

DEBRECENI EGYETEM
INFORMATIKAI KAR
ADATTUDOMÁNY ÉS VIZUALIZÁCIÓ TANSZÉK

Anonim üzenetküldés VANET hálózatokban



Témavezetők:

Dr. Pintér-Husztai Andrea

egyetemi docens

Girászi Tamás

PhD hallgató

Szerző:

Vágner Máté

programtervező informatikus MSc

Bírálatra való beküldéséhez hozzájárulok

Debrecen, 2024

Tartalomjegyzék

Kivonat	3
1. Bevezetés	4
2. Irodalmi áttekintés	7
2.1. VANET protokollok	7
2.2. Pseudonym-based Hybrid, Privacy-preserving Broadcast Protocol	10
2.3. Rövid távú kommunikáció VANET-ekben	11
2.3.1. IEEE 1609 - WAVE Architektúra	11
2.3.2. IEEE 802.11 - VANET Hozzáférési Réteg Szabványok	12
2.3.3. Intelligens Közlekedési Rendszerek	13
3. A javasolt protokoll	14
3.1. Résztvevők	14
3.1.1. Fedélzeti egység, OBU	14
3.1.2. Útmenti egység, RSU	15
3.1.3. Megbízható harmadik fél, TA	15
3.1.4. Blokklánc, BC	15
3.2. Biztonsági elvárások	16
3.3. Elméleti háttér	17
3.3.1. Elliptikus görbék	17
3.3.2. Schnorr aláírás	19
3.3.3. Nulla ismeretű protokollok	20
3.4. A protokoll lépései	21
3.4.1. Inicializáció	21
3.4.2. Regisztráció	22
3.4.3. Incidensek jelentése	23

3.5. Biztonsági elemzés	24
4. Implementáció	26
4.1. Használt technológiák	26
4.1.1. Veins szimulációs keretrendszer	26
4.1.2. Használt WAVE szabványok	28
4.1.3. Veins modulok	30
4.2. Hálózati modell	31
4.3. A protokoll implementáció alapegységei	32
4.3.1. Adatkapcsolati réteg fejlécei	32
4.3.2. Üzenet továbbadási mechanizmus	33
4.4. A protokoll fázisainak implementálása	34
4.4.1. Inicializáció	35
4.4.2. Regisztráció	36
4.4.3. Incidensjelentés	39
4.4.4. Biztonsági szolgáltatások	40
5. A rendszer elemzése	41
5.1. A rendszer szimulációjának elemzése	41
5.2. Kommunikációs hatótávolság városi környezetben	43
6. Összefoglalás	46
Saját munka leírása	48
Köszönetnyilvánítás	50
Irodalomjegyzék	51
Ábrajegyzék	57
Algoritmusjegyzék	58

Kivonat

A járművek közötti kommunikációs hálózat kialakítása, és az ebben rejlő lehetőségek kihasználása már jó ideje vizsgált téma. Ezen hálózatok, legyen szó akár csak a forgalom vezérlésére fókuszáló, vagy akár már a multimédiás szolgáltatásokat is kínáló rendszerekről, sok érzékeny és személyes adatot is kezelnek. Az egyik ilyen legérzékenyebb adat a járművek helyzete és az ebből megállapítható útvonaluk. Ezt többek között megfigyelésre és nyomon követésre is fel lehet használni, így a védelmére nagy figyelmet kell fordítani.

Bemutatunk egy protokollt, ami biztosítja a járművek és az infrastruktúra közötti anonim és ugyanakkor hiteles kommunikációt, mely forgalmi incidensek (pl. baleset, forgalmi dugó) bejelentését teszi lehetővé. Ezt egy decentralizált környezetben valósítjuk meg, amihez a Solana blokklánc használatát javasoljuk. Ez egy hibrid rendszer, ami ötvözi az EU-ban is használt WAVE kommunikációs szabvány elemeit és a blokklánc technológiát. A WAVE alkalmas a közelben lévő járművek gyors értesítésére, míg a blokklánc technológia az anonim, elosztott és ellenőrizhető adattárolást teszi lehetővé, melyhez a távolabbi járművek is hozzáférnek.

A rosszindulatú, valótlan bejelentések elkerülésére a blokklánc technológiában alkalmazott ösztönző-büntető megoldást alkalmazzuk, mely egy egyszerűbb és hatékonyabb protokollt eredményez. Ezentúl figyelmet fordítunk arra is, hogy az anonim hálózati kommunikáció ne csak az alkalmazási rétegben valósuljon meg, hanem az alacsonyabb hálózati rétegekben is. A kriptográfiai protokoll lépésein túl, a megvalósításához szükséges WAVE hálózati modellben megjelenő csomagokat és eljárásokat is bemutatjuk. Az elkészített protokoll hálózati kommunikációs részét egy szimulációban le is implementáltuk, és elemeztük a működését is.

1. fejezet

Bevezetés

A különböző hálózatok az elmúlt évtizedekben a mindennapi életünk szerves részévé váltak. Az élet különböző területein különféle eszközöket használunk, melyek, felhasználási céljuktól függően, többféle hálózaton keresztül kommunikálhatnak. Ezen hálózatok lehetnek vezetékes vagy vezetékek nélküli kapcsolatokon keresztül is szervezve.

Az ad hoc hálózatok a vezetékek nélküli hálózatok egy típusát képezik. Ezek a hálózatok autonóm rendszerként működnek, amelyeket kitelepített vagy mozgó csomópontok alkotnak. Komplex infrastruktúra nélküliek, önhangolóak, önszerveződők és önvezérlők. Előnyei közé tartozik, hogy könnyen felállítható vagy telepíthető bárhová és bármikor. Általában egyszerű infrastruktúrával rendelkeznek és csak minimális központi vezérlést igényelnek. Ha egy ilyen hálózatban a csomópontok többsége olyan mobil egység, ami szabadon határozhatja meg saját mozgását, miközben önkényesen szervezheti működését, akkor azt mobil ad hoc hálózatnak (Mobile Ad hoc NETWORK, MANET) nevezzük. Egy MANET hálózat topológiája gyorsan és kiszámíthatatlanul változik.

A járművek ad hoc hálózata (Vehicular Ad hoc NETWORKS, VANET) egy olyan MANET hálózat, amelynek csomópontjai járművek. Ezek az eszközök az úthálózati infrastruktúra, a közlekedési szabályok és az aktuális közlekedési viszonyok által meghatározott módon változtathatják helyzetüket. Célja a biztonságosabb és hatékonyabb közlekedés elősegítése, így létrehozva egy intelligens közlekedési rendszert (Intelligent Transport System - ITS). Ennek érdekében a résztvevők út- és közlekedési információkat osztanak meg egymással. Ezt az alapcél egészítik ki az ilyen hálózatokra épülő egyéb szolgáltatások, mint például az elektronikus fizetés vagy a médiamegosztás. Egy ilyen hálózatban lehetőség van direkt és együttműködés alapú jármű-jármű (Vehicle-to-Vehicle, V2V), jármű-infrastruktúra (Vehicle-to-Infrastructure,

V2I) és jármű-bármilyen (Vehicle-to-everything, V2X) kommunikációra. A VANET hálózatok a közlekedő járművek miatt rendkívül dinamikusak és gyorsan változó hálózati topológiával rendelkeznek.

A járművekbe fedélzeti egységeket szerelnek (On Board Unit, OBU), amelyek a kommunikációért és a kriptográfiai kulcsok tárolásáért felelősek. Az útszakaszok mellett, az infrastruktúra kialakításához, útmenti egységeket (Road Side Unit, RSU) helyeznek el.

A járművek helyzete és ennek időbélyegzett sorozata érzékeny információkat hordoz, mivel lehetővé teszi a felhasználók nyomon követését. Például, egy járművezető vallási hovatartozása kikövetkeztethető, ha a helyinformációk szerint gyakran jár egy bizonyos vallású intézményekbe. Ezért egy VANET rendszerben kiemelt fontosságú az **anonimitás megőrzése**. Emellett elengedhetetlen, hogy az adatok hitelességét is ellenőrizzük, így megakadályozva, hogy támadók hamis információkkal félrevezessék a többi résztvevőt.

Problémát jelent a VANET rendszerek esetén az **infrastruktúra kialakítása és fenntartása, valamint ezeknek a költségei**. Egy RSU maximális kommunikációs távolsága 1000 m, de városi környezetben ez 300 m-re csökkenhet. Ez azt jelenti, hogy a legkedvezőbb esetben is minden 4 km^2 területen szükség van egy RSU telepítésére. Debrecen város teljes 461.7 km^2 területének a lefedése legalább 116 RSU telepítését igényelné, amely jelentős költségekkel járna. Ezen egységek fenntartása további egyéb kiadást követelne meg.

Ebből adódóan kutatásunk egyik fő irányvonala az volt, hogy olyan rendszert dolgozzunk ki, amely a felmerülő költségeken csökkenteni tud. A járművek egymás közötti kommunikációjának segítségével lehetséges az RSU által ténylegesen lefedett területet növelni. Ebben az esetben a tartomány, ahonnan közvetetten elérhető az RSU, nagy mértékben függ az épp aktuális, dinamikusan változó környezettől. Egy másik lehetőség ennek megoldására az, hogy ha a járműveket a hálózatra kötjük, és így biztosítunk egy másodlagos csatlakozási lehetőséget. Viszont meg kell jegyezni, hogy egy ilyen megoldás esetén a hálózat késleltetése nagyobb, mint ha a rövidtávú kommunikációs technológiát használnánk.

Ezek az igények vezettek a jelenlegi, személyes adatok védelmét biztosító algoritmusok (User Privacy-Preserving Mechanisms, UPPMs) alkalmazásához. Az eddig született megoldások többnyire [6], [23], [32], [37], [39] egyetlen hálózati rétegre fókuszálnak, viszont a támadók a rendszer több rétegét is célba veszik, komplex támadást indítva. Dolgozatunk célja, hogy ezen rendszerekhez olyan megoldást ajánljon, amellyel képesek lesznek megfelelni a velük szemben támasztott biztonsági elvárásoknak összetett szituációkban is. Ennek eléréséhez bemutatjuk a

Pseudonym-based Hybrid, Privacy-preserving Broadcast Protocol (PHP-BD) névre keresztelt protokollt, amivel az alábbi hozzájárulásokat tesszük:

- Készítettünk egy kriptográfiai protokollt, amely blokklánc-alapú tanúsítványokat kezel, elliptikus görbe kriptográfián (Elliptic Curve Cryptography, ECC) alapul, és nem igényel nagy számú előre hitelesített tanúsítványok kiállítását.
- A javasolt protokoll nem igényli a járművek fizikai bevonását az egységek álneveinek frissítéséhez és a nem kívánatos egységek kitiltására.
- A javasolt rendszer hibrid, amely a blokklánc technológiára és a WAVE protokollra épül. Lehetővé teszi a közlekedési incidensek közelében levő járművek számára az üzenetek gyors terjedését (WAVE-alapú üzenetküldés), ezen túl a távolabbi résztvevők is időben értesülnek az incidensről (blokklánc-alapú üzenetküldés), ami segíthet az útvonal tervezésében és az adott szakasz tehermentesítésében.
- A mobilhálózaton keresztül elérhető blokklánc segítségével a rendszer kiterjeszthető olyan területekre is, ahol nincs kiépített infrastruktúra, vagy nincs elegendő jármű a közelben ahhoz, hogy biztosítsa a WAVE-alapú kommunikációt. Következésképpen, az információk még azokra a helyekre is eljutnak, ahol korlátozottak a kommunikációs lehetőségek.
- A hibrid rendszernek köszönhetően a hálózat infrastruktúrájának kitelepítési és karbantartási költsége is csökken, mivel nagyobb területet rendelhetünk egy-egy RSU-hoz.
- A blokklánc technológia decentralizált vezérlésével, elosztottan biztosítjuk a rendszerparaméterek és az egyéb nyilvános paraméterek hitelességét, valamint a tisztességtelen járművek anonimitásának visszavonhatóságát az RSU és TA együttes kérésére.
- A bemutatott kommunikációs rendszert implementáltuk egy szimulációs környezetben.

A dolgozat fő célja a tervezett kriptográfiai protokoll és a VANET hálózatának megvizsgálása és annak szimulációjának bemutatása. A dolgozat megemlíti, hogy egy blokklánc technológiát hogyan használna fel a működéséhez, de ezen folyamatok pontos definiálása nem tárgya. Először bemutatjuk a témához kapcsolódó szakirodalmat (2. fejezet). Ezután részletesen ismertetjük az ajánlott PHP-BP protokollt (3. fejezet), bemutatjuk az általunk készített szimulációt (4. fejezet), majd lezárásként elemezzük (5. fejezet) is.

2. fejezet

Irodalmi áttekintés

2.1. VANET protokollok

A VANET hálózatokban felmerülő biztonsági kérdések orvosolására általában álnév (pseudonym) alapú hitelesítést használunk. Ezen módszerek lehetővé teszik, hogy a résztvevők elfedjék a kilétüket egy álnév segítségével, az üzenetek hitelesíthetőségének megtartása mellett. A résztvevők, a nyomon követés megakadályozása céljából, folytonosan módosítják álneveiket.

Általában az álnevek alapvetően egy aszimmetrikus kulcspárhoz tartoznak. A titkos kulcsot digitális aláírásra használjuk, melynek célja az üzenetek forrásának hitelesítése, és integritásának ellenőrzése. Ezzel védekezve, hogy az üzenet tartalmát támadók ne módosítsák, annak a hálózaton belül történő terjedése alatt.

Az alapján, hogy mit használ egy megoldás az álnevek alapjaként, beszélhetünk publikus kulcs infrastruktúra (public key infrastructure, PKI)[4] és identitás alapú (identity-based)[39] megoldásokról.

Publikus kulcs infrastruktúrájú megoldást használ például az IEEE [19] és ETSI [11] által kibocsátott VANET standardok biztonsági kiegészítése is, valamint Raya és Hubaux [4]. Ez esetben a járművek a rendszer vezérlőjétől egy hosszú lejáratú tanúsítványt, valamint több rövid életidejű álnevet kapnak.

Számos javaslatban a járművek fedélzeti egységére feltöltenek jelentős számú, előre legenerált, hiteles álnevet. Ez elég lehet 1 hétre, hónapra vagy évre is, de ennek egyik hátránya a tárigény. Ezentúl, ha offline frissítjük ezen kulcsokat, akkor a sűrűn igényelt frissítések nem teszik praktikussá a használatát. Egy kódbasis feltörése esetén pedig bármilyen támadó küldhet hamis üzenetet hiteles álnévvel[47].

Ma és társai javaslata [6] lehetővé teszi, hogy tetszőleges időben, folyamatosan újra töltsék az álnevek halmazát, de ez rengeteg tárhely és számítási igényt tesz a központi megbízható vezérlőegységre (Central Authority, CA). Az ilyen rendszerekben a központi egységek nagyon sokszor szűk keresztmetszetet is jelentenek.

Lu és társai javaslata[5] egy hatékony feltételes személyazonosság megőrzési (Efficient Conditional Privacy Preservation, ECPP) protokollt mutat be, ahol minden OBU a legközelebbi RSU-tól kér ideiglenes tanúsítványokat. Ez a megoldás támogatja azt, hogy az OBU-k sűrűn kérhessenek újabb és újabb tanúsítványokat, ami extra számítási igényt jelenthet az RSU-nak.

A nagy mennyiségű, rövid életidejű tanúsítványok kezelése, esetleges visszavonása is komoly kérdés. Rigazzi és társai javaslata [21] ismertet egy tanúsítvány visszavonási listát (Certificate Revocation List, CRL), ami lehetővé teszi, hogy a vezérlőszerv generáljon, és kiiltson járműveket a kommunikációból. Így védekezik az esetlegesen rossz kezekbe került és ártó szándékú járművek ellen. Viszont, a központi ellenőrzés miatt, ez szintén nagyon hamar gyenge keresztmetszetet jelenthet. Wasef[14] egy üzenet hitelesítési protokollt javasol, ami a tanúsítvány visszavonási lista helyett hash alapú üzenethitelesítési kódot (Hash-based Message Authentication Code, HMAC) használ, az ellenőrzés gyorsítása céljából.

Lu és társai[25] egy olyan PKI alapú protokollt ajánlanak, ami blokklánc technológiára épül. Megoldásukban három tárolt láncra van szükség. Egy a tanúsítványoknak, egy a küldött üzeneteknek, és egy a CRL-nek.

Nitschke és társai [42] egy olyan protokollt javasolnak, ami a csomagok összekapcsolhatatlanságát biztosítja, csoportos aláírások és mixnetek együttes alkalmazásával. Itt az OBU-k több csoport részei is, és válthatják, hogy épp mikor, melyik csoporttal írják alá üzeneteiket. Ez a megoldás feltételezi, hogy minden jármű esetén legalább 5 szomszédos eszköz tartózkodjon a környezetében, amik közül legalább 3 részlegesen megbízható, ami közel sem garantálható minden esetben.

Az álnevek módosítására használt módszer alapján három kategóriába lehet sorolni a protokollokat: álnév változtató[6] (Pseudonym Change Schemes), álnév cserélő[26] (Pseudonym Swap Schemes), vagy hibrid[9], [31] megoldások. A fentebb említett protokollokat mind az álnévváltoztató protokollok közé lehet sorolni.

Az álnévcserélő protokollok résztvevői egymás között cserélik ki álneveiket úgy, hogy ugyanaz az álnév már egy másik járművet fed el. Ezeket az új álnévkapcsolatokat, viszont jelezni kell a központi vezérlőszerv felé, amit az RSU hajt végre, merevvé téve ezeket a sémá-

kat. Ezt a cserét Wang és társai[26] ajánlásában a járművek kezdeményezik a szomszédjaikkal az RSU közreműködésével. Megjegyzendő, hogy ezen rendszerek infrastruktúrájának kiépítése jóval több RSU telepítését igényelheti, ami költségeit növeli, mivel ezen rendszerekben az egy RSU által lekezelhető egységek száma szűk keresztmetszetet jelenthet. Eckhoff és társai[9] javasolnak egy olyan protokollt, ahol az egységek RSU nélkül végzik az álnévcserét, viszont ezeknél a megoldásoknál felmerül az ártó szándékú járművek kizárásának problémája, azaz nem biztosítják a letagadhatatlanságot.

A hibrid megoldások ötvözik a két módszert. Résztevői változtatják és cserélik is álneveket egymás között. Előnyük a tárhely és számítási igény csökkentése úgy, hogy meg tudják tartani a VANET felhasználók személyes adatainak védelmét (ami kifejezetten nehéz a csak álnévcserét használó protokollok esetében[47]). Singh és társai [31] javaslatában egy fix-méretű álnévhalmoz van minden egyes időablakhoz, és minden álnév csak ennek lejártá után változik. A rendszer újrahasználja a már lejárt álneveket, ezzel biztosítva, hogy a fixált mennyiségű álnévhalmoz elég az igények kiszolgálásához.

Ravi és társai tanulmánya [38] olyan biztonsági architektúrát ismertet, amely a blokklánc technológiát és a mobil peremszámítást(Edge computing) ötvözi. Az architektúra három réteget foglal magában: az érzékelési réteg, amely a járműveket és az útmenti egységeket (RSU) tartalmazza, a peremszámítási réteg, amely számítási erőforrásokat és szolgáltatásokat biztosít, valamint a szolgáltatási réteg, ahol az adatok tárolásra kerülnek. A járművek korlátozott számítási kapacitásuk miatt csak alapvető blokklánc funkciókat látnak el. Az RSU-k stabil blokklánc hálózatot alkotnak, egy egységes adatbázist biztosítva. A peremszámítási réteg feladata a blokklánc konszenzus folyamatához tartozó számítási igények kezelése, valamint további számítási igényes feladatok ellátása. Ez a tanulmány egy általános vázat javasol, és nem törődik az egyéb biztonsági kérdésekkel. A mi protokollunk kihagyja az RSU-k blokkláncba szervezését, és a hálózattól teljesen független blokklánc használatát javasoljuk. Ennek előnye az, hogy olcsóbb és kisebb számításiigényű RSU-k is elegendőek lehetnek. Léteznek olyan láncok és konszenzusprotokollok, amelyek nagy tranzakció mennyiséget képesek feldolgozni, így szükségtelessé válik az extra számítási réteg, mivel ezt a blokklánc kezeli. A nagyobb és ismert láncok használata emellett a rendszer rendelkezésre állását is javítja.

Luo és társai [30] egy blokkláncon alapuló megbízhatóság-orientált helyadat-védelmi rendszert javasolnak, amely a helymeghatározáson alapuló szolgáltatások használata során fellépő járművek helyadat-védelmét célozza meg. Az előzetes k-anonimitáson alapuló módszerek hi-

ányosságait felismerve, amelyek nem veszik figyelembe a résztvevők megbízhatóságát, egy új trust management módszert vezet be. Ez a módszer csak a megbízhatónak ítélt járművek közötti együttműködést teszi lehetővé, kezelve azokat a sebezhetőségeket, amelyek a meglévő elosztott k-anonimitási módszereknél fordulhatnak elő. Ebben a rendszerben egy megbízható harmadik fél állítja ki az álneveket és tanúsítványokat a kommunikáló felek számára. Emellett a kommunikáló felek információhoz jutnak a másik fél korábbi kommunikációjáról. A mi rendszerünk mellőzi ezt a harmadik felet, és decentralizált módon történik az álnevek meghatározása.

Zhang és társai tanulmánya [27] a járművek közötti ad hoc hálózatok (VANET) biztonságának javítására összpontosít, különös tekintettel a blokklánc technológia alkalmazására. A blokklánc technológia integrálása a VANET rendszerekbe a biztonság növelésére szolgál, csökkentve a központosított hitelesítő hatóságoktól való függőséget. A tanulmány kitér a jármű-az-infrastruktúrához (V2I) és jármű-a-járműhöz (V2V) kommunikációs modellek biztonsági kihívásaira és azok kezelésére. A tanulmány hangsúlyozza, hogy a blokklánc alkalmazása jelentős mértékben javíthatja a VANET rendszerek biztonságát, lehetővé téve a biztonságos kommunikációt a járművek között. Ez a protokoll a Bitcoin lánc implementációjára épül, és diszkrét logaritmus alapú rendszereket alkalmaz. Ezzel szemben a mi megoldásunk nagyobb számú tranzakciót képes feldolgozni és elliptikus görbékre épít, amely elősegíti a kulcsok méretének csökkentését.

2.2. Pseudonym-based Hybrid, Privacy-preserving Broadcast Protocol

A 2.1. fejezetben tett észrevételek és javaslatok alapján dolgoztunk a protokollunk továbbfejlesztésén, amit a Pseudonym-based Hybrid, Privacy-preserving Broadcast Protocol (PHP-BP) névre kereszteltünk.

A PHP-BP az elliptikus görbe Schnorr aláírási sémán és non-interaktív nulla ismeretű protokollokon alapszik, az identitás alapú kriptográfia és bilineáris leképezések használata helyett [10], [41].

A protokollunk nem igényli nagyszámú álnév előre generálását. Minden járműhöz csupán egy blokklánc-alapú tanúsítvány és egy aktuális álnév tartozik. Ezzel használata praktikusabb, és kevésbé tárigényes. Ezt az álnevet a mi protokollunkban a blokklánc kezeli, ahonnan minden

OBU és RSU is lekérdezheti. Így decentralizált rendszert eredményezve, csökkentve a harmadik felektől való függést.

A többi kutatással ellentétben, a protokollunk ösztönzést nyújt a rendszerünk használatára, így segítve elő az információk megosztását. Ezt úgy éri el, hogy rendszerhasználati díjat von le a használoktól, de ezt jutalommal együtt visszautalja a valós jelentéseket szolgáltató felhasználóknak, míg a hamisnak bizonyuló jelentések díját nem adja vissza, megbüntetve őket. A fent említett rendszerek továbbá nem vették figyelembe a kommunikációs hálózaton kívüli járműveket sem. Lehetőség van emellett a rosszindulatú felek kizárására egy harmadik fél bevonása nélkül. Lehetővé tettük a rendszerből történő teljes kizárást is, ám ehhez nem elégséges egyetlen központi fél.

2.3. Rövid távú kommunikáció VANET-ekben

2.3.1. IEEE 1609 - WAVE Architektúra

A Wireless Access in Vehicular Environment (WAVE) protokoll célja, hogy lehetővé tegye a járművek közötti kommunikációt ad hoc mobil környezetben. Az első verziója 2013-ban került kidolgozásra (IEEE Std 1609.0-2013) [15], majd 2019-ben az architektúrát felülvizsgálták, és létrehozták a jelenleg is aktív szabványt, amely a WAVE hálózatok architektúráinak kiépítéséhez és működtetéséhez nyújt útmutatást [28].

A WAVE a IEEE 1609 és IEEE 802.11 [7], [15], [28], [45] szabványcsaládok különböző elemein alapszik, és számos lehetséges kiegészítést tartalmaz, mint például hálózatbiztonság, közlekedésbiztonság, vagy kommunikációs hatékonyság növelését célzó szolgáltatások.

Ezentúl még, főleg az új generációs rendszerekre jellemző szolgáltatásokat is definiál, mint például elektronikus fizetési protokollok intelligens közlekedési rendszerek (ITS) számára (IEEE Std 1609.11TM).

Megjegyzendő, hogy az Amerikában szabványnak számító Dedikált Rövidtávú Kommunikáció (Dedicated Short Range Communications, DSRC) és a WAVE technológiai alapjai megegyeznek, mivel a 802.11p-2010[7] standard alapvető része a DSRC-nek. Azóta a WAVE több lehetséges szolgáltatással is bővült, új szabványok készültek mellé, valamint más technológiák is felhasználták és továbbfejlesztették.

2.3.2. IEEE 802.11 - VANET Hozzáférési Réteg Szabványok

IEEE 802.11p

Az IEEE 802.11p[7] standard az 5.9 GHz frekvenciasávon működik, és a járműhálózatokra specializált változata a 802.11-es szabványnak, mely a WAVE architektúrának is alapja. Ez a szabvány a meghatároz egy hozzáférési réteget és annak működését. Ennek része a hálózat fizikai és adatkapcsolati (MAC) rétegje, valamint az adatkapcsolati réteg alrétegei is. A WAVE további MAC rétegbeli kiegészítéseket is tartalmazhat.

IEEE 802.11a standardon alapszik, ami a Wi-Fi technológia alapja is. Az alaptechnológiához képest bevezetett változásoknak köszönhetően sokkal megbízhatóbb hálózatot biztosít a VANET-ek dinamikus topológiájában is. A fizikai rétegen belül, az egyik legnagyobb eltérés az, hogy a sávszélesség és a segédvívő-frekvenciák közötti különbség feleakkora. A szabvány legfeljebb 200 km/h sebességet támogat 100ms késleltetési idővel, és 99% megbízhatósággal, legfeljebb 1000m-es hatótávon belül [43], amely sűrűn épített, és forgalmas városi környezetben, általában 300m-re csökken. Ugyanakkor a [20] szerzői tapasztalata szerint a gyakorlatban megvalósított rendszerek az üzeneteket várhatóan csak 78%-s valószínűséggel juttattja célba. Az alacsony késleltetés eléréséhez a csatorna elérése előtt nincs hitelesítés és az üzenet újra küldése se engedélyezett [35].

IEEE 802.11bd

A 802.11p leváltására fejlesztett, "következő generációs" VANET hálózat hozzáférési protokoll a 802.11bd (IEEE 802.11bd-2022 [45]). Ennek a feladatcsoportja azután formálódott, miután a 802.11p-re épülő biztonsági rendszerek megbízhatósága és késleltetése, a fizikai és MAC rétegek limitációi miatt, kevésnek bizonyultak az önvezető járművek esetében (99,99%-os megbízhatóságra és 3ms késleltetésre van szükség, a sikeres működéshez). A 802.11ac standardon alapszik, ami a Wi-Fi 5 technológia alapja [43]. A szabvány csatornái már a 60 GHz-es frekvenciatartományt használják kommunikációra, 20 MHz-es sávszélességgel. A 802.11p-hez képest kapcsolati hatótávja, és átviteli képessége is akár, annak 3x lehet[40], melyek a fizikai és MAC rétegben bevezetett fejlesztéseknek köszönhetőek. A technológia teljes potenciáljának kiaknázása érdekében javasolt az optimalizált többcsatornás működés bevezetése, valamint az üzenetismétlés alkalmazása az egész hozzáférési rétegben, ami az IEEE 802.11p standardban hiányzott. Az ismétlések újbóli bevezetése jelentős teljesítménynövelést eredményez. A szimu-

lációk alapján a teljesítmény növekedése már 1 ismétlés esetén is 0.5-0.8 dB-el nő IEEE 802.11p állomások, valamint 3-4 dB-el IEEE 802.11bd állomások esetében. Ugyanez 3 ismétlés esetén 1.0-1.7 dB és 6-8 dB növekedést eredményez [40].

2.3.3. Intelligens Közlekedési Rendszerek

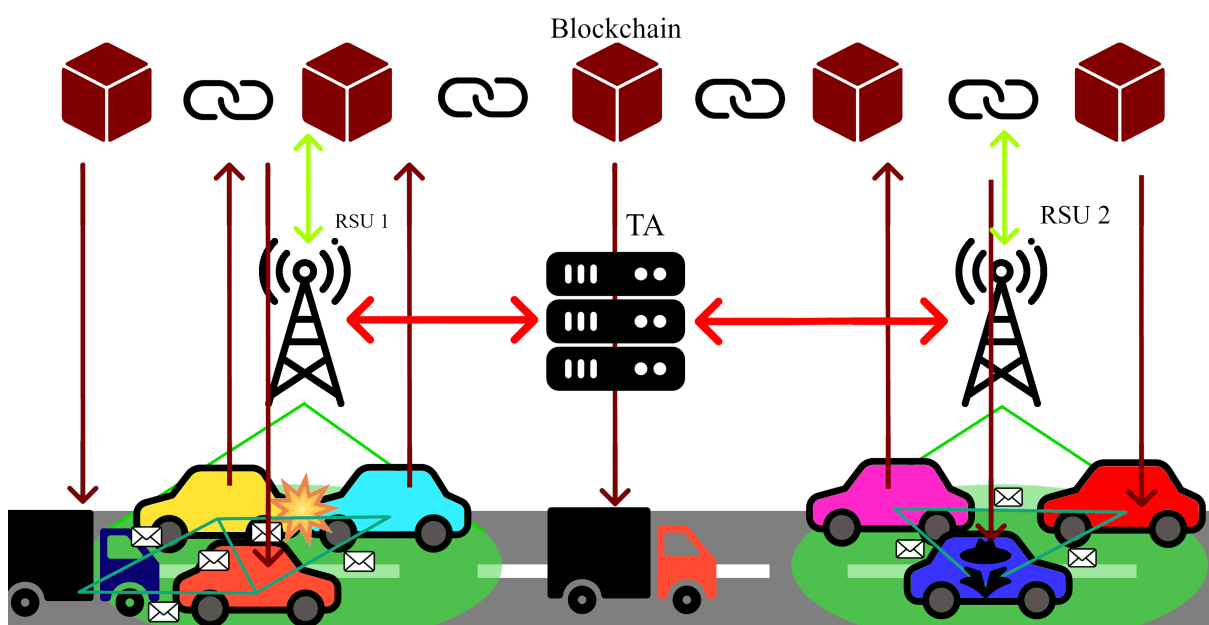
Egy másik említést igénylő standard az Európai Távközlési Szabványosítási Intézet (European Telecommunications Standards Institute, ETSI) által fejlesztett Intelligens Közlekedési Rendszer ötödik generációjának (ITS-G5) szabványcsaládja. Ez úgyszintén az 5GHz frekvenciasávon működik, és szintén a 802.11p szabványra épít [43].

Ezentúl, a CAR 2 CAR Communication Consortium (C2C-CC) is a 802.11bd standardot veszi az ajánlott vezeték nélküli rádiófrekvenciás standard alapjaként. Ennek előnye, hogy lehetővé teszi az egyszerűsített átállást a 802.11p alapú rendszerekről, mivel képes az együttműködésre az előző generációs állomásokkal, eszközökkel és szolgáltatásokkal, valamint a már korábban kiépített ITS hálózatokkal is. Igaz, hogy az előző generáció 10 MHz-es csatornákkal működik, viszont a kidolgozott modell lehetővé teszi, hogy nagyobb átviteli rátát érjenek el ezek a rendszerek is. Ugyanis két, egymás melletti 10MHz-es csatornát fel lehet használni akár két független, vagy egy egységes 20MHz-es csatornaként is. Ezt "csatorna kötegelésnek" (channel bonding) nevezik [40].

Ezeket a tényezőket alapul véve terveztük meg a protokollunkat, különös tekintettel az előzőleg bemutatott szabványokra. Ez azért fontos, mert biztosítja, hogy a protokoll illeszkedjen az aktuális és jövőbeli környezethez, és megfeleljen az EU szabványainak és előírásainak.

3. fejezet

A javasolt protokoll



3.1. ábra. A PHP-BP protokoll felépítésének ábrázolása

3.1. Résztvevők

3.1.1. Fedélzeti egység, OBU

A fedélzeti egységeket (OBU) a járművekbe építik be, amely a többi résztvevőhöz képest alacsonyabb számítási kapacitással és a kulcsok tárolására alkalmas speciális megbízható platform modullal (Trusted Platform Module, TPM) rendelkeznek. Az OBU-k számítások elvégzé-

sére és kommunikációra képes eszközök. Ezek az eszközök felelősek az incidensek bejelentésért, mint például rossz útviszonyok, forgalmi dugók, balesetek.

3.1.2. Útmenti egység, RSU

Az útmenti egységek (Road Side Unit, RSU) az út mentén elhelyezett eszközök. Minden egyes RSU-hoz tartozik egy tartomány, amelyet felügyel. Az RSU-k biztosítják a protokoll területi jellegét, mivel adott fizikai tartományához saját paraméterekkel, listákkal rendelkeznek. A területiségből és a hálózat jellegéből adódóan adott RSU-hoz kapcsolódó gépjárműnek fizikailag is az RSU területén kell lennie. Ezek az eszközök összegzik az incidens jelentéseket és szolgáltatnak hiteles információt az útviszonyokról. A blokkláncra folyamatosan publikálják az összegzett incidensjelentéseket és az útinformációkat.

3.1.3. Megbízható harmadik fél, TA

A megbízható fél (Trusted Authority, TA) felelős a rendszer paramétereinek meghatározásáért. Feltételezzük, hogy a TA megbízható. A TA tipikusan a rendőrség vagy a közúti hatóság, aki felügyeli az RSU-k működését. Az RSU-knak jelenteniük kell a forgalom kritikus eseményeit, például a halálos baleseteket. Az RSU-k és a TA függetlenek, de a TA bármikor ellenőrizheti bármelyik RSU működését. Jogában áll, hogy eltávolítson egy RSU-t kommunikációból.

3.1.4. Blokklánc, BC

A kriptográfiai primitívekre és protokollokra épülő blokklánc (Blockchain, BC) elosztott főkönyvként működik. Elsődleges célja a rendszerek decentralizált vezérlése azáltal, hogy minimalizálja vagy megszünteti egy központi vezérlőtől való függést. Emellett a kriptográfiai primitívek felhasználásával biztosítja a tárolt adatok megváltoztathatatlanságát. A blokklánc hibatűrő, replikált állapotgépként is leírható.

A blokklánc elsődleges feladata a bizonyító erejű és hitelesítő információk tárolása és szolgáltatása. Ha RSU nincs a közelben, a blokkláncot használjuk az incidensjelentések és az útviszonyok elküldésére. A blokklánc fogja biztosítani a rendszer paramétereit a regisztráció és az incidensjelentések alatt is. Ezeket a paramétereket az RSU egy okosszerződésen keresztül módosíthatja.

A protokollunkhoz a Solana [44] láncot javasoljuk, amely magas tranzakciós sebességet kínál, több ezer tranzakció másodpercenkénti feldolgozását teszi lehetővé. Alacsony tranzakciós díjai és nagy skálázhatósága lehetővé teszi a gyors és költséghatékony alkalmazások létrehozását.

3.2. Biztonsági elvárások

Célunk egy olyan kriptográfiai protokoll tervezése, mely támogatja a biztonságos közlekedést úgy, hogy biztosítja a forgalomban résztvevő autóvezetők személyes adatainak védelmét. A rendszerrel szemben támasztott biztonsági elvárásokat már a tervezés során figyelembe kell venni.

Az elsődleges szempont az autóvezetők magánéletének védelme. A VANET résztvevői közötti kommunikáció célja a forgalmi incidensek bejelentése, melyek helyszíni adatokat is megadnak. Fontos, hogy ezek az incidens információk hiteles forrásból származzanak, ugyanakkor ne szivárogtassák ki a küldő kilétét. Célunk, hogy a kommunikáció során küldött üzenetek alapján ne lehessen meghatározni és nyomon követni az egyes üzenetek küldőjét.

A protokollal szemben támasztott biztonsági elvárások a következők.

1. Személyes adatok védelme.

A felhasználók személyes adatainak védelméhez az alábbi elvárásoknak kell teljesülniük:

- Személyes adatok bizalmassága (data privacy): A kommunikáció során keletkezett adatok alapján a támadó nem ismerheti meg, vagy adhat jó becslést a küldő kilétére. [46].
- Összekapcsolhatatlanság (unlinkability): A támadó nem lehet képes az ugyanazon forrásból származó üzenetek beazonosítására, hiszen ez lehetővé tenné a küldő nyomon követését [8].
- Kontextusbeli megfigyelhetetlenség (contextual unobservability): A támadó nem ismerheti meg a felhasználó privát adatait az üzenetek kontextusának elemzésével [36].

A személyes adatok bizalmasságát elérhetjük, ha egyrészt csak olyan adatokat küldünk kommunikáció közben, ami megfelelően elfedi, hogy pontosan melyik járműhöz tartozik

az azt tartalmazó csomag. Másrészt biztosítjuk az üzenetek sértetlenségét, hitelességét is, hogy manipulációval, megszemélyesítéssel ne lehessen bizalmas információhoz jutni.

Az összekapcsolhatatlanság eléréséhez, biztosítani kell, hogy ne lehessen a felhasználókat megkülönböztetni a hálózaton belül terjedő útvonal információk alapján.

A kontextusbeli megfigyelhetetlenség pedig azt várja el, hogy az előbb említett védelmet terjesszük ki a csomagok és a kommunikációs folyamat többi elemére, annak metaadataira, kontextusára is, hogy az esetleges forgalomelemzéssel se lehessen megjósolni az üzenetcsomag küldőjét.

2. Jogosultságvizsgálat.

Csak az arra jogosult, forgalomba helyezett jármű vehet részt a kommunikációban. A TA felelős a járművek hivatalos dokumentumainak ellenőrzéséért.

3. Üzenethitelesség.

További biztonsági elvárás a kommunikáció során küldött üzenetek hitelességének biztosítása, mely az üzenet forrásának és integritásának ellenőrizhetőségét jelenti.

4. Feltételes anonimitás.

Ha egy jármű valótlan üzenetet generál, akkor az üzenet küldőjének kilétét meg kell tudni határozni, hogy TA részvételével a jármű jogosultságát vissza lehessen vonni.

3.3. Elméleti háttér

A protokollunk az elliptikus görbe kriptográfiára (ECC) és a hozzá kapcsolódó nehéz problémákra épül. Egy ilyen rendszer, kisebb kulcsméretek mellett is megfelelő biztonságot nyújt, és számos támadási módszerrel szemben ellenálló.

3.3.1. Elliptikus görbék

Egy adott K test feletti E elliptikus görbe azon (x,y) pontok halmaza, amely az

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

egyenletet kielégíti, ahol az $a_1, a_2, a_3, a_4, a_6 \in K$, és feltételezzük, hogy a görbe diszkriminánsa $\Delta \neq 0$.

Ha L egy K feletti testbővítés, az E görbe L -racionális pontjainak halmaza

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{O\}$$

ahol O végtelen távoli pont. Az O pont az egységelem, amely rajta van minden az y tengellyel párhuzamos egyenesen, és az x tengelyre vonatkozó tükörképe önmaga.

Ha a K test karakterisztikája nem 2 és nem 3, az E görbe egyenlete egyszerűsített, Weierstrass egyenlet formában írható fel

$$E : y^2 = x^3 + ax + b$$

ahol $a, b \in K$ és $\Delta = -16(4a^3 + 27b^2)$.

Két alapvető művelet létezik, amelyek a görbén lévő pontok közötti kölcsönös viszonyát írják le. A pontösszeadás során két különböző pontot, P és Q -t összeadva egy harmadik pontot, R -t kapunk a görbén. Az R pont a P és Q pontokra húzott egyenes és a görbe metszéspontjának x tengellyel vett tükörképe. Egy pont önmagával is összeadható, melyet pontduplázásnak nevezzünk. Itt az érintőt rajzoljuk a P pontban a görbéhez, majd ezen az érintő metszéspontját a görbével x tengelyre tükrözzük. A pontok az O -val együtt az összeadásra nézve Ábel-csoportot alkotnak.

1. Definíció. A legjelentősebb kriptográfiai probléma az ECC-ben az **Elliptikus Görbe Diszkrét Logaritmus Probléma (ECDLP)**. Legyen E egy Z_q feletti elliptikus görbe, ahol q prím. Adott $G \in E(Z_q)$, melynek rendje n és legyen $A \in \langle G \rangle$. Elliptikus Görbe Diszkrét Logaritmus Probléma (ECDLP) az $a \in [0, \dots, n-1]$ egész kiszámítása, ahol $A = aG$. Az a egészt A pont G alapú diszkrét logaritmusának nevezzük.

$$a = d\log_G A$$

Elég nagy n esetén az ECDLP nehéz, megoldására nem ismerünk polinomiális idejű algoritmust.

2. Definíció. Az ECDLP problémára épül az **Elliptikus Görbe Diffie-Hellman kiszámíthatósági probléma**, amely esetén feladat az $a, b \in [0, \dots, n-1]$ egészek esetén aG és bG értékéből meghatározni abG -t, a és b számok ismerete nélkül.

3. Definíció. Az ECDHP problémára épül az **Elliptikus Görbe Diffie-Hellman eldönthetőségi probléma (ECDDHP)**, amely esetén az $a, b \in [0, \dots, n-1]$ véletlen egészek és $R \in E(Z_p)$ véletlen görbepont esetén aG és bG értékek alapján $abG = R$ eldöntését, a és b számok ismerete nélkül. Ha ECDHP nehéz, akkor az eldönthetőségi probléma is nehéz.

A protokoll elkészítéséhez előre definiált, szabványnak megfelelő **secp256k1** görbét használunk, amelynek biztonsági tulajdonságai a használt kriptográfiai protokollok szempontjából bizonyítottan megfelelőek.

3.3.2. Schnorr aláírás

A Schnorr digitális aláírási séma [2] jelentős előnyökkel rendelkezik a kriptográfiai alkalmazások széles körében. Ez a séma könnyen implementálható, hatékony, alacsony tárolási és számítási igényű aláírások generálását teszi lehetővé, amely jelentős mértékben optimalizálja a rendszer teljesítményét.

Kulcsgenerálás. Legyen $\langle G \rangle$ elliptikus görbe csoport G generátor ponttal és n renddel, melyet E egyenlet ad meg, valamint H egy kriptográfiai hash függvény. A rendszer felhasználói ekkor választanak $y \in [0, \dots, n-1]$ véletlen számot és előállítják yG számot. Az y a privát kulcs, míg yG a publikus kulcs. Ekkor

Rendszerparaméterek E, G, n, H

Felhasználó kulcspárja: (y, yG)

Aláíró algoritmus. Az aláíró fél egy tetszőleges M üzenetet az alábbi lépések végrehajtásával tudja aláírni:

1. választ egy $r \in [0, \dots, n-1]$ titkos és véletlen számot és kiszámítja
2. $R = rG$
3. $h = H(R || M)$
4. $s = yh + r$

Az M üzenethez tartozó aláírás $S = (s, R)$ pár lesz.

Aláírás ellenőrzése. Az aláírás ellenőrzéséhez a következő lépéseket kell végrehajtani M és $S = (s, R)$ ismeretében:

$$h = H(R||M)$$

Ha $sG = h * yG + R$, akkor az aláírás érvényes.

3.3.3. Nulla ismeretű protokollok

Partner-hitelesítési protokollok célja, hogy két kommunikáló fél számára lehetővé tegyék egymás identitásának megbízható ellenőrzését. Nulla ismeretű protokollok egy speciális kriptográfiai módszert jelentenek, amelyek lehetővé teszik egy bizonyító fél számára, hogy bebizonyítsa egy állítás helyességét és ezzel az identitását is igazolja egy ellenőrző fél számára anélkül, hogy bármilyen további információt közölne az állítás konkrét tartalmáról. Ebben az esetben az ellenőrző nem szerez új ismereteket az állítás részleteiről, csupán annak igazságát ismeri fel. Ha az állítás igaz, a bizonyító képes lesz meggyőzni az ellenőrzőt annak igazságáról. Amennyiben az állítás nem igaz, a bizonyítónak rendkívül alacsony esélye van arra, hogy meg tudja győzni az ellenőrzőt az állítás helyességéről, feltéve, hogy a ellenőrző megfelelően követi a protokoll előírásait. Ezekben az algoritmusokban a tisztességes bizonyító fél képes egy bizonyíték előállítására, amely igazolja őt.

A protokollunk során arra törekszünk, hogy a bizonyító fél igazolja, hogy ismeri a titkos kulcsot, amelyhez tartozó publikus kulcsot regisztráltak az RSU területén. Ehhez a diszkrét logaritmusok egyenlőségén (Equality of Discrete Logarithms) alapuló algoritmust használjuk fel, amely a Chaum-Pedersen ötletén alapul[3]. Ebben az algoritmusban azt igazolja a bizonyító fél két kifejezés segítségével, hogy a két diszkrét logaritmust ismeri, és egyenlők.

Az algoritmust $\mathbb{Z}_q$ feletti E görbére vonatkozóan ismertetjük. Adottak az (E, q, G, n) görbeparaméterek, ahol E egy szabványnak megfelelő elliptikus görbe, q prím, $G \in \mathbb{Z}_q$ generátor elem, melynek rendje n , valamint a G_1 és G_2 generátor pontok. Ekkor a bizonyító fél bizonyítja, hogy ismeri $y \in \mathbb{Z}_n$, ahol $P_1 = yG_1$ és $P_2 = yG_2$. Az identitásának igazolásához a felhasználó bizonyítja y ismeretét úgy, hogy nem árulja el, illetve megmutatja, hogy P_1 és P_2 pontok G_1 és G_2 alapú elliptikus diszkrét logaritmusai egyenlők.

Az algoritmus a következő:

1. A bizonyító fél választ egy $r \in \mathbb{Z}_n$ titkos és véletlen számot,
2. elküldi $T_1 = rG_1, T_2 = rG_2$ értékeket.
3. Az ellenőrző fél generál és visszaküld egy $c \in \mathbb{Z}_n$ véletlen kihívást.

4. A bizonyító fél kiszámolja $s = r + cy$ és visszaküldi.
5. Az ellenőrző fél megvizsgálja, hogy a következő egyenlőségek teljesülnek -e:

$$sG_1 = T_1 + cP_1$$

$$sG_2 = T_2 + cP_2$$

A protokollunk során az ellenőrző féltől kapott c kihívást a Fiat-Shamir [1] ötletét követve egy hash értékkel helyettesítjük, azaz $c = H(G_1, G_2, P_1, P_2, T_1, T_2)$, mely egy nem-interaktív algoritmust eredményez. Jelölje $EDL - NIZKP(G_1, G_2, P_1, P_2) = (T_1, T_2, c, s)$.

3.4. A protokoll lépései

A protokoll három fő lépésre tagolható. Az inicializálási fázisban a rendszerparaméterek, a kulcsok, valamint a blokklánc tárcák generálása és egy előre meghatározott összeggel történő feltöltése történik meg. Ahogy az OBU belép egy RSU tartományba lefut regisztrációs fázis, melynek célja az OBU rendszerhasználati jogosultságát ellenőrzése. A protokoll harmadik fázisa a közúti incidensek jelentése (útviszonyok, balesetek, forgalmi dugók stb.) és ezek ellenőrzése.

3.4.1. Inicializáció

A rendszer inicializációs fázisa 2 fő lépésből áll:

1. TA legenerálja és okoszerződés segítségével tárolja a BC-n a $((E, q, G, n), H : \{0, 1\} \rightarrow \{0, 1\}^l, l \in \mathbb{N})$ rendszerparamétereket, ahol (E, q, G, n) az elliptikus görbe paraméterei és H egy kriptográfiai hash függvény. Mi a **secp256k1** görbét és **SHA-256** hash függvényt javasoljuk.
2. Az OBU-k és az RSU-k megválasztják saját $y, z \in \mathbb{Z}_n$ véletlen értékeiket és kiszámolják yG és zG görbepontokat. Ekkor y, z a titkos és yG, zG publikus kulcsok, melyeket a hozzá tartozó metaadatokkal (pl. érvényességi idő) együtt blokkláncra helyezi titkos kulcsának segítségével. A publikus kulcs és metaadatai egy blokkláncon kezelt tanúsítványként kezelődik. Létrehozzák saját Solana tárcáikat. OBU-k feltöltik azokat egy előre meghatáro-

zott mennyiségű pénzüsszeggel. RSU-k publikus kulcsait és a hozzá tartozó tárcacímeket a blokklánc fogja szolgáltatni.

3.4.2. Regisztráció

A regisztráció során az RSU meggyőződik arról, hogy az OBU rendelkezik a rendszer használatához szükséges jogosultsággal és ténylegesen az RSU területén tartózkodik.

Az OBU belép egy RSU területére és jelzi csatlakozási szándékát a BC-on, amelyről megkapja RSU-nak a publikus zG kulcsát. Az OBU kulcspárja (y, yG) segítségével igazolja kilétét úgy, hogy az RSU publikus kulcsával titkosítva hozza az tudomására saját yG kulcsát a láncon keresztül. Ezzel biztosítva, hogy a nyilvános blokkláncon tárolt adatok ne szivárogtassák ki, hogy egy adott jármű mely RSU tartományban van.

Amikor egy jármű belép egy RSU által ellenőrzött területre, az RSU megerősíti az eszköz tényleges jelenlétét. Ha az OBU az RSU területén tartózkodik, az RSU a TA segítségével ellenőrzi az OBU rendszerhasználati jogosultságát (pl. forgalomban van -e a jármű). Ha a jármű ellenőrzése sikeres, az RSU kezdeményezi a jármű yG publikus kulcsának felvételét az RSU whitelist-jére.

Minden RSU-hoz tartozik egy a sikeresen beregisztrált OBU-k nyilvános paramétereit tartalmazó lista, amit whitelist-nek nevezünk. Ezek a paraméterek a nulla-ismeretű protokoll futtatásához szükséges hiteles, nyilvános értékeket tartalmazza. A listára történő feltöltést és az arról történő törlést az RSU kezdeményezi. A witelist módosítását viszont a BC elosztottan, decentralizáltan végzi okosszerződés segítségével. A whitelist két alkalommal változik, ha új OBU vagy OBU-k egy csoportja sikeresen beregisztrál, vagy incidens történik a tartományban.

A blokklánc működtetésében résztvevő csomópontok együtt meghatároznak egy $a \in \mathbb{Z}_n$ titkos értéket, valamint az a -hoz tartozó aG publikus generátor elemet. A lista minden elemét megszorozza az a értékkel, így kapva az $aG || ay_1G, ay_2G, \dots, ay_mG$ listát, ahol m az adott RSU-hoz csatlakozott OBU-k száma. A listát ezen kívül még a lánc permutálja, majd tárolja ezzel nyilvánossá téve azt.

A regisztráció több alkalommal is végrehajtható, attól függően, hány incidens történik a területen. Ezzel biztosítva az incidenseket bejelentő járművek RSU tartománybeli ellenőrizhetőségét. Ha viszont valaki téves adatot küld, az OBU egyedi azonosítóját eltávolítják a whitelist-ről, ezzel megakadályozva további hozzáférését a rendszerhez. Ilyen esetben a jármű új regisztrációval kérheti a rendszer újbóli használatának lehetőségét.

A sokszorosan rosszindulatú tevékenységet végző járműveket TA és az RSU közösen a BC segítségével képesek azonosítani ayG alapján. Ha szükséges véglegesen, megvonhatják a rendszer használatának jogosultságát. Ez biztosítja, hogy csak a szabályokat betartó járművek férhessenek hozzá a szolgáltatáshoz.

3.4.3. Incidensek jelentése

Egy incidensjelentés akkor történik, ha a közúti rend megváltozik és ezáltal a forgalom akadályozva van, amely lehet forgalmi dugó, baleset, rossz útviszonyok stb. Egy incidensjelentés tartalmaz egy M üzenetet, ami

$$M = (\text{GPS_Coord} || \text{Incident_Code} || \text{Time_Stamp})$$

formátumú. Ezt tartalmazza, hogy milyen GPS koordinátán (GPS_Coord) és milyen típusú eseményt (Incident_Code) mikor (Time_Stamp) észlelünk.

Egy jelentés létrehozásának algoritmus a következő

1. OBU választ egy $k, r \in \mathbb{Z}_n$ véletlen értéket
2. tárcája segítségével wG Solana címet generál
3. y titkos kulcsával és aG generátor elemmel kiszámolja yaG
4. Incidensjelentés: $w + H(M || wG)ky, wG, EDL - NIZKP(kyG, kG, ayG, aG), M$

Egy ellenőrzése BC-ről letöltött whitelist segítségével történik, amelynek algoritmus a következő:

1. ayG szerepel-e a whitelist-en
2. Ellenőrzi $EDL - NIZKP(kyG, kG, ayG, aG)$
3. Ha az előző lépés teljesül, akkor kiszámolja $h = H(M || wG)$ és ellenőrzi $(w + H(M || wG)ky)G = wG + hkyG$

Ha minden ellenőrzés a megfelelő eredményt szolgáltatva, akkor az incidensjelentés egy olyan OBU-tól származik, amit az RSU hitelesített és nem követett el rosszindulatú üzenetküldést (azaz a whitelist-en szerepel).

Az incidensjelentés a WAVE hálózaton keresztül kerül közlésre az OBU szomszédságának. A közelben levő járművek számára hasznos az üzenetek továbbítása, hiszen elősegíti az információ gyors terjedését. A járművek a kapott más OBU-tól eredő üzeneteket is továbbítják a *Time_Stamp*-tól számítva egy adott időtartamig. A WAVE hálózatban történő csomagküldést a 4. fejezetben részletesen megadjuk.

Az OBU az incidensjelentést a BC-re is feltölti mobilhálózat segítségével. A BC levonja a tranzakciós és rendszerhasználati díjat. A BC-re feltöltött jelentések tartalmi hitelesítése után, az erre jogosultaknak a rendszer visszautalja a levont összeget, ezen felül a rendszer működtetési jutalmát is megkapják a wG címre. A tartalmi szempontból félrevezető bejelentésekhez tartozó címre nem történik utalás és a hozzátartozó ayG azonosítót is eltávolítja a lánc a listáról. Ezt módszertant ösztönző-büntető (incentive-punishment) technikának nevezzük. Célja a rendszer tisztességes működtetésének elősegítése, megelőzve a nagy számú valótlan bejelentéseket.

Előfordulhat, hogy az RSU tartományában úgy történik incidens, hogy a környezetben kevés jármű van, azaz a WAVE hálózaton csak korlátozottan terjed az információ az adott incidensről. Az ilyen járművek esetén jelentős előnyt jelent a mobilhálózaton elérhető blokklánc. Ezeknek az üzeneteknek a jelentése ugyanúgy a már bemutatott algoritmussal történik.

3.5. Biztonsági elemzés

A protokoll biztonsági elemzése során nem vesszük figyelembe a fizikai térben végezhető, az identitást és az üzenetküldést kompromittáló tényezőket és támadásokat, mint például a jármű fizikális nyomon követése.

- **Személyes adatok bizalmassága.** A regisztráció során az OBU nyilvános kulcsa titkosítva kerül a láncra. EA titkosítási séma biztonsági jellemzői miatt a küldő OBU kiléte titokban marad.

Incidensbejelentés során, az M üzenet kódokat (incidens és GPS koordináta) tartalmaz, mely személyes információktól mentes. A aG, ayG, kG, kyG paraméterek ismeretében, ahol a és k számok titkosak és véletlennek, az y vagy yG értékek meghatározása (Definíció 1 és Definíció 2 nehéz). A $w + H(M || wG)ky, wG$ kifejezésből y -t megismerni nehéz a Schnorr aláírási séma biztonsága és k véletlensége és titkossága miatt. Mivel a wG érték minden tranzakció és incidensjelentés során változik, valamint a Solana címek biztosítják a felhasználó anonimitását, így a küldő kiléte biztonságban marad. Az alacsonyabb

rétegekben MAC címcserével (lásd 4.4.4. alfejezet) is biztosítjuk a küldő kilétének bizalmasságát. Nem juttatunk el a kommunikáció során más személyes információt.

- **Összekapcsolhatatlanság.** Az különböző incidensjelentések során a résztvevők újrasztják az a, k értékeket, amelyek titkosak és véletlenek. Ezzel a Schnorr aláírási séma (yk, ykG) kulcspárja, valamint a nulla ismeretű protokoll kyG, kG, ayG, aG elemei véletlenek, melyek, a primitívek biztonsági jellemzőivel együtt biztosítják, hogy ugyanazon forrástól származó üzenetek között nincs kapcsolat. Az összekapcsolhatatlanság további feltétele még, hogy a rendelkezésre álló nyilvános információk se szivárogtassanak információit. A whitelist a BC által folyamatosan randomizált és permutált. A megváltozott listák közötti összekapcsolhatatlanságot a ECDDHP biztosítja.
- **Kontextusbeli megfigyelhetetlenség.** A fentebbi két pontban igazoltuk, hogy a felhasználóhoz nem köthető az elküldött üzenet alapján semmilyen formában az üzenete. A fenti két biztonsági elvárás az alkalmazói réteghez kapcsolódó támadásokat védi ki. A VANET rendszer dinamikus topológiája, valamint az alacsonyabb rétegekhez kapcsolódó biztonsági megoldásaink (lásd 4. fejezet) biztosítják, hogy forgalom- vagy egyéb kontextuselemzéssel szemben is védett a rendszerünk.
- **Jogosultságvizsgálat** Csak az arra jogosult, forgalomba helyezett jármű vehet részt a kommunikációban. A TA felelős a járművek hivatalos dokumentumainak ellenőrzéséért. Amennyiben az OBU jogosult a rendszer használatára, akkor kiállítja annak blokklánc-alapú tanúsítványát. Ha megszűnik jogosultsága (pl. kikerül a forgalomból), akkor tanúsítványát visszavonási listára helyezi.
- **Üzenethitelesség.** A küldött üzenetek integritásának és hitelességének védelmét a regisztráció során a BC, incidensbejelentésnél a Schnorr aláírási séma és EDL-NIZKP biztosítja. Az üzenet módosulása az ellenőrzések során kiderül. A protokollban a Schnorr aláírási séma és EDL-NIZKP tulajdonságai miatt csak az arra jogosult személy tud érvényes aláírással rendelkező üzenetet generálni.
- **Feltételes anonimitás.** TA a blokkláncon keresztül képes visszavonni az anonimitást, ha az szükséges.

4. fejezet

Implementáció

A javasolt protokollunk egy hibrid rendszer, ami két különböző technológia - a blokklánc és a WAVE - erősségét is kihasználja. Egyszerre biztosítja azt, hogy a járművek minél hamarabb értesüljenek a körülöttük történt eseményekről és az aktuális forgalomról, illetve lehetővé teszi azt is, hogy minél több felhasználó számára elérhető legyenek a fontosabb forgalominformációk. Az implementációban a jelenleg is használt WAVE technológia alapjait alkalmazzuk és az ezek által biztosított implementációt egészítjük ki a saját protokollunkhoz kapcsolódó elemekkel.

A következő fejezetben bemutatjuk a protokollunkhoz ajánlott, és az implementációhoz felhasznált rövidtávú kommunikációs szabványokat és technológiákat, valamint az implementációhoz használt szimulációs rendszert. Ezután szemléltetjük saját implementációnkat, valamint a javasolt protokoll lépéseihez tartozó adatsomagtípusokat és folyamatokat.

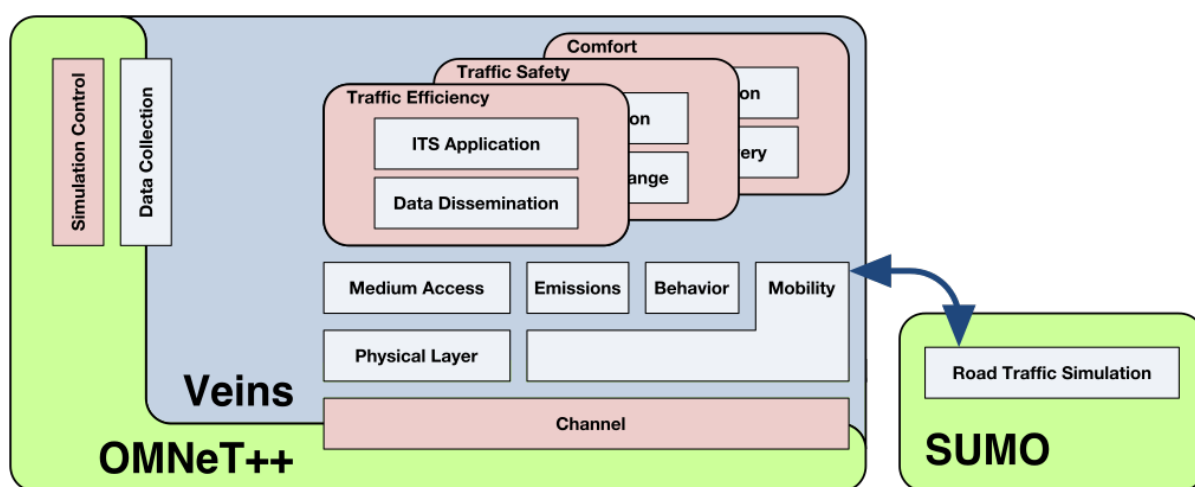
4.1. Használt technológiák

A következőkben röviden ismertetjük a szimulációs platformot, a használt WAVE szabványok működését, és a szimulációt pontosabbá tevő modulokat is.

4.1.1. Veins szimulációs keretrendszer

Az implementációt a "Vehicles in network simulation" (Veins, Járművek hálózatban szimuláció) nevű szimulációs keretrendszerben valósítottuk meg. Ez egy nyílt forráskódú hálózati szimulációs keretrendszer, ami kifejezetten járműhálózatokra fejlesztett szimulációs model-

lek készletét biztosítja. A keretrendszer architektúráis felépítése a 4.1 ábrán látható. A Veins modelljei az OMNeT++ [29] esemény vezérelt C++ szimulációs keretrendszeren futnak, amik folyamatosan kapcsolatban vannak egy SUMO [48] nevű közlekedés szimulátorban futó szimulációval. A keretrendszer többi komponense felel a szimuláció felállításáért, futtatásáért és megfigyeléséért. Az OMNeT++ egy bővíthető, moduláris, komponens-alapú keretrendszer, ami elsődlegesen hálózati szimulációk építésére készült. A SUMO (Simulation of Urban MObility, Városi Mobilitás Szimulációja) pedig egy nyílt forráskódú, könnyen portolható, **mikroszimulációs** és folytonos multimodális közlekedésszimulációt biztosító csomag, amit a nagy hálózatok kezelésére terveztek. A Veins ebben a két rendszerben futtat két szimulációt párhuzamosan.



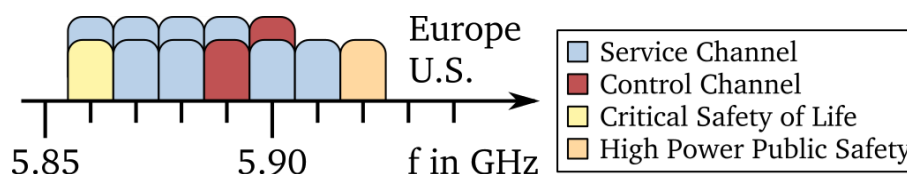
4.1. ábra. A Veins keretrendszer architektúrája[33].

Egyet az OMNeT++-ban a hálózat, és egyet a SUMO-ban az utcai közlekedés szimulálására. Használata kényelmes és hatékony, mivel az elmúlt években rengeteg fejlesztésen esett át, amit egy későbbi alfejezetben bővebben bemutatunk. Úgy tekinthetünk rá, mint egy eszközkészletre, ami lehetőséget ad, hogy a számunkra megfelelő modelleket tovább építsük a saját elképzeléseink alapján, és tesztelhessük elképzeléseinket segítségével. A rendszer tervezésén, felépítésén és a keretrendszer fejlesztésével kapcsolatban született publikációkból is látszik, hogy kutatók és szakemberek készítették, kutatók és szakemberek számára [33].

A keretrendszer egyetlen munkaállomáson képes egy egész városblokkot és teljes scénáriókat szimulálni. OpenStreetMap térképek segítségével is dolgozik, így bármilyen környezet szimulálását elvégezhetjük. Épületeket, sebességhatárokat, sávokat, lámpákat, táblákat, és más egyéb adatokat is képes értelmezni, amik segítségével még valósághűbb szimulációkat tud futtatni. Képes imitálni venni a járművek és épületek hatásait is a környezetre.

4.1.2. Használt WAVE szabványok

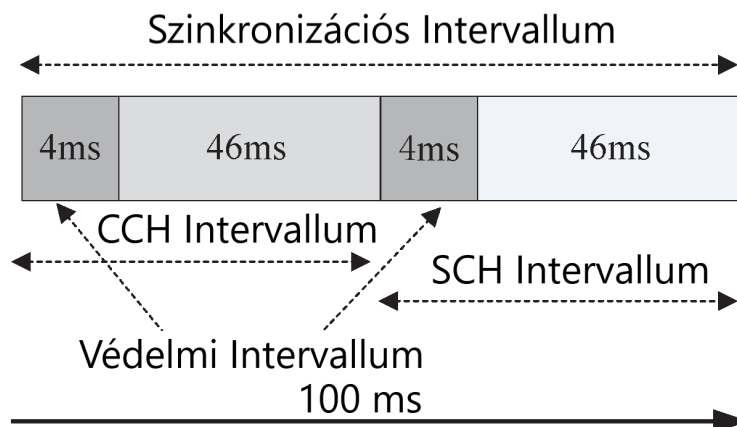
Az implementációnk a Veins platform IEEE 802.11p és IEEE 1609.4 szabványon alapuló modelljére épül. Ezek közösen definiálnak egy fizikai és adatkapcsolati réteget. Az IEEE 802.11p adatkapcsolati rétegét az IEEE 1609.4 szabvány egészíti ki a többcsatornás működéssel.



4.2. ábra. Az IEEE 1609.04 szabvány által definiált csatornák[33].

Ez az amerikai DSRC szabványban 7, míg az Európai szabványokhoz ajánlott variánsban 5 csatornát definiál. a 4.2 ábrán látható módon. Ezek egyike a vezérlési (Control Channel, CCH) és négy pedig szolgáltatási csatorna (Service Channel, SCH). A vezérlési csatornán a kommunikáció lebonyolítását segítő csomagok továbbítódnak. Ezt a csatornát használják például a különböző szolgáltatást biztosító csomópontok, hogy hirdessék a szolgáltatásukat, és informálják a többi egységet arról, hogy mégis milyen szolgáltatást érhetnek el, és melyik szolgáltatási csatornán keresztül. A hálózatban részt vevő egységek a hirdetett szolgáltatásokat tudják igénybe venni. A többcsatornás megoldás abban segít, hogy a különböző csoportokban, és különböző szolgáltatásokon keresztül kommunikáló, viszont fizikailag egy környezetben lévő egységek a csatornán belüli versenyhelyzet kialakulása nélkül tudjanak kommunikálni. A DSRC esetében az extra 2 csatorna speciális szolgáltatásokat biztosít. A legalacsonyabb frekvenciasávban egy magas szintű rendelkezésre állású, rövid késleltetési idejű (High Availability Low Latency, HALL) csatornát biztosít az élet védelmének támogatása céljából működtetett kritikus szolgáltatásoknak. A legmagasabb frekvenciasávon pedig egy nagy erősségű távolsági (High Power Long Range, HPLR) csatornát, ami a közbiztonsági szolgáltatások számára biztosít egy dedikált csatornát.

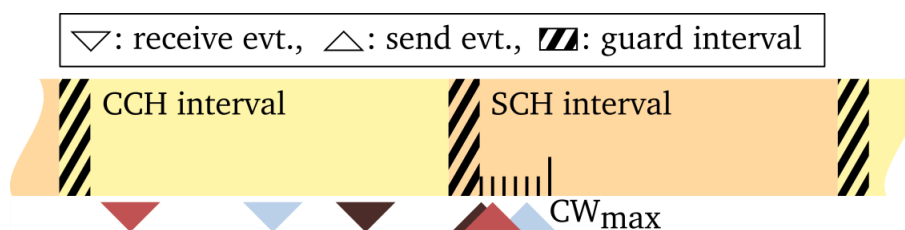
A többcsatornás modell a következőképpen működik. Minden egyes eszköz antennája folyamatosan vált a vezérlési csatorna és valamelyik szolgáltatási csatorna között. A folyamat szinkronizációs intervallumokra (Synchronization Interval, SI) van osztva, amik hossza egységesen 100ms. Ez két, 50ms-os belső egységre osztható, egy vezérlésre és egy szolgáltatásra. Mindkét csatorna esetén 46ms van biztosítva a tényleges kommunikációra, amihez egy 4ms



4.3. ábra. A többcsatornás modell felosztása [22].

várakozási intervallum tartozik az antenna csatornaváltásra a két frekvencia között, az alábbi módon (4.4 ábra):

- Az első 4ms-ban a protokoll várakozási intervallumot biztosít a rendszer számára, hogy az antenna sikeresen ráhangolódjon a vezérlési csatorna frekvenciasávjára.
- Majd 46ms áll az antenna rendelkezésére, hogy figyelje a CCH-n történő kommunikációt.
- Ezután megint 4ms várakozási intervallum áll az antenna rendelkezésére, hogy a vezérlési csatornán kapott információk alapján, a használni kívánt szolgáltatás által meghatározott szolgáltatási csatornára hangolja magát.
- Végül ismét megnyílik egy 46ms időablak, mely az előző lépésekben, vagy valamelyik korábbi szinkronizálási intervallumban meghatározott üzenetküldés és keretfogadás számára biztosított.



4.4. ábra. A többcsatornás modell egy szinkronizációs intervalluma[33].

Minden jármű ugyanarra az egy CCH-ra hangolódik, tehát minden egység ugyanazokat a vezérlési információkat és szolgáltatáshirdetéseket kapja meg. Viszont az, hogy melyik SCH-ra

hangolódnak, maguk határozzák meg, mivel ez a használt szolgáltatásonként más és más lehet [22]. Ezentúl, ha egy eszköz küldeni akar egy üzenetet, akkor egy random várakozási idő generálódik, mely meghatározza, hogy meddig vár az eszköz a küldési intervallumon belül mielőtt ténylegesen küldeni kezd. Ezt az időintervallumot verseny ablaknak (Contention Window, CW) nevezzük. A várakozása alatt figyeli a csatornát, és amennyiben foglaltnak találja, akkor vár a következő intervallumra a küldéssel, ha pedig a csatorna üres, akkor elindítja a küldést. A 4.4 ábrán ennek maximum értéke $CW_{\max}$ -al van jelölve.

A szimulációnk az előbb bemutatott többcsatornás kommunikációs modell, az IEEE 802.11p fizikai és adatkapcsolati rétegjeire épül. Ez a Veins rendszerben kiegészül a fizikai réteg optimalizált szimulációs modelljével, ami a szimulációk sebességében nagyságrendbeli növekedést tesz lehetővé, ezzel jelentősen növelve a rendszer hatékonyságát [24].

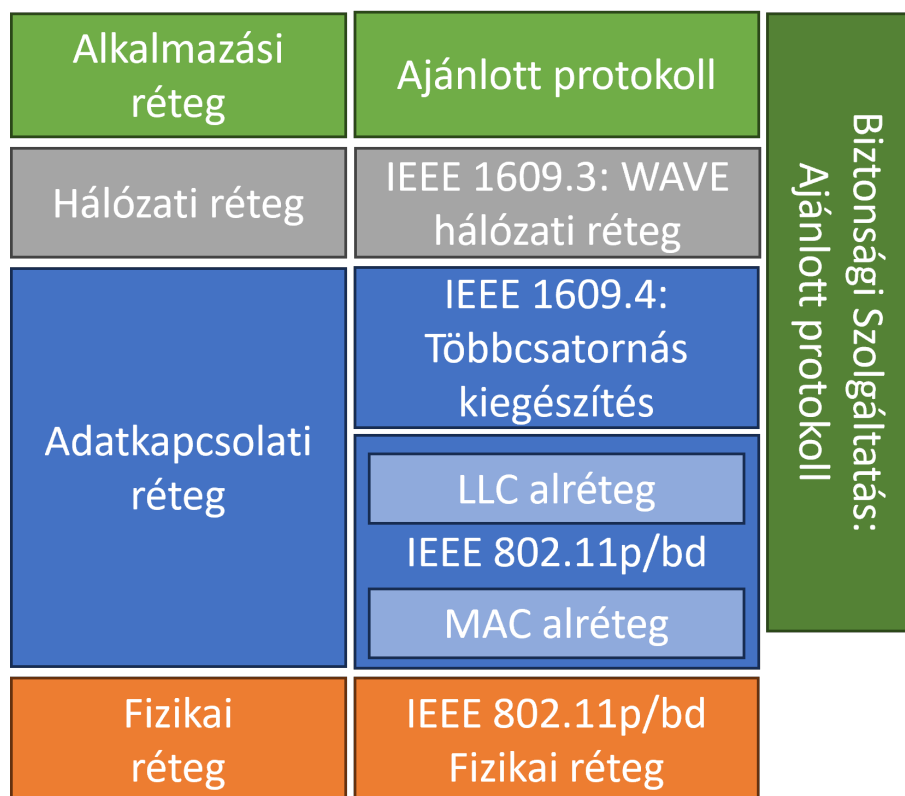
4.1.3. Veins modulok

A Veins szimulációs keretrendszer további modulokkal is bővül, melyek fő célja a szimulált modellek pontosságának növelése. Ez azért fontos, mert gyakran előfordul, hogy a VANET tesztrendszerek laboratóriumi körülmények között olyan eszközöket alkalmaznak, amelyek eredetileg más célra lettek tervezve, és csak módosításokkal alkalmasak VANET-szimulációra. Kevés egységből felépülő hálózatok szimulálása esetén az eltérő hálózati viselkedés nem jelent jelentős problémát. Azonban sűrű hálózati környezetben pontos szimulációs modellek elengedhetetlenek annak érdekében, hogy a szimulációk megbízható eredményeket adjanak. [12]

A Veins a valósághű szimuláció kialakításához az alábbi modelleket alkalmazza:

- Hullámok közötti interferencia modell[13]
- Akadályok és zajt generáló tényezők[16][17].
- Eszközök beállításait figyelembe vevő modellek[18].

Emellett a keretrendszer beépített implementációkat kínál különféle vezeték nélküli technológiák modellezésére, valamint lehetőséget nyújt egyedi modellek beillesztésére a MATLAB vagy a Simulink segítségével.



4.5. ábra. Az implementált hálózati modell rétegei.

4.2. Hálózati modell

A hálózati modellünk az előző fejezetekben bemutatott architektúrákra épül. Az alkalmazási rétegben jelenik meg az incidensjelentéseket megvalósító protokoll.

A hálózati modellünket a MAC (Media Access Control) és az alkalmazási rétegben is kiegészítjük biztonsági szolgáltatásokkal. Implementáltunk egy MAC címcseré mechanizmust és egy öngenerált álneveket előállító modult. Ezek továbbá kiegészülnek a blokkláncon alapuló hitelesítést végző algoritmusokkal.

A rendszerben mind a fedélzeti, mind az útmenti egységek külön osztálymodellel rendelkeznek. A szimuláció esemény vezérelt, így az eszközök számára az elküldött vagy megkapott csomagok, egy-egy eseményként jelennek meg a szimulációban. A küldés esetén a csomag a generáló rétegtől adódik tovább a lentebbi rétegeknek, mindig az eggyel lentebbi réteg szimulálásért felelős osztályhoz, amíg a fizikai réteg szimulációs osztálya azt el nem küldi. Ezt akkor teszi meg, ha az adott célcsatornát üresnek érzékeli. Ezután minden hálózati résztvevő szimulálja, hogy az adott esemény üzenete eljut-e hozzá, és ha igen, akkor milyen jelerősséggel. Amennyiben a jelerősség nem ad okot megbízható kapcsolat feltételezésére, akkor egy

valószínűségi modell alapján dönti el, hogy meg tudta-e kapni a csomagot a jármű, vagy sem, figyelembe véve az árnyékoló környezeti tényezőket és az egyéb rádiófrekvenciás jelek zavarótényezőjét. Ha a fizikai réteg modulja ténylegesen érzékelt üzenetet az adott eszköz számára, akkor azt feldolgozza. Üzenetszórás esetén továbbküldi a felsőbb rétegeknek, amíg az el nem jut és fel nem dolgozzák a célrétegben. Minden más esetben eldobja az üzenetet.

Fontos megjegyezni, hogy egy üzenet csak addig a rétegig jut el felfelé haladva, amelyik rétegtől kiindult. Ez azért fontos, mert például a címzett üzenetszere lehetővé teszi a nyugtázást. A nyugtát a MAC réteg állítja elő ahogy a kereteket megkapja. A fogadó egység MAC rétegében generálódik és a küldő MAC rétegének szól, azaz nem fog fentebb terjedni, például a hálózati vagy alkalmazási réteg felé.

A jelenlegi implementációnk nem alkalmaz hálózati rétegbeli modellt, mivel a protokoll közvetlenül keretezésre küldi csomagjait az adatkapcsolati rétegnek. Ha szükség lenne rá, lehetőség van az IEEE 1609.3 szabvány által meghatározott hálózati réteg és szolgáltatásainak felhasználására. Ez kiegészíthető egy helyalapú útválasztási protokollal (Location-Based Routing Protocols). [34].

A jövőbeli implementációk során, amelyek az IEEE 802.11bd szabványt használják, továbbra is javasolt az IEEE 1609.4 szabvány alkalmazása is. Ezt azért emeljük ki, mert a jövőbeli fejlesztéseknél az IEEE 802.11bd szabvány modelljének implementálását ajánlják mind a fizikai, mind az adatkapcsolati réteg működésének szimulálásához, a modell, szimuláció és implementáció időállóságának biztosítása érdekében.

4.3. A protokoll implementáció alapegységei

A fejezetben bemutatjuk a rendszer pár alapvető üzenettípusát és működési mechanizmusát.

4.3.1. Adatkapcsolati réteg fejlécei

A fizikai rétegben megjelenő üzenettípus egy fizikai keret (AirFrame), ami a jelek bit-áradatának egy egységét közvetíti az antennákon keresztül. Ezt egy *AirFrame11p* nevű üzenettípus kezeli, aminek rakománya egy IEEE 802.11 alapú MAC packet. Ezt implementációnkban a *MacPck802-11* üzenettípus definiálja. Ezen a csomag lehet IEEE 1609.04 szabvány alapján definiált keret, vagy ennek kibővítései. A protokollunk által definiált üzene-

tek mind a *BaseFrame1609-4* nevű üzenettípust bővítik ki és *AirFrame11p(MACPck802-11(BaseFrame1609-4||Kibővítések))* felépítésű üzenetként jelennek meg.

MacPck802-11	BaseFrame1609-4
destAddr : LAddress::L2Type srcAddr : LAddress::L2Type sequenceId : long address3 : int address4 : int fragmentation : int informationDS : int retry: bool duration : simtime_t	channelNumber : int userPriority : int psid : int recipientAddress : LAddress::L2Type
Rakomány: BaseFrame1609-4 alapú csomag.	A protokoll többi típusa kiegészíti

4.6. ábra. MacPck802-11 és BaseFrame1609-4 mezői.

A protokoll által implementált üzenettípusok és fejlécek felépítését a 4.6 ábra szemlélteti. Itt és a többi ábrán is az üzenettípusok mezőinek nevét, és a tartalmuk adattípusát írják le, ahogy az implementációnkban meg van valósítva. A *BaseFrame1609-4* *psid* mezője a protokoll szolgáltatási azonosítót jelöli. Ennek a tartalma egy azonosító, ami az adott üzenetet biztosító szolgáltatást jelöli.

Két egyedi adattípust is tartalmazhatnak az üzenetmezők. A *LAddress::L2Type* adattípussal ábrázoljuk az eszközök adatkapcsolati rétegben, azok azonosítására használt fizikai címét. A *simtime_t* adattípus pedig a szimulációs időt jelenti. A rendszerben ugyanis külön használja a munkaállomás belső óráját a folyamatok futási idejének naplózására, és egy külön, szimulált órát használ a szimuláción belüli időmúlás ábrázolására.

4.3.2. Üzenet továbbadási mechanizmus

Minden érkező üzenet azonosításra kerül az egységek számára. A protokoll működtetéséhez különböző csomagtípusokat használunk, amik könnyen felismerhetők és megkülönböztethetők egymástól. Üzenet továbbadást akkor használunk, ha egy információt szeretnénk terjeszteni a hálózatban. Amikor érzékelünk egy csomagot, először ellenőrizzük annak hitelességét. Ha ez sikeres, akkor a fogadó fél egy üzenetszórás folyamatot indít az adott csomaggal, saját adatkapcsolati és fizikai azonosítóival. Ez az eljárás segíti az üzenetek összekapcsolhatatlanságát a rendszer rádiókommunikációs csomagcseréje közben. Mivel ugyanaz a csomag több fizikai azo-

nosítóval is továbbításra kerül, elősegíti a kontextus megfigyelhetetlenségét, mivel egy eszköz különböző álneveinek összekapcsolása így nem lehetséges ilyen metaadat alapján.

Az üzenet továbbadás folyamatát az 1. algoritmus szemlélteti. Amikor üzenetet fogad egy OBU először ellenőrzi, hogy milyen régi az üzenet. Amennyiben az előállítási ideje egy megadott időintervallumon kívül esik, akkor eldobjuk a csomagot. Egy nem túl régi időbélyeggel ellátott üzenet esetében ellenőrzi, hogy korábban már feldolgozta-e. Ha még nem, akkor rövid időre eltárolja és elkezd feldolgozni. Célunk ezzel, hogy a kritikus balesetbejelentések esetén minél kisebb késleltetéssel tudjon döntést hozni a vezérlés segítő alkalmazás.

1. Algoritmus Üzenet feldolgozás és tovább küldés

Require: Inicializáció és regisztráció befejeződött

Ensure: *msg* egy üzenet

```
while OBU aktív do
  if msg üzenet érkezett then
    if msg időbélyege nem régebbi mint 5 mp then
      if msg üzenet még nem tárolt then
        msg üzenet tárolása
        msg tartalmának értelmezése és hitelességének ellenőrzése.
        if msg tartalma hiteles then
          msg üzenet tovább küldése
        else
          msg hiteltelennek nyilvánítása
        end if
      else
        nem foglalkozok msg üzenettel
      end if
    else
      msg elvetése
    end if
  end if
end while
```

Eközben az eszköz ellenőrzi az üzenet hitelességét is. Amennyiben hiteles, akkor továbbküldi az üzenetet. Amennyiben nem, akkor eldobja és tartalmát is semmisnek tekinti. Ha több, egymásnak ellentmondó üzenet is érkezik egy eseményről, akkor a többségre hallgat az egység.

4.4. A protokoll fázisainak implementálása

A következő részben bemutatjuk a szimuláció során használt implementáció részleteit. Két alkalmazási rétegű modellt definiáltunk a szimulációban, mindkettő ugyanazon

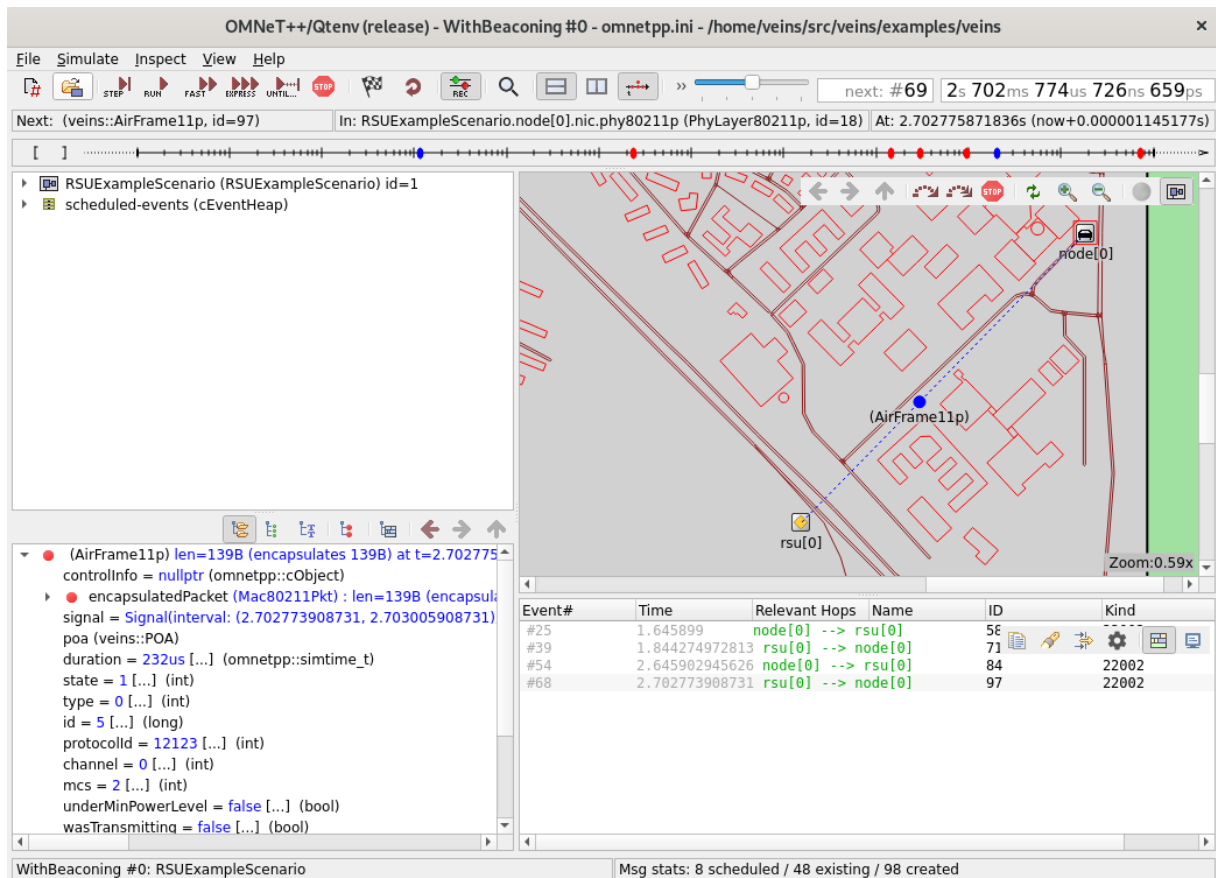
BaseApplicationLayer osztály leszármazottja. Az egyik modell az RSU-k, míg a másik az OBU-k működését írja le. Emellett implementáltunk néhány kiegészítő szolgáltatást is a MAC és a többszörös adatkapcsolati rétegkiterjesztést.

Az alábbiakban részletesen ismertetjük, hogy milyen csomag típusokat definiáltunk egyes lépésekhez, hogyan állítjuk elő azokat, valamint hogyan kerülnek feldolgozásra az események.

4.4.1. Inicializáció

Az inicializáció során a résztvevő felek lekérdezik BC-ről az oda feltöltött rendszerparamétereket, ezentúl megválasztják saját titkos, és kiszámolják saját publikus kulcsait is.

Az eszközök a szimuláció elemzésének megkönnyítéséhez elindítanak egy naplózási folyamatot és inicializálják az elemzési metrikák meghatározásához szükséges változókat is. A 4.7 ábra a szimulációs rendszer inicializáció utáni állapotát mutatja. A kezelőfelület jobb felső sarkában a szimulációs és nem a valós idő látható.



4.7. ábra. A szimuláció egy inicializált RSU és OBU eszközzel.

4.4.2. Regisztráció

A regisztráció alatt megtörténik az RSU és az OBU kölcsönös hitelesítése. Az OBU ebben a lépésben, az RSU által kezdeményezve, felkerül a BC által karbantartott whitelist-re és lekérdezi a regisztrált domainjéhez tartozó friss whiteliset BC-től. Ebben azonosítani tudja saját, de csakis a saját ayG álnevét aG érték és y privát kulcsa alapján. Az folyamat használt üzenettípusait lásd a 4.9. ábrán.

Az implementációnkban egy RSU, annak sikeres inicializációja után elkezd hirdetni magát, mint RSU, melyet minden 2. másodpercben megismétel. Ehhez a 4.8 ábrán szemléltetett üzenettípust használja. Ezen szolgáltatás *psid* azonosítója 69. Az *targetChannel* mező az RSU-hoz tartozó szolgáltatás csatornát jelöli meg. Ez alapértelmezetten az 1-es szolgáltatás csatorna (sch1).

ConnectionServiceAdvertisement
BaseFrame1609-4 fejléc rsuId : string rsuPublicAddr : byte (optional)
targetChannel : int serviceDescription : string

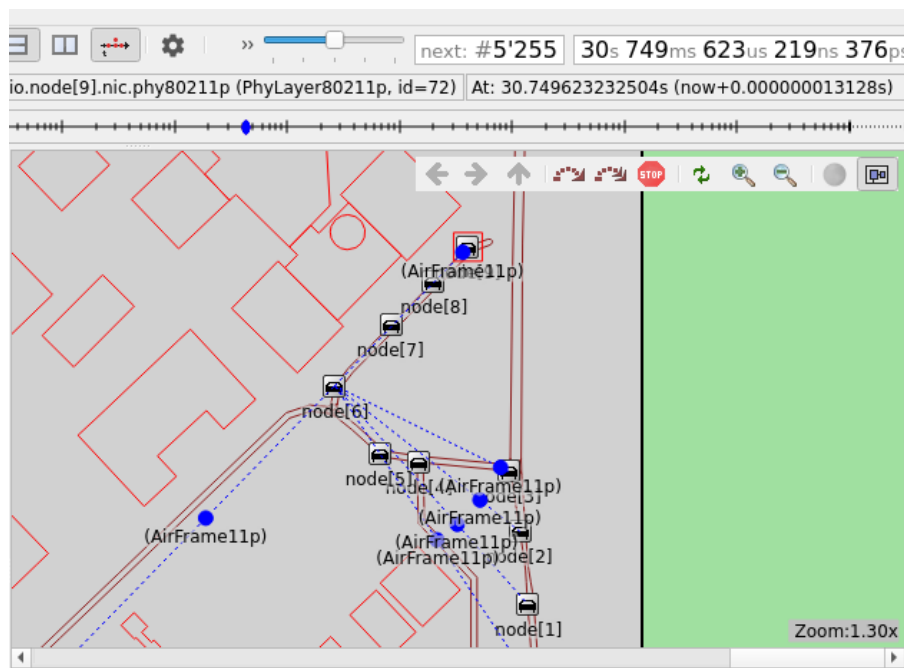
4.8. ábra. Az RSU saját szolgáltatását hirdető üzenetének felépítése.

Kapcsolódási adatcsere

ConnectionRequest	GetPublicList
keyLen : int publicKey : byte	keyLen : int currValidationKey : byte timeStamp : simtime_t
encCert : byte	whitelist : byte list

4.9. ábra. A regisztrációs adatcsere üzeneteinek felépítése.

A regisztrációs folyamat elkezdéséhez az OBU a láncról lekérdezi RSU publikus kulcsát. A 4.8 ábra modelljén az RSU *rsuPublicAddr* publikus azonosító megadása opcionálisként van megjelölve, mivel közlése lehetővé teszi az algoritmusok előszámítását. De OBU azt csak akkor veszi hitelesnek, amennyiben ennek helyességét a blokkláncról történő lekérdezéssel meg tudta erősíteni.



4.10. ábra. node[6] azonosítójú szimulált OBU üzenetküldése kérése

A 4.10 ábra szemlélteti, hogy egy bármilyen elküldött üzenet eljut a küldő környezetén belül minden egységhez, az eszközök antennáinak működésének köszönhetően. Akkor is ilyen viselkedés tapasztalható, ha címzett üzeneteket használunk.

RSU whitelist frissítés hirdetések

Az RSU egy *UpdateAdvertisement* üzenetet (4.12 ábra) küld, amikor egy whitelist permutáció sikeresen lefutott. Ezen értesítés *pingType* ping típusa és *psid* azonosítója 77. Az RSU nyilvántart egy frissítési üzenet sorszámot, hogy elősegítse az csatlakozott egységek számára, a számukra is érdekes frissítések felismerését.

UpdateAdvertisement
BaseFrame1609-4 fejléc rsuId : string
pingType : int pingNumber : int

4.11. ábra. Az RSU saját szolgáltatását hirdető üzenetének felépítése.

Amikor egy OBU megkap egy *UpdateAdvertisement* üzenetet, akkor ellenőrzi a küldő RSU azonosítóját, a frissítési üzenet típusát és a frissítési üzenet sorszámát is. Amennyiben észleli,

hogy számára új whitelist létezéséről kapott információt, akkor lekérdezi azt a blokkláncról. Ezután ő is elismétli a ping üzenetet. Az RSU által használt üzenetküldési mechanizmust a 2. algoritmus, míg annak OBU általi kezelését a 3. algoritmus szemlélteti.

2. Algoritmus Listafrissítés értesítő üzenet generálása RSU által

Require: Inicializáció befejeződött

Ensure: *ua* egy *UpdateAdvertisement* üzenet, *myId* az RSU azonosítója

pingSeq $\leftarrow$ 0

while RSU aktív **do**

if Regisztráció befejezve vagy incidens report történt **then**

ua populálása

pingSeq növelése

ua.rsuId $\leftarrow$ *myId*

ua.pingType $\leftarrow$ 77

ua.pingNumber $\leftarrow$ *pingSeq*

ua üzenetszórása

end if

end while

3. Algoritmus Listafrissítés értesítő üzenet kezelése OBU által

Require: Inicializáció befejeződött

Ensure: *ua* egy *UpdateAdvertisement* üzenet, *curRsu* a domain RSU azonosítója

pingSeq $\leftarrow$ 0

while OBU aktív **do**

ua $\leftarrow$ elkapott *UpdateAdvertisement* üzenet

if *ua.rsuId* == *curRsu* **then**

if *ua.pingType* == 77 **then**

if *ua.pingNumber* > *pNum* **then**

pingSeq $\leftarrow$ *ua.pingNumber*

ua üzenetszórása

end if

else if ping reset üzenet érkezett **then**

pingSeq $\leftarrow$ 0

end if

end if

end while

Minden OBU tárol egy másolatot az álnevek listájáról, és ezt frissíteni a blokkláncról történő lekérdezéssel tudja.

UpdateAdvertisement
BaseFrame1609-4 fejléc rsuId : string
pingType : int pingNumber : int

4.12. ábra. Az RSU saját szolgáltatását hirdető üzenetének felépítése.

4.4.3. Incidensjelentés

Az incidens jelentéshez használt két üzenettípust a 4.13 ábra mutatja. Az *IncidentReport* üzenettípus "SchnorrSign" mezője tartalmazza a $w + H(M || wG)ky$, wG párt és a "EDL-NIZKP" mező a $EDL - NIZKP(kyG, kG, ayG, aG)$ értékeit.

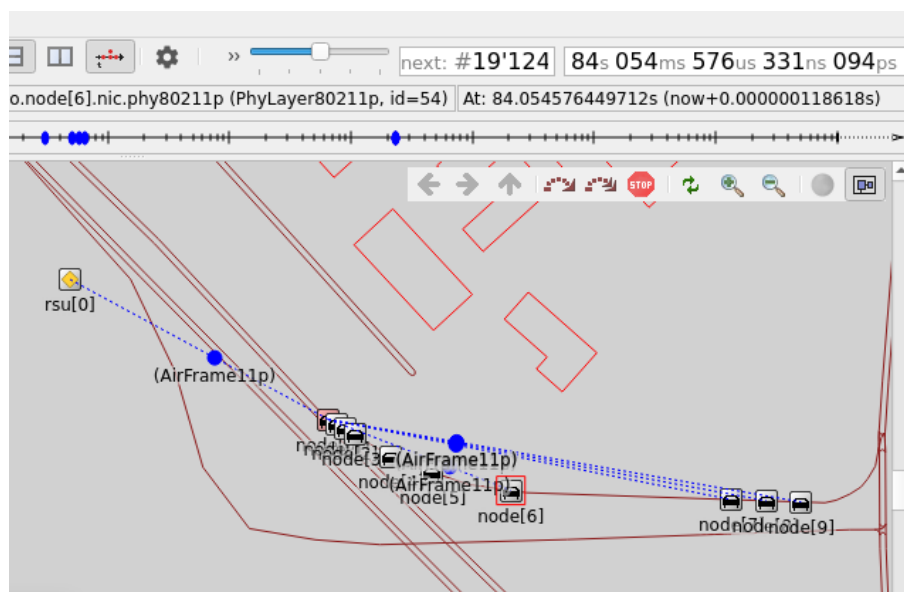
ServiceAdvertisement	IncidentReport
BaseFrame1609-4 fejléc	BaseFrame1609-4 fejléc SchnorrSign : byte EDL-NIZKP : byte
targetChannel : int serviceDescription : string	gpsZone : string incidentCode : int timeStamp : simtime_t

4.13. ábra. Az incidensbejelentés és szolgáltatás hirdetés üzenettípusok.

Egy incidensjelentéssel együtt a bejelentő egy értesítési szolgáltatást is indít. Erről értesíti a többi résztvevőt a vezérlési csatornán, miközben a jelentése üzenetszórását végzi valamelyik szolgáltatási csatornán (alapértelmezetten sch1). Ezen bejelentést egy *ServiceAdvertisement* típusú üzenettel tesszük meg. A bejelentés után a küldő elismétli a generált *IncidentReport* üzenetet számos alkalommal, hogy azon eszközök is, amelyek más szolgáltatási csatornát hallgattak, értesülhessenek a jelentésről. Az incidens bejelentés szolgáltatáshoz tartozó *psid* azonosító értéke 42. Szimulációja a keretrendszerben a 4.14. ábrán látható.

A bejelentő elindítja az incidensjelentés feltöltést a blokkláncra is. Befizeti a szükséges költséget, és amint az üzenetét a protokoll hasznosnak ítéli, megjuttalmazza.

Amikor egy hálózati egység elkap egy incidensjelentést, akkor először ellenőrzi, hogy milyen régen állították elő, majd ellenőrzi hitelességét is. A megadott időintervallumon kívül eső üzenetek feldolgozásával és megosztásával a rendszer már nem foglalkozik. Ezen információkat



4.14. ábra. node[0] azonosítójú szimulált OBU incidensjelentés üzenetküldése

az eszközök a blokklánctól kérdezhetik le. Az üzenet feldolgozásának menetét az 1. algoritmusban szemléltetett üzenet továbbadási folyamat írja le.

4.4.4. Biztonsági szolgáltatások

MAC címcseré

Az implementációnk megvalósít egy egyszerű, randomizált MAC cím módosító szolgáltatást, amely biztosítja az eszközök fizikai címe alapján történő összekapcsolhatatlanságot. A fedélzeti egységek minden különböző incidensjelentés megosztása után fizikai címet módosítanak, legyen az saját, vagy elismételt üzenet.

A protokoll közeli kommunikációs hálózatában üzenetszórással valósítja meg az incidensjelentés megosztását, és konkrét fizikai címezést nem használ, így azok változtatása nem okoz problémát.

5. fejezet

A rendszer elemzése

5.1. A rendszer szimulációjának elemzése

A rendszer szimulációjával becsüljük meg a rendszer működését és hatékonyságát. A számítási és futási időket a 5.1 táblázat, míg a terjedési időket a 5.2 táblázat mutatja be.

A szimulált rendszerben egy üzenet értelmezéséhez (nem feldolgozásához) szükséges műveletek elvégzéséhez szükséges idő, átlagosan $\sim 3,64 \mu s$ szolgáltatás hirdetések és $\sim 10,94 \mu s$ tartalommal rendelkező üzenetek esetén. Egy üzenet másolása, ellenőrzés nélkül, szolgáltatási üzenet esetén $\sim 1,927 ms$, míg vezérlési üzenet esetén $\sim 5,75 \mu s$ vesz átlagosan igénybe. Egy szolgáltatás elindításához és az első hirdetés elküldéséhez $\sim 7,031 ms$ szükséges. Mindez igaz a fizikai küldés ideje nélkül, ami a csatornák telítettségétől függően változhat. Egy frissítési értesítő üzenet generálásához átlagosan $\sim 81.77 \mu s$ szükséges.

Folyamat	Szükséges átlagos futásidő (ms)
Szolgáltatás hirdetés indítása	7,03100 ms
Vezérlési üzenet értelmezése	0,00364 ms
Szolgáltatási üzenet értelmezése	0,01094 ms
Vezérlési üzenet másolása	0,00575
Szolgáltatási üzenet másolása	1,937 ms
Frissítési értesítés készítése	0,08177 ms
Incidens report generálása	8,81277 ms

5.1. táblázat. Általános üzenetkezeléshez és vezérlési üzenetek generálásához szükséges idő

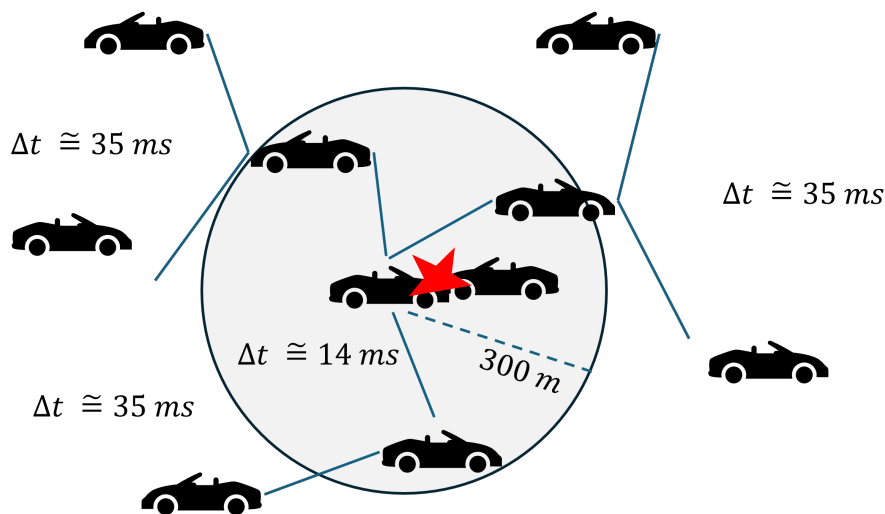
A szimulációban egy szolgáltatás hirdetése értesíti a felhasználókat, hogy milyen típusú üzenet közlekedik melyik szolgáltatási csatornán. Egy ilyen hirdetés terjedési ideje, két egység

között, a szimulációban átlagosan ~11,154 ms. Ez egy hirdetés küldése, és az erről értesülő fél saját szolgáltatás hirdetésének első üzenetküldése között eltelt idő.

Folyamat	Átlagos terjedési idő (ms)
Szolgáltatás hirdetés terjedése	11,154 ms
Incidens report értelmezése és ellenőrzése közvetlenül	14,032 ms
Incidens report terjedése	19,019 ms
Incidens report értelmezése és ellenőrzése közvetetten	35,034 ms

5.2. táblázat. Üzenetek terjedéséhez szükséges idők.

Egy incidens riport előállítási ideje átlagosan ~8.8 ms. Ez csak az üzenet előállítás ideje, a tényleges incidens bekövetkezése és érzékelése között még telhet el idő. Az üzenet elküldése után a szimulációban átlagosan ~14.03 ms később már az üzenetet a hozzá közel lévő egységek el tudták kapni, értelmezni tudták, és már ellenőrizték is annak hitelességét és integritását. Ez ideális esetben lehetővé tenné, hogy egy 46 ms-os szolgáltatási intervallumban (lásd 4.4. ábra) 3 hopp távolságra, azaz 3 más autón keresztül 3x olyan messzire is eljuttassuk.



5.1. ábra. Üzenetterjedés a hálózatban

Előbbi csak akkor lehetséges, amennyiben egy köztes eszköz csak egy másik eszköztől hallja az üzenetet. Mert minden olyan jármű, aki közvetlenül hallja az üzenetet, az eredeti üzenet küldése után ~14ms már ellenőrizték, és ~19ms-al már akár küldhetik is tovább. Ez pedig ahhoz vezet, hogy az első megosztás után ~4ms-ként történik egy további megosztása ugyan annak az üzenetnek, ami foglaltan tartja a csatornát (amennyiben hallják egymást). A küldési láncban

második jármű, már ~35-38ms-al az eredeti üzenet küldése után értelmezte, ellenőrizte és küldené is tovább az üzenetet, de sokszor azzal szembesül, hogy ezt nem tudja megtenni, mivel épp foglalt a csatorna.

5.2. Kommunikációs hatótávolság városi környezetben

A IEEE 802.11p maximális hatékony hatótávolsága 1000m. Ez egy nagy zajszintű, sűrű, városi környezetben, a hatékonyság megtartása mellett, 300m-re csökken. A tényleges kommunikációs távolság nagyban függ a környezettől, viszont a hálózat résztvevői megoszthatják egymással az információikat. Így figyelembe véve a WAVE működését és az OBU-n történő feldolgozási időt, az RSU kommunikációs hatótávolsága városi körülmények között is elérheti a 900-1000 métert. Ezt akkor lehetséges, amennyiben egy üzenetet még 2 másik OBU is tovább küld az RSU felé, mint egy küldési lánc. Ezt a távolságot vesszük annak, amelyen belül gyorsabb információterjesztést valósíthatunk meg a láncolathoz képest.

A változó környezeti viszonyok, mint a romlott látási viszonyok és az nem megfelelő út-állapotok, hosszabb féktávolságot eredményezhetnek. Rossz útviszonyok esetén bár ajánlott az alacsonyabb sebesség, még a legóvatosabb sofőrök számára is nehéz lehet elkerülni a baleseteket ilyen körülmények között. Ez azt jelenti számunkra, hogy a kommunikáció sebességét valahogyan növelni kell, hogy időben értesüljön a jármű vezetője és biztonságosan tudjon közlekedni.

Az üzenetek továbbítása és a WAVE használata releváns lehet, de a kommunikációs hatótávolságnak kisebbnek kellene lennie. Ideális esetben a WAVE használata nem haladhatja meg a 600m, figyelembe véve a maximális megállási távolságot, a haladási sebességet és a feldolgozási időket.

A sebesség egy test azon jellemzője, amely megmutatja, hogy a pozíciója, hogyan változik egységnyi idő alatt, a pozíció változás gyorsasága. A sebesség vektormennyiség, ami azt jelenti, hogy iránnyal és nagysággal rendelkezik. A sebesség irányát az adott pálya érintőjének az iránya határozza meg, míg a nagyságát az időegység alatt megtett út hossza adja meg.

$$v = \frac{s}{t}$$

Az erő az a fizikai mennyiség, amely a testek állapotváltozását okozza. Megmutatja, hogy egy adott rendszert tápláló kölcsönhatás, milyen mértékben változtatja meg a rendszer állapotát.

Az erő képes megváltoztatni a testek sebességét és irányát. Az erő vektormennyiség, vagyis rendelkezik nagysággal és iránnyal egyaránt. Egy test gyorsulása egyenesen arányos a rá ható erővel és fordítottan arányos a test tömegével.

$$F = ma$$

ahol m a jármű tömege és a a gyorsulása.

A tapadási súrlódási erő a közlekedés során kulcsfontosságú szerepet játszik, mivel ez az erő felelős azért, hogy a járművek biztonságosan közlekedhessenek. A tapadási súrlódás a jármű kerekei és az úttest közötti kölcsönhatás eredményeként jön létre, és befolyásolja a jármű mozgását. A fellépő erő nagysága függ a két felület fizikai minőségétől, a súrlódási együtthatótól, ami a felületek anyagi minőségétől és állapotától függ, valamint a felületek között ható nyomóerőtől.

$$F_t = \mu F_{ny}$$

ahol F_t a tapadási súrlódási erő, μ a tapadási súrlódási együttható, és F_{ny} a felületek közötti nyomóerő, amely a jármű összsúlyából adódik. Ha egy adott járművek paramétereit állandónak tekintjük, akkor csak a környezettől függ a tapadását útközben. Legyen

$$F_{t_1} = \mu_1 * F_{ny_1}$$

az ideális körülmények közötti tapadás, és

$$F_{t_2} = \mu_2 * F_{ny_1}$$

az egy megváltozott, az ideálistól eltérő tapadás mellett fellépő erő. Ekkor

$$\frac{F_{t_2}}{F_{t_1}} = \frac{\mu_2 * F_{ny_1}}{\mu_1 * F_{ny_1}} = \frac{\mu_2}{\mu_1}$$

Ebből a hányadosból következtetni tudunk arra, hogy a fékezőerő és a fékezéshez szükséges út hossza, hogyan változik.

Rossz környezeti viszonyok mellett a következő képlet alkalmazható a WAVE hatósugara:

$$600 * c * \frac{\mu_2}{\mu_1}$$

ahol $c \in [0, 1]$ a látási viszonyok mértékét, és $\mu_2, \mu_1 \in [0, 1]$ pedig az ideális és a romlott útviszonyok tapadási jellemzőit jelöli.

6. fejezet

Összefoglalás

A dolgozatban bemutattuk a Pseudonym-based Hybrid, Privacy-preserving Broadcast Protocol (PHP-BP) névre keresztelt kriptográfiai protokollt. Ez elősegíti a vezeték nélküli járműhálózatok anonim hiteles kommunikációját, és a dolgozatunkban megadott működési modell irányadó lehet a jövőbeli implementációk és tesztrendszer fejlesztése számára. PHP-BP betölti a 3.2. fejezetben vele szemben támasztott elvárásokat. Ezt a 3.5. fejezetben bemutatott biztonsági elemzés szemlélteti.

A protokoll sikeresen tudja csökkenteni a hozzá szükséges infrastruktúra kiépítési és karbantartási költségeit azzal, hogy nem igényli, hogy egy város és út minden területén legyenek kitelepített út menti egységek. Ezzel megoldható, hogy egy városhoz csak pár RSU hozzárendelése is elegendő legyen, mivel minden információt képes terjeszteni a rendszer az egységek közötti üzenet továbbadási mechanizmussal (lásd 4.3.2. fejezet). Ezen segít a kósza autó probléma megoldásával is, amivel lehetőséget ad, hogy a ritkább jármű sűrűségű környezetben közlekedő autók is el tudják kérni a friss információkat, és lehetőségük legyen részt venni működésében.

Ez a két megoldás, kiegészítve fizikai RSU-hoz több fizikai interfész kiépítésének lehetőségével, egy erős alap infrastruktúrát tud adni. Mivel hibrid rendszerről beszélünk, ahol az információ tárolás decentralizáltan történik, így a rendszerben nem jelennek meg, a VANET rendszerekben általános single point of failure egységek. Ezentúl az egyik alrendszer meghibásodása esetén egy környezetben, a másik biztosítja a rendszer rendelkezésre állását, még ha csökkentett hatékonysággal is.

A szimuláció sikeresen bemutatja a hibrid rendszer WAVE hálózatának működését. Implementációnk viszont nem fejt ki a protokoll blokklánccal történő kommunikációs lépéseinek működését. Így, habár a szimulációnk a vele szemben támasztott elvárásokat teljesíti,

ami csak a hálózat fizikai részének kifejtését követelte meg, nem tekinthető teljesnek. Emiatt ennek kidolgozása a jövőbeli fejlesztések egyik fő céljának kell lennie. A megvalósított implementáció hatékonyságát az elemzésről szóló fejezet első alfejezete mutatja be (5.1. fejezet). Az 5.2. fejezet szemlélteti, hogy egy kilométeres hatékony RSU tartománnyal, városi környezetben csak bizonyos feltételek teljesülése mellett számíthatunk. Ez szemlélteti, hogy mennyire nagy hatása van az aktuális környezetének egy VANET hálózatban a tényleges üzenet terjedési idejére és a hálózati kommunikáció hatékonyságára.

Végezetül pedig az alábbi jövőbeli fejlesztési irányokat javasoljuk. A protokollal kapcsolatos további kutatómunkának két fő feladatokat kell megoldania.:

- Először is meg kell határozni a protokoll lépéseinek végrehajtásához szükséges blokklánc oldali folyamatokat is. Ehhez okosszerződéseket, függvényeket és azok implementációját is meg kell adni. Ezen bővítésekkel együtt már a rendszer egésze szimulálható, amiből komplexebb összefüggések és következtetések vonhatóak le.
- Másodszor, a rendszer szimuláció legyen megvalósítva az IEEE 802.11bd fizikai és adatkapcsolati standardra építve is. Ennek az irodalomkutatás alapján sok előnye van, a jelenleg használt IEEE 802.11p standardhoz képest. Ezentúl több friss kutatás is ennek a használatát ajánlja. Az Európai unión belül esélye is van, hogy az épp formálódó standardok is erre fognak épülni, ezért a rendszer jövőállósága végett ajánlott ennek használata, akkor is, ha jelenleg még IEEE 802.11p eszközök vannak használatban.

Amint ezen két fő, még megoldásra váró feladat elvégzésre került, és a szimulációk alapján sikerül további fejlesztési irányokat meghatározni, akkor megfontolandó egy teszhálózat kiépítése is, a tovább tesztek és fejlesztések elvégzéséhez.

Saját munka leírása

A teljes kutatásom során sok tanácsot és támogatást kaptam témavezetőimtől. Ők mindvégig segítettek engem és lehetővé tették, hogy a kutatás alatt hatékony lehessen munkavégzésem. Ezen támogatás megköszönésére az elvégzett munkák felsorolását két részre osztom. Először megemlítem azokat, amiken együtt, közösen dolgoztunk a témavezetőimmel, majd azokat is felsorolom amiket egyedül, minimális útmutatással végeztem el.

A témavezetőimmel közösen végzett feladatok:

- A javasolt PHP-BP protokoll kriptográfiai protokoll működésének és lépéseinek definiálása.
- A blokklánc, mint támogató kommunikációs platform használatának kutatása (lásd 2. fejezet.)
- A protokoll kriptográfiai számításainak implementálása Python és C++ függvényekként.
- A kommunikáció hatékony távolságának számítása (lásd 5.2. fejezet).
- A dolgozat tartalmi és szerkezeti felépítésének meghatározása.
- A dolgozat 3. fejezetének megfogalmazása.

Az általam elvégzett feladatok:

- Irodalomkutatás a VANET rendszerekkel, a bennük használt hálózati technológiákkal és szimulációs platformokkal kapcsolatban. Továbbá kutatómunka végzése más protokollok működésével kapcsolatban, és azok elemzése. (lásd 2. fejezet.)
- A WAVE, mint kritikus információk közléséhez használható kommunikációs technológia kutatása. (lásd 4.1.2. fejezet.)
- Implementációs hálózati modell tervezése, bemutatása. (lásd 4.2. fejezet)

- PHP-BP WAVE hálózati részének és lépéseinek implementálása veins szimulációs keretrendszerben (lásd 4.3. és 4.4. fejezetek).
- A készített implementáció alapján a rendszer szimulálása, elemzése és az erről szóló fejezet megírása (lásd 5.1. fejezet).
- A dolgozat 1., 4. és 6. fejezeteinek megfogalmazása.

Köszönetnyilvánítás

Szeretném megköszönni a támogató és segítő munkáját két témavezetőmnek, Dr. Pintér-Husztai Andreának és Girászi Tamásnak. A kutatási munka alatt és ezen dolgozat végleges formára hozásához is sok segítséget kaptam tőlük. Ezentúl szakmai fejlődésem alatt felmerült kérdésekkel és problémákkal kapcsolatban is mindig számíthattam jó tanácsaikra. Továbbá szeretném megköszönni a szeretteim és családom támogatását, akik megértésükkel és segítő-készségükkel járultak hozzá ezen dolgozat sikeres megírásához.

Ezentúl köszönöm a Debreceni Egyetem Informatikai Karának, a Debreceni Egyetem Tehetséggondozó Programjának (DETEP), és a Hajós György Adattudományi Szakkollégiumnak a szakmai támogatást. Ezen belül is kiemelt köszönet a szakkollégium Adatbiztonság Műhelyének, hogy támogatta és befogadta kutatómunkámat.

Végül, de nem utolsó sorban szeretném megköszönni Kulturális és Innovációs Minisztérium új nemzeti kiválóság programjának támogatását, és az ügyintézésben dolgozó egyetemi munkatársak segítőkészségét. Nagyban megkönnyítették a szükséges adminisztráció elvégzését.

A bemutatott tudományos diákköri dolgozat és a dolgozattal kapcsolatos kutatómunka a Kulturális és Innovációs Minisztérium ÚNKP-23-2-I-DE-365 kódszámú új nemzeti kiválóság programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.



Irodalomjegyzék

- [1] A. Fiat és A. Shamir, „How To Prove Yourself: Practical Solutions to Identification and Signature Problems”, A. M. Odlyzko, szerk., 186–194. old., 1987.
- [2] C. Schnorr, „Efficient signature generation by smart cards”, *Journal of Cryptology*, 4. évf., 161–174. old., 1991. jan. DOI: 10.1007/BF00196725.
- [3] D. Chaum és T. P. Pedersen, „Wallet Databases with Observers”, E. F. Brickell, szerk., 89–105. old., 1993.
- [4] M. Raya és J.-P. Hubaux, „Securing vehicular ad hoc networks”, *J. Comput. Secur.*, 15. évf., 39–68. old., 2007. cím: <https://api.semanticscholar.org/CorpusID:12962125>.
- [5] R. Lu, X. Lin, H. Zhu, P.-H. Ho és X. Shen, „ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications”, *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008, 1229–1237. old. DOI: 10.1109/INFOCOM.2008.179.
- [6] Z. Ma, F. Kargl és M. Weber, „Pseudonym-On-Demand: A New Pseudonym Refill Strategy for Vehicular Communications”, *2008 IEEE 68th Vehicular Technology Conference*, 2008, 1–5. old. DOI: 10.1109/VETECF.2008.455.
- [7] „IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments”, *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)*, 1–51. old., 2010. DOI: 10.1109/IEEESTD.2010.5514475.

- [8] A. Pfitzmann és M. Hansen, *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, v0.34, 2010. aug. cím: http://dud.inf.tu-dresden.de/literatur/Anon%5C_Terminology%5C_v0.34.pdf.
- [9] D. Eckhoff, R. German, C. Sommer, F. Dressler és T. Gansen, „SlotSwap: strong and affordable location privacy in intelligent transportation systems”, *IEEE Communications Magazine*, 49. évf., 11. sz., 126–133. old., 2011. DOI: 10.1109/MCOM.2011.6069719.
- [10] C. Zhang, P.-H. Ho és J. Tapolcai, „On batch verification with group testing for vehicular communications”, *Wireless Networks*, 17. évf., 1851–1865. old., 2011. nov. DOI: 10.1007/s11276-011-0383-2.
- [11] E. T. S. I. (ETSI), *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*, TS 102 941 v1.1.1, 2012. jún. cím: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.01.01_60/ts_102941v010101p.pdf.
- [12] D. Eckhoff, C. Sommer és F. Dressler, „On the Necessity of Accurate IEEE 802.11P Models for IVC Protocol Simulation”, *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, 2012, 1–5. old. DOI: 10.1109/VETECS.2012.6240064.
- [13] C. Sommer, S. Joerer és F. Dressler, „On the applicability of Two-Ray path loss models for vehicular network simulation”, *2012 IEEE Vehicular Networking Conference (VNC)*, 2012, 64–69. old. DOI: 10.1109/VNC.2012.6407446.
- [14] A. Wasef és X. Shen, „EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks”, *IEEE Transactions on Mobile Computing*, 12. évf., 1. sz., 78–89. old., 2013. DOI: 10.1109/TMC.2011.246.
- [15] „IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture”, *IEEE Std 1609.0-2013*, 1–78. old., 2014. DOI: 10.1109/IEEESTD.2014.6755433.
- [16] C. Sommer, D. Eckhoff és F. Dressler, „IVC in Cities: Signal Attenuation by Buildings and How Parked Cars Can Improve the Situation”, *IEEE Transactions on Mobile Computing*, 13. évf., 8. sz., 1733–1745. old., 2014. DOI: 10.1109/TMC.2013.80.
- [17] C. Sommer, S. Joerer, M. Segata, O. K. Tonguz, R. L. Cigno és F. Dressler, „How Shadowing Hurts Vehicular Communications and How Dynamic Beaconing Can Help”, *IEEE Transactions on Mobile Computing*, 14. évf., 7. sz., 1411–1421. old., 2015. DOI: 10.1109/TMC.2014.2362752.

- [18] D. Eckhoff, A. Brummer és C. Sommer, „On the impact of antenna patterns on VANET simulation”, *2016 IEEE Vehicular Networking Conference (VNC)*, 2016, 1–4. old. DOI: 10.1109/VNC.2016.7835925.
- [19] „IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages”, *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, 1–240. old., 2016. DOI: 10.1109/IEEESTD.2016.7426684.
- [20] 5. A. Association, „An assessment of LTE-V2X (PC5) and 802.11p direct communications technologies for improved road safety in the EU”, techn. jel., 2017. dec.
- [21] G. Rigazzi, A. Tassi, R. J. Piechocki, T. Tryfonas és A. R. Nix, „Optimized Certificate Revocation List Distribution for Secure V2X Communications”, *CoRR*, abs/1705.06903 évf., 2017. arXiv: 1705.06903. cím: <http://arxiv.org/abs/1705.06903>.
- [22] C. Song, „Performance Analysis of the IEEE 802.11p Multichannel MAC Protocol in Vehicular Ad Hoc Networks”, *Sensors*, 17. évf., 12. sz., 2017, ISSN: 1424-8220. DOI: 10.3390/s17122890. cím: <https://www.mdpi.com/1424-8220/17/12/2890>.
- [23] S. Wang és N. Yao, „LIAP: A local identity-based anonymous message authentication protocol in VANETs”, *Computer Communications*, 112. évf., 154–164. old., 2017, ISSN: 0140-3664. DOI: <https://doi.org/10.1016/j.comcom.2017.09.005>. cím: <https://www.sciencedirect.com/science/article/pii/S0140366417309520>.
- [24] F. Bronner és C. Sommer, „Efficient Multi-Channel Simulation of Wireless Communications”, *2018 IEEE Vehicular Networking Conference (VNC)*, 2018, 1–8. old. DOI: 10.1109/VNC.2018.8628350.
- [25] Z. Lu, W. Liu, Q. Wang, G. Qu és L. Zhenglin, „A Privacy-preserving Trust Model based on Blockchain for VANETs”, *IEEE Access*, PP évf., 1–1. old., 2018. aug. DOI: 10.1109/ACCESS.2018.2864189.
- [26] S. Wang, N. Yao, N. Gong és Z. Gao, „A trigger-based pseudonym exchange scheme for location privacy preserving in VANETs”, *Peer-to-Peer Networking and Applications*, 11. évf., 2018. máj. DOI: 10.1007/s12083-017-0557-5.
- [27] X. Zhang, R. Li és B. Cui, „A security architecture of VANET based on blockchain and mobile edge computing”, 258–259. old., 2018, Inner Mongolia University, College of Computer Science, Hohhot, China.

- [28] „IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture”, *IEEE Std 1609.0-2019 (Revision of IEEE Std 1609.0-2013)*, 1–106. old., 2019. DOI: 10.1109/IEEESTD.2019.8686445.
- [29] O. Ltd. „OMNeT++ Documentation”. (2019), cím: [https : / / omnetpp . org / documentation/](https://omnetpp.org/documentation/) (elérés dátuma 2024. 03. 29.).
- [30] B. Luo, X. Li, J. Weng, J. Guo és J. Ma, „Blockchain Enabled Trust-Based Location Privacy Protection Scheme in VANET”, *IEEE Transactions on Vehicular Technology*, 68. évf., 12. sz., 11543–11556. old., 2019. DOI: 10.1109/TVT.2019.2957744.
- [31] P. K. Singh, S. N. Gowtham, T. S és S. Nandi, „CPESP: Cooperative Pseudonym Exchange and Scheme Permutation to preserve location privacy in VANETs”, *Vehicular Communications*, 20. évf., 100183. old., 2019, ISSN: 2214-2096. DOI: [https : / / doi . org / 10 . 1016 / j . vehcom . 2019 . 100183](https://doi.org/10.1016/j.vehcom.2019.100183). cím: [https : / / www . sciencedirect . com / science / article / pii / S221420961930230X](https://www.sciencedirect.com/science/article/pii/S221420961930230X).
- [32] I. Ali, T. Lawrence és F. Li, „An efficient identity-based signature scheme without bi-linear pairing for vehicle-to-vehicle communication in VANETs”, *Journal of Systems Architecture*, 103. évf., 101692. old., 2020, ISSN: 1383-7621. DOI: [https : / / doi . org / 10 . 1016 / j . sysarc . 2019 . 101692](https://doi.org/10.1016/j.sysarc.2019.101692). cím: [https : / / www . sciencedirect . com / science / article / pii / S1383762119304990](https://www.sciencedirect.com/science/article/pii/S1383762119304990).
- [33] M. LLC. „Veins Documentation”. (2020), cím: [https : / / veins . car2x . org / documentation/](https://veins.car2x.org/documentation/) (elérés dátuma 2024. 03. 29.).
- [34] A. Srivastava, A. Prakash és R. Tripathi, „Location based routing protocols in VANET: Issues and existing solutions”, *Vehicular Communications*, 23. évf., 100231. old., 2020, ISSN: 2214-2096. DOI: [https : / / doi . org / 10 . 1016 / j . vehcom . 2020 . 100231](https://doi.org/10.1016/j.vehcom.2020.100231). cím: [https : / / www . sciencedirect . com / science / article / pii / S2214209620300024](https://www.sciencedirect.com/science/article/pii/S2214209620300024).
- [35] B. Yacheur, T. Ahmed és M. Mosbah, „Analysis and Comparison of IEEE 802.11p and IEEE 802.11bd”, 2020. dec., 55–65. old., ISBN: 978-3-030-66029-1. DOI: 10.1007/978-3-030-66030-7_5.
- [36] I. T. Almalkawi, J. Raed, A. Alsarhan, A. Abdallah és E. Abdallah, „A Novel and Efficient Priority-Based Cross-Layer Contextual Unobservability Scheme Against Global Attacks for WMSNs”, *International Journal of Interactive Mobile Technologies*

- (*iJIM*), 15. évf., 3. sz., pp. 43–69., 2021. febr. DOI: 10.3991/ijim.v15i03.18327.
cím: <https://online-journals.org/index.php/i-jim/article/view/18327>.
- [37] A. Huszti, S. Kovács és N. Oláh, „Hybrid anonymous message broadcast for VANETs”, *2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2021, 103–108. old. DOI: 10.1109/WiMob52687.2021.9606302.
- [38] N. Ravi, S. Verma, Kavita, N. Jhanjhi és M. Talib, „Securing VANET Using Blockchain Technology”, 1979. évf., 12035. sz., 2021. DOI: 10.1088/1742-6596/1979/1/012035.
- [39] U. Bansal, J. Kar, I. Ali és K. Naik, „ID-CEPPA: Identity-based Computationally Efficient Privacy-Preserving Authentication scheme for vehicle-to-vehicle communications”, *Journal of Systems Architecture*, 123. évf., 102387. old., 2022, ISSN: 1383-7621. DOI: <https://doi.org/10.1016/j.sysarc.2021.102387>. cím: <https://www.sciencedirect.com/science/article/pii/S1383762121002654>.
- [40] C. 2. C. C. Consortium, „Next Generation V2X – IEEE 802.11bd as fully backward compatible evolution of IEEE 802.11p”, techn. jel. 2098, 2022. febr., v1.0.
- [41] X. Deng, T. Gao, N. Guo, C. Zhao és J. Qi, „PCP: A Pseudonym Change Scheme for Location Privacy Preserving in VANETs”, *Entropy*, 24. évf., 5. sz., 2022, ISSN: 1099-4300. DOI: 10.3390/e24050648. cím: <https://www.mdpi.com/1099-4300/24/5/648>.
- [42] M. Nitschke, C. Roth, C. Hoyer és D. Kesdoğan, „Harmonic Group Mix: A Framework for Anonymous and Authenticated Broadcast Messages in Vehicle-to-Vehicle Environments”, *Information Systems Security and Privacy*, S. Furnell, P. Mori, E. Weippl és O. Camp, szerk., Cham: Springer International Publishing, 2022, 178–200. old., ISBN: 978-3-030-94900-6.
- [43] M. Uzair, „Vehicular Wireless Communication Standards: Challenges and Comparison”, *International journal of electrical and computer engineering systems*, 13. évf., 379–397. old., 2022. júl. DOI: 10.32985/ijeces.13.5.6.
- [44] A. Yakovenko. „Solana: A new architecture for a high performance blockchain”. v0.8.14. (2022), cím: <https://github.com/solana-labs/whitepaper/blob/master/solana-whitepaper-en.pdf> (elérés dátuma 2024. 04. 07.).

- [45] „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 Amendment 5: Enhancements for Next Generation V2X”, *IEEE Std 802.11bd-2022 (Amendment to IEEE Std 802.11-2020 as amended by IEEE Std 802.11ax-2021, IEEE Std 802.11ay-2021, IEEE Std 802.11ba-2021, IEEE Std 802.11-2020/Cor 1-2022, and IEEE Std 802.11az-2022)*, 1–144. old., 2023. DOI: 10.1109/IEEESTD.2023.10063942.
- [46] B. Ma, X. Wang, X. Lin és tsai., „Location Privacy Threats and Protections in Future Vehicular Networks: A Comprehensive Review”, *ArXiv*, abs/2305.04503 évf., 2023. cím: <https://api.semanticscholar.org/CorpusID:258558056>.
- [47] A. P. Mdee, M. T. R. Khan, J. Seo és D. Kim, „Security Compliant and Cooperative Pseudonyms Swapping for Location Privacy Preservation in VANETs”, *IEEE Transactions on Vehicular Technology*, 72. évf., 8. sz., 10710–10723. old., 2023. DOI: 10.1109/TVT.2023.3254660.
- [48] E. Foundation. „SUMO”. (2024), cím: <https://eclipse.dev/sumo/> (elérés dátuma 2024. 03. 29.).

Ábrák jegyzéke

3.1. A PHP-BP protokoll felépítésének ábrázolása	14
4.1. A Veins keretrendszer architektúrája[33].	27
4.2. Az IEEE 1609.04 szabvány által definiált csatornák[33].	28
4.3. A többcsatornás modell felosztása [22].	29
4.4. A többcsatornás modell egy szinkronizációs intervalluma[33].	29
4.5. Az implementált hálózati modell rétegei.	31
4.6. MacPck802-11 és BaseFrame1609-4 mezői.	33
4.7. A szimuláció egy inicializált RSU és OBU eszközzel.	35
4.8. Az RSU saját szolgáltatását hirdető üzenetének felépítése.	36
4.9. A regisztrációs adatcsere üzeneteinek felépítése.	36
4.10. node[6] azonosítójú szimulált OBU üzenetküldése kérése	37
4.11. Az RSU saját szolgáltatását hirdető üzenetének felépítése.	37
4.12. Az RSU saját szolgáltatását hirdető üzenetének felépítése.	39
4.13. Az incidensbejelentés és szolgáltatás hirdetés üzenettípusok.	39
4.14. node[0] azonosítójú szimulált OBU incidensjelentés üzenetküldése	40
5.1. Üzenetterjedés a hálózatban	42

Algoritmusjegyzék

1.	Üzenet feldolgozás és tovább küldés	34
2.	Listafrissítés értesítő üzenet generálása RSU által	38
3.	Listafrissítés értesítő üzenet kezelése OBU által	38