Transmission of IPv6 Packets over IEEE 802.11-OCB Networks
draft-haerri-ipv6-over-80211OCB-00

IETF 96, Berlin, Germany
July 21, 2016

Jérôme Härrri*, Alex Petrescu, Christian Huitema
*Editor E-mail Address: haerri@eurecom.fr
Introduction to 802.11-OCB (a.k.a. DSRC)

- **Scenario:**
  - IPv6 is for non-safety related traffic ONLY (according to the ITS charter)
  - Single hop IPv6 communication – Multi-hop is in MANET (according to ITS charter)
  - Vehicles contain one or multiple IPv6 ‘things’
  - Vehicles are not specifically connected to Internet (or only episodically)
  - IPv6 stack may co-exist with non-IP stack…or not
    - some ‘things’ may only have an IPv6 stack
  - **For Cars:** Any car with its engine turned ‘on’ and participating to traffic MUST transmit non-IP traffic on ch. 178 (US)/ch. 180 (EU).
    - IPv6 traffic may co-exist but shall not break any non-IP mechanism or generate any interference with non-IP traffic

---

<table>
<thead>
<tr>
<th>Classic 802.11 WLAN</th>
<th>IEEE 802.11p – aka IEEE 802.11-2012 OCB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronizing</td>
<td>OPTIONAL HIGHER LAYER Synchronization</td>
</tr>
<tr>
<td>Scanning</td>
<td>NO Scanning</td>
</tr>
<tr>
<td>Authentication</td>
<td>HIGHER LAYER Authentication</td>
</tr>
<tr>
<td>Association</td>
<td>IMPLICIT Association</td>
</tr>
<tr>
<td>Communication</td>
<td>DIRECT Communication</td>
</tr>
</tbody>
</table>

Concept of Basic Service Sets (BSS)

“Communication outside of the context of the BSS”
Challenges (some of them…)

- IPv6 over WiFi OCB:
  - Scanning
    - How can we dynamically ‘find’ a channel
      - CCH (ch. 178 US, ch. 180 EU) forbidden for IPV6
      - Need service announcement on a ‘well-known’ channel!
  - Security
    - If an RSU is connected to Internet, what is forbidding me to hacking into the Internet?
    - For OBUs or other RSUs: how can we be sure that the one claiming to transmit is truly the transmitter?
  - WiFi OCB link:
    - Link asymmetry (Tx power, antenna heights): how can IPv6 and IPv6-related mechanisms adapt to asymmetric IPv6 links (non-reflective & non transitive) ?
      - E.g.: IPv6 ND (e.g. 6lowPAN ND: RFC 6775)
  - IP addressing & Privacy:
    - How can I generate my IPv6 address ? DaD not fully working…(RFC4429 an option..)
    - How can I generate my IPv6 ‘temporary/optimistic’ address?
      - How can IPv6 mechanisms softly handle spontaneous change of IPv6 addresses (including routers)? IETF WG DMM/MIP?
    - Privacy:
      - IPv6 prefix shall not reflect my true subnetwork, not allow anybody to trace me back to my home network
        » IPv6 Link Local address required, when not connected to DHCPv6
      - NIC/MAC shall not reflect my true ID: need NIC/MAC pseudonyms
Security in 802.11-OCB Systems - Asymmetric Cryptography

- In order to initiate the system, a set of public/private keys needs to be obtained.

- Who generates these keys?
  - A Certifying Authority / PKI third party

- Vehicles are „pre-loaded“ with a set of public/private key
  - Similar to registering a vehicle and getting a license plate
  - For anonymity, vehicles receive a „pool“ of public/private keys
Authentication in 802.11-OCB systems: Elliptic Curve Digital Signature Algorithm (ECDSA)

- Signing a hash version of the message is more efficient than signing the message itself
  - The crypto-hash algorithm is SHA-256
Encryption in 802.11-OCB systems - Elliptic Curve Integrated Encryption Scheme (ECIES)

• Encrypting each message using an asymmetric cipher is computationally too expensive
  ▪ Use the property of shared secret from asymmetric cryptography
    • Bob combines his private key with Alice's public key
    • Alice combines her private key with Bob's public key

• Extract an Encryption and a MAC key from the shared secret
Exchanging Security Credentials

- Example: Authentication and Integrity
  - Single Hop Communication:

- Multi-hop Communication:

  - For a 500 bytes message, the security overhead may reach up to 71%...
  - But more important:
    - Who is assigning my ID?
    - Who is assigning my certificate?
Address Randomization

• Identifiers enable tracking
  ▪ MAC Address,
  ▪ IPv6 Prefix,
  ▪ IPv6 Host Identifier

• Randomization needs to be coordinated
  ▪ Certificate, MAC Address, IPv6 address all change on “renumbering event”

• Perform changes at the right time
  ▪ When it is safe, e.g., car is stopped
  ▪ Preferably “in a crowd”
Proposal

• Disclaimer:
  ▪ If a vehicle is having access to the IEEE 1609.2 or ETSI ITS security mechanisms
    • USE THEM
  ▪ Here, we look at the case where vehicles or other IPv6-compliant ‘things’ would not have access to them..

• Pseudonyms:
  ▪ Random generation of a 48-MAC address,
  ▪ Coordinated with certificate change, IPv6 address generation
  ▪ Alternative: RFC4941

• Security:
  ▪ Use well used/known security mechanisms to generate public/private keys, certificate (+ we b-of-trust)
    • CGA+RSA as in RFC 3971 (SEND) could be an option
    • IPSec..but need mechanisms for preshared secret
    • PGP..
  ▪ Each associated to one of the random pseudonym
  ▪ Challenge: PKI? Root certificate? (vendors, specific ITS-related IPv6 service?)