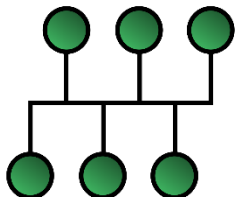


Intelligens közlekedés biztonsága

Dr. Fehér Gábor

Intelligens közlekedés biztonsága



Belső hálózat (CAN)
+ Külső kapcsolódások



VANET biztonság
(Inter-vehicular, road-vehicle)



Privátszféra,
anonimitás

Jármű belső hálózata

Controller Area Network (CAN)

- 1983- Bosch fejlesztés
- 1986: Hivatalos megjelenés
- 1991: CAN 2.0 (A és B részek)
- 1993: ISO 11898-1 (adatkapcsolati réteg)
ISO 11898-2 (fizikai réteg) gyors
ISO 11898-2 (fizikai réteg) lassú, megbízható
- 2012: CAN FD (flexibilis adatráta)

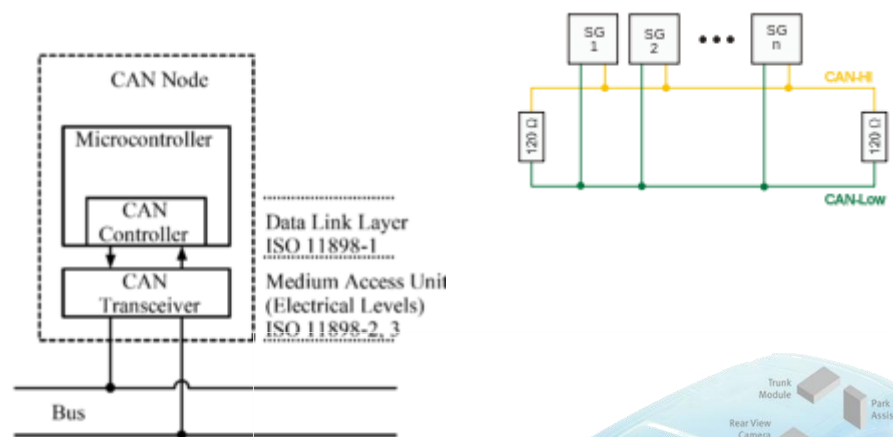
BMW 8xx: Az első
CAN busz (1988)

Az első “drive by wire”

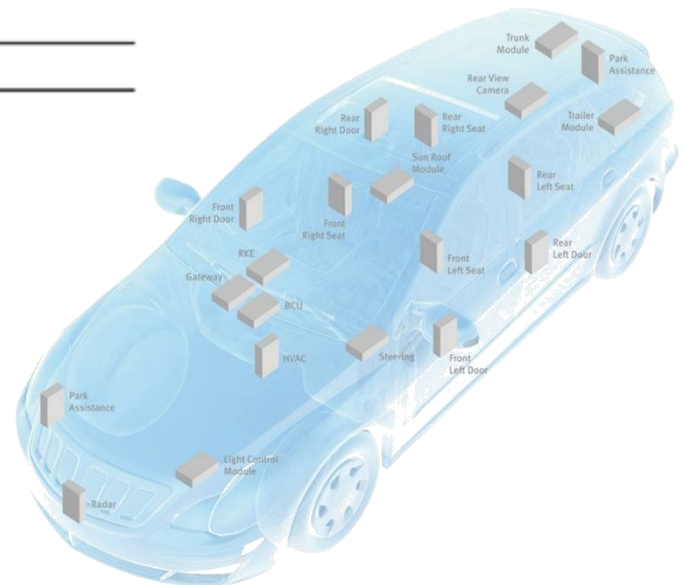


CAN architektúra

- Többvezérlős soros busz
- Prioritásos rendszer
 - ID szerinti prioritás
- CRC hibavédő kódok

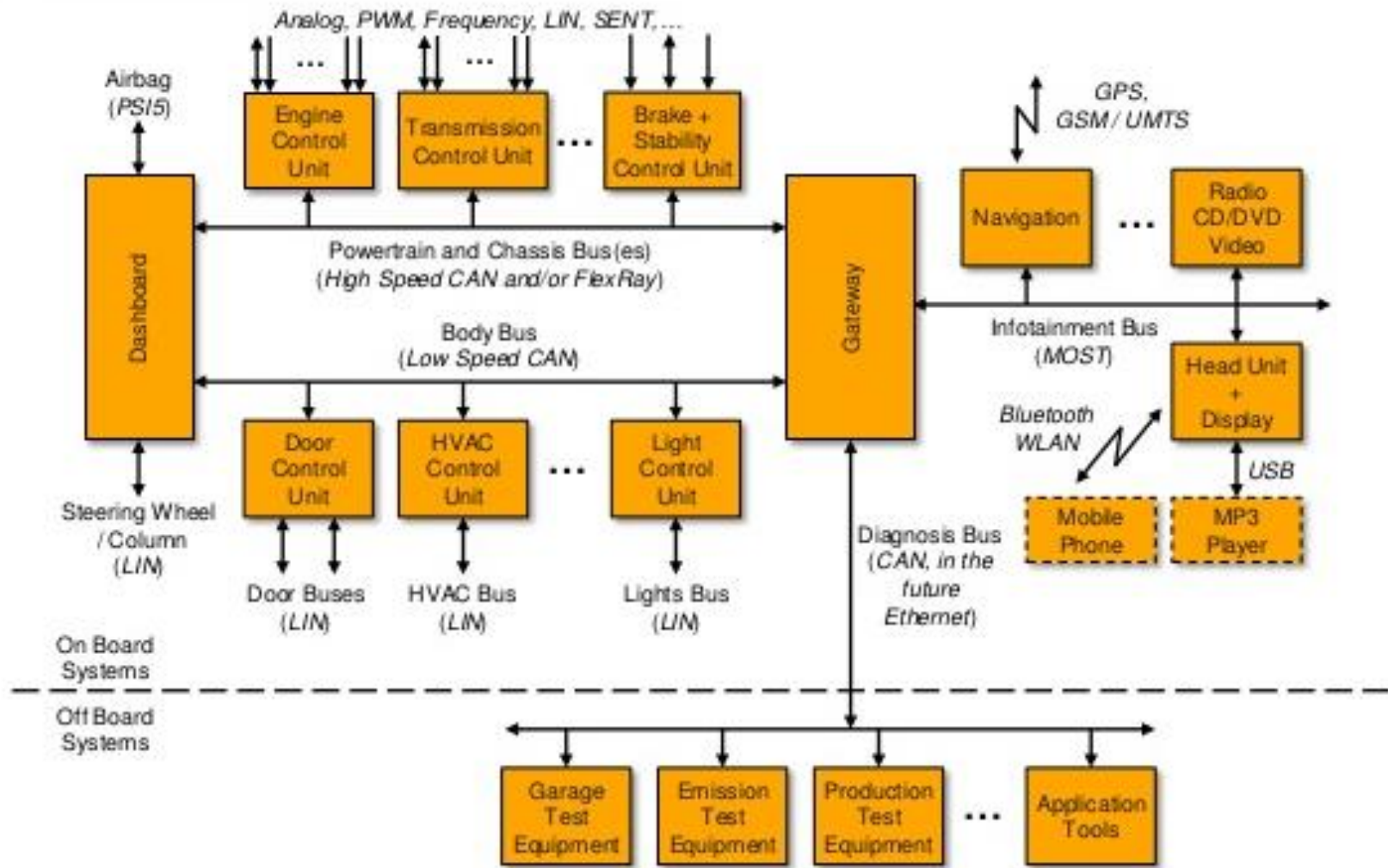


- Autón belüli CAN buszok
 - ECU (Electronic Control Unit) összekötések
 - Nagy sebesség és kis sebesség
 - ECU együttműködések



- Adatkapcsolati szinten
NINCS SEMMILYEN BIZTONSÁG !
 - Az alkalmazásnak kell megoldania a biztonságot egy felsőbb rétegben

CAN + LIN + Others



Picture from Continental

CAN biztonság

▪ Támadási vektorok

- Fizikai közelség
 - Szerelő, parkoló, alkatrészecseréje, nem gyári komponensek beszerelése
 - Az eszköz állandó elhelyezése / Más komponensek átírása
- Vezetéknélküli hálózatok



OBD, nem CAN, de hasonlít

▪ Kihívások

- Broadcast hálózat
- DoS támadásokkal sebezhető
- Forrás azonosításának hiánya
- Forrás hitelesítésének hiánya
- Gyenge hozzáférés védelem (márka specifikus)
- Eltérések a szabványtól



CAN SecurityAccess

- Szolgáltatás az ECU teszteléséhez/programozásához
- Kihívás/válasz alapú hitelesítés (seed / key)



- Az algoritmus legtöbbször titkos
 - Nem tárolható az eszközön (mert kiolvasható), csak kérdés/válasz párok vannak tárolva
 - De a teszternél akár ismert lehet
 - Tuning oldalak jópár algoritmust ismernek...

CAN SecurityAccess 2.

- Brute force támadás lehetséges nem csak elméletben (2-3-4 byte)
 - 2 byte, 10 mp/próba esetén 1 hét kell a töréshez
 - Egyszerre több eszköz is törhető
 - Időkorlátozás esetén az eszközt újra lehet indítani
- A kommunikáció lehallgatása egyszerűen megoldható
 - A CAN busz broadcast csatorna, nincs titkosítás
- Session hijacking: A hozzáférés ellenőrzés után a kommunikáció módosítható
- Kiadható parancsok
 - Pl.: DeviceControl, ECUReset, RequestDownload, RequestUpload, InputOutputControl

CAN SecurityAccess 3.

- A biztonság érdekében általában a hozzáférés le van tiltva menetközben
 - Ez nem mindig igaz azonban
 - Újraírás esetén leáll a motor
- Sok esetben nem teljesülnek a protokoll előírásai
 - Ugyanaz a seed/key minden esetben (minden eszközön)
 - A kulcs ellenőrzésének hiánya
 - A kulcsok területének kiolvashatósága
- Eszközök biztonságos kezelése
 - Az ECU blokkolhat veszélyes műveleteket
 - Gyakran azonban ez nem teljesül (tesztelés alatt mégis lehet)
 - Sőt, néha hitelesíteni sem kell

CAN szegmentálás

- A legtöbb esetben minimum 2 CAN busz található
 - Nagy sebességű CAN busz: Kritikus eszközök (pl. fék, ABS, motor)
 - Alacsony sebességű CAN busz: Kevésbé kritikus eszközök (pl.: fűtés, rádió)
 - A két hálózat között átjárók lehetnek (tipikusan vannak)
- A szabvány szerint a nagy sebességű busz megbízhatóbb
 - Az átjárót programozni csak a nagysebességű busz felől lehet
- Van pár eszköz, amely mindkét buszon szerepel (és nem átjáró)
 - Pl. Telemetrikai eszköz

Ezt támadva az átjáró is felülírható a megbízhatóbb busz felől !

CAN tapasztalatok

- A vezérlés visszafejtése sok időt igényelne, azonban a „fuzzing” jellegű tesztek meglepően sikeresek
- A hozzáférés védelem több esetben nem megfelelően vagy egyáltalán nem működik még kritikus ECU esetén is (akár ajtónyitás is)
- A buszok közötti átjárók védelme sok esetben nem megfelelő. Több ECU esetén a helyzet még bonyolultabb lehet
- Bár az egységek újraprogramozása nem egyszerű, a nyomok eltűntetése azonban az. Így a felelősség és a tettes megállapítása szinte lehetetlen

CAN biztonság megoldások

- Diagnosztika és újraírás esetén fizikai védelem
 - A kritikus műveletek csak az autó fizikai elérése esetén lehetségesek
 - Külső hozzáférés tűzfalazása (megoldható?)
 - Valós menet közben tilos a diagnosztika!
- Megbízható mediátor utángyártott alkatrészek esetén
 - A mediátor csak azokat az üzeneteket engedi át, amelyek valóban az adott eszközből származhatnak
 - Az átjáróknak is megbízhatóaknak kell lenniük
- Megelőzés helyett felismerés
 - Anomáliák felderítése
 - Lehetséges-e időben leállítani egy támadást?
 - Nem biztos, hogy megelőzhető a támadás, de a következmények talán elmaradhatnak

CAN támadások felismerése

- Támadás felismerés
 - A CAN broadcast hálózat, így a megfigyelő mindent lát
 - A CAN üzenetek nem túl változatosak, tartalmuk előrejelezhető
 - A támadások nagy eltérést mutatnak, így könnyebben azonosíthatóak
 - Gyorsabban küldött üzenetek, hogy elnyomják a valós üzeneteket
- Lehetséges lépések támadás felismerése esetén
 - A vezető figyelmeztetése
 - A CAN hálózat leállítása
 - A jármű biztonságos megállítása
 - Bizonyos üzenetek figyelmen kívül hagyása
- A megfigyelő elhelyezése
 - Külön modul (IPS ECU) a CAN buszon
 - A meglévő szoftverek kiegészítése
 - OBD II porton csatlakozás

CAN biztonság megoldások 2.

- Kriptográfia használata az üzenetek védelmére
 - Titkosítás az alkalmazás rétegben
 - Sajnos sokszor nem fér össze a valós idejű elvárásokkal
 - A kulcsmenedzsment szintén kritikus
 - Az eszközök visszafejthetőek maradhatnak
- Sok esetben a titkolózást gondolják megoldásnak
 - NEM működik !!!

Telematikára épülő szolgáltatások

- GM OnStar
 - Assistance szolgáltatások (Biztonság – safety)
 - Állapotfelmérés
 - RelayRide (autó megosztás)
- Ford Sync
- Chrysler Uconnect
- BMW Connected Drive
- Lexus Enform



Önjáró autók

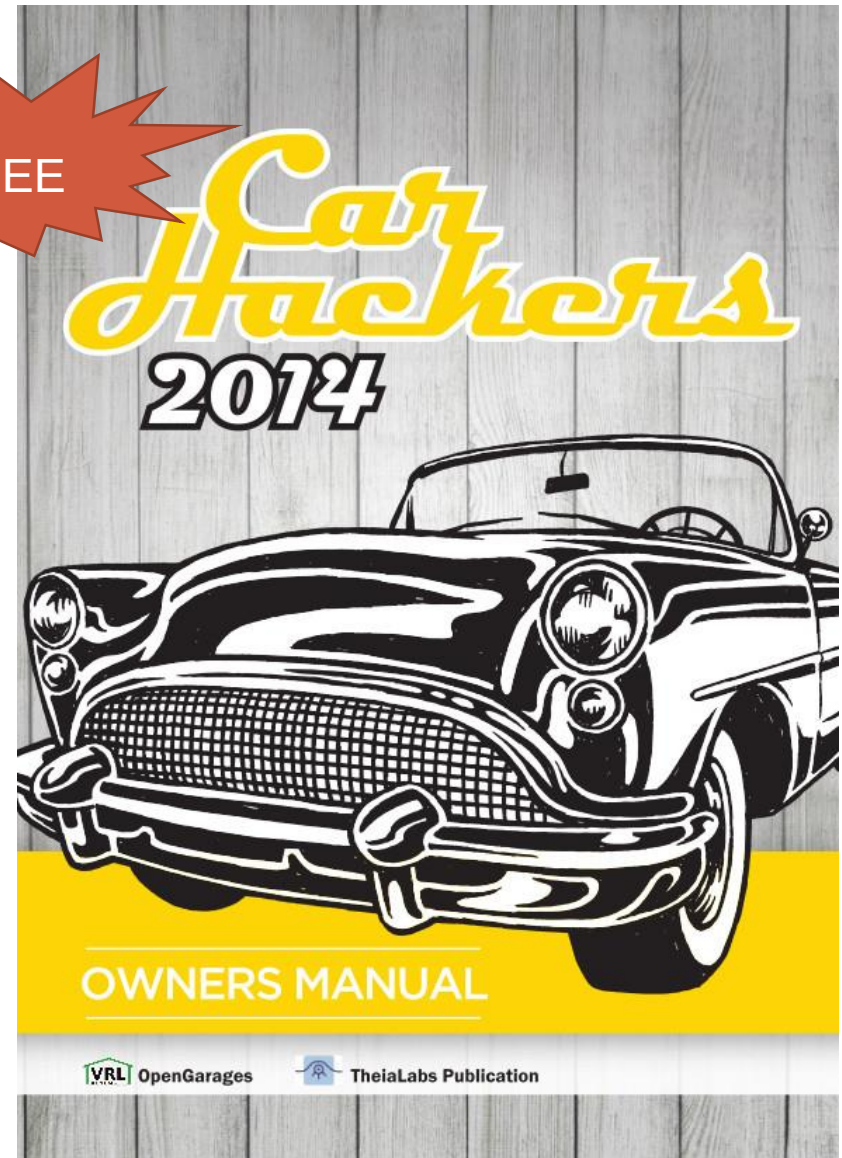
- Sávtartás
- Parkolás
- Vezetés



Ajánló

▪ <http://opengarages.org/handbook/>

- Intro
- Understanding Attack Surfaces
- Infotainment Systems
- Vehicle Communication Systems
- Engine Control Unit
- CAN Bus Reversing Methodology
- Breaking the Vehicle
- CAN Bus Tools
- Weaponizing CAN Findings
- Attacking TPMS
- Ethernet Attacks
- Attacking Keyfobs and Immobilizers
- FLASHBACK - Hotwiring
- Attacking ECUs and other Embedded Systems
- What does your hacker garage need?



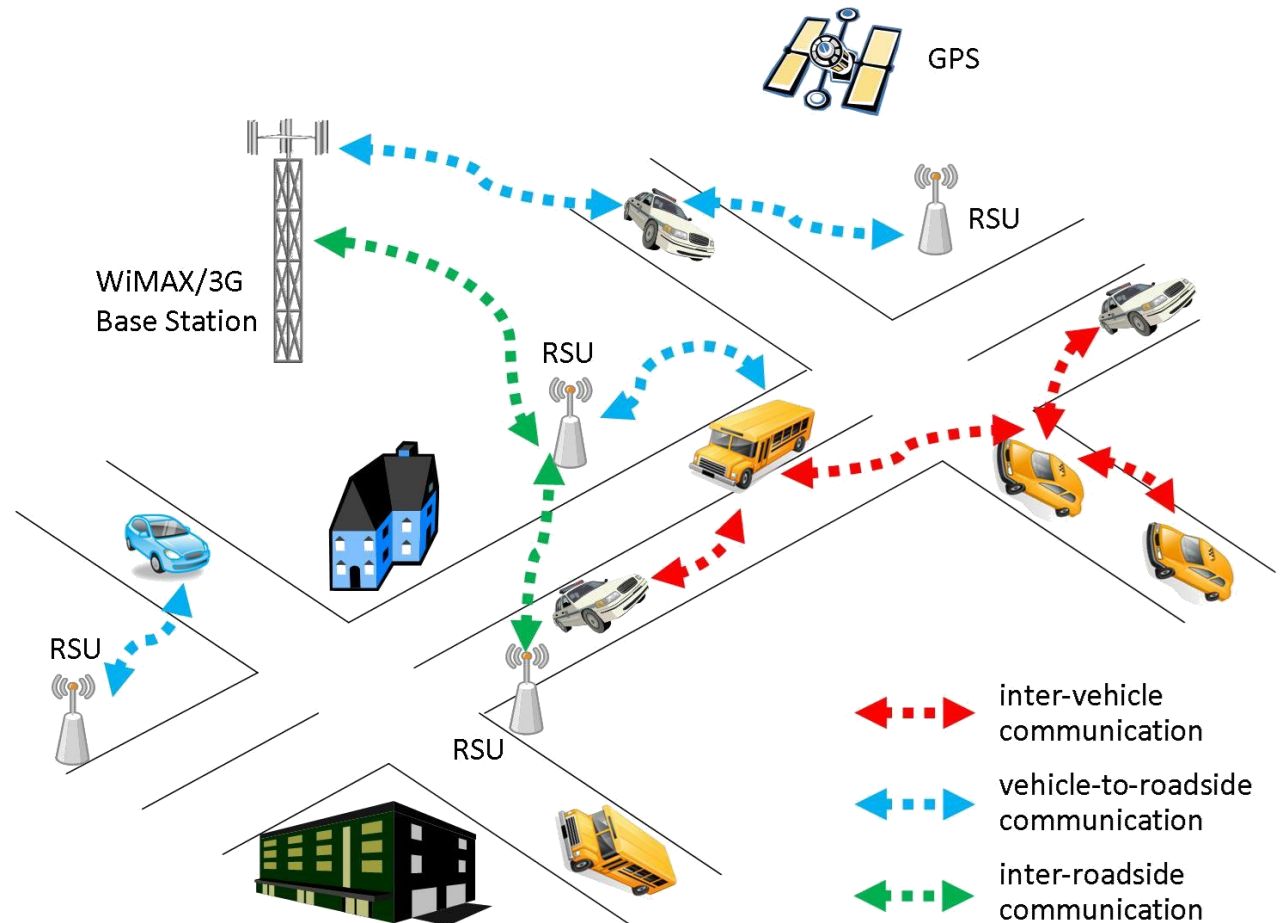
Járművek közötti hálózat

Vehicular Ad Hoc Network - VANET

- Jármű – Jármű és Jármű – infrastruktúra kommunikáció
 - V2V: Vehicle to Vehicle, V2R: Vehicle to Roadside, IVC: Inter-Vehicle Communications, OBU: On-Board Unit, RSU: Road-Side Unit
- Szabványok
 - Hasonló megoldások az IEEE 802.11p –re épülve
 - Európa: ETSI ITS G5 és USA: IEEE 1609 WAVE (Wireless Access in Vehicular Environments)
 - 5.9 GHz, 5/7 csatorna
 - Japán: ARIB STD-T109
 - 700 MHz, 1 csatorna
- Legnagyobb kihívások
 - Biztonság
 - Magánszféra védelme

Vehicular Ad Hoc Network - VANET

- Szolgáltatások
 - Biztonság (safety)
 - Kényelem
 - Kereskedelmi, szórakozás, telemetria



Forrás: Jung-Chun Kao's

VANET szolgáltatás példák

- Biztonság
 - Vészfékezés (pl.: EEBL: Emergency Electronic Brake Light)
 - Segítségnyújtás (pl.: PCN: Post Crash Notification)
 - Útviszonyok (pl.: RFN: Road Feature Notificaton)
 - Vezetés biztonsága (pl.: LCA Lane Change Assistance, CCW: Cooperative Collision Warning)
- Kényelem
 - Torlódásjelzés
 - Dinamikus úttervezés
 - Parkolóhely keresés
- Kereskedelem, szórakozás, telemetria
 - Távdiagnosztika
 - Hirdetések

VANET és MANET

- A MANET hálózatok már régóta kutatások tárgyai
 - Sok a hasonlóság a két hálózat között (megoldások átvehetőek)
 - Különbségek:
 - A VANET jobban strukturált hálózat
 - Az egyes nodeok dinamikusabbak, gyorsabban és többet mozognak
 - Az tároló és számítási kapacitások VANET esetében nem szűkösek
 - Jóval több node VANET esetén

VANET támadások

- DoS támadások
 - A csatorna elárasztása/zavarása (jamming)
 - Hatására az üzenetek nem jutnak el a járművekhez
- Üzenetek eldobása
 - Szelektív továbbítás, az üzenetek később felhasználhatóak
- Hamis üzenet gyártás
- Üzenetek módosítása
- Üzenetek visszajátszása
- Többszörözés (Sybil támadás)
 - A jármű azt tettet, hogy sok másik jármű is ugyanolyan állapotban van
 - Hatására a közölt (általában hamis) információ nagyobb prioritást kap

VANET támadók

- Önző vezetők
 - Saját érdekükben hamis információk terjesztése
 - Pl.: dugó szimulálása, hogy az útszakaszon csökkenjen a forgalom
- Felelősségre vonás elől menekülők
 - Információ blokkolása, hogy bizonyos tettek ne derüljenek ki
- Rosszindulatú támadások
 - Terrorizmus
 - Pl.: Baleset okozása, majd az információ blokkolása
- „Viccelők”, dicsekvők

VANET kihívások

- Titkosítás
 - Az üzenetek csak meghatározott eszközök számára értelmezhetőek
- Integritás védelem
 - Az üzenetek nem megváltoztathatóak
- Hitelesítés
 - Az üzenet forrásának hitelesítése
 - RSA nem használható, mert lassú. Hitelesítés más módszerekkel

VANET kihívások 2.

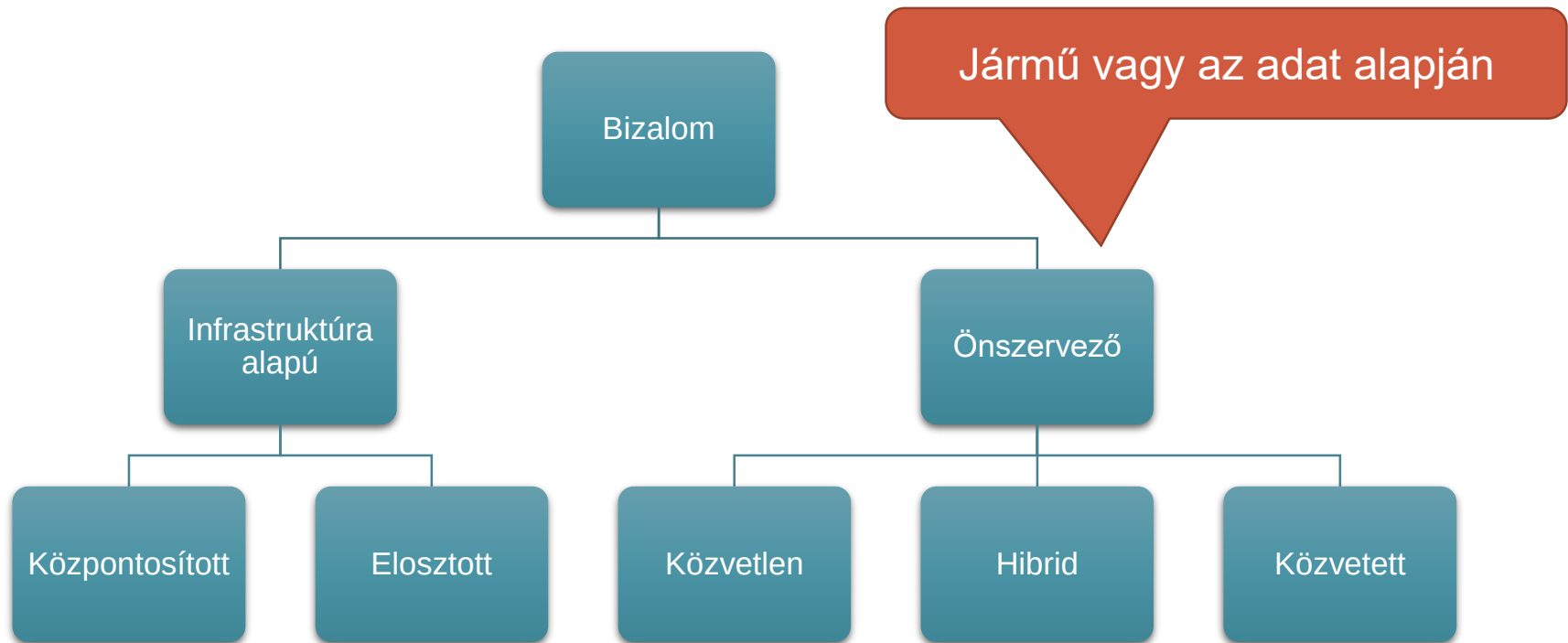
- Rendelkezésreállítás
 - Az üzeneteknek kritikus időn belül el kell jutniuk más járművekhez
- Letagadhatatlanság
 - Támadás esetén az elkövetőket azonosítani lehet a támadás naplózásával
 - A lehetséges támadók elriasztása
- Magánszféra védelme (privacy)
 - Kéretlen megfigyelők távoltartása
 - Anonimitás biztosítása (hitelesítés mellett!)
 - Elektronikus rendszámtábla
- Untraceability: A jármű különböző műveletei nem köthetők össze
- Unlinkability: A jármű és tulajdonosa nem köthető össze

VANET megoldások

- Létező MANET megoldások alkalmazása is lehetséges
- ARAN (Authenticated Routing for Ad hoc network)
 - Biztonságos Ad-Hoc forgalomirányítás PKI segítségével
 - Visszajátszás, megszemélyesítés elleni védelem + letagadhatatlan
- SEAD (Secure and Efficient Ad hoc Distance Vector)
 - Biztonságos forgalomirányítás egyirányú hash függvények segítségével
 - DoS elleni védelem
- SMT (Secure Message Transmission)
 - Biztonságos üzenettovábbítás end-to-end alapokon MAC alapú hitelesítés segítségével
- NDM (Non-Disclosure Method)
 - Anonimitás ügynökök segítségével. A forgalom mixelése és aszimmetrikus titkosítása
- ARIADNE
 - Forgalomirányítás biztonsága MAC, TESLA, szimmetrikus titkosítása épülve

VANET megoldások 2.

- Bizalom menedzsment (Trust management)
 - Tanúsítvány alapú bizalom
 - Reputáció alapú bizalom



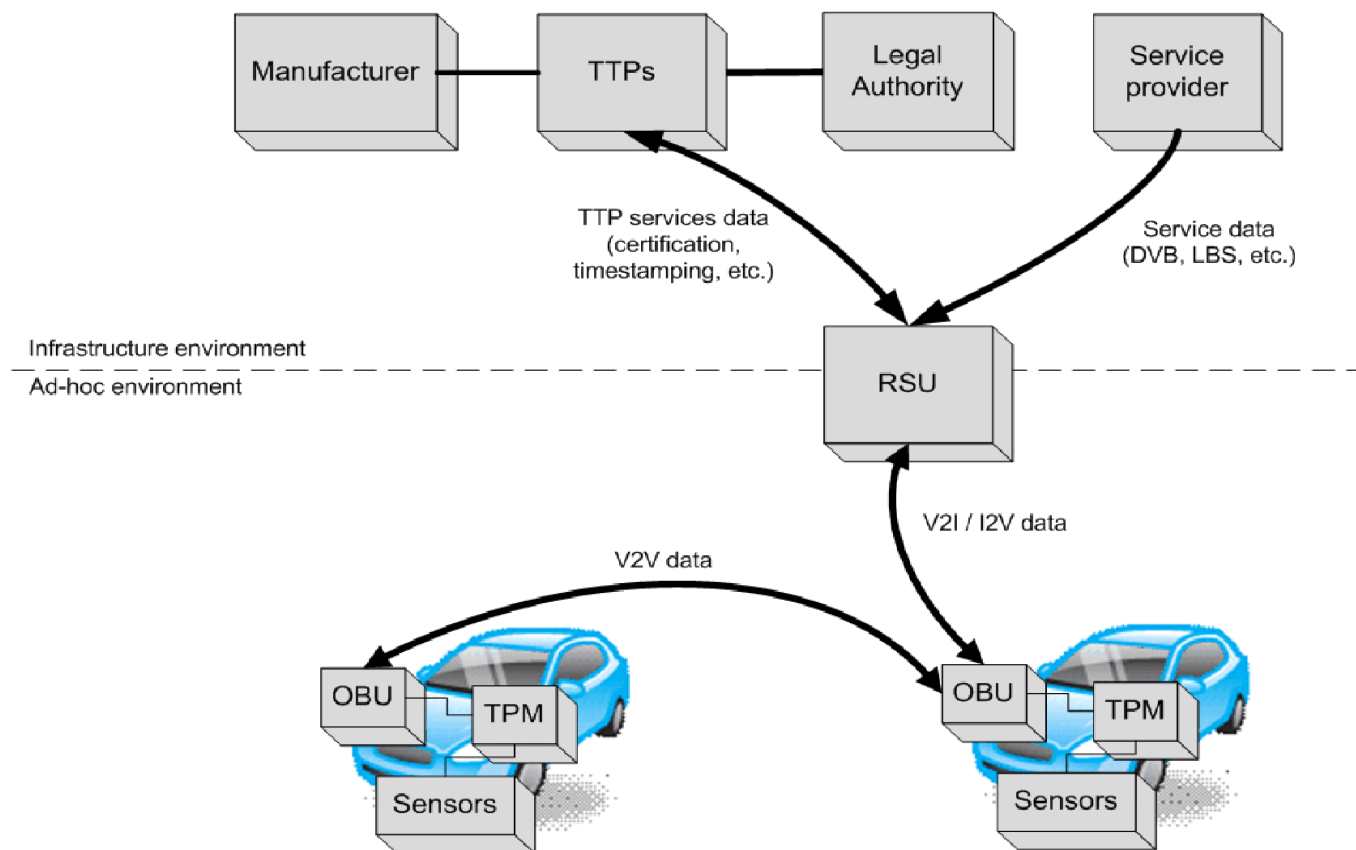
VANET megoldások 3. – IEEE 1609.2

- VPKI megoldások (Vehicular Public Key Infrastructure)
 - A forrás digitálisan aláírja az üzenetet, majd csatolja tanúsítványát
 - $V \rightarrow r: M, \text{Sig}_{\text{PrKV}} [M|T], \text{CertV}$
- Az RSA helyett más is használható ECC (Elliptikus görbén alapuló kriptográfia) vagy NTRU (N-th degree truncated polynomial ring)
- Csoport kulcsok és ellenőrzés
 - Kijelölt csoportvezető, aki nyilvántartja a csoportot és aláír. Anonim
 - Egyelőre kérdéses a hatékonysága, illetve a csoportvezető választás
- CA (Tanúsítvány kiállító központ) is kérdéses
 - Jelenleg több CA, nincsen globális világra szóló CA
 - A tanúsítvány visszavonásának ellenőrzése nehezen megoldható
- A hitelesítés mellett titkosítani (AES vagy aszimmetrikus) is lehet
- A magánszféra védelme nem biztosított!

Időbélyeg is

VANET megoldások 4.

- VANET komponensek



Forrás: Sumegha Sakhreliya, Neha Pandya

Jelenlegi kutatások

- ABE (Attribute Based Encryption)
 - CP-ABE: Cyphertext-Policy Based Encryption (policy a titkos adatban)
 - KP-ABE: Key-Policy Based Encryption (policy a kulcsba kódolva)
- Megoldható a hozzáférés vezérlés a titkosítás pillanatában
 - Pl.: titkosított adat, de a tűzoltó, rendőr (attribútumok) hozzáférnek
- Központi kulcsmenedzsment
 - Lehet több központi kulcsmenedzser is
 - Hierarchikus felépítés is lehetséges