
A V2X járműkommunikáció alapjai

Petkovics Ármin, Szabó Csaba Attila, Wippelhauser András, Varga Norbert, Bokor László

petkovics@hit.bme.hu, szabo@hit.bme.hu, wandris1210@gmail.com, vnorbert@hit.bme.hu, bokorl@hit.bme.hu
Budapesti Műszaki és Gazdaságtudományi Egyetem, Hálózati Rendszerek és Szolgáltatások Tanszék
BME Informatika épület, 1117 Budapest, Magyar tudósok körútja 2.

Bevezetés

Az elektronika és a távközlés fejlődésével az érzékelésen alapuló vezérlő és beavatkozó rendszerek hihetetlen sebességgel kezdtek terjedni, és az 1970-es évektől kezdődően a közúti járműveket is fokozatosan ellepték a mikro-elektromechanikai megoldások (microelectromechanical systems, MEMS) és általuk a multifunkcionális, kis hatótávú és kisméretű szenzorokra támaszkodó rendszerek világa. Törték a nagy hőingadozást és a rezgéseket, ezáltal gépjárművekbe történő építésre is alkalmassá váltak: kezdetben a meghajtott tengely forgási sebességét (és ebből a jármű sebességét) mérték vele, valamint az olaj és hűtővíz hőmérsékletet. Ma már egészen extrém és sokféle felhasználási módjuk is ismert, a hangsúly pedig eltolódott az alapfunkciók támogatása felől a biztonsági- és komfortfunkciók irányába.

A biztonsági funkciók egy ideje már nem luxus, hanem kötelező elemei a közúti járműveknek: 2004 óta minden EU-ban forgalomba állított autónak kötelező blokkolásgátlót alkalmaznia (Anti-lock Braking System, ABS), ugyanitt, 2014 óta az ESP menetstabilizáló is kötelező alapfelszereltség (Electronic Stability Program). Gondoljuk csak végig: az ABS működéséhez minden keréknél szükség van egy-egy szenzorra, ami figyeli azt, hogy fékezéskor blokkol-e a kerék, az ESP-nél pedig minden kerékhez kell egy forgássebesség-szenzor, egy giroszkóp-gyorsulásmérő páros az oldalirányú gyorsulás érzékelésére, valamint még egy szenzor, ami a kormányszögállást érzékeli. De ezeken kívül is rengeteg, az autókban már most is széles körben használt szenzorokat sorolhatunk fel: lambdaszenzor az üzemanyag-levegő keverék arányának beállítására, esőszensor az automatikus ablaktörléshez, külső és belső hőmérsékleti szenzorok melyek figyelmeztetnek, ha kinn fagyponthoz közelre süllyed a hőmérséklet, illetve egészen komfortosan, fél fokos pontossággal állítják be a vezetői fülke hőmérsékletét. Újabban a RADAR (Radio Detection and Ranging) és LIDAR (Light Detection and Ranging), valamint a kamerarendszerek is egyre elterjedtebbek. A radar rendszer pl. a parkolásnál segít, illetve a LIDAR-ral együttműködve automatikus távolság- illetve sávtartást tesz lehetővé. Természetesen ez azzal jár, hogy szükség esetén gyorsítja vagy lassítja az autót, tehát már „beszól” annak közvetlen irányításába is. A kamerarendszer is besegíthet parkolásnál, de szabad parkolóhelyek keresésére is alkalmas. A RADAR-ra, LIDAR-ra és kamerákra alapozó vezetéssegítő, támogató, kényelmi rendszereket ADAS alkalmazásoknak nevezik (Advanced Driver-Assistance Systems). Ezek a rendszerek a járművek autonóm, azaz önálló mozgása irányába mutatnak: az önvezetés természetesen itt még nem teljes, de a cél az, hogy a szenzorokkal nagy biztonsággal kezelhető helyzetek megoldásának terhére levegyék a sofőrök válláról.

Az autókba telepített szenzorokat alapvetően két típusra oszthatjuk. Az egyik csoportba tartozók az autó alkatrészeinek állapotát monitorozzák, az autó üzemeltetését segítik: visszajelzést adnak annak állapotáról. A környezeti érzékelők a vezetéssegítő rendszert látják el információval, a környezet megfigyelésére összpontosítanak: sávjelzéseket értelmeznek, időjárási paramétereket gyűjtenek, közelben közlekedő autókat észlelnek, mérik azok gyorsulását, stb. Vannak viszont olyan helyzetek, ahol szenzorokkal együtt sem tud egy autó biztonságosan áthaladni. Ilyen például egy beláthatatlan kereszteződés: nincs ugyanis több releváns információja egy emberi sofőr által begyűjthetőnél, hiszen a szenzor sem tudja, hogy mi van a „kanyar mögött”, a legmodernebb megoldások sem látnak át házakon. Viszont, ha van autó a kanyarban, akkor az akár „szólhatna” is arról, hogy érkezik, és mi nem mennénk ki elé: megszületik tehát az igény a kommunikációra. Ha egy autó nem is tud mindent az útszakaszról, többen, kooperatív módon együttműködve, az adatforrásaikat (szenzoradataikat) megosztva egészen pontos képet alakíthatnak ki az útszakasz állapotáról, forgalmáról, jellemzőiről. Ez a V2V, azaz Vehicle-to-Vehicle, autók közötti kommunikáció, mi a járművek együttműködésével hoz létre kooperatív tudatosságot: minél több forrás, annál több és megbízhatóbb a leszárt információ mennyiség. Azonban míg a járművek egymás közötti

„beszélgetése” megoldhatja a helyzetet bizonyos szituációkban, addig más esetekben be kell vonni az infrastruktúrát, pl. a közlekedési lámpákat, meteorológiai állomásokat, változtatható jelzésképű táblákat is, mivel az útinfrastruktúra üzemeltetője olyan információkat birtokolhat, melyeket nem lehet előrejelezni, melyeket nála pontosabban senki sem tudhat. Itt válik szükségessé a V2I és I2V (Vehicle-to-Infrastructure, és fordított irányban), azaz jármű-infrastruktúra-jármű kommunikáció. Mindennek az összefoglaló neve a napjainkban már ismerősen csengő V2X (Vehicle-to-Everything) vagy C2X (Car-to-Everything), azaz járművek kommunikációja „minden mással” [1]. A magas szintű kooperáció eredménye pedig a kooperatív intelligens közlekedési rendszerek (Cooperative Intelligent Transport Systems, C-ITS) ökoszisztémája, melyben a járműkommunikációs infrastruktúrára épülve a fejlett szolgáltatások széles skálája biztosítható [2].

A járműkommunikáció céljai és kihívásai

A V2X lehetővé teszi, hogy az autók együttműködjenek az útinfrastruktúra és/vagy a város közlekedésirányításával, valamint más járművekkel, így optimalizálva, és persze elsősorban *biztonságosabbá* téve a közlekedést. Az autó vezetőjének információja lesz a nem belátható területekről érkező veszélyekről, eseményekről, döntéseit így lépésről lépésre segítik a járműkommunikációs rendszerek.

Régóta léteznek már olyan megoldások, melyek mobiltelefonos applikáció formájában jeleznek a sofőrnek az útvonalon várható eseményekről, kátyúkról, balesetekről: ilyen például a jól ismert Waze alkalmazás is [3]. A V2X viszont többet kínál: a Waze frissítési ideje nem versenyezhet a V2X milliszekundumos késleltetésével: éles szituációkban, ütközésselkerülésnél a Waze, vagy más, applikációba ültetett közlekedést segítő rendszerek nem versenyképesek és nem is ez a céljuk. Amit tehát szeretünk a Waze-ben azt a V2X alapból tudja majd, és nem csak informáló-segítő alkalmazásként, hanem biztonságkritikus döntési helyzetekben is megállja a helyét. Az elsődleges célja a járműkommunikációnak tehát a biztonság, a közúti halálesetek és alapvetően a balesetek visszaszorítása.

A biztonságon felül a takarékoság is motiválja a V2X kommunikációra épülő szolgáltatások bevezetését: a szenzorok által egyformán nagyon gyors „reakcióidővel” rendelkező autók, teherautók konvojban, gyorsan, egymáshoz nagyon közel haladva spórolhatnak rengeteg üzemanyagot a légellenállás okozta veszteségek minimalizálásával.

További célok közt lehet említeni a real-time multimédiás alkalmazásokat, a dugók elkerülését, a károsanyag-kibocsátás csökkentését is, tehát sok olyan szolgáltatást, amit az okos város koncepció is megcélóz: ehhez a V2X egy megfelelő eszköznek bizonyul.

Megvalósítás, de legalábbis engedélyezés és elfogadottság szempontjából mindenképpen jövőbe mutató célterülete a V2X fejlesztésének az önvezető járművek támogatása és széleskörű alkalmazhatóságuk, elterjedésük segítése. Az autonóm járművek jelenleg elérhető változatai ott tartanak, hogy az emberi vezetőt próbálják gépekkel emulálni: szenzorokkal lát, hall és érzékel, az aktuátorok (beavatkozók) pedig helyettesítik az ember reakcióit (pl. elektromos működtetésű hidraulikus kormányrásegítés, elektromechanikus fékrendszerek, stb.). Viszont, ahogyan a beláthatatlan kanyarnál is említettük: az emberi sofőr emulálásával és szenzorokkal/beavatkozókval történő helyettesítésével csak maximum egy emberhez hasonló módon érzékelő szerkezetet fejlesztünk. A V2X-szel viszont jóval több információ biztosítható az autonóm működéshez, megalapozottabb döntéseket hozhatna az önvezető jármű, melyekhez az összes közlekedő és maga az infrastruktúra is hozzájárulhat az információi megosztásával [4]. Így létrejöhet a kooperatív tudatosság, melyre alapozva komplex szolgáltatások és alkalmazások építhetők fel.

A célkitűzések között a felhasználási területek és a hozzájuk kapcsolódó alkalmazások továbbfejlesztése mellett fontos megemlíteni egy világszinten szerveződő direktívát, a Vision Zero-t [5]: célja hosszabb távon minden emberi hibalehetőség kizárása a közlekedésből, ezzel a balesetek és halálesetek nullára csökkentése és a közlekedési dugók elkerülése. Utóbbit a közlekedni kívánók, illetve az őket szállító (autonóm) járművek tökéletes informáltságával céljuk elérni. Mindez természetesen a környezetet is pozitívan érinti majd: városonként évente több milliányi feleslegesen dugóban töltött óra gazdasági hátrányt okozó hatása és felesleges károsanyag-kibocsátása takarítható majd meg általa.

Az EU sem fukarkodik a nagy szavakkal: az aktuális célkitűzés szerint 2030-ra 40%-al kell csökkenteni a gazdaságok kibocsájtását az 1990-es szinthez képest [6]. Merész gondolatok ezek, a jövő megmutatja, sikerül-e megvalósítani, mindenesetre elég nagy a törekvés erre, és nem csak az Európai Unióban.

Természetesen a szabványosítás és a kezdeti megvalósítások közben már előjöttek a technológia kihívásai is, amikkel meg kell birkózni. Ilyen például az elsősorban autópályákon jelentkező autók közötti nagy relatív sebesség: két szemben haladó jármű viszonylagos sebessége 2-300 km/h is lehet. Ebből eredően a topológia is nagyon gyorsan változhat, a szemben haladó autók nagyon rövid ideig vannak egymás „hatótávolságában”, így az üzenetek továbbítása ebbe a rövid időbe kell, hogy beleférjen, vagy alternatív megoldást kell kifejleszteni egy hatékonyabb, ad-hoc szerveződő hálózati struktúra képében. A túlzottan sok kommunikáló eszköz is lehet gond: dugóban állva, ha mindenki csak periodikusan küld magáról információkat, az is a rádiós/hálózati közeg túlterheléséhez vezethet. Ilyen esetben viszont nagy újdonságértékkel sem rendelkezik az, hogy az autó még mindig ugyanazon az útszakaszon vesztegel, tehát érdemesebb ritkábbra venni a jelzéseit vagy eseményvezéreltté tenni: elindulás, dugóból kiszabadulás esetére például. Az ilyen és ehhez hasonló kihívásokat tartalmazó komplex igényrendszert [7][8] kell tudnia kezelni a kooperatív intelligens közlekedési rendszerek architektúráinak, a megvalósítandó járműkommunikációs szolgáltatási rendszereknek.

A C-ITS architektúra

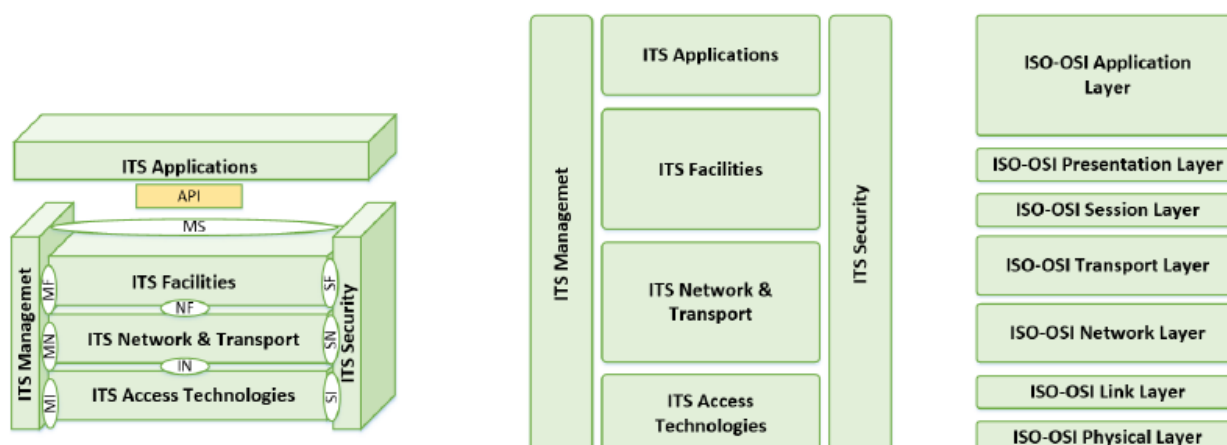
A C-ITS kommunikációs architektúra már több mint tíz éve szabványosítás alatt van, kisebb kiegészítéseket kap még, de alapvetően letisztult és stabil (1. ábra) [9]. Érdemes összehasonlítani az Internet működésének alapjául szolgáló, az ISO OSI által a számítógépek kommunikációjához definiált protokoll-hierarchia szerkezetével [10]: a C-ITS-ben vannak vertikális rétegek is. Ezek a Security és a Management rétegek: nem csak a közvetlen felettük vagy alattuk lévő réteggel vannak direkt összeköttetésben, hanem mindegyikkel: ez javítási lehetőségeket rejt magában a rétegek közötti (cross-layer) optimalizáció [11] révén.

A Menedzsment réteg (ITS Management Layer) azzal foglalkozik, hogy a megfelelő helyre elküldje az egyes rétegekből származó információkat. Egy nagyrészt járművekből álló hálózatban folyamatosan változik a rádiós összeköttetések topológiája, ebből eredően a jel/zaj viszony, és változik az is, hogy milyen átviteli technológiával, milyen kódolási eljárást használva és milyen sáv szélességre optimalizálva érdemes átvinni az adatainkat. Például egy 50 Mbit/s-os Wi-Fi linken 4K felbontású videó is átvihető, míg egy 3G cellás hálózaton ezzel meg sem szabad próbálkozni. Ilyen és ehhez hasonló információk birtokában, folyamatosan végzett mérésekre támaszkodva a Management réteg időben dönthet az átviteli mód különböző paramétereinek változtatásáról és értesítheti az architektúra különböző elemeit, ezzel javítva, optimalizálva a kommunikációt.

A Biztonság réteg (ITS Security Layer) természetesen a hozzáférés-szabályozás, hitelesítés, bizalmasság megőrzése, a letagadhatatlanság biztosítása és az adatok hitelességének és sértetlenségének biztosítása alapvető céljait szolgálja: state-of-the-art, minden réteget érintő biztonsági és privátszféravédelmi mechanizmusok kerültek szabványosításra. Ehhez elengedhetetlen volt az, hogy a többi réteggel közvetlen kapcsolatban legyen, hogy a működéshez szükséges információ rendelkezésre álljon és megfelelően gyorsan terjedjen.

További hasonlóság az OSI-rétegszerkezettel, hogy mindkettőben megtalálható hozzáférési (ITS Access Layer), hálózati és transzport (ITS Network and Transport Layer) valamint az alkalmazási réteg (ITS Applications Layer). A C-ITS architektúrában azonban megjelenik egy új, ún. Képesség réteg (ITS Facilities Layer) is. Ez a réteg arra szolgál, hogy a C-ITS/V2X-alkalmazások speciális igényeit közvetlenül, speciális C-ITS fókuszú képességekkel ki lehessen elégíteni. Ilyenek például a kooperatív tudatosságot előidéző üzenetváltások: periodikus- és eseményvezérelt információadás a közlekedésben részt vevő komponensek állapotáról, amit a többiek elfognak és az alapján tudnak reagálni, illetve a hordozott információkat be tudják építeni a „világképükbe”.

A következőkben áttekintjük a C-ITS protokoll hierarchia és szabványos kommunikációs architektúra fentebb felsorolt alapvető rétegeit, fontosabb jellemzőiket és feladataikat, a közeghozzáféréstől az alkalmazási rétegig bezárólag.

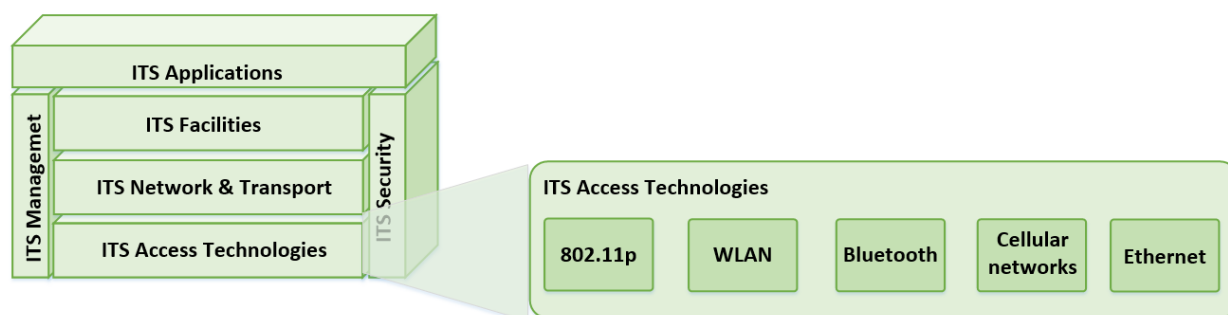


1. ábra. A C-ITS-architektúra összehasonlítása az ISO OSI-rétegekkel.

Közeghozzáférési réteg (ITS Access Layer)

Transzpárens réteg, felcserélhetők benne a Wi-Fi alapú, Bluetooth-os, cellás és vezetékös hozzáférési módok (2. ábra). Az aktuális C-ITS telepítési és továbbfejlesztési erőfeszítések a rendelkezésre álló rádiós hozzáférési technikákon alapulnak. Ezek az IEEE 802.11p/ETSI ITS-G5 (röviden ITS-G5) [12], valamint a 3G és 4G cellás szabványok [13]. Ebben a jelenleg elérhető kombinációban az ITS-G5 megoldás adja a rövid hatótávolságú, ad-hoc hálózati technikákra épülő kommunikációs technológiát, melyet kiegészítenek a nagy hatótávolságú 3G/4G mobil celluláris rendszerek. Az IEEE 802.11p szabvány [14] használatos leginkább az aktuális pilot projektekben (pl. EU C-ROADS [15], US Connected Vehicle Test Bed [16]), ennek megfelelő 5,9 GHz-es frekvenciatartomány [17] és a definiált kódolás használatos a világ legnagyobb részén, néhány kivétellel (Japánban 700 MHz a kijelölt sáv, illetve Kínában inkább celluláris megoldásokat tesztelnek). Ez a szabvány hasonló az otthoni használatra szánt Wi-Fi-hez, de nem az ISM (Industrial, Scientific, Medical) szabad frekvenciasávjában működik, hanem engedélyköteles. Napjainkra már kiforrott, „automotive grade” szintű. Az 1980-as években megkezdett C-ITS kutatási munka 2008-ban ért oda, hogy az Európai Bizottság kijelöljön egy 30MHz-es tartományt (5875 - 5905 MHz az 5,9 GHz-es frekvenciasávon belül a biztonsággal kapcsolatos ITS alkalmazásokhoz (EC/2008/671) [18]. 2013-ban került kiadásra az első, valós telepítéseken végzett teszteken alapuló ITS-G5 európai szabványcsalád, melyre támaszkodva napjainkban már off-the-shelf termékek és éles környezetben használható C-ITS rendszerek érhetők el világszerte.

A 802.11p alapú C-ITS közeghozzáférés hatótávolsága ~800–1600 méter a rádiós és földrajzi viszonyoktól függően. Ezen távolságon belül rengeteg autó feltorlódhat, így nagyon fontos, hogy a haladási sebességtől függően adaptívan szabályozzuk a „levegőben lévő” csomagok számát, mivel a rádiós erőforrás egyrészt túltelítődhet, másrészt viszont egy lassan haladó járműről értelemszerűen nem jelent több hasznos információt az, ha másodpercenként többször is jelent magáról, mintha lassú haladás esetén mindezt csak másodpercenként tenné meg. Ez az adaptív változtatás a közeghozzáférési réteget érinti, de az ITS Management vertikális rétege segítségével kivitelezhető megfelelő gyakorisággal és megfelelően rövid idő alatt. Szintén *flexibilitást* követel meg az egyéb, 5 GHz sávban működő alkalmazásokkal való együttélés: több helyen (Olaszország, Németország) az autópálya fizetőkapunak egy része az 5795 MHz – 5815 MHz sávban működő DSRC technológiákat alkalmazza [19], ami potenciális interferencia lehetőség a C-ITS 5855 MHz – 5925 MHz sávjával. Így a V2X átvitelt használó járműveknek észlelniük kell, ha ilyen kapuhoz közelednek és vissza kell venniük ezen időszakban az adási teljesítményükből [20]. Ezzel a hatótáv, vagyis az a távolság „ameddig ellátnak”, csökken, de ez nem különösebben jelent gondot, hiszen a kapuknál egyébként is lassítaniuk kell. Nem meglepő módon ebben is a vertikális Management réteg működik közre.



2. ábra. Az ITS közeghozzáférési rétege.

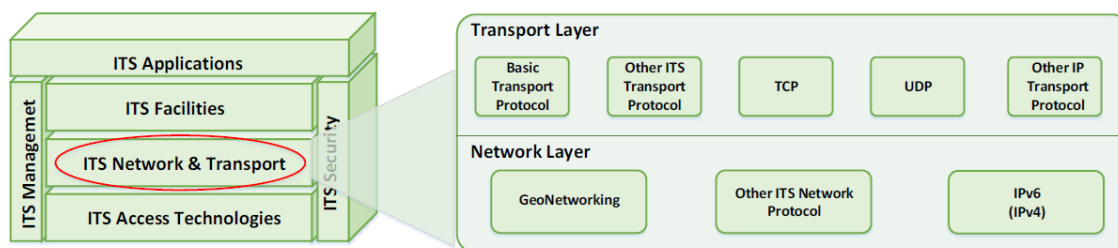
A hozzáférési technológiák fejlődése természetesen még nem zárult le: a Wi-Fi megoldások közé tartozó IEEE 802.11p és a 3GPP celluláris LTE-V2X illetve az 5G megoldásai is versenyeznek és itt elsősorban a gyártók csapnak össze. A celluláris hálózatokat fejlesztők már nehezen indokolják az újabb mobil hozzáférési generációk bevezetését, de a járműkommunikáció egy kiváló használati eset, megfelelő motiváció. Itt már nem az a cél, hogy 100 Mbit/másodperc fölé vigyék a letöltési sebességeket (bár ez is megtörténik), hanem az, hogy a késleltetést csökkentsék milliszekundumos nagyságrendre és ennek az ingadozását minimalizálják: real-time közeli alkalmazásoknak ugyanis elsősorban erre van szükségük. Éppen ezért a további szabványosítási munkák során elkezdték egységesíteni az LTE-V2X technológiát is [21], valamint folynak az 5. generációs celluláris hálózatok (5G) kutatási-fejlesztési munkálatai is [22]. Azonban az ITS-G5 és a C-V2X (celluláris V2X, 4G és 5G technológiákra alapulva) közötti átjárhatóság továbbra is problémát jelent. Így egy jármű, ami csak ITS-G5-tel van felszerelve, további harmonizálási erőfeszítések nélkül nem fog tudni kommunikálni egy olyan járművel, ami csak LTE-V2X vagy 5G C-V2X technológiával van felszerelve. Éppen ezért az alábbi megfontolások kiemelkedő jelentőségűek [23][24]:

- Az átjárhatóság az ITS-G5 és az újabb celluláris C-ITS hozzáférési technológiák között elengedhetetlen. Az emberi élet védelme elsődleges prioritás és ebbe nem fér bele az a tény, hogy azért alakult ki baleset, mert a járművek nem tudtak egymás között kommunikálni, vagy mert egy RSU nem volt képes kommunikálni átjárhatósági probléma miatt.
- Az úthálózatok üzemeltetőit nem szabad arra kényszeríteni, hogy két vagy több egymással versengő hozzáférési technológiával ellátott RSU-kal legyenek felkészülve, amelyek a hozzáférési technológiától függetlenül ugyanazt a használati esetet szolgálnák, vagy azonos szolgáltatást biztosítanának a vezetőknek/autonóm járműveknek.
- Az 5G felé irányuló celluláris mobil hálózati szabványok fejlődése várhatóan tovább javítja a nagy hatótávú kommunikációt (például a lefedettség javítását és a jelátviteli hatékonyságot), hozzájárulva egyúttal a hibrid kommunikációs rendszer javításához és kiegészítve a rövid hatótávolságú kapcsolatot is.
- A visszafelé kompatibilitás (backward compatibility) megközelítését mindenképpen követni kell, vagyis az új, Day-1 szintet meghaladó C-ITS eszközöknek támogatniuk és továbbra is biztosítaniuk kell a már telepített C-ITS szolgáltatásokat és alkalmazásokat.
- Az LTE-V2X és jövőbeli 5G technológiáknak nem szabad károsan befolyásolniuk az ITS-G5 használhatóságát, az együttműködésre, együttélésre kell törekedni.
- Az úthálózatok üzemeltetőinek szabadon kell tudni dönteniük arról, hogy hogyan lehet a hibrid kommunikációs megközelítésen keresztül biztosítani az összeköttetést, beleértve minden jövőbeli járműkommunikációra alkalmas megoldást is.

Hálózati- és szállítási réteg (ITS Network and Transport Layer)

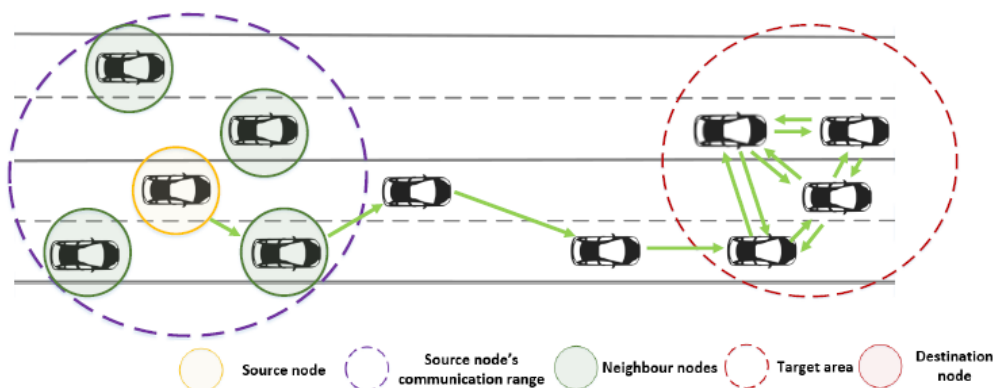
Ahogy a 3. ábra is mutatja, az ITS hálózati és a szállítási réteg [25][26] az OSI-modellben megszokott módon épül egymásra. Az Internet világában a hálózati rétegben az IP (Internet Protocol) végzi a címzés és az adatsomagok útvonalirányításának alapvető feladatait. A C-ITS világban is felmerül az internetes erőforrások elérésének szükségessége [27]. Itt már kizárólag az IPv6 (Internet Protocol version 6) használatára kell a jövőben számítani a járművek nagy száma miatt, de az elsődleges, közlekedésbiztonsági (safety) alkalmazásokkal kapcsolatban az IP a megoldások/telepítések első hullámából mégis kiszorul. Ennek legfontosabb oka, hogy a biztonsági alkalmazások esetén az IP alapú kommunikáció túlzottan nagy terhelést (overhead-et) eredményezne az átviteli késleltetés és a sávszélesség paramétereiben egyaránt, így az IP-t (valamint a rá épülő transzport rétegbeli megoldásokat) ilyen esetekben nem érdemes alkalmazni, speciális megoldásokra van igény.

Nagyon fontos az ITS hálózati rétegben, hogy tudjunk földrajzi alapon is címezni, például a mögöttünk lévő öt kilométer hosszú útszakaszon közlekedőket, vagy a városban egy adott kereszteződés adott sugarú környezetében lévőket. Ez egy releváns alkalmazási igény a járműkommunikációnál: ha például érzékeltünk egy úthibát vagy az előrehaladást befolyásoló tényezőt, akkor azt a mögöttünk haladóknak kell tudniuk, aki már túl van rajta, azt kár terhelni az üzeneteinkkel. Ezt az IPv6 alapról nem tudja. IPv6-ban multicast van, ami csoportcímezést végez, de továbbra is IP címek alapján működik. Kell tehát a geográfikus címzés és útvonalirányítás (addressing és routing), amit a GeoNetworking speciális V2X hálózati rétegbeli protokolljának a feladata.



3. ábra. A V2X hálózati és szállítási rétege és főbb protokolljai.

A GeoNetworking leggyakoribb felhasználása a geobroadcast, azaz a téglalap, kör vagy ellipszis választható alakú és felparaméterezhető célterületeken belül tartózkodók megcímezése (4. ábra). A terület általában nagyobb vagy messzebb van, mint a V2X közeghozzáférési technológia hatótávja, tehát amikor egy jármű megkap egy ilyen üzenetet, akkor kötelessége továbbítani is mindaddig, amíg mindenki, aki az adott területen belül tartózkodik, meg nem kapja, és ameddig a hirdetett esemény releváns, azaz az üzenet időzítője le nem jár. A GeoNetworking része tehát az ad-hoc routing protokoll, ami összetett algoritmusokat kíván [28]. Míg USA-ban csak egy ugrásig szabad terjednie a V2X üzeneteknek, tehát ilyen összetett megoldásokat nem alkalmaznak, addig az EU-ban használható a több „hop”-on keresztül üzenet célbajuttatás is, azaz a szabványok alapján a járművek továbbíthatják a csomagokat egymást között is, például egy célterület felé.

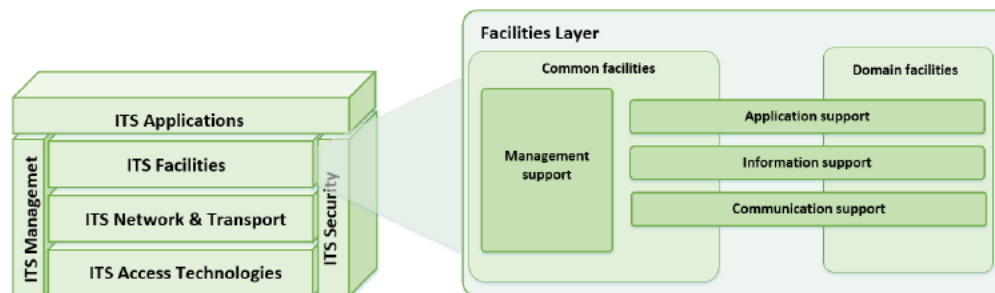


4. ábra. Geobroadcast példa: a sárga autó üzenetének útja a piros körrel jelölt területre.

ITS Képesség réteg (ITS Facilities Layer)

Az „új” réteg, ami nincs az OSI-struktúrában, de a V2X-architektúrában megjelent [29]. Különböző alkalmazásokat támogató funkciókat valósíthatunk meg ezzel a réteggel (5. ábra).

A legalapvetőbb ide tartozó protokoll a CAM (Cooperative Awareness Message) üzenetváltást definiáló szolgáltatás [30]. A CAM üzenet egy „heartbeat”, azaz „itt vagyok” jellegű folyamatos, *periodikus* üzenet, ami segít megtudni minden járműről azt, hogy hol van, merre halad, hányan ülnek benne, hány kg a súlya, mi a sebességvektora, stb. Itt is megjelenik a rétegek közötti optimalizáció: ha a jármű gyorsabban halad, akkor az üzenetek sűrűségét akár másodpercenként tíz alkalomra is tudja állítani, fordított esetben, lassú haladásnál csak egy üzenet kerül kiküldésre másodpercenként.



5. ábra. A V2X-architektúra „Facilities” rétege.

A másik legismertebb protokoll ebből rétegből a DENM (Decentralized Environmental Notification Message) üzeneteket definiáló [31]. Ez *eseményvezérelt*, a CAM-mel ellentétben: csak akkor küld üzenetet, ha valamilyen esemény bekövetkezett. Például, ha megállunk a leállósávban, akkor küld egy „álló jármű a leállósávban” üzenetet. Előre definiált eseményekhez kódokat rendelnek és az üzenetek magukat a kódokat tartalmazzák, csak idő- és geopozíció bélyeggel ellátva.

Vannak persze további üzenet típusok is a Facilities rétegben, melyek a közlekedési lámpák beállításait közlik (SPaTEM) [31], és ez alapján tudja az autó beállítani a sebességét, hogy pont zöld jelzésre érjen oda; vannak, amelyek szervíz üzeneteket továbbítanak [32]; olyanok melyek a kereszteződések geometriáját közlik a közeledő járművekkel (MAPEM) [31], vagy akár a különböző szenzorok által gyűjtött adatok megosztására képesek [33]. Ezekkel az ismeretterjesztő cikk terjedelmi korlátai miatt bővebben nem foglalkozunk.

Menedzsment réteg (ITS Management Layer)

Az ITS Menedzsment réteg – a következő szakaszban tárgyalt biztonsági réteghez hasonlóan – nem feleltethető meg egyik OSI modellben szereplő rétegnek sem. Ez a réteg felelős az ITS architektúrában található, a biztonsági rétegen kívül valamennyi réteg irányításáért, működésük összehangolásáért [9][34]. Az összehangoltság rendkívül fontos a kooperatív funkciókra kihegyezett C-ITS infrastruktúrákban, hiszen minden működési inkonzisztencia, nem kívánt késleltetés felboríthatja az optimalizált rendszert és komoly problémákkal járhat. A menedzsment réteg a cross-layer optimalizáció központja a C-ITS architektúrában (például itt található a hatékony közeghozzáférést megvalósító Decentralized Congestion Control, vagyis a DCC központi modulja is), éppen ezért áll kapcsolatban az összes többi réteggel.

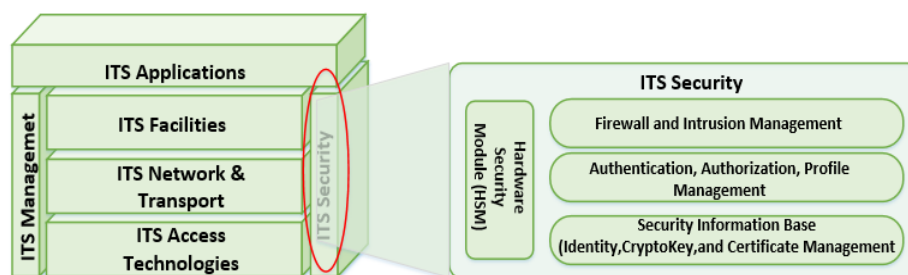
Biztonsági réteg (ITS Security Layer)

Az ITS Biztonság réteggel [35][36] ellátott szolgáltatások számára alapvető követelmény a megbízhatóság, integritás, autentikálás (confidentiality, integrity, authenticity), valamint a privát szféra védelmének biztosítása. Az alábbi pontokban röviden összefoglaljuk ezeket a fontos követelményeket:

- **Megebízhatóság (Confidentiality):** azt jelenti, ha Alice Bobnak küld egy üzenetet harmadik fél nem tudhat meg semmit sem az üzenet tartalmából (esetleg a hosszát). Ez gyakorlatilag az enkriptálással valósul meg.

- **Integritás (Integrity):** azt jelenti, hogy ha Alice küld egy üzenetet Bobnak, Bob egyértelműen képes azonosítani, ha valaki megpróbálta megmásítani a küldött üzenetet.
- **Autentikálás (Authenticity):** azt jelenti, ha Alice Bobnak küld egy üzenetet, akkor biztos lehet abban Bob, hogy az üzenet Alicetől származik és nem hamisan akart valaki Alice nevében üzenetet küldeni
- **Anonimitás (Anonymity):** A V2X kommunikáció által küldött üzeneteknek nem szabad semmilyen olyan információt tartalmazniuk, ami egyértelműen azonosítaná a gépjárművet, a gépjármű sofőrjét, vagy az utast.
- **Összekapcsolhatatlanság (Unlinkability):** a jármű által küldött üzenetek alapján ne legyen könnyen követhető a jármű. Ne legyen könnyebben követhető a V2X segítségével, mint a hagyományos vizuális módon.

Ezeket a követelményeket a V2X biztonsági réteg (6. ábra) megbízható hardverelemek (Hardware Security Module - HSM), biztonsági és tanúsítvány attribútumok, valamint a digitális aláírás (és azok ellenőrzése) valamint a hozzá tartozó PKI (Public Key Infrastructure) mechanizmusok segítségével biztosítja.



6. ábra. Az ITS Biztonság réteg szerkezete és feladatai.

A hardveres biztonsági modul (Hardver Security Module, HSM) jellemzően egy külső periféria. Feladata, hogy privát kulcsokat generáljon, tároljon és ezekkel speciális kriptográfiai műveleteket végezzen. Mivel egy privát kulcs egy randomszám, ezek generálásához a HSM modul egy valódi hardveres véletlenszám generátort (true random number generator) tartalmaz. A privát kulcs generáláson túl, a HSM feladata még az aláírások generálása is.

A digitális aláírás egy matematikai módszer arra, hogy kiszűrjessük azokat az üzeneteket, amik nem megbízható forrásból származnak, egyértelműen azonosíthatunk valakit. V2X-ben az ECDSA (Elliptic Curve Digital Signature Algorithm) [37] megoldást használják. Az ECDSA alapú PKI működése nagyon vázlatosan az alábbi: a járműben lévő HSM-mel generáltatunk egy kulcspárt. A publikus kulcsot elküldjük a Certificate Authority (CA) nevű entitásnak (a privát kulcs végig a járműhöz tartozó HSM-ben marad). A CA aláírja az ő privát kulcsával a jármű által elküldött publikus kulcsát. Ezt az aláírt publikus kulcsot nevezzük tanúsítványnak. Ezután ezt a tanúsítványt a CA visszaküldi a járműnek, ami a tanúsítványt mindenkinek elküldi rádióan, akinek aláírt üzenetet akar küldeni. A tanúsítvány segítségével az üzenetet fogadók biztosak lehetnek abban, hogy az információ a CA által hitelesített forrásból származik. Az üzenetet fogadók onnan tudják, hogy a küldő tanúsítványa megbízható, hogy ők is rendelkeznek a CA tanúsítványával. Így tudják hitelesíteni a rádióan fogadott tanúsítványt. Ez a PKI infrastruktúra az EU C-ITS Credential Management System (EU CCMS) rendszer [38][39] magjában működve biztosítja a járművek közötti biztonságos kommunikációt.

Alapvető V2X alkalmazások (ITS Applications Layer)

A cikkben követett „bottom-up” megközelítéssel a hozzáférési rétegtől eljutottunk egészen az alkalmazási réteghez [40][41], mellyel kapcsolatban az un. „Day 1” alkalmazásokat fogjuk bővebben tárgyalni, vagyis azokat, amelyeket a C-ITS/V2X technológia bevezetésének első lépéseinek tartanak. Közülük sok már most is használható vagy bemutatásra került pilot telepítések, demók, tesztek során.

A Car-2-Car Communication Consortium [42] megközelítését alapul véve a következő három csoportba soroljuk a V2X szabványosítás alatt lévő és tervezett alkalmazásait [43]: az első csoportban a „Day 1” alkalmazások vannak, melyek már most is működnek vagy tesztelés alatt állnak. A második és harmadik csoportban az előző csoport(ok)ra építő, magasabb hozzáadott értékű és persze ezzel párhuzamosan egyre bonyolultabb szolgáltatások tartoznak, ezeket villantjuk fel érdekességgként, hogy lássuk mi mindenre lehet majd képes a V2X a jövőben.

1. Tudatos vezetés (Awareness driving via status data)

A tudatosság arra utal itt, hogy a Facilities rétegnél tárgyalt CAM/DENM/stb. üzenetek révén a sofőr, illetve az autó tisztában van a környezetével, a környéken közlekedőkkel azáltal, hogy veszi és feldolgozza ezeket a periodikus/eseményvezérelt üzeneteket az autóktól. Előre „látja” ha a leállósávban vesztegel valaki, ha beláthatatlan helyről tolat kifelé az útestre, vagy ha baleset történt valahol. Ide tartozó alkalmazások a teljesség igénye nélkül:

- ütközési figyelmeztetés a kereszteződéseknel;
- rendőr, mentő, tűzoltó járművek közelségére vonatkozó értesítés;
- általános veszélyre való figyelmeztetés az útvonalon;
- álló/lassú járműre való figyelmeztetés.

2. Érzékelésekre alapuló vezetés (Sensing driving via sensor data)

A CAM- és egyéb szolgáltatások által közvetített alapadatok mellett, a V2X kommunikációra képes járművek a legkülönbözőbb szenzorai adatait is megoszthatják egymással: környezetükről pontosabb és mélyebb képet közvetíthetnek, így a közelükben közlekedő autók ismerete teljesebb lesz a környezetről. Figyelembe vehetnek például olyan környezeti tényezőket, közlekedési paramétereket, amelyeket más járművek vagy az útinfrastuktúra elemei érzékelnek. Így egy kanyarodó jármű tisztában lehet azzal, hogy útját a jobbra fordulás után egy gyalogos keresztezi majd. Ebbe a csoportba tartozó alkalmazások például a következők:

- „előzés alatt állsz” figyelmeztetés;
- távol(abb)i kereszteződés előtti figyelmeztetés;
- csoportos adaptív sebességtartó automatika;
- vészfékezés-jelzés;
- úttesttel kapcsolatos figyelmeztetések, távol(abb)ról, jóval az odaérkezés előtt.

3. Kooperatív és szinkronizált kooperatív vezetési műveletek (Cooperative and synchronized cooperative driving with intention and coordination data)

A CAM-üzenetek és a hatótávon belül tartózkodó vagy azon kívül lévő, de releváns adatokkal bíró autók szenzoradatai mellett a V2X kommunikációra képes járművek összehangoltan műexit

ködnak: segítik egymás döntéseit összetett forgalmi szituációkban: kifordulhat-e mellékútról, belekezdhet-e az előzésbe adott helyzetben, ha igen akkor hogyan soroljon be és a többi jármű hogyan segítheti a besorolását, stb. Ebbe a csoportba várt jövőbeli alkalmazások:

- kooperatív előzés (mindenki besegít az előző autó döntésébe és manőverének meghatározásába);
- kooperatív holttér-figyelmeztetés;
- kooperatív sávváltás;
- rajban/konvojban/csoportban haladás (pl. teherautóknál, üzemanyag-megtakarítási célzattal).

A járművek közötti kommunikáció lényege tehát az, hogy ha a járművezető vagy a járműszenzor nem is érzékeli, a jármű akkor is értesülhet arról, hogy a másik autó, az akadály, a dugó, a kátyú vagy a gyalogos ott van, amerre a jármű tart, és ezt az információt a jármű felhasználhatja (például a vezetőt értesítheti),

hála annak, hogy a közlekedésben részt vevő valamennyi elem kooperatív, és „elmondja” a többieknek a környezet általa felfedezett és digitálisan leképzett, közlekedés szempontjából releváns adatait.

Összefoglalás

A járműkommunikáció napjaink egyik legígéretesebb, nemzetközi szabványosítás alatt lévő fejlesztése. A közlekedés meghatározó szereppel bír mindennapjainkban, a mobilitás javulását gyakran egyenlővé teszik a gazdasági fejlődéssel: ahol autópálya épül, ott felvirágzik a környék, csak azért mert könnyebben, gyorsabban elérhetővé válik a régió az országban meghatározó szerepet játszó „csomópontokból”: a fővárosból és az ipari, logisztikai központokból. A közlekedés mindemellett negatív hatásokkal is bír: szennyezi a környezetet és sok ember haláláért felelős. A károsanyag-kibocsátást csak csökkenteni tudja a V2X járműkommunikáció, azáltal, hogy például a közlekedés ütemezését tökéletesíti, segít elkerülni a forgalmi dugókat, illetve konvojban, egymástól nagyon alacsony követési távolságra utaztatja a kamionokat, melyek így a légellenállás drasztikus csökkentése miatt rengeteget spórolnak. A haláleseteket viszont a jövőben akár teljesen ki is tudja majd küszöbölni: a V2X elsődleges célja a közlekedésbiztonság sokkal magasabb szintre emelése azáltal, hogy a járművek egymással kommunikálva megosztják azt a „tudást” amit szenzoraiak segítségével környezetükről begyűjtöttek.

A V2X-technológiák bevezetésének első lépései („Day 1” alkalmazások) már tesztelés alatt vannak, egyre szélesebb körben kezdik alkalmazni őket: arra alapulnak, hogy periodikus CAM-üzenetekkel és eseményvezérelt DENM-üzenetekkel a járművek értesítik egymást érkezésükről, megkülönböztető jelzést alkalmazó jármű közeledtéről, úthibákról, lassú vagy veszteglő járművekről. Itt az információ előre definiált üzenetekre alapuló megosztására építenek a szolgáltatások, de nincs benne még valódi kooperáció: ezt nevezik tudatos vezetésnek (awareness driving).

A következő szinten már további információkat is megosztanak egymással a járművek: az egyik autó által a zebrán érzékelt gyalogos annak is hasznos információ, aki még a sarok mögött autózik és pont arra készül befordulni, ahol a gyalogost érzékelték. Itt az információk továbbítása távolabbra is lehetséges, több ugráson keresztül és magasabb szintű információkat közvetít: vészfékezés jelzés a kettővel előttünk haladó autótól, „előzés alatt állsz” jelzés, valamint ide tartozik a csoportos adaptív sebességtartás is.

A harmadik szinten, ami egyelőre még bőven a jövőbe mutat, megjelennek a *kooperatív vezetési műveletek*, azaz a többi autó segít annak megítélésében, hogy belekezdhetek-e az előzésbe, a holtteret már nem csak a saját szenzorom figyeli, hanem a belső sávban 300 km/h-val érkező motorosról a többi autótól is értesülök, és ide tartozik a konvojban haladás is, ugyanis itt is szoros együttműködésre, szinkronizált gyorsulásra/lassulásra van szükség.

A V2X fejlesztésének távlati célja természetesen a teljesen *autonóm járművek* kiszolgálása. Az önvezetés kezdeti szintjét (saját, auton belüli) szenzoralapú, embert emuláló megoldások jellemzik. Minden autonóm járműnek szüksége van a környezetet leíró digitális reprezentációra: és ha mindenki csak a saját szenzorjaira támaszkodik, az sokkal kevesebb adat, mintha mindenki meg is osztaná a saját érzékeléseit. Ehhez kell a járműkommunikáció, melynek a szintjétől, szolgáltatásainak bonyolultságától, hozzáadott értékétől függően jutunk el az *önvezetés* magasabb szintjeire, ezt pedig a vázolt három lépcsőfokon való előrehaladás modellezi. A fejlődéssel fokozatosan létrejön a kooperatív tudatosság az egyes elemek (járművek, útmenti szenzorok, közlekedési lámpák, változtatható jelzésképű táblák, stb.) közt, kicserélik azt, hogy mit látnak a környezetből, és ezzel egyre teljesebb képet tudnak alkotni róla, ami a megfelelő beavatkozással egyre magasabb szintű közlekedésbiztonságot és hatékonyságot jelent.

Viszont az önvezetés akkor sem lesz teljes megoldás, ha majd egyszer szabályozott körülmények közt, széleskörűen megvalósul: megtörténhet majd, hogy a vezérlő intelligencia meghibásodik, nem képes vezetni, de az autó még vezethető lenne, motorikusan semmi baja. Ekkor jön képbe a „távoli vezetés” (remote driving), azaz az irodában ülő operátor szervízbe/a bázisra vezethetné az autót távolról. Ehhez tehát már nem kell működőképes vezérlő algoritmus, elég, ha a kommunikáció jól működik, megfelelően nagy sáv szélességgel és nagyon alacsony késleltetéssel. Itt már csak az 5G-6G alapú megoldásoknak [44] lehet létjogosultsága, ezek tudják ill. fogják tudni teljesíteni az extrém alacsony késleltetésre és a megfelelően nagy átviteli kapacitásra, küldetáskritikus működésre vonatkozó elvárásokat.

Végül a távoli jövőre való kitekintésként megemlíthetjük a V2X – IoT (Internet of Things) várt jövőbeli összefonódását [45]: ezzel újabb, óriási adatforráshoz juthatnak a közlekedők, ugyanis az IoT eszközök

lassan mindenhol (szinte minden újabb készülékben) megtalálhatók. A személyekhez köthető adatok továbbítása még jogi szempontból megoldandó kérdéskör, de amikor ez sikerül, egy még jobb minőségű adathalmazra alapozó, városi, sőt akár országszintű egyéni és közösségi közlekedés optimalizáló rendszer lesz megvalósítható, amivel már egészen közel kerülhet a V2X a kitűzött „nulla halálos áldozat a közlekedésben” céljához.

Hivatkozások

- [1] H. Zhou, W. Xu, J. Chen and W. Wang, "Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities," in *Proceedings of the IEEE*, vol. 108, no. 2, pp. 308-323, Feb. 2020, doi: 10.1109/JPROC.2019.2961937.
- [2] Booz Allen Hamilton, U.S. Department of Transportation, Intelligent Transportation Systems Joint Program Office History of Intelligent Transportation Systems, May 2016. https://rosap.ntl.bts.gov/view/dot/30826/dot_30826_DS1.pdf (utoljára megnyitva: 2020.05.10)
- [3] Waze, A legjobb útvonal valós időben – a többi autóvezető segítségével, <https://www.waze.com/hu>, (utoljára megnyitva: 2020.05.10)
- [4] T. Edwards, "Connected and automated vehicles: concepts of V2x communications and cooperative driving," *Autonomous Passenger Vehicles*, London, 2015, pp. 1-14, doi: 10.1049/ic.2015.0060.
- [5] Vision Zero: Safety. Health. Wellbeing, <http://visionzero.global/>, (utoljára megnyitva: 2020.05.10)
- [6] 2030 climate & energy framework, https://ec.europa.eu/clima/policies/strategies/2030_en, (utoljára megnyitva: 2020.05.10)
- [7] H. Wymeersch, G. R. de Campos, P. Falcone, L. Svensson and E. G. Ström, "Challenges for cooperative ITS: Improving road safety through the integration of wireless communications, control, and positioning," 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, 2015, pp. 573-578, doi: 10.1109/ICCNC.2015.7069408.
- [8] G. Karagiannis et al., "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," in *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584-616, Fourth Quarter 2011, doi: 10.1109/SURV.2011.061411.00019.
- [9] ETSI EN 302 665 V1.1.1 (2010-09), Intelligent Transport Systems (ITS); Communications Architecture
- [10] ISO / IEC 7498-1: Open Systems Interconnection - Basic Reference Model, <https://www.iso.org/standard/20269.html>, (utoljára megnyitva: 2020.05.10)
- [11] Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijnen, Boangoat Jarupan, Kenneth Lin, and Timothy Weil: Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions, *IEEE Communications Surveys & Tutorials*, Vol. 13, No. 4, 4th Quarter 2011, page: 585-616
- [12] ETSI EN 302 663 V1.3.1 (2020-01), ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band
- [13] ETSI TS 123 285 V15.4.0 (2020-01), LTE; Architecture enhancements for V2X services (3GPP TS 23.285 version 15.4.0 Release 15)
- [14] IEEE, "IEEE Standard for Information technology - Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Standard 802.11-2016, December 2016, <https://standards.ieee.org/findstds/standard/802.11-2016.html>, (utoljára megnyitva: 2020.05.10)
- [15] C-ROADS Platform, <https://www.c-roads.eu/platform.html>, (utoljára megnyitva: 2020.05.10)
- [16] Connected Vehicle Test Bed, Testing Connected Vehicle Technologies in a Real-World Environment, https://www.its.dot.gov/research_archives/connected_vehicle/dot_cvbrochure.htm, (utoljára megnyitva: 2020.05.10)
- [17] ETSI EN 302 571 V2.1.1 (2017-02), Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
- [18] 2008/671/EC: Commission Decision of 5 August 2008 on the harmonised use of radio spectrum in the 5875 - 5905 MHz frequency band for safety-related applications of Intelligent Transport Systems (ITS), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0671>, (utoljára megnyitva: 2020.05.10)
- [19] ECC Report 250, Compatibility studies between TTT/DSRC in the band 5805-5815 MHz and other systems, <https://www.ecodocdb.dk/download/f4340389-e665/ECCRep250.pdf>, (utoljára megnyitva: 2020.05.10)
- [20] ETSI TS 102 792 V1.2.1 (2015-06), Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range
- [21] 3GPP TR 36.885 V14.0.0, Study on LTE-based V2X Services (Release 14), June 2016.
- [22] K. Ganesan, P. B. Mallick, J. Löhr, D. Karamatsis and A. Kunz, "5G V2X Architecture and Radio Aspects," 2019 IEEE Conference on Standards for Communications and Networking (CSCN), GRANADA, Spain, 2019, pp. 1-6, doi: 10.1109/CSCN.2019.8931319.
- [23] C-ROADS, Radio frequencies designated for enhanced road safety in Europe - C-Roads position on the usage of the 5.9 GHz band, https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/C-Roads_Position_paper_on_59GHz_final.pdf, (utoljára megnyitva: 2020.05.10)
- [24] ASECAP Position Regarding LTE-V2X in the 5GHz Band, https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/ASECAP_position_regarding_LTE.pdf, (utoljára megnyitva: 2020.05.10)
- [25] ETSI EN 302 636-3 V1.2.1 (2014-12), GeoNetworking; Part 3: Network Architecture

-
- [26] ETSI EN 302 636-5-1 V2.2.1 (2019-05), GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol
- [27] J. Jeong, Ed., IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases, draft-ietf-ipwave-vehicular-networking-14, March 9, 2020., <https://tools.ietf.org/html/draft-ietf-ipwave-vehicular-networking-14>, (utoljára megnyitva: 2020.05.10)
- [28] S. Kuhlmoorgen, I. Llatser, A. Festag and G. Fettweis, "Performance Evaluation of ETSI GeoNetworking for Vehicular Ad Hoc Networks," 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, 2015, pp. 1-6, doi: 10.1109/VTCSpring.2015.7146003.
- [29] ETSI TS 102 894-1 V1.1.1 (2013-08), Part 1: Facility layer structure, functional requirements and specifications
- [30] ETSI EN 302 637-2 V1.4.1 (2019-04), Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service
- [31] ETSI EN 302 637-3 V1.3.1 (2019-04), Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service
- [32] ETSI TS 102 890-1 V1.1.1 (2017-05), Facilities layer function; Part 1: Services Announcement (SA) specification
- [33] ETSI TR 103 562 V2.1.1 (2019-12), Basic Set of Applications; Analysis of the Collective Perception Service (CPS); Release 2
- [34] ETSI TS 103 175 V1.1.1 (2015-06), Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium
- [35] ETSI TS 102 731 V1.1.1 (2010-09), Security; Security Services and Architecture
- [36] ETSI TS 102 940 V1.3.1 (2018-04), Security; ITS communications security architecture and security management
- [37] Don Johnson, Alfred Menezes, Scott Vansto, The Elliptic Curve Digital Signature Algorithm (ECDSA), <https://www.cs.miami.edu/home/burt/learning/Csc609.142/ecdsa-cert.pdf>, 2001. (utoljára megnyitva: 2020.05.10)
- [38] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1.1 June 2018, https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf, (utoljára megnyitva: 2020.05.10)
- [39] Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1 December 2017, https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf, (utoljára megnyitva: 2020.05.10)
- [40] ETSI TS 102 637-1 V1.1.1 (2010-09), Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements
- [41] ETSI TR 102 638 V1.1.1 (2009-06), Basic Set of Applications; Definitions
- [42] CAR 2 CAR Communication Consortium – Key player with high reputation in driving C-ITS developments and assisting to achieve vision zero, <https://www.car-2-car.org/>, (utoljára megnyitva: 2020.05.10)
- [43] CAR 2 CAR Communication Consortium, Guidance for day 2 and beyond roadmap, https://www.car-2-car.org/fileadmin/documents/General_Documents/C2CCC_WP_2072_RoadmapDay2AndBeyond.pdf, (utoljára megnyitva: 2020.05.10)
- [44] K. B. Letaief, W. Chen, Y. Shi, J. Zhang and Y. A. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks," in IEEE Communications Magazine, vol. 57, no. 8, pp. 84-90, August 2019, doi: 10.1109/MCOM.2019.1900271.
- [45] A. Kunz, L. Nkenyereye and J. Song, "5G Evolution of Cellular IoT for V2X," 2018 IEEE Conference on Standards for Communications and Networking (CSCN), Paris, 2018, pp. 1-6, doi: 10.1109/CSCN.2018.8581830.