Hogyan védekezzünk az önvezető járművek külső manipulációja ellen?

Kiss Gábor*

**Obuda University, Budapest, Hungary; e-mail: kiss.gabor@bgk.uni-obuda.hu*

Abstract: Az önvezető autó témaköre manapság felkapott, miközben az ötlet nem újdonság. Már 1925-ban létezett rádió-irányítású autó. 1958-ban a Chrysler Imperial már képes volt a sebesség megtartására, hasonlóan a mai tempomat működéséhez. 1995-ben egy Mercedest ruháztak fel szinte teljes önvezető funkcióval, mellyel 2000 km-t meg is tett, igaz a sofőrön kívül más számára nem maradt hely a sok elektronikus berendezés miatt. 2009-ben indította el a Google az önvezető autó projektjét, 2015-ben pedig a Tesla elérhetővé tette az Autopilot szoftverét, melyet napjainkig frissít. Az teljesen önvezető autók elterjedésétől azt várják, hogy az éves szinten 1.3 millió halálesetet okozó balesetek száma, melyeknél kb. 90%-ban az emberi tényező a fő kiváltó ok [Singh, 2015], jelentős csökkenést fog mutatni azáltal, hogy a szenzorokból érkező adatok információvá történő feldolgozása, valamint a szituációhoz kapcsolódó megfelelő döntéshozatal és szükség szerinti beavatkozás gyorsabban történik majd meg a felhasznált mesterséges intelligenciának köszönhetően az emberhez képest A cikkben bemutatunk pár külső manipulációs technikát, mellyel a teljesen önvezető jármű döntéshozatala befolyásolható, illetve javaslatot teszünk olyan módosításokra a fejlesztési folyamat során, mellyel a külő manipuláció megelőzhető.

1. BEVEZETÉS

Az emberiség által elért technikai fejlődésnek köszönhetően, már nem álom a teljesen önvezető járművek világa. Egyre több országban folynak különböző kísérletek, és több autógyártó cég is kereskedelmi forgalomban elérhetővé tette a részleges önvezetésre alkalmas járműveit. A hagyományos járművek esetében a baleseteknél a biztosító kb. 2 másodperccel számol, amíg a vezető felismeri a veszélyes helyzetet és elkezdi a hatékony beavatkozást annak elkerülésére, valamint a fékberendezés is működni kezd [Green, 2013]. Árnyaltabb a kép a részleges önvezetéssel rendelkező járművekben, hiszen ezekben még van pedál és kormánykerék annak érdekében, hogy a sofőr szükség esetén beavatkozhasson, viszont adott közlekedési szituáció esetén akár 5-6 mp is eltelhet, mire a sofőr valóban képes a helyzetet felismerni és megfelelő beavatkozást megkezdeni [Funkhouser and Drews, 2016]. A Tesla autókkal 2018. novemberének végéig 1 milliárd mérföldet tettek meg a 2015-ben bemutatott Autopilot rendszerű önvezető módban, mely a Nap-Föld távolságának ötszöröse. A baleseti statisztika ez 3,34 millió mérföldenként egy baleset, vagy balesetszerű esemény, míg az Amerikai Közlekedési Hatóság a teljes amerikai autóközlekedésben 492 ezer mérföldenként számol egy balesettel, tehát az önvezető mód jelenleg kb. hétszer biztonságosabb [Friedman, 2019].

2. SAE SZINTEK

Az önvezető járműveket 6 szintre osztja a SAE szabvány [SAE, 2018].

2.1 SAE Level 0

Ezen a szinten azok a hagyományos járművek vannak, melyek a ma kapható járművekben elérhető vezetőtámogató rendszereket még nem tartalmaznak. A sofőr feladata minden közlekedési helyzet megoldása, semmilyen figyelmeztetés nem segíti az érzékelését.

2.2 SAE Level 1

A ma újonnan megvásárolható járművek szintje, ahol már valamilyen vezetéstámogató rendszer (pl. tempomat, városi fékasszisztens, sávkövetés, holttér figyelő, stb.) működik ezzel segítve a balesetek számának csökkenését, hiszen hangjelzéssel, fényjelzéssel hívja fel a figyelmet a veszélyessé válható közlekedési helyzetekre, illetve szükség esetén fékezéssel avatkozik be, így csökkentve egy baleset súlyosságát.

2.3 SAE Level 2

Ezzel a szinttel rendelkező járművek képesek a megfelelő körülmények (jellemzően szembejövő forgalomtól mentes, jól látható felfestésekkel ellátott útszakasz) teljesülése esetén az önvezetésre, de a vezetőnek adott időközönként jeleznie kell a rendszernek (pl. megfogni a kormányt), hogy bármikor képes átvenni az irányítást.

Jellemzően a parkolásban, közlekedési dugóban történő araszolásban, valamint autópálya környezetben a rendszer által megkövetelt feltételek esetén gyors haladásban segédkeznek a 2-es szintű rendszerek. Itt elegendő a jármű közvetlen környezetének felderítése is. Előfordulhat, hogy amennyiben a 2. szintű önvezetéshez szükséges körülmények nem adottak, a jármű nem veszi át a kontrollt a vezetőtől.

2.4 SAE Level 3

A 3. szintű önvezetési funkció esetében a vezető hosszabb időre elengedheti a kormányt, de továbbra is készen kell állnia arra, hogy a teljes kontrollt szinte azonnal visszavegye a jármű felett. Amennyiben a sofőr nem veszi át a irányítást, a jármű hang- és fényjelzést ad és egy idő után fékezgetni kezd. Ha még ekkor sem veszi át a vezető az irányítást, bekapcsolja a vészvillogót, megáll, és automatikus segélyhívást kezdeményez.

2.5 SAE Level 4

A 4. szinten a vezető akár aludhat is az utazás alatt, de szükség esetén készen kell állnia a vezetésre. Probléma esetén az autó kivezeti magát a forgalomból és felébreszti a sofőrt, így lehetővé téve a továbbutazást, probléma elhárítást. Ezen a szinten már megjelenik az igény arra, hogy a távolabbi környezetről is információval rendelkezzen a jármű, hosszabb távra előre tervezhetővé téve az utazást.

2.6 SAE Level 5

Az 5. szint, ahol már teljes mértékben utasként jelenik meg a vezető, nincs módja a szükség szerinti beavatkozásra (nem lesz pedál, kormány a járműben, max. opcióként), hogy egy esetleges balesetet elkerüljön. Információbiztonság szempontjából pont emiatt, ez a szint a leginkább védendő.

3. ÖNVEZETŐ JÁRMŰVEKBEN HASZNÁLT SZENZOROK

Az önvezető járművek megfelelő működéséhez a környezetének megfelelő érzékelését ellátni képes szenzorok által szolgáltatott adatok biztosítanak alapot. A jelenleg elérhető szenzorok, melyeket az egyes autógyártók használnak: a LIDAR, radar, kamera és UH szenzor, melyek segítségével térképezi fel a jármű a környezetét.

3.1 LiDAR

A LiDAR (Light Detection and Ranging) a környezetről egy 3D-s pontfelhőt alkot lézeres letapogatással kb. 100 méter távolságig, ezáltal a háttértől el tud választani egyes objektumokat. Rosszabb a felbontása, mint egy HD kamerának, ennek ellenére nagy mennyiségű adatot szolgáltat a 3D miatt. Előnye, hogy éjjel is használható, nincs szükség közúti világításra a működéséhez, hátránya, hogy drága, illetve nem minden időjárási viszony mellett használható jól, ugyanis havas, ködös környezetben nem szolgáltat megbízható adatokat.

3.2 Radar

A radar sokkal olcsóbb, mint a fény, illetve lézersugaras megoldás, jóval kevesebb adatot is szolgáltat a HD kamerához képest a rosszabb felbontása miatt, viszont nem befolyásolják az adatokat az időjárási és a látási viszonyok sem. Az általa visszaadott eredmény a tárgy méretét és távolságát tartalmazó objektumlista. A közúti forgalomban viszont nem csak az adott tárgyról, hanem az útról, a szalagkorlátról és esetleg más objektumról való visszaverődéssel is számolni kell az adatok feldolgozása során. Távolságtartásnál, fékezés előrejelzésénél használható.

3.3 Kamera

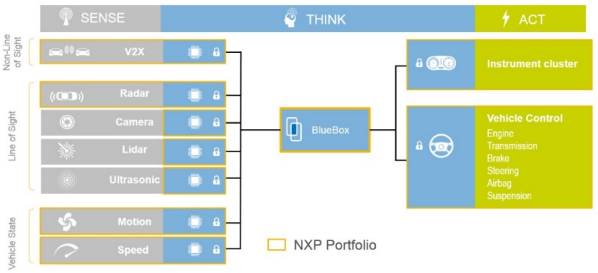
A HD felbontású kamerák viszonylag olcsók, képesek a színek megkülönböztetésére (megfelelő körülmények között), a jármű körbeépíthető velük, pl. 10 kamera elegendő egy gépkocsi teljes környezetének figyelésére. A felbontásból és a felvételkészítés gyakoriságából adódóan (30 kép/másodperc) sok adatot szolgáltatnak, amit fel kell dolgoznia a központi egységnek.

3.4 UH szenzor

Az ultrahang szenzorokat a járműveknél rövid hatótávolságuk (kb. 10 méter) miatt jellemzően a parkolásnál, vagy sávváltás esetén a közeli mögöttes forgalomra való figyelmeztetésnél használják. Olcsó és megbízható eszközök.

4. KÖZPONTI EGYSÉG

Az önvezető funkció ellátása nagyon nagy számítási igényű, hiszen több érzékelőből, kamerából érkezik feldolgozásra adat, melyek szigorú határidejű feladatok. Nem lehet percekig dolgozni azon, megálljon-e a jármű a piros lámpánál, vagy nem, félrerántsa a kormányt egy szembejövő másik jármű elől, elkerülve az ütközést, vagy nem, stb. (1. ábra).



1. ábra Önvezető járművek vezérlése

Mivel különböző szenzorok, kamerák szolgáltatják az irányításhoz szükséges adatokat, emiatt azok párhuzamos feldolgozására van szükség, melyet a GPU (Graphical Processor Unit) architektúra tesz lehetővé.

5. MESTERSÉGES INTELLIGENCIA

Napjainkban egyre többször hallunk a mesterséges intelligencia széleskörű felhasználásáról. Segít a Karaoke előadásokat a közönség számára is elviselhetőbbé tenni [Wager et al, 2018], hamarabb képes megállapítani a csecsemők vérmérgezését felismerni [Masino et al, 2019],

használja a rendőrség a bűnesetek felderítésénél [Sisak, 2019], vagy pénzmosás felderítésénél [Shane, 2019]. A mesterséges intelligencia napjainkban szinte minden ágazatban megjelenik az iparban, melyek alapja az utóbbi években elért kutatási eredményeknek köszönhetők a mesterséges neurális hálózatok [Aizenberg, et al, 2000], a gépi látás [Fukushima, 1980], valamint a több rétegű logikai neurális hálózatok területén [Carvalho et al, 1994]. Magától értetődő, hogy az önvezető járművek fejlesztésénél, ahol különböző szenzorokból folyamatosan áramló, nagy mennyiségű információ alapján kell döntést hozni a jármű megfelelő irányítása során, szintén a mesterséges intelligencia alkalmazása merült fel a fejlesztések során. Amíg egy mesterséges intelligencia az iparban a képfelismerés alapján a selejtes darabok kiválogatásáról dönt, a rossz döntés jó mintadarabok selejtezéséhez, vagy hibás darabok megfelelőnek ítéléséhez vezethet, illetve humánpolitikában alkalmazott mesterséges intelligencia az egyik nem preferálásához a pályázatok elbírálásánál [Lee, 2018a], addig az önvezető járművek esetében egy rossz döntés emberéletekbe kerülhet, ahogy láttuk az Uber baleseténél [Wakabayashi, 2018]. Az MIT egyik kutatócsoportja sikeresen hozta létre a világ első pszichopata mesterséges intelligenciáját, mely rámutatott a mesterséges intelligencia tanításának felelősségére [Yanardag et al, 2018].

5.1 Az önvezető járművekben használt mesterséges intelligencia tanítása

Az nem kérdés, hogy az önvezető járművekben mesterséges intelligenciát kell használni a megfelelő sebességű és minőségű döntéshozatalhoz, köszönhetően az utóbbi években a mesterséges intelligencia kutatásában elért eredményeknek. A különböző szenzorokból, kamerákból érkező adatokból nyert információk alapján 1/30-ad másodperc alatt kell a feldolgozást elvégezni és a szükséges döntést is meghozni.

A tanítás során a legegyszerűbb az lenne, ha a KRESZ szabályokat vennénk csak figyelembe a döntéshozatalnál. Ez jogilag is jobban védhető baleset esetén.

A Tesla mérnökei egy ún. árnyékmódot is fejlesztettek az Autopilot-nak, ami ugyanúgy elemezi közlekedési helyzeteket, amikor az ember vezet, és ezeket az adatokat is visszaküldi a központba, felhasználva azokat is a következő verzió fejlesztésekor. Az ötlet jó, a rutinos sofőrök sok veszélyes helyzetet tudnak elkerülni. Gondot az okozhat, ha rutintalan sofőr ügyetlenkedései is megoldási javaslatként kerülnek bele a rendszerbe.

Az NVIDIA egyik legújabb fejlesztésével interaktív világot lehet létrehozni, mely nem csak a játékiparban használható fel még látványosabb környezet létrehozásához, hanem az önvezető járművek tanításánál is lehet vele könnyen szimulálni életszerű környezetet [Brown, 2018].

A Hyundai CRADLE befektetett a Perceptive Automata startup vállalkozásba, melynek technológiája többek között a gyalogosok gondolatait próbálja kitalálni, pl. hogy átkelés közben meggondolják-e magukat és inkább elengedik az önvezető járművet [Cha, 2018].

Hasonlóan fontos lehet az átmeneti időszakban, amikor még az önvezető járművek mellett a hagyományos járművek is forgalomban lesznek, a bizonytalan vezetők felismerése. Akinek már sofőrként elég nagy rutinja van, a jármű mozgásából meg tudja ítélni, mennyire képes az előtte haladó jármű vezetője uralni az általa irányított autót. Ha az előttünk haladó bizonytalankodik, minél hamarabb megpróbáljuk megelőzni, illetve lemaradunk, hogy elkerüljük ebből a bizonytalanságból esetlegesen kialakuló veszélyes helyzeteket. Az önvezető járműveknél a mesterséges intelligenciát is fel lehetne készíteni a környezetében lévő bizonytalan vezetők felismerésére, hogy minél hamarabb biztonságos távolságra kerülhessen tőlük.

5.2 Etikai kérdések

Az önvezető autók világában is lesznek elkerülhetetlen balesetek, bár köszönhetően a gyorsabb helyzetfelismerésnek várhatóan lényegesen alacsonyabb számban. A klasszikus Trolley probléma kapcsán [Thomson, 1985] az MIT tudósai egy globális kutatást végeztek 233 országból 39,6 millió választ feldolgozva [Awad et al, 2018]. Az általuk létrehozott Moral Machine weboldalon több baleseti szituációban lehet kiválasztani az általunk helyesnek vélt döntést az önvezető jármű részéről. Ki élje túl az elkerülhetetlen balesetet? A szabályosan közlekedő idős úr, a piroson babakocsit áttoló fiatal anyuka, vagy az autóban ülő utasok?

Globálisan a legkevésbé a babakocsiban lévő, illetve a kis gyereket vélték feláldozhatónak a válaszadók, és leginkább feláldozhatók az állatok voltak. Ezt a rangsort eddig természetesnek is gondolnánk, viszont a kutatás rámutatott a kulturális és vallásbeli különbségeknek a feláldozhatóságra vonatkozó hatására. Például a keleti országokban az idős emberek nagyobb megbecsülésének köszönhetően a rangsorban kevésbé feláldozhatók, mint a gyerekek, ellentétben a nyugati országokban élők válaszaival. Ezt azt jelenti, hogy az önvezető autókban a döntésekért felelős mesterséges intelligenciának esetlegesen figyelembe kell vennie az adott országra jellemző feláldozhatósági preferenciát, így növelve a társadalmi elfogadottságát az adott elkerülhetetlen tragikus eseménynek.

Az Intel által felvásárolt Mobileye fejlesztése azon a logikán alapul, hogy minden körülmények között be kell tartani a KRESZ szabályait, így jogilag jobban kezelhető a baleset (mobileye.com). Viszont az is lehet, hogy az adott baleset elkerülhető lett volna, ha a jármű megszegi a KRESZ szabályait, pl. átlépve a záróvonalat kerüli ki a balesetveszélyes szituációt, amennyiben nincs szembejövő forgalom.

A Google-Waymo rendszere elkerülhetetlen baleset esetén azt az objektumot választja, amelyik kisebb méretű, ezáltal alacsonyabb sérülést okoz a járműben utazók részére, miközben a helyzet védtelenebb szereplőit (gyalogosokat, biciklistákat) megpróbálja megkímélni (waymo.com).

A fentiek alapján látható, milyen lényeges működésbeli különbségek érhetők el az önvezető járművek esetében a bennük lévő mesterséges intelligencia különböző tanítási folyamata által.

6. ÖNVEZETŐ JÁRMŰVEK KÜLSŐ MANIPULÁCIÓS LEHETŐSÉGEI

Teljesen biztonságos rendszer nem létezik, így lesz ez az önvezető járművek esetében is. John S. Chen, a BlackBerry vezetője szerint cége 90 százalékban biztonságos rendszert lesz képes fejleszteni, de az éles használatba kerüléstől kezdve folyamatos felülvizsgálatot igényel majd, hogy ez a biztonsági szint tartható legyen [Chen, 2018].

A fejezetben nem az önvezető járművek rendszerének megtörését vizsgáljuk, hanem olyan szituációkat veszünk górcső alá, melyek alkalmasak lehetnek az önvezető járművekben üzemelő mesterséges intelligencia összezavarására, esetlegesen a károkozó számára előnyös döntés meghozatalára. Célunk ezen helyzetek felvetésével az, hogy a gyártók ezeket és ehhez hasonló szituációkat is teszteljenek a fejlesztés során, így téve biztonságosabbá az önvezető járművek által a közeljövőben uralt közlekedést.

6.1 Emberi viselkedésben várható változás veszélyei

Az önvezető járművek gyorsabb helyzetfelismerésre és reakcióra lesznek képesek az embernél, így téve biztonságosabbá a közúti közlekedést. Ezt a gyorsaságot felismerve az átmeneti időszakban, amikor még a hagyományos járművek is részt vesznek a forgalomban, azok vezetői bízva az önvezető jármű gyors reakciójában olyan szituációkat is bevállalhatnak, melyet egy hagyományos jármű környezetében nem tennének meg. Bevágnak más autó elé a sávjába, kihajtanak elé egy kereszteződésben, besorolnak elé felhajtva az autópályára. Ezzel a forgalom lelassítható, esetenként baleset is előidézhető, ha az önvezető jármű mögött, mely képes lesz a balesetet a gyorsabb reakciójának köszönhetően elkerülni, a mögötte haladó hagyományos jármű sofőrjét kényszeríti olyan veszélyes helyzetbe, melyet ő már nem tud elkerülni lassabb reakcióideje miatt. Ezzel szándékosan is elő lehet idézni egy önvezető jármű balesetét, ugyanis akkor kell hirtelen bevágni elé, amikor hagyományos autó halad mögötte, így az belerohanhat majd, míg a veszélyes helyzetet előidéző jármű sérülésmentesen megússza a helyzetet az önvezető jármű gyorsabb reakciójának köszönhetően.

6.2 Lane tracking rendszer becsapása

A modern járművek rendelkeznek sávkövető automatikával, mely megfelelő minőségű felfestés esetén a sávban tartja az autót. Sávváltásra akár már két fehér pont megfelelő helyre történő felfestésével is kényszeríthetjük a járművet [Tencent 2019].

A Mercedes digital light technológiája képes arra, hogy a fényszóróba épített tükrök segítségével különböző szimbólumokat, akár sávot is vetíthet a jármű elé (mercedes-benz.com). Hasonlóan lehet a kerékpár mellé is sávot vetíteni, így biztonságosabbá téve a közlekedésüket. A technológia felhasználható arra is, hogy az önvezető jármű számára vetítsünk hamis sávot, így esetlegesen összezavarni, eltéríteni az eredeti útvonaláról azt.

6.3 Táblafelismerő rendszer becsapása

A táblafelismerő rendszer alkalmas ma is arra, hogy az adaptív tempomat a közlekedési táblán látható értékhez igazítsa a jármű sebességét. Az Európai Bizottság 2018 májusában javaslatot tett többet között arra, hogy 2022-től minden forgalomba helyezett gépjármű rendelkezzen intelligens sebességszabályozó rendszerrel, mely térképadatok és táblafelismerés alapján a jármű végsebességét automatikusan a megengedett sebességre korlátozza, mely a gázpedál lenyomásával felülbírálható lenne [EU, 2018]. Egy kutatás rámutatott arra, hogy a táblafelismerő a rendszerek is becsaphatók [Sitawarin et al, 2018].

A kutatásomban a forgalmi helyzet változtathatóságára, baleset előidézhetőségére helyezem a hangsúlyt. Ha egy mindkét irányból behajtani tilos táblát, mely pl. egy sétálóutcát zár el a forgalom elől, lefedünk egy egyirányú táblával mindkét végén, az önvezető járművek hogyan fognak dönteni? Ha a táblán az üres fehér részre ráragasztjuk a 70-es számot, rögtön sebességkorlátozás lesz a behajtani tilos táblából. Autópályán a 130-as sebességkorlátozó táblából kitakarjuk a számokat, mindkét irányból behajtani tilos táblát kapunk. Megakaszthatjuk vele a forgalmat és így dugót idézhetünk elő? Felmerül a kérdés, hogy a jármű a saját térképadatainak higgyen, vagy bírálja felül a kamerája által felismert jelentéssel és módosítsa ennek megfelelően a haladását? Minek legyen nagyobb prioritása? Egy központilag időnként frissített térképnek, mely akár valótlan adatokat is tartalmazhat annak károkozás szempontjából történő módosítása esetén, vagy az adott pillanatban felismert közúti jelzésnek, mely akár szándékos félrevezetés része is lehet?

6.4 Megvakítás

Az önvezető járművek egyik legfontosabb része a döntéshozatalnál a több kamerából érkező adathalmaz. Mi van akkor, ha latyakos időben az előttünk haladó jármű teljesen besározza a kamerák látómezejét? A szélvédő még tisztítható menet közben, de az oldalsó kamerák felülete már nem. A szélvédő is teljesen bekoszolható, ha olajat öntenek rá egy mellette elhaladó járműből. Ködös, havas időben, illetve ködgéppel szintén vakká tehető a szenzorok egy része, pl. a LiDAR is. Lézerekkel pedig a kamerák tehetők vakká, hasonlóan ahhoz, ahogy a mai járművekben a felkelő, illetve a lemenő nap fénye okoz gondot [Polsky, 2019]. Ilyen esetben az önvezető jármű a mai tendencia alapján megáll, és nem folytatja az útját, tehát az utasok késlekedésre kényszeríthetők, lekésve pl. egy fontos tárgyalást, vonat, illetve repülőgép indulását.

6.5 Foglyul ejtés, irányváltásra kényszerítés, hajsza

Az önvezető jármű a balesetek elkerülésére lesz programozva. Ha viszont egy piros lámpánál álló járművet körbeállnak gyalogosok, kerékpárosok, nem lesz képes elindulni és az 5. SAE szinten még a benne ülőknek sem lesz lehetőségük irányításra, hogy egy ilyen helyzetből kiszabaduljanak. Ehhez kapcsolódóan felmerül az a probléma is, hogy a sötétebb bőrű gyalogosokat nehezebben ismeri fel az önvezető jármű [Wilson et al, 2019], mely tulajdonság szintén kihasználható bizonyos helyzetekben.

Haladás közben is foglyul ejthető egy önvezető jármű hasonló logika alapján, ha motorosok, hagyományos járművek veszik körül és folyamatosan lassítanak, így kényszerítve az önvezető járművet is lassításra, illetve megállásra, ahogyan a rendőrök állítottak meg egy önvezető módban lévő Tesla gépjárművet [Kadvany, 2018].

A körbevétellel irányváltásra is kényszeríthetünk egy baleset elkerülésére programozott önvezető járművet és pl. autópályáról egy kihajtóra irányíthatjuk, így módosítva az eredeti haladási irányát.

Amennyiben hagyományos járművekkel, vagy motorokkal beállunk az önvezető jármű mögé és folyamatosan, egyre gyorsítva haladunk mögötte elég közel ahhoz, hogy a járművet gyorsításra késztessük az ütközés elkerülése érdekében, hajszolhatjuk a járművet. A kérdés az, hogy olyan sebességre is, amikor már az önvezető jármű gyors döntéshozatala és reakciója is kevés lehet egy baleset elkerülésére? Megengedett-e az önvezető járművekben ilyen esetekre egy „Pánikgomb” beépítése, mely akár a jármű sérülése árán is, de kitör az ilyen helyzetekből kimentve a benne utazókat? Mi történik akkor, ha valaki siet és a piros lámpánál állva a gyalogosok közzé hajtatja ezzel a megoldással a járművet? Ez akár terrorcselekmény végrehajtására is alkalmassá tenné a járművet.

7. MEGOLDÁSI JAVASLATOK A KÜLSŐ MANIPULÁCIÓ ELLENI VÉDEKEZÉSRE

Az előbbiekben több külső manipuláción alapuló támadást soroltunk fel, melyekre érdemes az önvezető járművek rendszereit felkészíteni. Ebben a fejezetben szeretnék pár megoldási javaslatot tenni a külső manipuláció elleni védekezésre.

7.1 Prioritási szintek kialakítása a különböző forrásból származó adatok kiértékeléséhez

A jövőben a teljesen autonóm járművek által uralt közlekedésben elkerülhetetlen a szereplők közötti kommunikáció, mely sok problémaforrásra megoldás lehet, pl. a kátyút érzékelő, előttünk haladó autó jelezhet hamarabb, mint ahogy a mi járművünk érzékelné. Sok esetben előnyösebb, ha a járművek megoszthatnák egymással az általuk már tapasztalt rendellenességeket, így felkészítve a többieket azok elkerülésére, és csökkentve a lehetséges balesetek számát (2. ábra). A kérdés az, hogy a rendelkezésre álló térképinformációkhoz viszonyított eltéréseket a központnak továbbítsák-e (új kátyú esetén akár az útfelújítónak), vagy csak azokkal osszák meg, akik a közelükben vannak. Az utóbbinak az előnye, hogy a központ terhelése csökken, nem kell feltétlenül minden járművet értesíteni a városban az adott kátyúról, ezáltal a hálózati forgalom is csökken. Ebben az esetben javasolt egy olyan egység beépítése az autonóm járművekbe, mellyel rövid távolságon belül adatokat tud megosztani és fogadni egy szabványosított protokollon keresztül. Ennek fényében pedig egyértelműen kell szabályozni, hogy milyen anomália legyen a központ számára bejelentve pl. baleset, és melyek legyenek csak a környező járművekkel megosztva.

2. ábra Önvezető járművek egymás közötti kommunikációja

Ugyan látható, hogy a járművek közötti kommunikáció sok veszélyhelyzet elkerülésében segíthet, ebben is rejlik némi veszély. Amennyiben ezt a kommunikációs rendszert sikerül meghekkelni, egy jármű hamis figyelmeztetések kiadásával balesetbe sodorhat, útvonal változtatásra késztetheti a környezetében haladókat. Ennek elkerülése érdekében érdemes végiggondolni, milyen prioritása legyen a különböző forrásokból származó adatoknak a döntéshozatal során.

A legalacsonyabb szintre az autóban lévő, vagy központilag megosztott térkép-információkat javaslom tenni, hiszen a birtokolt információ nem feltétlenül a legfrissebb adatokat tartalmazza egy balesetről, esetleges útfelújításról (pl. hirtelen csőtörés esetén), kivéve, ha központilag állandóan frissítik azt, de itt is fennáll az a veszély, hogy a központi adatok sérültek és nem a valós eseményt takarják.

A középső szintre a környező járművektől kapott információ sorolható, de ezek is lehetnek már elévültek, pl. úton álló autó, mely már elhagyta az adott helyszínt, mire mi odaérünk, vagy módosultak.

A legmagasabb szintre a jármű saját szenzorai által érzékelt adatokat sorolnám, mivel azok a mindenkori pillanatnyi állapotnak megfelelőek, és a legaktuálisabbak (1. táblázat).

1. táblázat. Prioritási szintek az önvezető jármű különböző adatforrásaiból származó adatok felhasználására

Prioritási szint	Adatforrás
1	Telepített térkép adatok
2	Szomszédos járművektől kapott adatok
3	A jármű saját szenzorai, mérőberendezései által szolgáltatott adatok

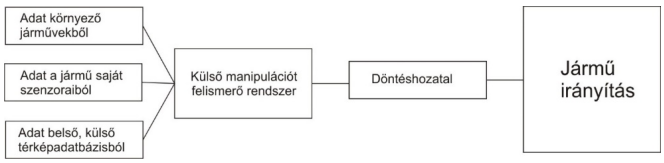
Ezt a prioritási sorrendet érdemes a járműnek a döntéshozatalkor figyelembe venni a legmegfelelőbb művelet elvégzéséhez, amennyiben a három forrásból származó adat eltér egymástól.

7.2 Mesterséges intelligencia alapú döntéshozatali modul elé telepített, külső manipulációt felismerő modul bevezetése

Előfordulhat olyan eset is, amikor a különböző forrásból származó adatok jelentősen eltérnek egymástól, pl. a térkép szerint 130 km/h-al lehet haladni, a környező járművek azt továbbítják, hogy az előttem haladók (pl. hagyományos járművek), melyek a szenzorok hatókörén kívül vannak, csak 70 km/h sebességgel haladnak, a kamera pedig egy mindkét irányból behajtani tilos táblát érzékel.

Ebben az esetben a jármű a 6. fejezetben említett külső manipulációknak lehet kitéve, melyek újabb veszélyforrást jelentenek az utasok és a környezet számára baleset esetén. Javaslom, hogy az adatoknak a különböző forrásokból döntéshozatalra történő továbbítása előtt legyen még egy mesterséges intelligencia alapú modul beépítve a járművekbe (External Manipulation Recognition System, EMRS), melyet minden gyártó saját maga taníthat be, figyelembe véve a gyártó kockázatvállalási hajlandóságát, és amely modul feladata a külső manipuláció veszélyének felismerése és a döntéshozatalnál a különböző forrásokból származó, eltérő adatok megfelelő kiértékeléséhez történő javaslattétel a szituáció felismerésével (3. ábra). Ennek az egységnek a tudását egy-egy szervizlátogatás alkalmával lehet frissíteni a megfelelő biztonsági intézkedések mellett.

Ilyen esetekben az is előfordulhat, hogy az 7.1. fejezetben javasolt prioritási sorrend az adatforrások között megváltoztatható a biztonságos továbbhaladás érdekében.



3. ábra Külső manipulációt felismerő modul beágyazása a döntéshozatali modul elé

8. ÖSSZEFOGLALÁS

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

KÖSZÖNETNYILVÁNÍTÁS

A cikk kutatásaihoz az Új Széchenyi Terv keretein belül az EFOP-3.6.2-16-2017-00016 számú projekt biztosított forrást. A kutatás az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósult meg.

HIVATKOZÁSOK

Aizenberg, I.; Aizenberg, N. N.; Vandewalle, J. P. L. (2000): Multi-Valued and Universal Binary Neurons: *Theory, Learning and Applications*. Springer Science & Business Media

Brown K. (2018): Invention Has Potential to Create Virtual Worlds for Gaming, Automotive, Robotics, VR, https://nvidianews.nvidia.com/news/new-nvidia-research-creates-interactive-worlds-with-ai, letöltve: 2020. május 31.

Carvalho, A. (1994: Fairhurst, M. C.; Bisset, D. L.: An integrated Boolean neural network for pattern classification, *Pattern Recognition Letters*, **15 (8)** pp: 807–813

Cha J. (2018): Hyundai CRADLE Invests in Perceptive Automata to Bring Human Intuition Software to Self-Driving Cars, https://www.hyundai.com/worldwide/en/news/news-room/news/hyundai-cradle-invests-in-perceptive-automata-to-bring-human-intuition-software-to-self-driving-cars-0000016052?pageNo=4&searchKey=&rowCount=6&type[]=RES&listPageUrl=news.release.all, letöltve: 2020. május 31.

Chen J. (2018): Driverless cars could be hacked and deployed as "fully loaded weapons", https://techsecurity.news/2018/09/blackberry-ceo-john-chen-warns-driverless-cars-could-turn-into-fully-loaded-weapons-if-hacked/, 2020. május 31.

EU. (2018): Az Európai Parlament és a Tanács rendelete a gépjárműveknek és pótkocsijaiknak, valamint az ilyen járművek rendszereinek, alkotóelemeinek és önálló műszaki egységeinek az általános biztonság, továbbá az utasok és a veszélyeztetett úthasználók védelme tekintetében történő típusjóváhagyásáról, 2018/0145(COD),

Friedman L. (2019): Tesla Vehicle Deliveries and Autopilot Mileage Statistics, DOI: 10.5281/zenodo.2530449, https://hcai.mit.edu/tesla-autopilot-miles-and-vehicles/, letöltve: 2020. május 31.

Fukushima, K. (1980): Neocognitron: A self-organizing neural network model for a mechanism of pattern recognition unaffected by shift in position, *Biological Cybernetics*. **36 (4)**, pp: 193–202

Funkhouser K., Drews F.: (2016): Reaction Times When Switching From Autonomous to Manual Driving Control, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, ISSN: 1541-9312

Geen, M. (2013): Driver Reaction Time, https://www.visualexpert.com/Resources/reactiontime.html, letöltve: 2020. május 31.

Kadvany E. (2018): Los Altos planning commission chair arrested for Tesla DUI, Palo Alto Weekly, https://www.paloaltoonline.com/news/2018/11/30/los-altos-planning-commissioner-arrested-for-tesla-dui, letöltve: 2020. május 31.

Lee, D. (2018a): Amazon scrapped 'sexist AI' tool, BBC News, October 10, 2018, https://www.bbc.com/news/technology-45809919, letöltve: 2020. május 31.

Lee, D. (2018b): Why Big Tech pays poor Kenyans to teach self-driving cars, BBC News, November 03, 2018, https://www.bbc.com/news/technology-46055595, letöltve: 2020. május 31.

Masino AJ, Harris MC, Forsyth D, Ostapenko S, Srinivasan L, et al. (2019): Machine learning models for early sepsis recognition in the neonatal intensive care unit using readily available electronic health record data. *PLOS ONE* **14 (2)**: e0212665. https://doi.org/10.1371/journal.pone.0212665

Polsky M. (2019): Sunshine Can Sabotage Cadillac's Super Cruise; GM Reportedly Working On Fix, The Truth About Cars, https://www.thetruthaboutcars.com/2019/04/sunshine-can-sabotage-cadillacs-super-cruise-gm-reportedly-working-on-fix/, letöltve: 2020. május 31.

SAE J 3016-2018 (2018): Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, Society of Automobile Engineers, sae.org

Shane D. (2019): Big banks are using AI to keep out of trouble, CNN Business, https://edition.cnn.com/2019/03/21/tech/banks-artificial-intelligence-silent-eight/index.html, letöltve: 2020. május 31.

Singh, S. (2015): Critical reasons for crashes investigated in the National Motor Vehicle Crash Causation Survey. (Traffic Safety, Facts Crash Stats. Report No. DOT HS 812 115). Washington, DC: National Highway Traffic Safety Administration

Sisak M. R. (2019): NYPD partners with a high-tech detective: Algorithm helps spot crime patterns, *USA TODAY*, https://eu.usatoday.com/story/tech/2019/03/12/nypd-uses-algorithm-analyze-crime-patterns/3138284002/, letöltve: 2020. május 31.

Sitawarin, C. Bhagoji, A. N. Mosenia, A. Chiang, M. and Mittal, M.: DARTS (2018): Deceiving Autonomous Cars with Toxic Signs. PACM on Interactive, *Mobile, Wearable and Ubiquitous Technologies* **0 (0)**, 27 pages,

Tencent K.S. L. (2019): Experimental Security Research of Tesla Autopilot, Tencent Keen Security Lab, https://keenlab.tencent.com/en/2019/03/29/Tencent-Keen-Security-Lab-Experimental-Security-Research-of-Tesla-Autopilot/, letöltve: 2020. május 31.

Thomson, J. J. (1985): The Trolley Problem. *The Yale Law Journal* **94 (6)**, 1395-1415

Wager S., Tzanetakis G., Wang C., Gou L.,Sivaraman A., Kim M.. (2018): Deep Autotuner: A data-driven approach to natural-sounding pitch correction for singing voice in karaoke performances, http://homes.sice.indiana.edu/scwager/deepautotuner.html, letöltve: 2020. május 31.

Wakabayashi, D.: Uber's Self-Driving Cars Were Struggling Before Arizona Crash, *The New York Times* March 23, 2018, https://www.nytimes.com/2018/03/23/technology/uber-self-driving-cars-arizona.html, letöltve: 2020. május 31.

Wilson B, Hoffman J., Morgerstern J. (2019): Predictive Inequity in Object Detection, Georgia Tech, https://arxiv.org/pdf/1902.11097.pdf, letöltve: 2020. május 31.

Yanardag, P. ; Cebrian, M.; Rahwan, I.: Norman, World's first psychopath AI, 2018, http://norman-ai.mit.edu, letöltve: 2020. május 31.

Appendix A. FIRST APPENDIX

Appendix B. SECOND APPENDIX