Budapesti Műszaki és Gazdaságtudományi Egyetem
Hálózati Rendszerek és Szolgáltatások Tanszék

Új módszerek a CAN hálózatok biztonságának és adatvédelmének a növelésére

Tézisfüzet

Gazdag András

Témavezető:
Buttyán Levente, PhD, DSc

Budapest, Magyarország
2024

1. Bevezetés

A járműipar utóbbi évtizedeiben jelentős változást hozott a beágyazott vezérlők elterjedése. A korábban analóg módszerekkel vezérelt folyamatok felett digitális logikák, és szoftver komponensek vették át az irányítást. A változás fő motivációja, az össztettebb funkciók és szolgáltatások támogatása mellett a gyártási költségek csökkentése volt. Ez az átállás bár meghozta a várt eredményeket, egy nem kívánatos probléma megjelenését is okozta: a járművek megörökölték a számítógépek gyengeségeit is.

A kiber-fizikai rendszerek (amelyek közé a járművek is sorolhatóak) új veszélyek megjelenését vonták magunk után. Amennyiben egy támadás során egy számítógéppel vezérelt folyamat felett át tudja venni a támadó az irányítás, akkor azzal a valós életben okozhat már kárt. A közlekedés területén egy ilyen támadás könnyen emberéleteket veszélyeztethet, vagy jelentős anyagi kárt okozhat.

Szerencsére, egyenlőre nincs tudomásunk arról, hogy ilyen támadás történt volna, azonban a probléma súlyosságát jól mutatja, hogy a szakértők által talált sérülékenységek javítása miatt több alkalommal is járművek millióit kellett már gyártóknak visszahívniuk, ezzel jelentős költségeket vállalva. A problémát továbbá jól illusztrálja az is, hogy az Európai Unióban és világ más területein is több új szabályozás jelent meg az elmúlt években, amelyek célja, hogy az újonnan tervezett gépjárművekben a kiberbiztonságra is kiemelt kérdésként kelljen figyelni. Az ENSZ 155-ös számú előírása alapján 2024-től csak azok az új járműtípusok kaphatnak típusengedélyt, amelyek a kiberbiztonsági előírásoknak is megfelelnek.

A felmerülő kiberbiztonsági problémák megoldásán a kutatók is évek óta dolgoznak. A disszertációmban a kihívások egy részére adok megoldást. A kiberbiztonság javításáért a teljes problémakört több szempontból is vizsgálom. Végeztem kutatást, amely célja a támadások megállítása, illetve felderítése, valamint dolgoztam azon is, hogy a védelmi megoldásokat alaposabban lehessen tesztelni. A rendszerek támadásokkal kapcsolatos vizsgálatán túl a személyes adatok védelmében felmerülő kérdéseket is körüljártam.

A kibertámadások sajátossága, hogy egy támadás végrehajtása, és annak az észlelése, vagy az az által okozott kár megjelenése között jelentős idő is eltelhet. Ezt a szempontot figyelembe véve, az első terület, ahol új eredményt értem el, a járművek belső hálózatának adatrögzítéséhez kapcsolódik. Javasoltam egy új tömörítési eljárást, amely elősegíti az adatok hosszútávú hatékony tárolását, ezzel lehetővé téve egy esetleges támadás után hosszú idő elteltével is az elemzését. Megmutattam, hogy a javasolt eljárásom jelentősen jobb eredményt ér el, mint a széles körben elterjedt alternatív tömörítési eljárások. A módszer alkalmazása számos előnnyel jár az adatok helyben tárolása, vagy távoli szerverre végrehajtott feltöltése szempontjából is.

A támadások felismerése területén is új eredményeket értem el. Először a korábban ismertetett tömörítési eljárásról mutattam be, hogy üzenetbeszúrásos támadások detektálására alkalmas. Ez az eredmény tovább növeli a tömörítési eljárás értékét, mivel így a támadások egy részét már a tömörített adatokon is lehet vizsgálni, ezzel jelentős erőforrásokat spórolva. A következő javasolt detekciós módszerem az átvitt jelek közötti korrelációt használja ki, és bizonyítja, hogy a legfontosabb jelek elleni támadások a

korrelációkra épített modellek segítségével hatékonyan detektálhatóak. Végezetül, egy harmadik detekciós eljárást is javasltam, amely a CAN jelekre egyesével alkalmazható. A módszer gépi tanulás segítségével minden jelre képes előrejelezni, hogy várhatóan milyen értéket kell érzékelnünk, így ha egy támadás hatására egy jel nem várt módon változna, az ezzel a technikával detektálhatóvá válik.

A disszertációmban vizsgált utolsó terület a jármű adatok érzékenységét vizsgálja a személyes adatok biztonsága szempontjából. Megmutattam, hogy a hálózaton átküldött adatok segítségével a járművek mozgása rövid, illetve hosszabb távon is rekonstruálható. Ez az eredmény alátámasztja azt a feltételezést, hogy a rögzített adatok csak megfelelő körültekintéssel használhatók fel jogi és etikai problémák nélkül.

Ez a dokumentum a disszertációmban bemutatott eredmények összefoglalója.

2. Új eredmények

2.1. CAN forgalom szemantikus tömörítése

A CAN-busz hálózati forgalmának a visszamenőleges elemzése csak akkor lehetséges, ha az adatok tárolása hatékonyan megoldott. Két lehetséges megközelítés létezik a problémára: (1) a napló fájlok helyi tárolása vagy (2) a rögzített forgalom távoli szerverre továbbítása. Bármelyik lehetőséget is választja egy gyártó, a hálózati forgalom tömörítése jelentősen javítja a folyamat hatékonyságát. Ebben a disszertációban egy olyan tömörítési módszert javaslok, amely lehetővé teszi az adatok veszteségmentes, mégis hatékony tárolását. Ezt úgy érem el, hogy egyszerű szintaktikai tömörítés helyett szemantikus tömörítést végzek a CAN forgalmon. Az általam elért tömörítési arány jobb, mint a legkorszerűbb szintaktikai tömörítési módszerekkel, például a zip tömörítési algoritmussal, elérhető arány.

1.1 TÉZIS: Javasoltam egy szemantikus tömörítési módszert a CAN-forgalom tömörítésére [C2]-ben, és kimértem, hogy ez önmagában az eredeti méret 10%-ára tömöríti az adatokat. Továbbá megmutattam [J1]-ben, hogy a szemantikus és a szintaktikai tömörítés kombinálásával a szükséges tárhely az eredeti méret 5%-ára csökkenthető. Ez a megközelítés tehát lényegesen hatékonyabb eredményt nyújt, mint a szintaktikai tömörítés önmagában, amely csak az eredeti méret 30%-ára csökkenti a méretet.

Olyan tömörítési algoritmust javaslok, amely a CAN-forgalom nagyrészt periodikus jellegére épít. Algoritmusom magas szintű megközelítése az, hogy a forgalmat először szétválasztom üzenetfolyamokra, amelyek az azonos azonosítóval rendelkező üzeneteket tartalmazzák, majd az egyes üzenetfolyamokat külön-külön tömörítem, kihasználva a kommunikációban előforduló adatok gyakori ismétlődését. Az 1. példakódban található a tömörítési algoritmus pszeudokódja.

Két formátumot támogat kimenetként az algoritmusom. Az eredményt eltárolható szöveges fájlként (ASCII), valamint bináris formátumban is. Mindkét formátum ugyanazt a veszteségmentes információt tartalmazza.

Az algoritmusom jelentősen felülmúlja a legkorszerűbb szintaktikai tömörítési módszereket (lásd 1. és 2. táblázat). A szöveges formátumot használva 20%-nál kisebb végső fájlméretet tudtam elérni. A bináris reprezentáció még hatékonyabb tömörítést mutat, ezzel az eredeti fájl méretének 10%-a körül van az eredmény.

Javasoltam egy hibrid megközelítést is, amely során a szemantikus tömörítés mellett további szintaktikai tömörítést is alkalmaztam. Ez a módszer eredményezte a legkisebb fájlméretet: szöveges kimenet esetén a kombinált eredmény megközelítőleg 6%-os fájlméretet adott, míg a bináris esetben megközelítőleg 5%-os fájlméretet.

Algoritmus 1: Szemantikus tömörítés

Input: raw CAN log
Output: compressed CAN log

```
messages ← read CAN traffic log;
flows ← separate Messages into message groups;
for flow in flows do
    calculate_average_inter_arrival_time(flow);
    group_messages_with_identical_data(flow);
    for message in flow.messages do
        compress_timestamp(message);
for flow in flows do
    write_compressed_flow_to_output(flow);
```

1. táblázat. Szemantikus tömörítési arányok összehasonlítása

Teszteset	Eredeti fájl méret (byte)	Szöveges formátum fájl méret (byte)	Szöveges formátum fájl méret (százalék)	Bináris formátum fájl méret (byte)	Bináris formátum fájl méret (százalék)
1	10 095 971	1 710 920	16,94%	1 090 757	10,80%
2	7 040 165	1 334 902	18,96%	835 539	11,86%
3	19 143 383	3 747 229	19,57%	2 307 146	12,05%
4	21 936 245	4 233 994	19,30%	2 601 354	11,85%

2. táblázat. Szintetikus és szemantikus tömörítési arányok összehasonlítása

Teszteset	Eredeti fájl zip tömörítés fájl méret (byte)	Kombinált szintetikus és szemantikus tömörítés Szöveges formátum fájl méret (byte)	Szöveges formátum fájl méret (százalék)	Bináris formátum fájl méret (byte)	Bináris formátum fájl méret (százalék)
1	1 291 315	546 725	5,41%	499 998	4,95%
2	937 319	429 234	6,09%	390 467	5,54%
3	2 569 118	1 194 758	6,24%	1 092 183	5,70%
4	2 895 039	1 332 585	6,07%	1 223 677	5,57%

2.2. Támadás detekció tömörített CAN forgalmon

A járművekkel kapcsolatos igazságügyi vizsgálatok támogatásához a CAN-forgalmat folyamatosan rögzíteni és hatékonyan tárolni kell a későbbi elemzésekhez. Az én hozzájárulásom ennek az folyamatnak a támogatásához egy új anomáliadetekciós módszer az üzenetbeszúrásos támadások azonosítására, amely tömörített CAN forgalmon működik. A tömörített naplófájlokon végzett anomáliadetekció előnye, hogy kisebb mennyiségű adatot kell csak elemezni, így növelhető a vizsgálatok hatékonysága.

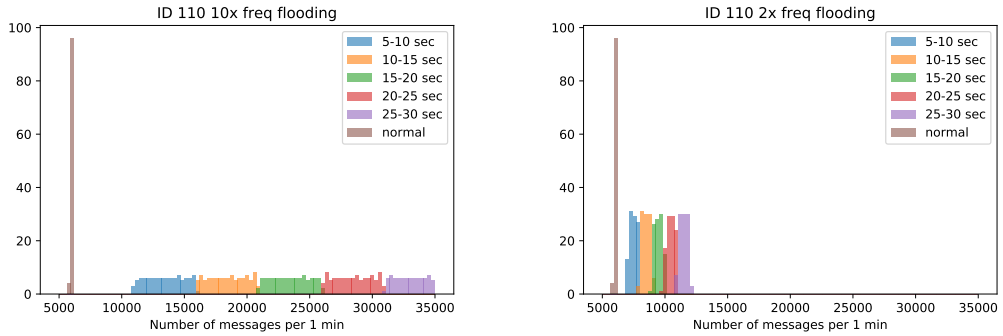
1.2 TÉZIS: Az igazságügyi vizsgálatok támogatása érdekében két adathalmazon végzett méréssel kimutattam, hogy a tömörített formátum alkalmas az üzenetbeszúrásos támadások nagy megbízhatóságú azonosítására [C4][1]. A korábbi eredmények azt mutatják, hogy egy sikeres üzenetbeszúrásos támadás végrehajtásához a támadás során a normál üzenetfrekvencia legalább ötszörösére van szükség. A javasolt algoritmus ezzel szemben már a normál frekvencia kétszeresétől képes észlelni az anomáliát.

Az anomáliadetekciós algoritmusom az azonos CAN-azonosítóval rendelkező üzenetek átlagos gyakoriságának elemzésén alapul. A tömörítési algoritmus, amelyet a 2.1 szakaszban mutattam be, a tömörített CAN-fájlokban könnyen elemezhető formában megőrzi az egy időegységre jutó üzenetek számát, ami lehetővé teszi az általam használt anomáliadetekciós algoritmus használatát a tömörített fájlokon. Megmutattam, hogy ez a megközelítés megbízhatóan működik számos esetben, beleértve a valós járművekben rögzített és szintetikusan generált támadásokkal módosított adathalmazokat, valamint a valós járművekben rögzített, valós támadások alatt rögzített adathalmazokaz is.

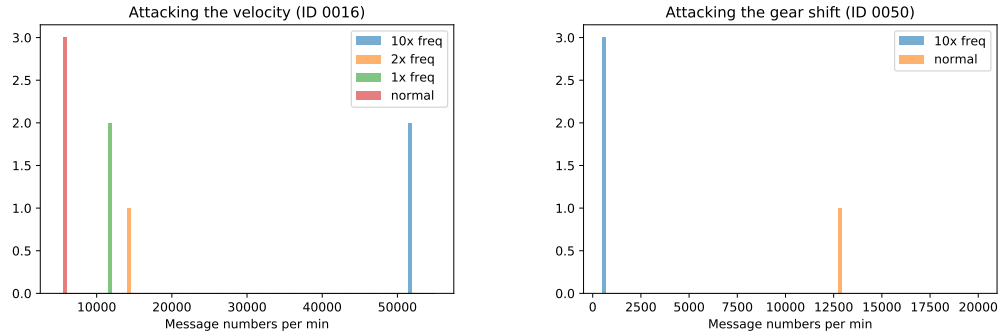
A szintetikus adatokon 100-100 normál és megtámadott mintát használtam különböző gyakoriságú támadásokhoz. A támadások eloszlásának hisztogramja az 1. ábrán látható. Ez azt mutatja, hogy a megtámadott forgalom még akkor is hatékonyan megkülönböztethető a normál forgalomtól, ha a támadott üzenetek gyakorisága csak kétszerese az eredetinek.

A valós támadások adatain ugyanezeket a számításokat végeztem el. A 2. ábra azt mutatja, hogy az algoritmusom a valós esetekben is ugyanolyan megbízható eredményeket ér el.

[1] Neubrandt Dóra implementálta a mérési algoritmust.



1. ábra. Az üzenetek számának az összehasonlítása 100-100 szintetikusan támadott és tiszta minta esetén.



2. ábra. Az üzenetek számának az összehasonlítása valós támadás és tiszta forgalom esetén.

2.3. Korreláció alapú anomáliadetekció

Bár a CAN-busz elleni támadások többsége az üzenetbeszúráson alapul[4, 7], nem ez az egyetlen technika a rosszindulatú célok elérésére. Az üzenetek gyakoriságának megjósolhatósága önmagában nem elegendő az olyan támadások felderítéséhez, amelyek nem szúrnak be új üzeneteket a CAN-buszra, vagyis amelyek csak üzenetmódosító támadások.

Ebben a szakaszban egy olyan anomáliadetekciós algoritmust javaslok, amely a CAN-üzenetekbe kódolt jelek közötti korrelációra épít. Normál körülmények között a különböző jelpárok közötti korreláció egy (jelpár-specifikus) intervallumon belül marad. Támadás esetén, amikor a támadó a korreláló jelpárnak csak az egyik tagját módosítja, az így kapott korreláció már nem marad az intervallumon belül, és ez anomáliaként felismerhető.

2.1 TÉZIS: [C6][2]-ban megmutattam, hogy a CAN-jelek közötti korrelációs mérésekre épülő modell képes az üzenetmódosító támadások azonosítására. A javasolt módszer pontosságát hét különböző támadási stratégiával szemben teszteltem. Az eredmények azt mutatják, hogy a más jelekkel erősen korreláló jeleket célzó támadások esetén a felismerés pontossága ∼90%, a kettős küszöbértékrendszer alkalmazása miatt 0%-os hamis pozitív arány mellett. Érdemes továbbá kiemelnem, hogy a jel legalább 8 bitjét módosító RANDOM, ADD-INCR és ADD-DECR támadások esetében 95%-os pontosságot tudtam elérni. Hasonlóképpen, ha a támadás egy jel legalább 12 bitjét módosítja, akkor a felismerési pontosság szintén 95%.

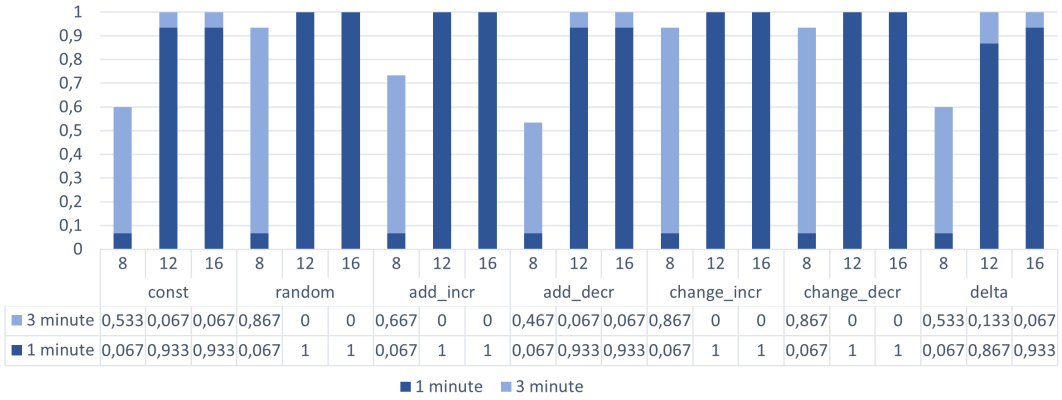
A tanítási szakaszban meghatároztam a jelek közötti korrelációs értékeket. Ennek részeként, többször megmértem a Pearson páronkénti korrelációt minden jelpár között egy egyperces és egy háromperces időablakban. Ezután e mérések alapján egy küszöbérték alkalmazásával eldöntöttem, hogy az értékek valós korrelációból adódnak-e. A tanítás következő részeként, a mért korrelációs értékek eloszlására különböző folytonos valószínűségi eloszlásfüggvényeket illesztettem. Amikor megfelelő illeszkedést találtam, hozzáadtam a jelpárt a modellemhez. Minden jelpárhoz tartozó eloszlásra négy küszöbértéket is kiszámítottam a normális viselkedés határainak meghatározására: (1) az első két küszöbérték egy szigorúbb intervallumot határoz meg a normális állapotra: az ezen intervallumon belüli méréseket normálisnak, az ezeken kívüli méréseket a további elemzés szempontjából potenciális anomáliáknak tekintem; (2) további két küszöbérték egy szélesebb intervallumot határoz meg: az ezen intervallumon kívüli méréseket azonnal anomáliáknak tekintem.

A detekciós fázisban a korrelációs értékek meghatározása szintén egy egyperces és egy háromperces ablakban történik. Ezután a mért értékeket összehasonlítom a korábban meghatározott küszöbértékkel az anomália észleléséhez.

Az algoritmus teljesítményének részletesebb értékelése érdekében a CAN-jeleket három különböző csoportra osztottam, és az algoritmust hatékonyságát minden csoportban külön-külön vizsgáltam. Az első csoport olyan jeleket tartalmaz, amelyek erősen korrelálnak több más jellel. Jellemzően egy jármű legfontosabb jelei tartoznak ebbe a csoportba. A második csoport olyan jeleket tartalmaz, amelyek erős korrelációt mutatnak egy másik jellel, a harmadik csoport pedig olyan jeleket tartalmaz, amelyek csak gyenge korrelációs értékekkel rendelkeznek.

A 3. ábra részletes eredményeket mutat egy erős korrelációkkal rendelkező jelre. A 16 bites jeleket több féle támadástípussal is támadtam. Minden támadástípus esetében három konkrét támadást hajtottam végre, ahol az érintett bitek száma 8-ról 16-ra nőtt. Az oszlopok két színe azt jelzi, hogy melyik időablakban volt sikeres a támadás észlelése. A felismerési arány 55% és 100% között változik, de a több mint 12 bitet módosító támadások esetében 90% feletti eredményt értem el minden esetben.

[2]Lupták György implementálta a korrelációszámítást és a statisztikai tesztelést.



3. ábra. Teszt eredmények egy erős korrelációval rendelkező 16 bit hosszú jel esetén.

A többi csoportban a elvárhatónak megfelelően kevésbé pontosak az eredmények. Az egy erős korrelációval rendelkező jelek támadásainak átlagos észlelési pontossága 58%, míg a harmadik csoport esetében, ahol a jelek csak gyenge vagy semmilyen korrelációval nem rendelkeznek, ez az érték ∼20%-ra csökken.

2.4. TCN alapú anomália detekció CAN jeleken

Az üzenetmódosító támadások általános azonosítása nehéz feladat. A CAN-forgalom bármilyen, csak az üzenetadatokon alapuló modelljének megalkotása különösen nagy kihívást jelent, mivel nem tudjuk, hogyan kell értelmezni az adatokat, ezért a modellalkotáshoz nem tudunk semmilyen szemantikai információt használni. Amint azt a 2.3. szakaszban bemutattam, az üzenetek közötti adatkorrelációk kihasználása hatékony észlelési mechanizmus a korreláló jelekre. Azonban nem minden jel korrelál erősen másokkal, így ez korlátozza a megoldás erejét. Ebben a szakaszban egy új, jelenkénti alapon működő detektálási módszert javaslok, amely kiegészíti a korábbi megoldásaimat.

2.2 TÉZIS: Javasoltam egy TCN-alapú detekciós modellt, amely képes a CAN-üzenet módosítását célzó támadásokat felismerni a CAN-jelek jövőbeli értékeinek előrejelzésével, majd az előrejelzés és a tényleges értékek összehasonlításával [C7][3]. Két adathalmazon végzett mérések alapján kimutattam, hogy a TCN-alapú detektálási módszerem 83% és 99% közötti pontossággal észleli a támadásokat, miközben a hamis pozitív arány 0,2% alatt marad. A javasolt módszert összehasonlítottam a korábban legjobban teljesítő megoldással, és megmutattam, hogy a detektáló algoritmusom 30 esetből 27 esetben jobban teljesít.

[3]Irina Chiscop implementálta a TCN hálózati architektúrát.

3. táblázat. A modell pontossága a SynCAN adathalmazon.

Model	Data	Normal	Cont.	Playb.	Flood.	Suppress	Plateau
TCN	ID 2	**0.9977**	**0.8660**	**0.8674**	**0.7678**	**0.8402**	**0.8336**
INDRA		0.9811	0.8584	0.8660	0.7600	0.8347	0.8133
TCN	ID 3	**0.9992**	**0.8664**	**0.8680**	**0.6422**	**0.8390**	**0.8394**
INDRA		0.9965	0.8653	0.8672	0.6420	0.8377	0.8386
TCN	ID 10	**0.9977**	**0.8637**	0.8577	0.7399	**0.8446**	**0.8282**
INDRA		0.9858	0.8546	**0.8638**	**0.7923**	0.8370	0.8100

4. táblázat. A modell pontossága a CrySyS adathalmazon.

Model	Data	Acc.	FPR	Precision
TCN	ID 280	**0.8833**	0.0426	**0.7766**
INDRA		0.7989	**0.0000**	0.0000
TCN	ID 290	**0.9159**	0.0687	0.7701
INDRA		0.8617	**0.0378**	**0.7755**

Egy TCN-alapú megoldást javaslok a módosított CAN-busz üzenetek felismerésére. A TCN-t felügyelet nélküli módon tanítom be, mivel a támadásokat általánosan jól leíró CAN-busz üzeneteket előállítani nehéz a gyakorlatban. A tanítási folyamat során a TCN megtanulja pontosan rekonstruálni a tiszta CAN-busz üzenetek egyes jeleit a konvolúciós rétegei segítségével, ami lehetővé teszi a korábbi adatmintákból származó információk megőrzését. Az adatminták osztályozása végül a helyreállítási folyamat során mért rekonstrukciós hiba meghatározásával folytatódik: a hiba mértékéhez egy megfelelő küszöbértéket határozok meg. A támadásdetekció alapja az, hogy olyan jeleket, amelyek adatait megváltoztatta egy támadó, a modell rosszul rekonstruál, és így a támadás felismerhetővé válik. Kiemelném, hogy a módszer megvalósításához nem feltétel a CAN-busz jelek szemantikájának ismerete, amely a gyakorlatban általában nem áll rendelkezésre, mivel azt a gyártók bizalmasan kezelik [6].

Az általam javasolt modell pontosságának a meghatározásához összehasonlítottam a teljesítményét a szakirodalomban korábban legjobbnak bizonyult eredménnyel. Legjobb tudomásom szerint a legfrissebb és legmegfelelőbb jelölt az INDRA keretrendszer [5]. Ez a megoldás egy rekurrens autoencoder hálózatot javasol, amely képes felismerni az olyan CAN-üzeneteket, amelyekben a jeleket manipulálták. Minden egyes üzenetazonosítóhoz egy ilyen rekurrens autoencodert tanítanak be, amely megtanulja rekonstruálni az adott üzenetazonosítóhoz tartozó jeleket. Ez a módszer a SynCAN-adathalmazon a legtöbb támadás esetén a pontosság és a hamis pozitív arány tekintetében felülmúlja a többi, nemrégiben javasolt felügyelet nélküli tanítást alkalmazó megoldást, például a Predictor LSTM [8], a Replicator Neural Network [9] és a CANet [3] módszereket.

Először a SynCAN-adathalmazon értékeltem ki a saját új módszerem és az INDRA-modell teljesítményét. A normál eseteknél és az egyes támadásoknál mért pontossági értékek a 3. táblázatban láthatók. Az eredmények alapján az első megfigyelésem az,

hogy a TCN a legtöbb esetben nagyobb pontosságot ér el, mint az INDRA, kivéve a visszajátszás és a 10-es azonosítójú elárasztásos támadások esetében. Ezenfelül a hamis pozitív arányok mindkét modell esetében meglehetősen alacsonyak. Összességében a pontossági értékek nagy eltéréseket mutatnak a különböző üzenetazonosítók között, ami összefügghet a támadások végrehajtásának módjával (a céljelek kiválasztása, a támadás időtartama stb.) és a különböző jelkorrelációkkal. A viszonylag alacsony pontossági értékek azt is mutatják, hogy a modellek a SynCAN-adatok időbeli jellemzőinek csak korlátozott részét képesek megragadni. Ez közvetlen következménye a tanítás során alkalmazott leállási mechanizmusnak, valamint a TCN esetében a kis méretű architektúra megtartása érdekében hozott döntéseknek.

A SynCAN-adathalmaz üzenetazonosítói olyan jeleket tartalmaznak, amelyek bár fizikailag kapcsolatban lévő folyamatokat írnak le, de mégis csak nagyon gyengén korrelálnak, ami szintén növeli a detektálási feladat bonyolultságát. Annak érdekében, hogy a két modell teljesítményét más környezetben is meg tudjam határozni, a modelleket egy új, CrySyS-adathalmazra is kiértékeltem. Ez az adathalmaz több erős korrelációval rendelkező jelet is tartalmaz. Ebben a mérésben a SynCAN-hez hasonlóan egyszerre csak egy támadott jel van. Az eredmények a 4. táblázatban láthatók. Kiemelem, hogy ebben a mérésben is igaz, hogy mindkét modell magas pontosságot (accuracy) és alacsony hamis pozitív arányt ér el. A TCN alapú megoldás azonban mindkét támadás esetén magasabb preciziót (precision) mutat, szemben az INDRA-val, amely például nem detektálta a támadást a 280 üzenetben.

Összefoglalva, az egyszerű TCN architektúra mindkét adathalmazon jobb pontosságot (accuracy) ér el az INDRA modellhez képest. A TCN figyelemre méltó eredménye, hogy szinte minden esetben jelentősen (tizedére) csökkenti a hamis pozitív eredmények számát: ez a gyakorlatban megbízhatóbb detektort jelent. A TCN további előnyei közé tartozik, hogy gyorsan betanítható, sokkal kisebb az erőforrásigénye, és általában alacsonyabb tanítási és validálási veszteséget ér el.

2.5. Érzékeny adatok veszélyben: járművek nyomkövetése

A járművekben folyamatosan keletkeznek adatok. Az egyre több beágyazott vezérlővel rendelkező autókban a vezetés közben mért jelértékek egyre részletesebb információkat szolgáltatnak a járműről és annak vezetőjéről. Az előző részekben amellett érveltem, hogy ezen adatok tárolása és feldolgozása a jövőben fontos feladat lesz a támadások azonosítása szempontjából, ugyanakkor azt is felismerhetjük, hogy ugyanezek az adatok más szempontból is értékesek lehetnek: felhasználhatóak adatvezérelt szolgáltatásokban. Ezen új szolgáltatások némelyike pedig aggályokat vethet fel a személyes adatok védelmével kapcsolatban[1]. A gyártó a járművekből begyűjtött adatokat felhasználhatja arra, hogy folyamatosan testreszabott szolgáltatásokat ajánljon a tulajdonosnak, vagy ezen túlmenően akár számos más vállalat felhasználhatná a járművezető viselkedési és helymeghatározási adatait egyéb szolgáltatások nyújtására. Az adatok ilyen jellegű felhasználása csak akkor elfogadható, ha eközben betartják a vonatkozó jogszabályokat.

Ebben a szakaszban bemutatom, hogy a CAN-adatok felhasználásával a járművek és így a járművezetők is nyomon követhetővé válnak. Egy jármű nyomon követése két lépés-

ben valósítható meg. Disszertációmban először bemutatom, hogyan lehet egy járművet külső segítség nélkül kizárólag a CAN-üzenetek alapján rövid távolságokra pontosan nyomon követni. Ezt a koncepciót mikrokövetésnek nevezem. Ez után bemutatom, hogyan lehet a nyomon követést hosszabb utakra kiterjeszteni további, nyilvánosan elérhető információk felhasználásával. Ezt a második problémát pedig makrokövetésnek nevezem.

3.1 TÉZIS: [J2]-ben javasoltam egy olyan (makrokövetési) algoritmust, amely képes megbízhatóan rekonstruálni egy jármű útvonalát nyers CAN-adatok és nyilvánosan elérhető térkép információk alapján. A módszer pontosságát mérésekkel igazoltam: az algoritmus képes volt rekonstruálni több hosszú, legalább 20 kereszteződésből álló tesztesetet, mindössze néhány méteres pontatlansággal.

A probléma hatékony megoldásához néhány segédinformációt használok, hogy csökkentsem a mikrokövetésnél előforduló hibák összeadódásának a problémáját. A helyreállításhoz a CAN-üzenetekből kinyert sebesség- és kormányszögértékekre van szükség, valamint a kiindulási pozíció és a kezdeti irány is előfeltétele az algoritmusomnak. Ezekből az adatokból kiindulva megmutatom, hogy a jármű útvonala hatékonyan helyreállítható, ezzel azonosítva az úticélt, ami a vezető magánéletének a megsértése. Ennek tehát az a következménye, hogy a rögzített CAN forgalmakat csak megfelelő körültekintéssel sza-

Algoritmus 2: Macrotracking CAN adatokra

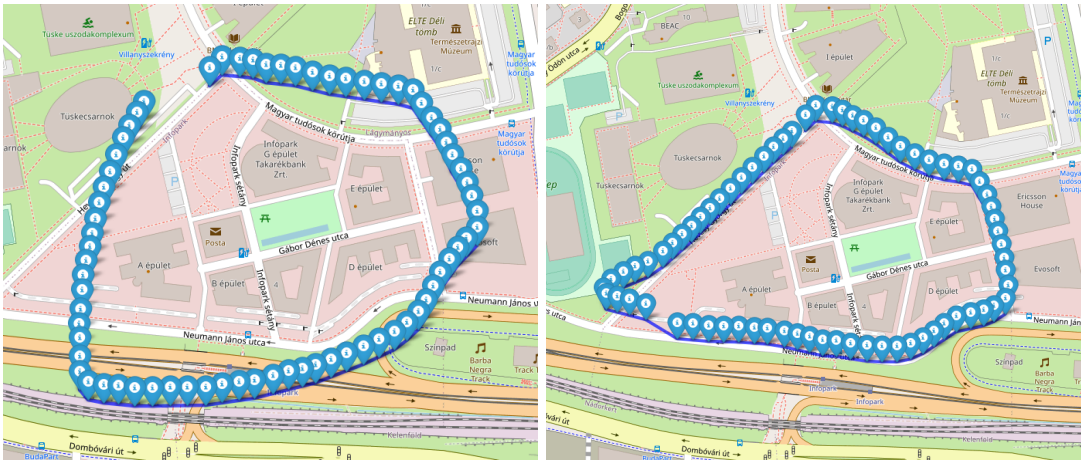
```
   Input: starting position and heading value, CAN log
   Output: Reconstructed trajectory 𝕋
 1 initialize current state to starting position and heading;
 2 load data from CAN log;
 3 filter relevant messages;
 4 while there is message to process do
 5     Model-based prediction:
 6         extract speed and steering wheel position from messages;
 7         compute heading from axle distance and steering wheel position;
 8         calculate next state from current state using heading and speed;
 9     Map-based correction:
10         if distance from last correction > minimum required then
11             find nearest road segment on map;
12             project current position and heading to selected road segment;
13             update map weight w based on distance from closest intersection;
14             update next state using the projected state with map weight w;
15     append next state to reconstructed trajectory 𝕋;
16     update current state to next state;
```

bad kezelni, hogy elkerülhető legyen az érzékeny adatok megsértése, valamint, az ebből következő adatvédelmi szabálysértés.

A jármű mozgásának rekonstruálására végző pszeudokódot a 2. algoritmus mutatja be. Ennek működése, hogy először a következő állapotot mindig az előző állapot alapján megjósolom azzal a modellalapú előrejelzéssel, amit a mikrotracking probléma megoldására javasoltam (5-8. sor), majd ennek az eredményét a térképinformációk alapján korrigálom (9-14. sor). Ezt a korrekciót csak akkor végzem el, ha az utolsó korrekciótól való távolság kellően nagy már, hogy megtartsam az algoritmus gyors futását (10. sor).

Az algoritmusom pontossága a modellalapú előrejelzés helyességétől és az úthálózat sűrűségétől függ. Limitáció, hogy a sok kereszteződéssel rendelkező területek nem teszik lehetővé, hogy a térképalapú korrekciók jelentősen javítsák a modell előrejelzését, mivel ekkor bizonytalannak tekinthető a térképről származó plusz információ. Ugyanakkor viszont a hosszú, kereszteződés nélküli szakaszokon pontos a térkép alapú korrekció, így ilyen esetekben a helyreállítás pontosságára csak minimális hatása van a modell pontatlanságának.

A 5. táblázat a tesztmérések eredményeit mutatja be. Ezekben a tesztekben különböző körpályákon vezettem, hogy bemutassam az algoritmusom pontosságát. Több különöböző mérést is végeztem, például a C3-as teszteset során szándékosan, a kormánykerék gyakori mozgatásával vezettem még az egyenes útszakaszokon is, hogy a rekonstrukciót megnehezítsem. A táblázat megfelelő sora mutatja, hogy algoritmusom még ebben az esetben is minimális hibával helyre tudta állítani az útvonalat. Az 4. ábrán látható a rekonstruált útvonal.



(a) C3 helyreállítás térkép nélkül (b) C3 helyreállítás térkép használatával

4. ábra. C3 teszteset

5. táblázat. Macrotracking tesztesetek összefoglalása

Test case		Average trajectory reconstruction error (meter)	Std. deviation of error (meter)	Endpoint reconstruction error (meter)	Total distance travelled (meter)	Number of decision points on map
C1	without map	30.2	25.13	9.3	2025.17	20
	with map	9.37	8.99	4.2	2039.11	20
C2	without map	39.37	34.02	35.58	2139.03	18
	with map	9.13	8.74	41.12	2158.48	18
C3	without map	55.04	36.07	82.17	1751.07	19
	with map	7.45	6.05	6.05	1817.81	19

2.6. Védekezési lehetőségek

Ezután a simítás és az aluláteresztő szűrő alkalmazását vizsgáltam meg, arra keresve a választ, hogy ezek az elterjedt jelfeldolgozási technikákat megfelelő védelmet nyújtanake az útvonalak egyedi jellemzőinek felismerésével szemben, a torzítás alkalmazásával. A mérések azonban azt mutatták, hogy ezek a technikák sem képesek erős adatvédelmi garanciákat nyújtani, csak abban az esetben, ha olyan mértékű torzítást alkalmaznak már, amely gyakorlatilag használhatatlanná teszi az anonimizált adatokat.

3.2 TÉZIS: Megmutattam, hogy a javasolt makrokövetési algoritmus robusztus a tipikus jeltorzítási technikákkal szemben, amelyek a magánélet védelmét szolgálnák [J2]. A módszer robusztusságát több méréssel igazoltam: még egy 20%-os torzítást megvalósító aluláteresztő szűrő alkalmazása után is 8 méter alatt maradt a pontatlanság. A simítás esetében az algoritmus még robusztusabb: egy 6,4 másodperces simítási ablak alkalmazása után is pontosan visszaállított útvonalat kaptam.

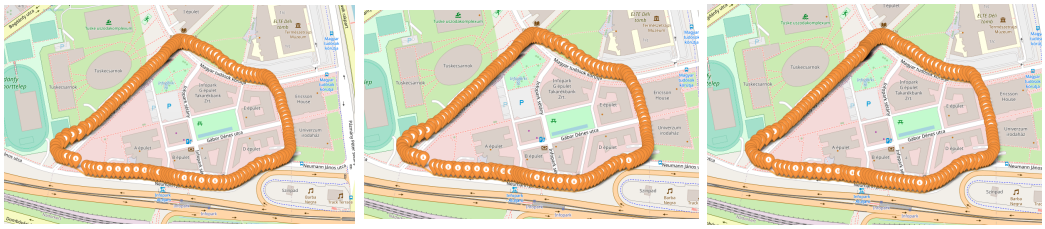
Simítás

A simítás egy mintavételezési technika. A rövid időtartamú kilengések eltávolítására alkalmazható, ami az eltávoltítással egyidőben a jel (vagy idősor) hosszútávú tendenciáit is kiemeli. Számos változata van, azonban mindegyik megvalósítás fő ötlete az, hogy egy fix méretű mozgóablakban vizsgáljuk a jelet, és minden egyes időpillanatban az ablak által kijelölt értékekre egy transzformációt alkalmazva állítjuk elő a jel új értékeit. A mérésem során egy időalapú mozgóablakot alkalmaztam, azaz az adatpontok egy rögzített időablakban vett átlagát számoltam ki (ez az úgynevezett *simító ablak*), amelynek időbeli mérete (w) paramétere a módszernek. Az átlag kiszámolása után, az ablakban vett összes értéket lecseréltem az átlag értékére. Az átlag számítását a teljes ablakra végeztem, ezért az egymás követő ablakok nem fedtek át egymással.

A módszer alkalmazásának az elvárt eredmény, hogy az egyes jelek w másodpercen belüli helyi eltéréseit elrejti, ezzel az útvonal egyedi jellemzőinek a számát csökkenti.

(a) Simítási ablak: 0.2s (b) Simítási ablak: 1.6s (c) Simítási ablak: 6.4s

5. ábra. C3 teszteset helyreállítása simított adatok alapján térkép nélkül



(a) Simítási ablak: 0.2s (b) Simítási ablak: 1.6s (c) Simítási ablak: 6.4s

6. ábra. C3 teszteset helyreállítása simított adatok alapján térkép használatával

Az 5. ábra a simítás hatását mutatja meg a C3 esetre a tisztán modellalapú helyreállítás (azaz mikrokövetés) esetén, vagyis ekkor nem alkalmaztam térképkorrekciót. Bár a simítás alkalmazása negatív hatással van a rekonstrukció pontosságára, a javasolt algoritmusom még a legnagyobb ablakméret esetén is képes az útvonal viszonylag pontos helyreállítására. Érdekesség, hogy a kormánykerék elforgatásának az üzenetekben alkalmazott kódolása miatt a simítás végrehajtása erre a jelre fordított hatást fejt ki: élesebb kanyarokat eredményez, mint ami az eredeti esetben megfigyelhető volt.

A makrokövetési algoritmusom (térképkorrekció alkalmazásával) simítás után is lényegesen pontosabb eredményt ad, mint a csak modellalapú rekonstrukció, és ekkor is sikeresen rekonstruálja az eredeti útvonalat. Bár a C3-as teszteset során gyakori kormánymozdulatokkal vezettem, ennek a szándékos zavarásnak a hatását valójában csökkenti a simítás, így a rekonstrukciós eredmények nagyobb ablakméret esetén még ténylegesen javulnak is az eredeti mérésekhez képest (6. ábra). A 6. táblázat tartalmazza a simítás elvégzése után a helyreállítás hatékonyságát alátámasztó mérési eredményeket. A táblázatban látható az útvonalak mentén mért átlagos hiba mértéke, valamint a végpont-helyreállítás hibája is, az összes tesztesetre három különböző ablakmérettel.

6. táblázat. Simítás hatása a macrotracking algoritmusra.

Test case	Smoothing windows size (second)	Average trajectory reconstruction error (meter)	Std. deviation of error (meter)	Endpoint reconstruction error (meter)
C1	0.201	32.2	26.4	22.76
	1.608	33.51	26.97	33.02
	6.4	38.58	27.97	132.94
C2	0.201	37.75	28.68	75.74
	1.608	38.92	32.83	76.72
	6.4	42.22	32.47	126.84
C3	0.201	50.78	32.74	64.71
	1.608	47.53	29.6	66.52
	6.4	20.47	18.15	70.09

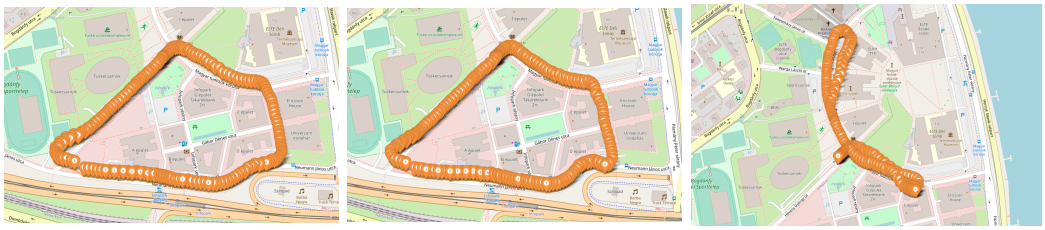
Aluláteresztő szűrő alkalmazása

Egy aluláteresztő szűrő alkalmazása nem csak jelek tömörítésére használható, hanem zajcsökkentésre is. Ezzel a módszerrel többféle hibát is el lehet távolítani adatokból, mint például az aliasing vagy rezonancia okozta hatásokat, anélkül, hogy módszer az eredeti jel hasznosságát jelentősen rontaná. Ezen felül, az egyre erősödő adatvédelemi igény hatására sikeresen alkalmaztak már aluláteresztő szűrést jelek anonimizálására is [2]. Az aluláteresztő szűrők működésük során egy meghatározott frekvencia felett minden jelkomponenst csillapítanak vagy megszüntetnek. Ezeknek a magas frekvenciájú komponenseknek a törlésével megszabadulhatunk a jel sajátosságaitól, ami után a jel általánosabb jellemzői maradnak csak meg. A simítással ellentétben, az aluláteresztő szűrés alkalmazása finomabb lehetőséget ad a hasznossági veszteség megadására.

(a) Filterezés: 10% (b) Filterezés: 20% (c) Filterezés: 40%

7. ábra. C3 teszteset helyreállítása aluláteresztő szűrő alkalmazása után térkép nélkül

Az aluláteresztő szűrést a következőképpen alkalmaztam. Először a jelet ortonormális diszkrét koszinusz transzformáció (DCT) segítségével frekvenciatartományba transzformáltam. A DCT-transzformáció után meghatároztam az eltávolítandó magas frekvenciájú komponensek számát. Általában minél több komponenst távolítunk el a jelből, annál kisebb marad az eredmény hasznossága. A transzformáció utáni jel hasznosságát az eredeti és a transformált jel közötti normalizált euklideszi távolság kiszámításával mértem.



(a) Filtering: 10% (b) Filtering: 20% (c) Filtering: 40%

8. ábra. C3 teszteset helyreállítása aluláteresztő szűrő alkalmazása után térkép használatával

7. táblázat. Aluláteresztő szűrő hatása a macrotracking algoritmusra.

Test case	Allowed reconstruction error	Average trajectory reconstruction error (meter)	Std. deviation of error (meter)	Endpoint reconstruction error (meter)
C1	10%	8.63	9.07	8.45
	20%	8.25	7.33	12.9
	40%	47.71	74.23	602.64
C2	10%	8.71	8.94	11.43
	20%	10.98	11.9	13.37
	40%	175.08	159.73	589.17
C3	10%	7.01	5.92	9.36
	20%	7.58	5.93	8.16
	40%	207.08	151.12	124.05

Így tehát, annyi magas frekvenciájú komponenst törlök, amennyi szükséges ahhoz, hogy az eredeti jelhez képest elérjek egy előre meghatározott hibatávolságot (más néven rekonstrukciós hibát). A kívánt hibaarány elérése után a szűrt jelet visszatranszformáltam az időtartományba.

A 7. ábra a C3 teszteset aluláteresztő szűrő alkalmazása utáni, térkép nélküli (azaz csak modellalapú módszer) útvonalhelyreállítás eredményét mutatja be. A simítással összehasonlítva az aluláteresztő szűrés a választott paraméterekkel az eredeti útvonalakat jelentősebben torzítja. A fordulási szögek ellenkező irányú változása itt is megfigyelhető.

A 8. ábra azt mutatja, hogy az általam javasolt makrokövetési algoritmus képes rekonstruálni az eredeti C3 pályát, ha az aluláteresztő szűrés előírt hibaaránya 40% alatt van. A rekonstrukció pontossága a különböző mértékű aluláteresztő szűrés alkalmazása után a 7. táblázban látható. A mérésekből látható, hogy 40%-os aluláteresztő szűrési hiba esetén megakadályozható a rekonstrukció, azonban ebben az esetben az adatok hasznossága már jelentősen csökken.

Köszönetnyilvánítás

Az itt bemutatott kutatás pénzügyi támogatást kapott a következő projektektől, programoktól valamint pénzügyi támogató szervezetektől:

- Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal [4,5,6,7,8,9];
- ECSEL[10];
- Közlekedéstudományi Intézet Innovatív Mobilitási program[11].

[4]The research presented here have been supported by the NRDI Office, Ministry of Innovation and Technology, Hungary, within the framework of the Artificial Intelligence National Laboratory Programme, and the NRDI Fund based on the charter of bolster issued by the NRDI Office.

[5]The research presented here have been supported by the NRDI Office, Ministry of Innovation and Technology, Hungary, within the framework of the Autonomous Systems National Laboratory Programme, and the NRDI Fund based on the charter of bolster issued by the NRDI Office.

[6]The work presented here was partially supported from the grant GINOP-2.1.1-15. The project has been supported by the European Union, co-financed by the European Social Fund. EFOP-3.6.2-16-2017-00002.

[7]Project no. 138903 has been implemented with the support provided by the Ministry of Innovation and Technology from the NRDI Fund, financed under the FK_21 funding scheme.

[8]Project no. 2019-1.3.1-KK-2019-00004 has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2019-1.3.1-KK funding scheme.

[9]Project no. 2018-1.2.1-NKP-2018-00004 has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme.

[10]This work has been funded by the European Commission via the H2020-ECSEL-2017 project SECREDAS (Grant Agreement no. 783119).

[11]The presented work was carried out within the MASPOV Project (KTI KVIG 4-1 2021), which has been implemented with support provided by the Government of Hungary in the context of the Innovative Mobility Program of KTI.

Saját publikációk listája

Konferencia és workshop cikkek

[C1] András Gazdag, Levente Buttyán, and Zsolt Szalay
Towards Efficient Compression of CAN Traffic Logs
34th Int. Coll. on Adv. Manufacturing and Repairing Vehicle Industry, 2017.

[C2] András Gazdag, Levente Buttyán, and Zsolt Szalay
Efficient lossless compression of CAN traffic logs
25th Int. Conference on Software, Teleco. and Comp. Networks (SoftCOM), 2017.

[C3] András Gazdag, Tamás Holczer, Levente Buttyán, and Zsolt Szalay
Vehicular can traffic based microtracking for accident reconstruction
Vehicle and Automotive Engineering, Springer, 2018.

[C4] András Gazdag, Dóra Neubrandt, Levente Buttyán, and Zsolt Szalay
Detection of Injection Attacks in Compressed CAN Traffic Logs
Security and Safety Interplay of Intelligent Software Systems, Springer, 2019.

[C5] András Gazdag, Csongor Ferenczi, and Levente Buttyán
Development of a Man-in-the-Middle Attack Device for the CAN Bus
1st Conference on Information Technology and Data Science, 2020.

[C6] András Gazdag, György Lupták, and Levente Buttyán
Correlation-based Anomaly Detection for the CAN Bus
Euro-CYBERSEC, 2021.

[C7] Irina Chiscop, András Gazdag, Joos Bosman, and Gergely Biczók
Detecting Message Modification Attacks on the CAN Bus with Temporal Convolutional Networks
Proceedings of the 7th International Conference on Vehicle Technology and Intelligent Transport Systems, 2021.

Folyóirat cikkek

[J1] András Gazdag, Levente Buttyán, and Zsolt Szalay
Forensics aware lossless compression of CAN traffic logs
Scientific Letters of the University of Zilina, 2017

[J2] András Gazdag, Szilvia Lestyán, Mina Remeli, Gergely Ács, Tamás Holczer, and Gergely Biczók
Privacy pitfalls of releasing in-vehicle network data
Vehicular Communications, 2023.

[J3] András Gazdag, Rudolf Ferenc, Levente Buttyán
CrySyS dataset of CAN traffic logs containing fabrication and masquerade attacks
Nature: Scientific Data, 2023.

Hivatkozások

[1] Cohen, A., and Nissim, K. Towards formalizing the gdpr's notion of singling out. *Proceedings of the National Academy of Sciences 117*, 15 (2020), 8344–8352.

[2] Cohen-Hadria, A., Cartwright, M., McFee, B., and Bello, J. P. Voice anonymization in urban sound recordings. In *2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP)* (2019), IEEE, pp. 1–6.

[3] Hanselmann, M., Strauss, T., Dormann, K., and Ulmer, H. CANet: An unsupervised intrusion detection system for high dimensional can bus data. *IEEE Access 8* (2020), 58194–58205.

[4] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., and Savage, S. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy* (2010), pp. 447–462.

[5] Kukkala, V. K., Thiruloga, S. V., and Pasricha, S. INDRA: Intrusion detection using recurrent autoencoders in automotive embedded systems. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 39* (2020), 3698–3710.

[6] Lestyan, S., Ács, G., Biczók, G., and Szalay, Z. Extracting vehicle sensor signals from CAN logs for driver re-identification. In *Proceedings of the 5th International Conference on Information Systems Security and Privacy, ICISSP 2019, Prague, Czech Republic, February 23-25, 2019* (2019), P. Mori, S. Furnell, and O. Camp, Eds., SciTePress, pp. 136–145.

[7] Miller, C., and Valasek, C. Remote exploitation of an unaltered passenger vehicle. Tech. rep., IOActive Labs Research, 2015.

[8] Taylor, A., Japkowicz, N., and Leblanc, S. Frequency-based anomaly detection for the automotive can bus. In *2015 World Congress on Industrial Control Systems Security (WCICSS)* (2015), pp. 45–49.

[9] Weber, M., Wolf, G., Sax, E., and Zimmer, B. Online detection of anomalies in vehicle signals using replicator neural networks. In *ESCAR 2018* (2018).