Simplified Message Types



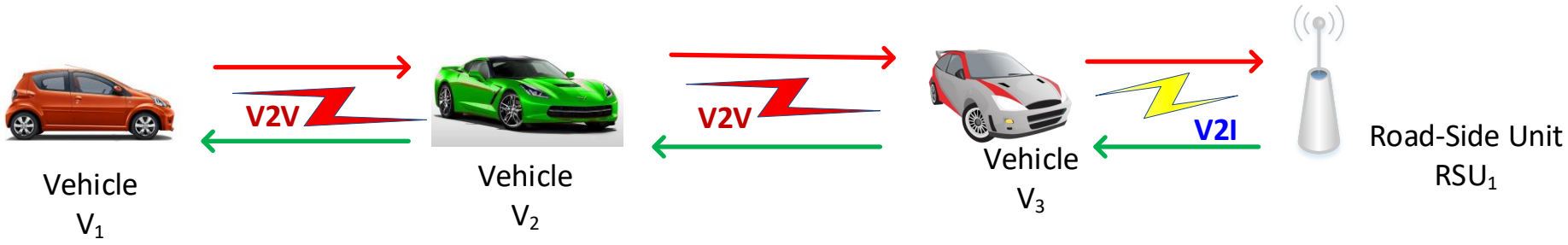
Extended Vehicular ND (2/3)

- Address Registration and DAD via multiple Relay Vehicles
  - ➢ Extend the serving range of road infrastructures (e.g., RSUs)



Extended Vehicular ND (3/3)

- New routing mechanism based on NCEs
  - ➢ Each relay vehicle records relay information (e.g., Vehicle address, next-hop address)



Node	NextHop
V_2	V_2

Node	NextHop
V_1	V_1
V_3	V_3

Node	NextHop
RSU_1	RSU_1
V_2	V_2
V_1	V_2

Node	NextHop
V_3	V_1
V_2	V_1
V_1	V_1

Next Steps

- **WG Adoption Call**
  - This Vehicular ND draft is a candidate for IPv6 ND in IP-based vehicular networks according to IPWAVE Problem Statement Document:
    - [draft-ietf-ipwave-vehicular-networking-12]

- **Proof-of-Concept**
  - We proved the concept of Vehicular ND and implemented in a vehicular network simulator (OMNeT++, VEINS, and SUMO).

Vehicular Mobility Management for IP-Based Vehicular Networks

(draft-jeong-ipwave-vehicular-mobility-management-02)

IETF 106, Singapore

Nov 21, 2019

Jaehoon (Paul) Jeong, Yiwen (Chris) Shen [Presenter], and Zhong Xiang

Sungkyunkwan University

Motivation

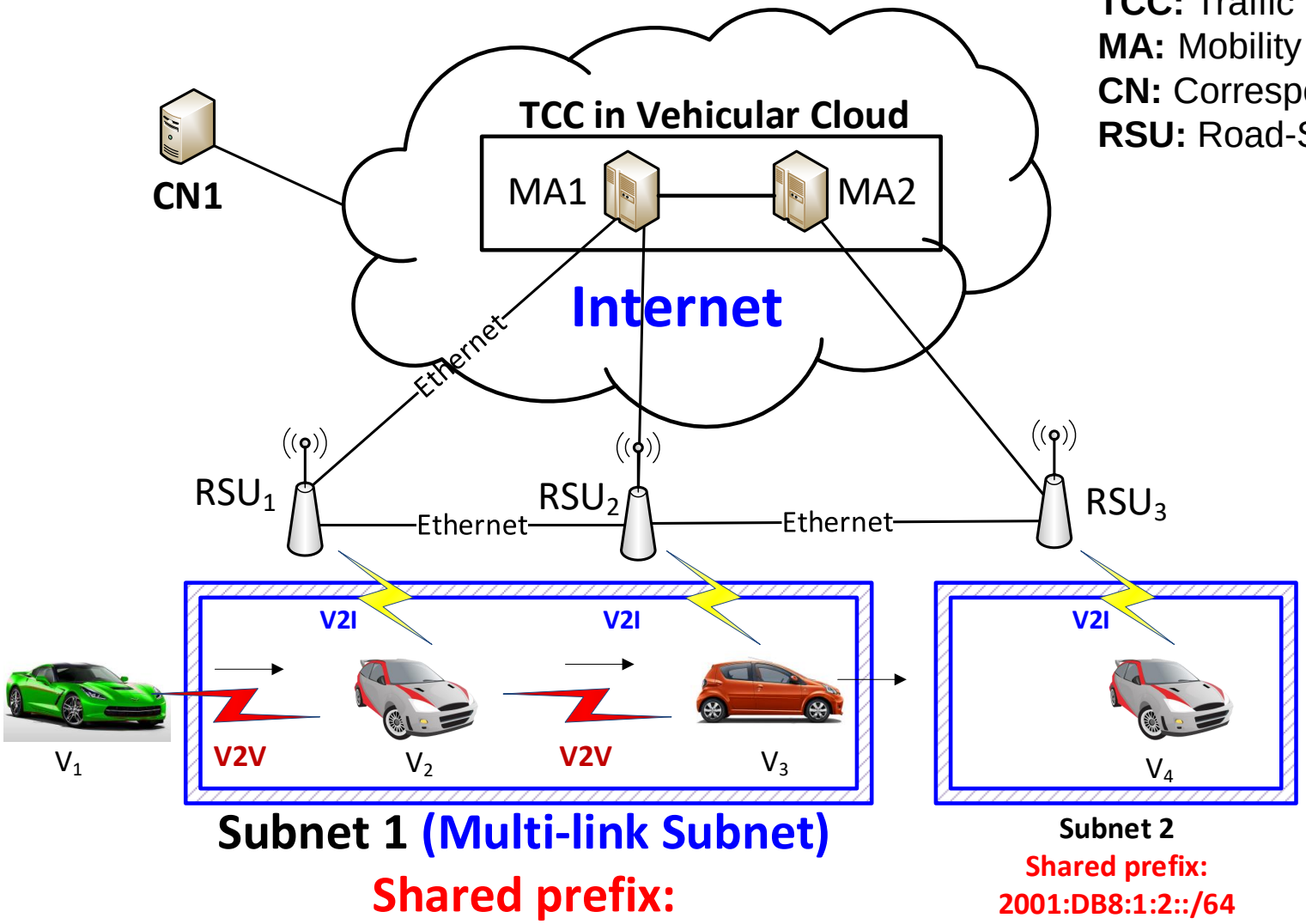
- Purposes of This Draft
  - A Key Work Item in IPWAVE Problem Statement
    - Vehicular Neighbor Discovery
      - draft-jeong-ipwave-vehicular-neighbor-discovery-08
    - **Vehicular Mobility Management**
      - draft-jeong-ipwave-vehicular-mobility-management-02
    - Vehicular Context-Aware Navigator
      - draft-jeong-ipwave-context-aware-navigator-00
    - Vehicular Security and Privacy
      - draft-jeong-ipwave-security-privacy-00
  - Shedding Light on Vehicular Mobility Management
    - IPWAVE WG can have a more concrete idea on mobility management for vehicular networks.
    - We can have clear requirements and design principles.

Update from -01 Version

- Major Changes from -01
  - In Section 4, the description of the vehicular network architecture is revised with easily identifiable expressions to remove ambiguity.
  - In Section 5.1, the Shared-Prefix model is clarified to support the definition of subnet.
  - In Section 5.2, the description on the switch of end-point of the bi-directional tunnel is revised.

Vehicular Network Architecture

TCC: Traffic Control Center
MA: Mobility Anchor
CN: Corresponding Node
RSU: Road-Side Unit



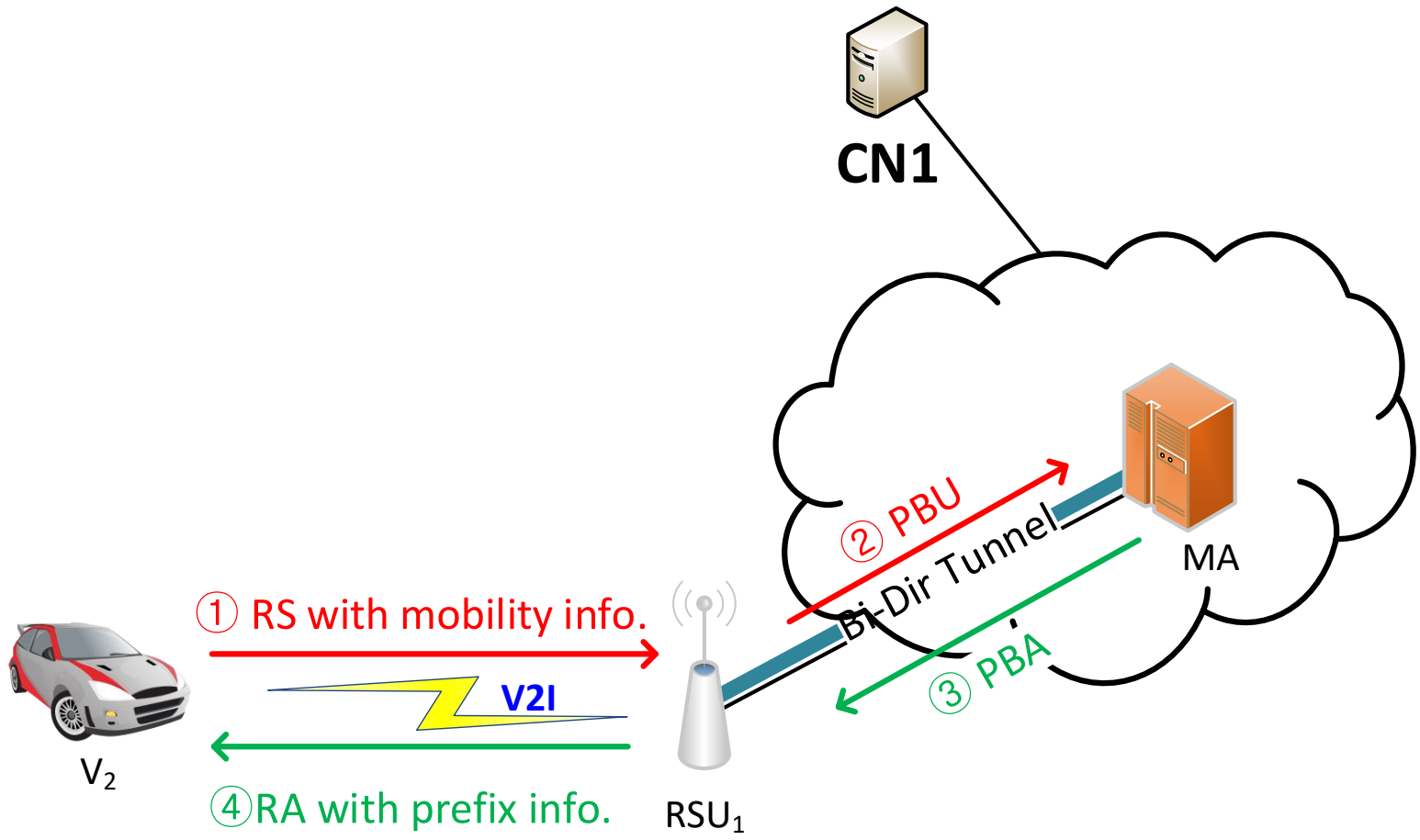
Requirements of Mobility Management

- Sharing a Single Prefix per Multi-link Subnet (i.e., Prefix Domain)
  - IP Address Registration through Multihop DAD [draft-jeong-ipwave-vehicular-neighbor-discovery-08]
- Seamless Handoff by Network-Based Mobility Management (MM)
  - MM based on Proxy MIPv6 (PMIPv6)
  - MM based on Distributed MM (DMM)
- Handoff between Multiple Prefix Domains
  - Connectivity Support with the Corresponding Node via V2I
  - Ad Hoc Networking Support with Neighboring Vehicles via V2V

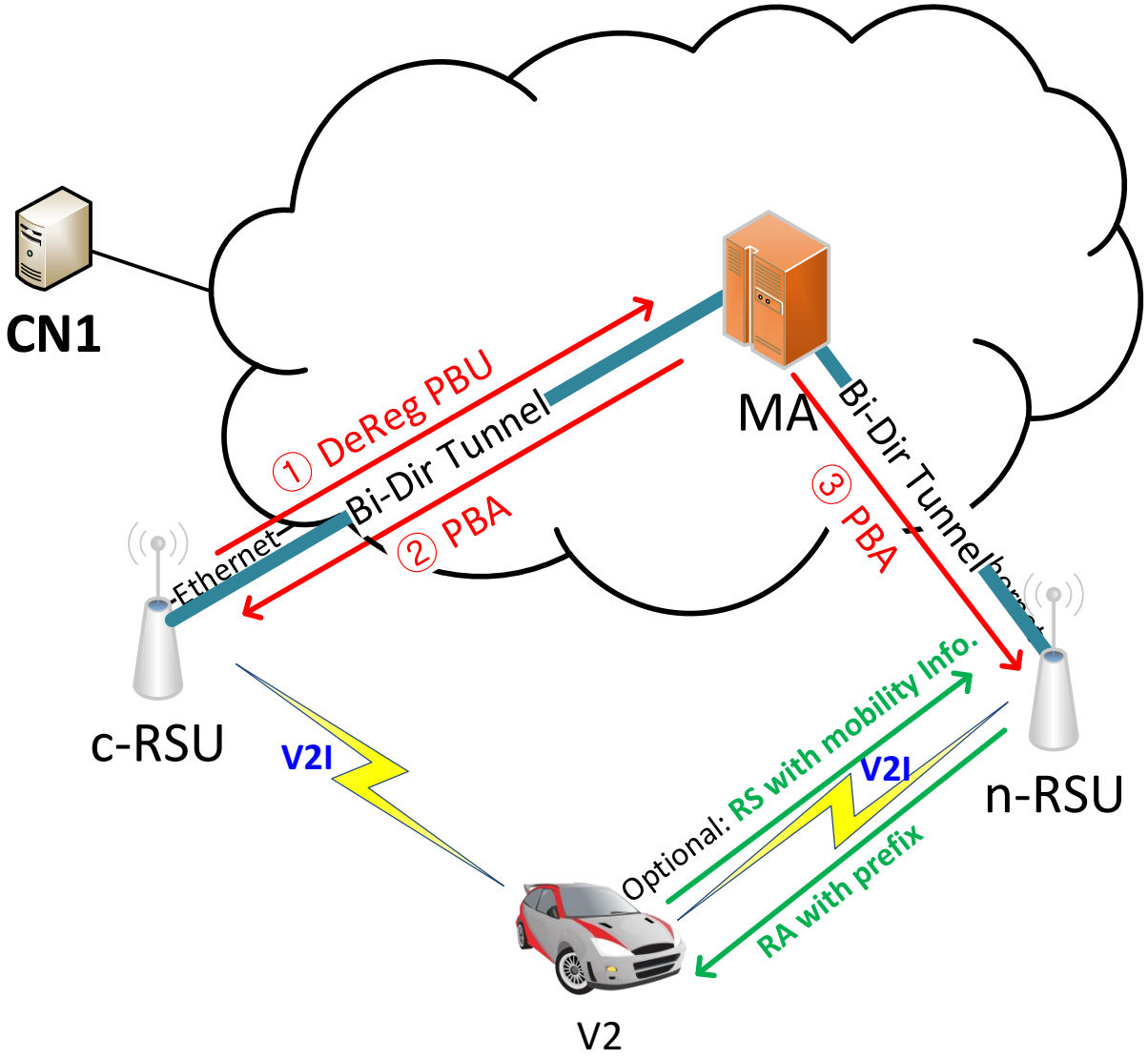
Design Principles

- **Key Ideas of Mobility Management**
  - **Proactive Mobility Management**
    - It performs handoff in advance along a vehicle's movement.
    - It uses a vehicle's mobility information (e.g., speed, direction, and position) and trajectory information (i.e., navigation path).
    - It uses L2 information (e.g., Received Channel Power Indicator (RCPI)) for movement detection.
  - **Network-Based Mobility Management**
    - Network infrastructure (e.g., RSUs and MAs) performs handoff transparent to vehicles.

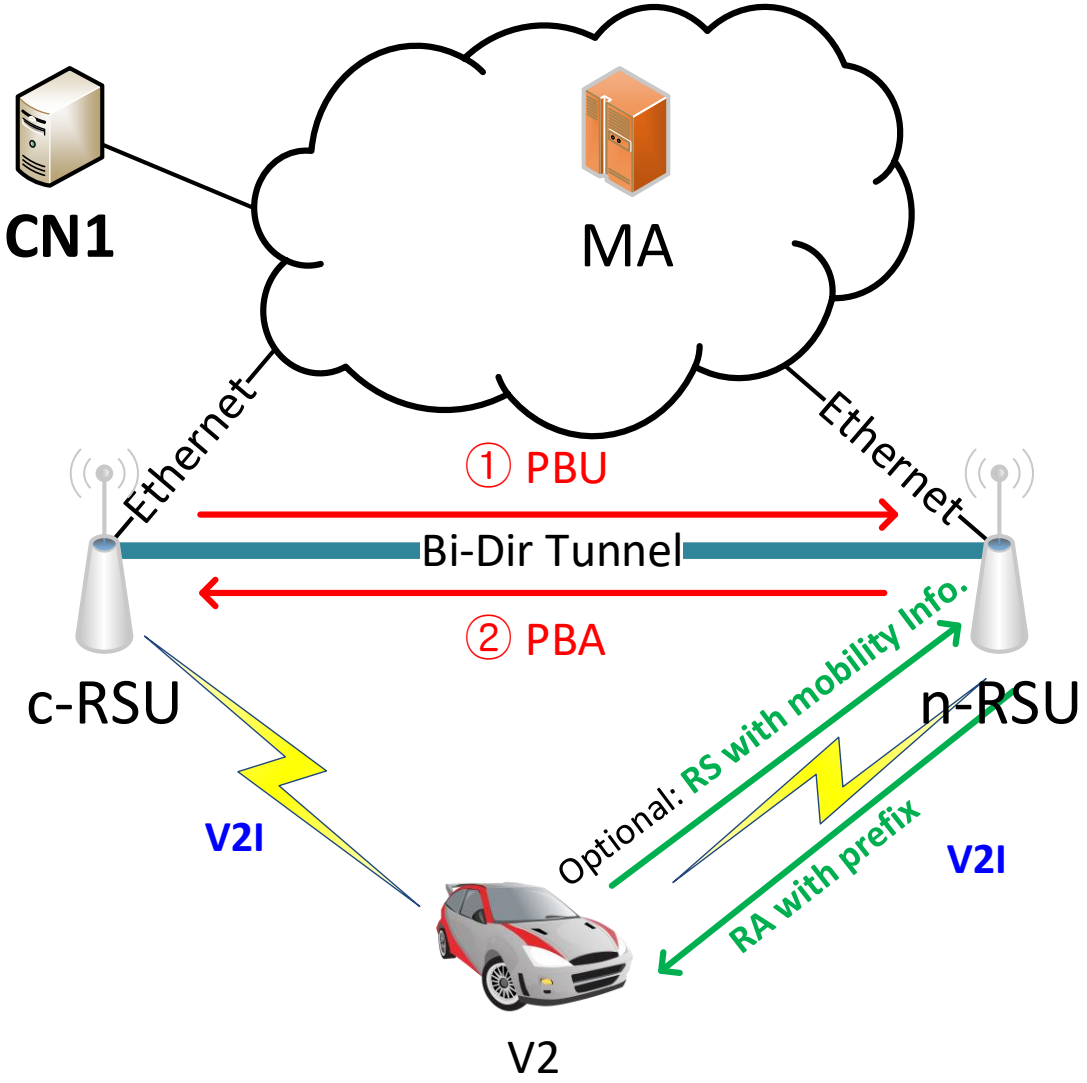
Network Attachment and IP Address Registration



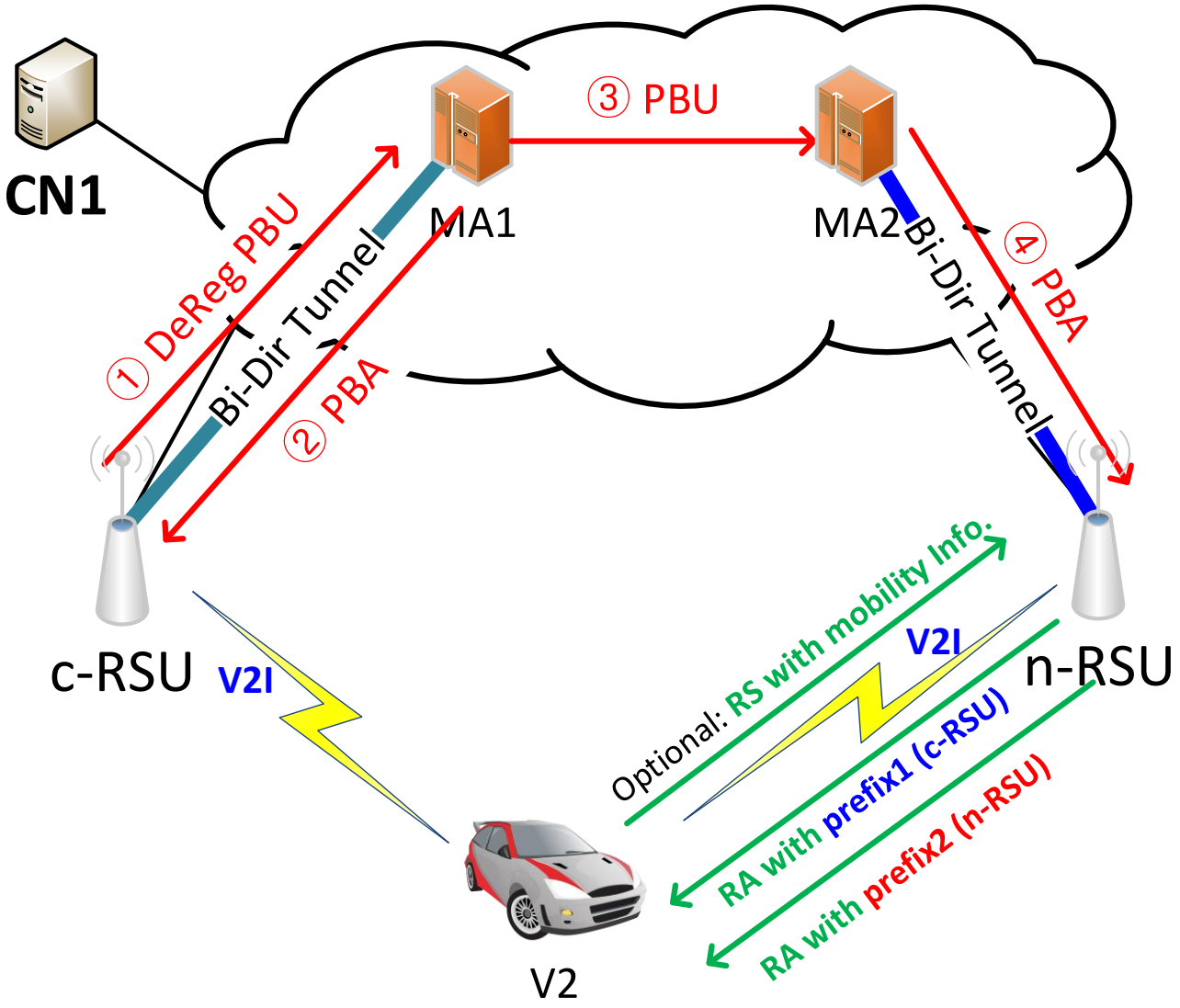
Handoff within a Multi-link Subnet through PMIPv6



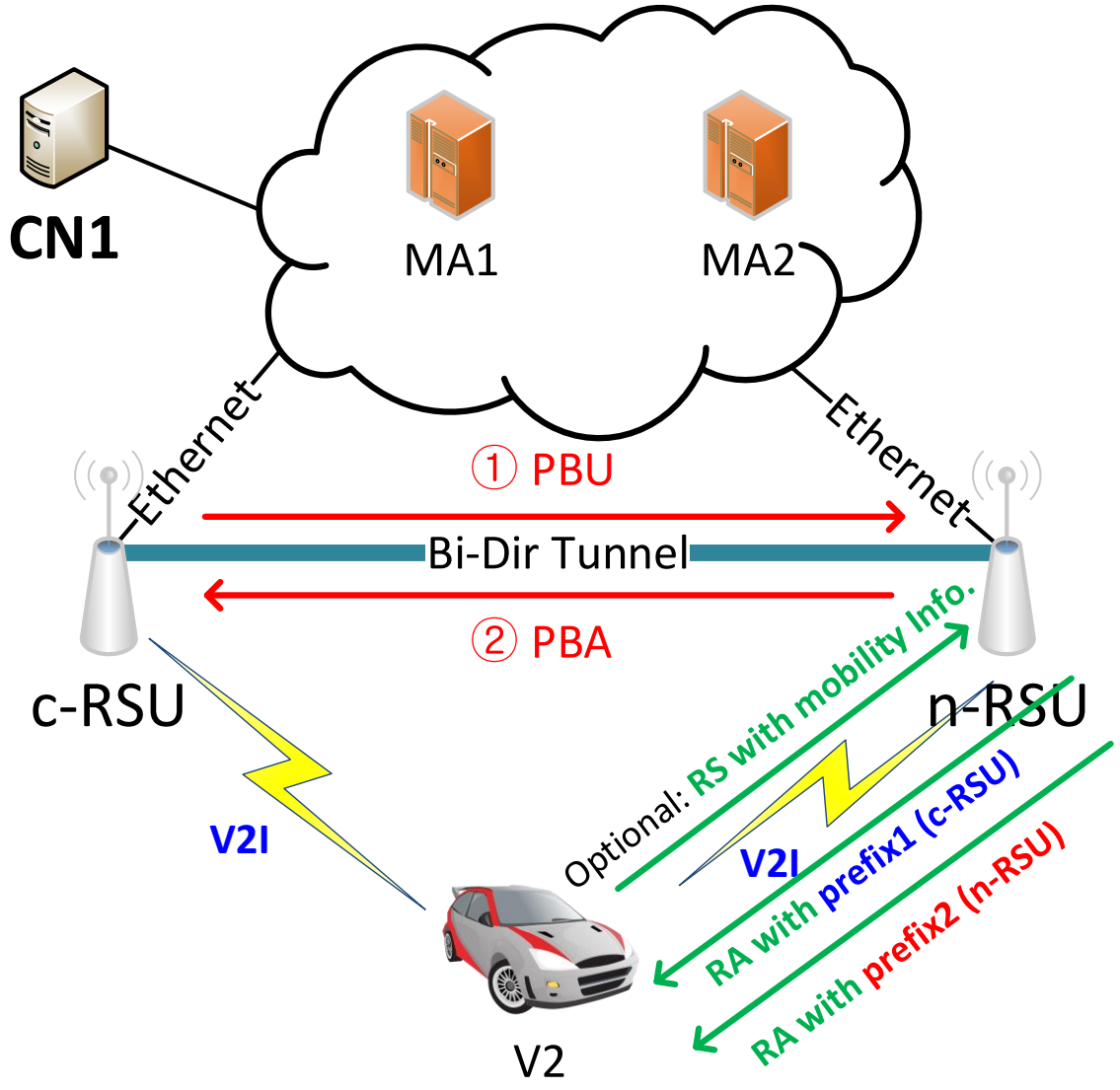
Handoff within a Multi-link Subnet through DMM



Handoff between Multi-link Subnets through PMIPv6



Handoff between Multi-link Subnets through DMM



Next Steps

- **Enhancement of the Draft**
  - We will enhance this draft through the consensus of IPWAVE WG.
  - It will can be used to clarify IPWAVE PS document.

- **Proof-of-Concept**
  - We will implement Vehicular Mobility Management (VMM) in realistic simulations.
    - Vehicular network simulator is based on OMNeT++, VEINS, and SUMO.
  - We have a plan to participate in IETF-107 Hackathon Project (IPWAVE VMM Project).

Basic Support for Security and Privacy in IP-Based Vehicular Networks

(draft-jeong-ipwave-security-privacy-00)

IETF 106, Singapore

Nov 21, 2019

Jaehoon (Paul) Jeong [Editor], Yiwen (Chris) Shen, and Jung-Soo Park

Introduction (1/2)

- Vehicles can construct Vehicular Ad Hoc Networks (VANET) by themselves without any infrastructure node such as a Road-Side Unit (RSU).

- CACC and Autonomous Driving services can use this vehicular networking for safe driving with vehicles.

Introduction (2/2)

- In vehicular networks, the information exchange among vehicles are critical to the safety of vehicles for vehicle maneuvers.

- Thus, identifying potential loopholes in the IP-based vehicular networks becomes crucial.

Security Attacks

- False Information Attack
- Impersonation Attack
- Denial-of-Service Attack
- Message Suspension Attack
- Tampering Attack
- Tracking

False Information Attack

- Malicious vehicles may intentionally disseminate false driving information (e.g., location, speed, and direction) to let the driving of other vehicles be unsafe and then other vehicles meet accidents.
- In vehicular networks, a malicious vehicle can create multiple virtual bogus vehicles, and generate global IPv6 addresses and register them with a Mobility Anchor (MA) via an RSU.
- This IP address autoconfiguration makes the RSU and MA waste their computation power and storage resources for IP address autoconfiguration and mobility management.
- Thus, the RSU and MA need to determine whether a vehicle is genuine or bogus in the IP address autoconfiguration and mobility management.

Impersonation Attack

- Malicious vehicles can pretend to be other vehicles with forged IP addresses or MAC address as IP address spoofing and MAC address spoofing, respectively.

- To detect such an impersonation attack, an authentication scheme needs to check whether the MAC address and IPv6 address of a vehicle is associated with the vehicle's permanent identifier (e.g., a driver's certificate identifier) or not.

Denial-of-Service Attack

- Malicious vehicles (or compromised vehicles) can generate bogus services requests to either a vehicle or a server in the vehicular cloud so that either the vehicle or the server is extremely busy with the requests, and cannot process valid request in a prompt way. This attack is called Denial-of-Service (DoS) attack.

- For example, in the IPv6 ND for vehicular networks, the vehicular-network-wide DAD can be performed via an RSU and a MA to guarantee that the IPv6 address of a vehicle's wireless interface is unique in the vehicular network. The ND packets for the DAD process are forwarded to other vehicles, an RSU, and an MA.

- To detect and mitigate this DoS attack, the vehicles need to collaborate with each other to monitor a suspicious activity related to the DoS attack, that is, the generation of messages more than the expected threshold in a certain service.

Message Suspension Attack

- Malicious vehicles can drop packets originated by other vehicles in multihop V2V or V2I communications, which is called a Message Suspension Attack.
- This packet dropping can hinder the data exchange for safe driving in cooperative driving environments. Also, in multi-hop V2V or V2I communications, this packet dropping can interfere with the reliable data forwarding among the communicating entities (e.g., vehicle, client, and server).
- For the reliable data transfer, a vehicle performing the message suspension attack needs to be detected by good vehicles and a good RSU, and it should be excluded in vehicular communications.

Tampering Attack

- An authorized and legitimate vehicle may be compromised by a hacker so that it can run a malicious firmware or software (malware), which is called a tampering attack.
- This tampering attack may endanger the vehicle's computing system, steal the vehicle's information, and track the vehicle. Also, such a malware can generate bogus data traffic for DoS attack against other vehicles, and track other vehicles, and collect other vehicles' information.
- The forgery of firmware or software in a vehicle needs to be protected against hackers. The forgery prevention of firmware such as the bootloader of a vehicle's computing system can be performed by a secure booting scheme.
- The safe update of the firmware can be performed by a secure firmware update protocol. The abnormal behaviors by the forgery of firmware or software can be monitored by a remote attestation scheme.

Tracking

- The MAC address and IPv6 address of a vehicle's wireless interface can be used as an identifier.
- An hacker can track a moving vehicle by collecting and tracing the data traffic related to the MAC address or IPv6 address.
- To avoid the illegal tracking by a hacker, the MAC address and IPv6 address of a vehicle need to be periodically updated.
- However, the change of those addresses needs to minimize the impact of ongoing sessions on performance.

Countermeasures

- Identification and Authentication
- Integrity and Confidentiality
- Non-Repudiation
- Remote Attestation
- Privacy

Identification and Authentication

- Good vehicles are ones having valid certificates (e.g., X.509 certificate), which can be validated by an authentication method through an authentication server [RFC5280].
- Along with an X.509 certificate, a Vehicle Identification Number (VIN) can be used as a vehicle's identifier to efficiently authenticate the vehicle and its driver through a road infrastructure node (e.g., RSU and MA), which is connected to an authentication server in vehicular cloud.
- X.509 certificates can be used as Transport Layer Security (TLS) certificates for the mutual authentication of a TCP connection between two vehicles or between a vehicle and a corresponding node (e.g., client and server) in the Internet.
- Good vehicles can also use a Decentralized Identifier (DID) with the help of a verifiable claim service. In this case, vehicles can use their DID as a unique identifier, and then check the identity of any joining vehicle with its verifiable claim.

Integrity and Confidentiality

- For secure V2I or V2V communications, a secure channel between two communicating entities (e.g., vehicle, RSU, client, and server) needs to be used to check the integrity of packets exchanged between them and support their confidentiality.
- For this secure channel, a pair of session keys between two entities (e.g., vehicle, RSU, MA, client, and server) needs to be set up.
- For the establishment of the session keys in V2V or V2I communications, an Internet Key Exchange Protocol version 2 (IKEv2) can be used [RFC7296].
- Also, for the session key generation, either an RSU or an MA can play a role of a Software-Defined Networking (SDN) Controller to make a pair of session keys and other session parameters (e.g., a hash algorithm and an encryption algorithm) between two communicating entities in vehicular networks [ID-SDN-IPsec].

Non-Repudiation

- In the case of the occurrence of an accident, it is important to localize and identify the criminal vehicle with a non-repudiation method through the logged data during the navigation of vehicles.

- For non-repudiation, the messages generated by a vehicle can be logged by its neighboring vehicles.
- As an effective non-repudiation, a blockchain technology can be used. Each message can be treated as a transaction and the adjacent vehicles can play a role of peers in consensus methods such as Proof of Work (PoW) and Proof of Stake (PoS) [Bitcoin].

Remote Attestation (1/2)

- To prevent a tampering attack by the forgery of firmware/software, a secure booting can be performed by Root of Trust (RoT) and a remote attestation can be performed through both the secure booting and RoT [ID-NSF-Remote-Attestation][ID-Remote-Attestation-Arch].

- The secure booting can make sure that the bootloader of the vehicle's computing system is a legitimate one with the digital signature of the boofloader by using the RoT of Trusted Platform Module (TPM) [ISO-IEC-TPM] or Google Titan Chip [Google-Titan-Chip].

Remote Attestation (2/2)

- A firmware update service can be made in blockchain technologies [Vehicular-BlockChain]. The validity of a brand-new firmware can be proven by a blockchain of the firmware, having the version history. Thus, This blockchain can manage a brand-new firmware or software and distribute it in a secure way.

- The remote attestation can monitor the behaviors of the vehicle's computing system such that the system is working correctly according to the policy and configuration of an administrator or user [ID-NSF-Remote-Attestation][ID-Remote-Attestation-Arch]. For this remote attestation, a secure channel should be established between a verifier and a vehicle.

Privacy (1/2)

- To avoid the tracking of a vehicle with its MAC address, a MAC address pseudonym can be used, which updates the MAC address periodically. This update triggers the update of the vehicle's IPv6 address because the IPv6 address of a network interface is generated with the interface's MAC address. The MAC address and IPv6 address can be updated by the guideline in [RFC4086] and a method in [RFC4941], respectively.

- The update of the MAC address and the IPv6 address affects the on-going traffic flow because the source node or destination node of the packets of the flow are identified with the node's MAC address and IPv6 address. This update on a vehicle requires the update of the neighbor caches of the vehicle's neighboring vehicles, and the neighbor tables of an RSU, and an MA in multihop V2I communications.

Privacy (2/2)

- Without strong confidentiality, the update of the MAC address and IPv6 address can be observed by an adversary, so there is no privacy benefit in tracking prevention. The update needs to be notified to only the trustworthy vehicles, RSU, and MA.

- Also, for the continuity of an end-to-end (E2E) transport-layer (e.g., TCP, UDP, and SCTP) session, the new IP address for the transport-layer session can be notified to an appropriate end point through a mobility management scheme such as Mobile IP Protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275] and Proxy MIPv6 (PMIPv6) [RFC5213]). This mobility management overhead and impact of pseudonyms should be minimized on the performance of vehicular networking.

Next Steps

- **Enhancement of the Draft**
  - We will enhance this draft through the consensus of IPWAVE WG.
  - It will can be used to clarify IPWAVE PS document.

- **Proof-of-Concept**
  - We will design and implement the framework for IPWAVE security and privacy in the future Hackathon.

I E T F®

Context-Aware Navigator Protocol for IP-Based Vehicular Networks

(draft-jeong-ipwave-context-aware-navigator-00)

IETF 106, Singapore

November 21, 2019

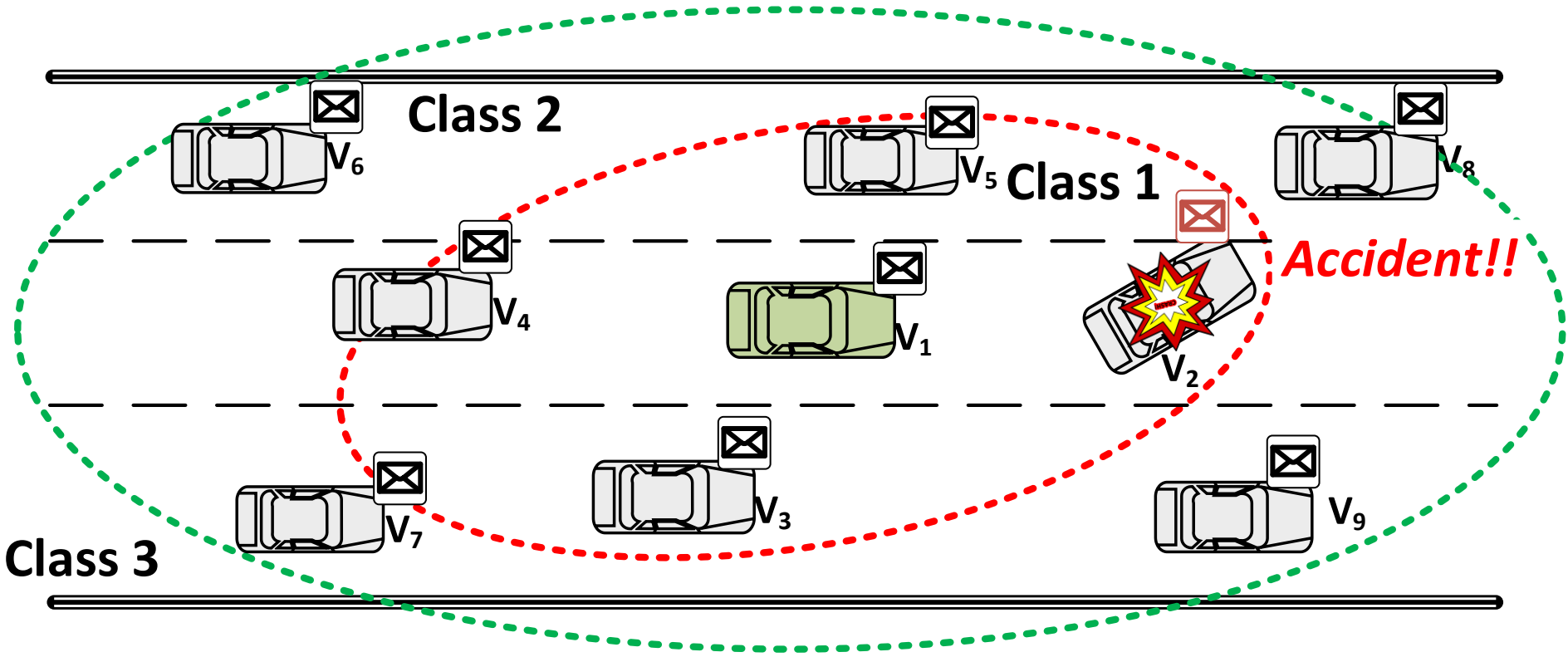
Jaehoon Paul Jeong, Bien Aime Mugabarigira, Zhong Xiang and Yiwen Chris Shen [Presenter], Sungkyunkwan University

Introduction

- CAN Protocol for IP-Based Vehicular Network Motivation
  - Use case of IPWAVE Problem Statement Document [draft-ietf-ipwave-vehicular-networking-10]

- Subjects of This Draft
  - Support the light-weight message exchange for vehicle safety
  - Two-type message:
    - Awareness: Cooperative Context Message (CCM)
    - Emergency context: Emergency Context Message (ECM)

Context Awareness in IP-Based Vehicular Networks



CAM

ECM

Context Awareness in IP based Network

Via lightweight messages

Context aware Messages (CAM)

Emergency Context Message (ECM)

Cooperative Navigation Among Vehicles

- Sensor Equipped Vehicle
  - Mobility information
    - Position
    - Speed
    - Acceleration
    - Direction
- Information Sharing
  - Light-weight message
    - Assess collision Risk
    - Maneuver change
    - Avoid accident

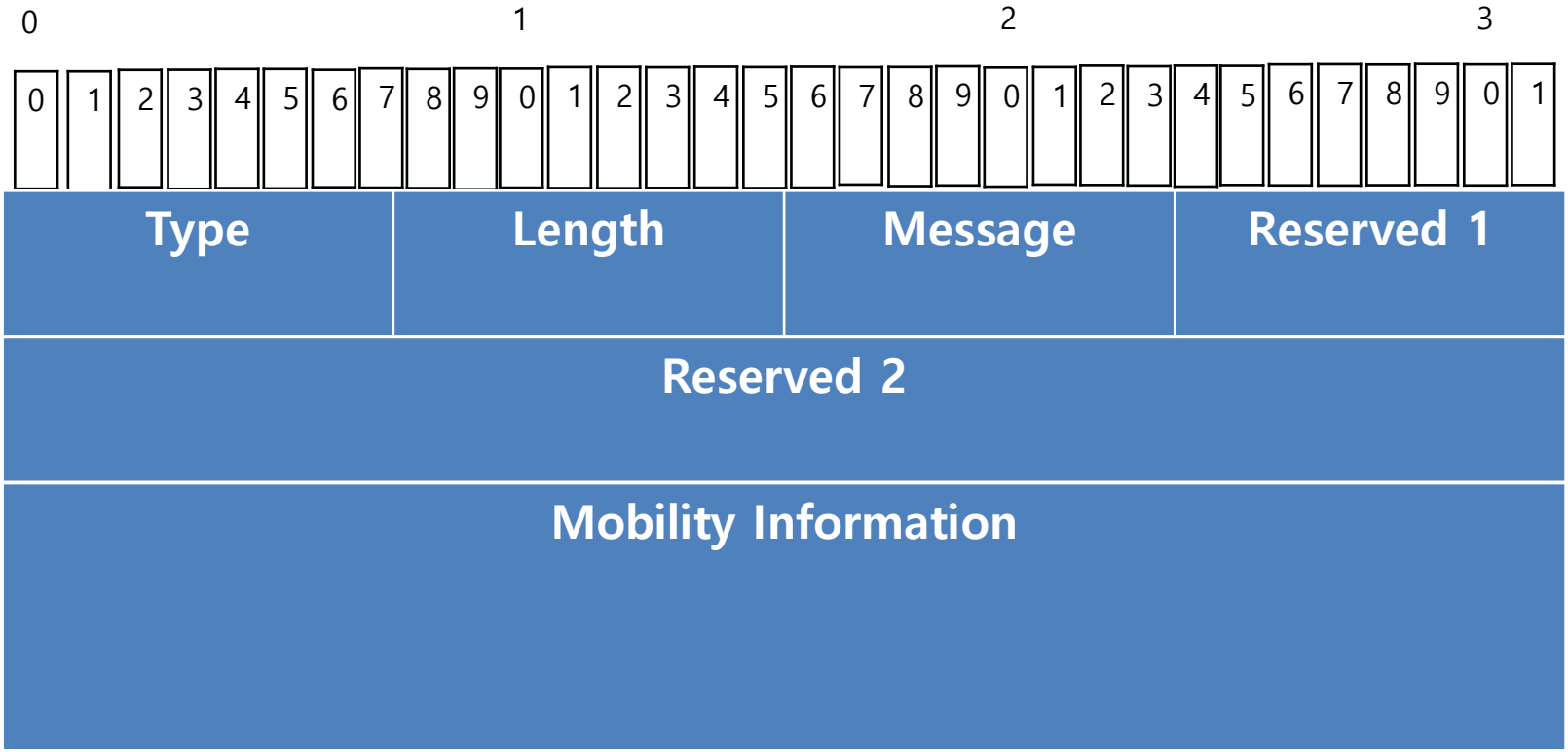
Emergency Context-Awareness and response

- Cooperative Context Message (CCM)
  - Deliver a vehicle's motion information
    - Position, Speed, Acceleration/Deceleration, direction
    - Diver's action (e.g., braking and accelerating)

- Emergency Context Message (ECM)
  - Emergency situation notification
    - Accident, dangerous situation
  - ECM has higher priority over CCM

Vehicle Mobility Information (1/3)

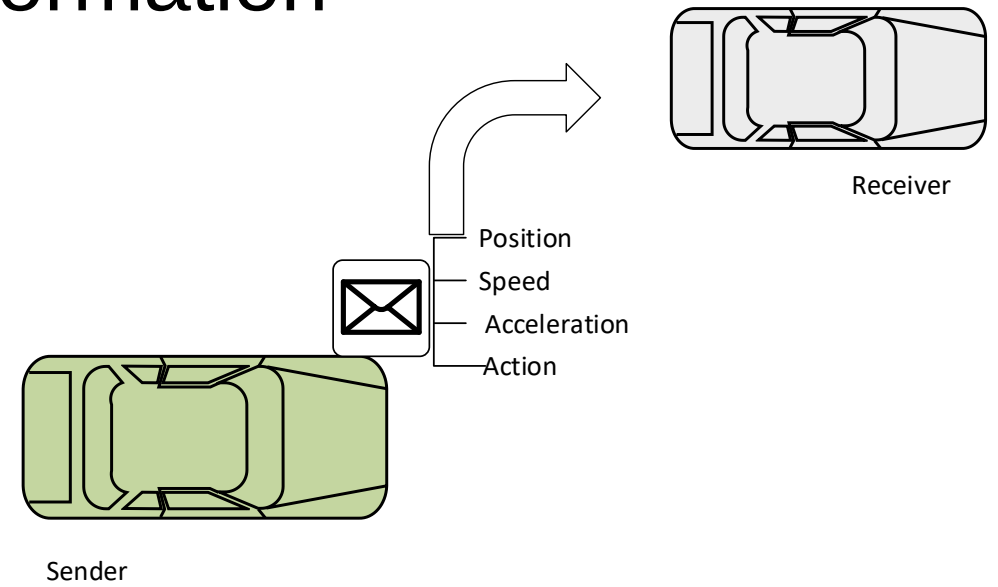
- VMI options:



- Type
  - Either: CCM and ECM

Vehicle Mobility Information (2/3)

- Vehicle Motion Information
  - Position
  - Speed
  - Acceleration
  - Driver action



- Vehicle Emergency Information
  - Obstacle Information
  - Accident Information

Vehicle Mobility Information (3/3)

- CCM
  - Included in an NA message that a vehicle transmits **periodically** to announce its existence and routing information to its one-hop neighboring vehicles
- ECM
  - Included in an NA message that a vehicle transmits to **immediately** announce an emergency situation to its one-hop neighboring vehicles
- ECM has a higher priority than the CCM
  - If a vehicle has an ECM and a CCM to send, it SHOULD transmit the ECM earlier than the CCM.

Next Steps

- **Welcome your input and feedback for IPWAVE-based applications.**
  - Context-aware navigator is one of them.

Action Items for IPWAVE WG

Action Items

- **Completion of IPWAVE PS document**
  - WGLC before IETF-107 meeting;
- **Invitation of automotive people**
  - We will invite Hyundai Motors to present their IPWAVE-related implementation and demonstration at IETF-107 IPWAVE WG meeting.
- **Preparation for IPWAVE WG Rechartering**
  - After IPWAVE PS document is approved as an informational RFC by IESG, we will start to discuss IPWAVE WG rechartering.