Gépjárművédelmi megoldások a modern lopási módszerek ellen

Dr. Szayer Géza
General Mechatronics Kft.
Budapest, Magyarország
geza.szayer@generalmechatronics.com

Dr. Kovács Bence
General Mechatronics Kft.
Budapest, Magyarország
bence.kovacs@generalmechatronics.com

***Absztrakt* – A cikk bemutatja a modern gépjármű lopási eszközöket és módszereket, illetve a Gorilla gépjárművédelmi rendszer fejlesztésből műszaki részleteket, mely a jelenleg alkalmazott módszerek ellen hatásos védelmet jelent. A cikk taglalja a gépjárművekbe utólagosan integrált eszközök rádiós megoldásainak műszaki és biztonságtechnikai nehézségeit is.**

I. BEVEZETŐ

Hazánkban a 90-es évek elején jelentek meg az első GPS-GSM alapú gépjárművédelmi rendszerek, majd a technika fejlődésével előtérbe kerültek a nyomkövetéhez kapcsolódó szerver oldali szolgáltatások is, mint például a flottakövetés. Ezen utólagosan beépített eszközök a mai napig népszerű kiegészítői a járműveknek, mert a gyári védelemmel ellátott autók eltulajdonítása gyerekjáték. Utóbbi különösen igaz a kulcs nélküli technológiák megjelenése óta, mert egy egyszerű jelismétlővel nyithatóvá és indíthatóvá válik az autó.

A. Gépjármű lopás a gyakorlatban

Közhiedelem, hogy a mai autókat technikailag magasan képzett szakemberek lopják el, azonban a valóság ennél jóval árnyaltabb: A járművek nyitásához és indításához ugyan szakemberek fejlesztenek speciális cél eszközöket, amelyeket megvásárolva egy laikus is el tud tulajdonítani egy gépjárművet. Hogy pontosan mire van szükség, az leginkább az autó típusától függ, főként, hogy kulcs nélküli indítású-e, vagy sem.

A hagyományos nyitású autókat un. Turbodecoder-rel [1] (1. ábra) nyitják ki mechanikusan. A kisméretű, automatikus szerkezettel egy autó zárja nagyságrendileg 10-15 másodperc alatt nyitható ki, majd a kódot rögzítve teljes értékű mechanikus kulcsként használható később a gyújtáskapcsolóban is.

1. ábra *Turbodecoder*, amely az autók zárának 10-15 másodpercen belüli nyitására alkalmas

Könnyű belátni, hogy ezzel már a kormányzárat is kiiktatta a tolvaj. Ezután következik az indításgátló kiiktatása, amelyre a diagnosztikai csatlakozón keresztül van lehetőség. Az autó alvázszámából online adatbázis segítségével [2] – mely Android telefonon applikációként is elérhető – az indításgátló PIN kódja, amelyet megadva betanítható az új „kulcs” RFID azonosítója. Az egész előbbi folyamatra autó-specifikus cél hardverek kaphatóak (2. ábra), amelyeket az OBDII diagnosztikai csatlakozóra illesztve 10-20 másodperc elteltével indítható a jármű.

2. ábra *Immo Bypass Device* (Aliexpress), segítségével másodpercek alatt kiiktatható az autó gyári immobilizer egysége

A napjainkban forgalomba helyezett új, kulcs nélküli nyitású és indítású autók lopása az eddigieknél még könnyebb, csupán egy jelismétlőre van szükség, amelynek vevő oldala a gyári kulcs közelében van, míg az adó oldala az autóval kommunikál, így megnövelve a hatótávolságot a tulajdonos (eredeti kulcs) és az autó között [3,4]. A jelismétlős lopásokhoz tehát két ember kell, az egyik a tulajdonost követi nyilvános helyen a jelvevővel, míg a másik fél úgy viszi el az autót, mintha csak a saját kulcsával tenné.

B. GSM-GPS zavarók

A modern autók lopásának további kiegészítő kelléke a GSM-et és más rádiócsatornákat zavaró un. jammer, amely bekapcsolást követően blokkolja az autóba szerelt rádiós rendszerek jeleit, így akadályozva, hogy az autó riasztási vészjelzést adjon le a tulajdonos felé. A kapható jammer-ek széles sávban, 400 MHz és 5 GHz között a teljes spektrumban nagy teljesítményű rádiós zajt bocsátanak ki, mellyel elnyomnak minden használt rádiós kommunikációt,

pl.: GSM, GPS, Lora, Bluetooth, kapu távirányító adók (433, 868, 915 MHz frekvenciákon működnek).

3. ábra 3G, GSM, GPS és WiFi jel blokkoló (jammer)

II. UTÓLAGOSAN BESZERELT VÉDELMI RENDSZEREK

Az előzőekből belátható, hogy a gyári védelmi rendszerekkel ellátott autók elmozdítása nagyságrendileg fél-másfél perces folyamat. Ezt a rövid időt bármilyen utólagosan beszerelt védelem nagyságrenddel meghosszabbítja, lényegesen növelve ezzel a tolvaj által vállalt kockázatot.

Az utólagos mechanikus védelmek jelentenek a legkisebb mértékű védelmet. Manuális váltós autók esetében a váltózárat gyakran úgy iktatják ki, hogy az autó alá feküdve feszítővassal, egy mozdulattal eltörik a váltó rudat, és kettesbe kapcsolják a váltót. Automata váltók esetén gyakran a váltó kapcsolót feszítik ki a helyéről.

Az elektronikus blokkoló rendszerek nagyobb védelmet jelentenek. A blokkolást minden esetben olyan vezeték/vezetékek megszakításával végzik, mely nélkül a jármű nem indítható (Pl: üzemanyag szivattyú). Ilyen eszközök széles palettáját alkalmazzák az utastérbe és a motortérbe szerelve is. A motortérbe szerelés hátránya, hogy a motorháztető feszítővassal gyorsan kinyitható, a motortéren belül pedig nem lehetséges elrejteni a riasztót. Tehát a gépháztető nyitását követően a tolvaj azonnal elvághatja a riasztó vezetékeit és összekötheti a blokkolási pontot. Az utastérbe szerelt riasztók esetében a blokkolási pont elhelyezhető akár a középkonzol, akár mélyen a légzsák szett alatt is, mely kiszerelése több tíz perccel növeli a lopáshoz szükséges időt, ráadásul a változatosan elrejtett eszközt ismeretlen helyen kell megtalálni.

Az elektronikus eszközök közül a legegyszerűbbek esetén egy rejtett kapcsoló megnyomása szükséges csak a motor engedélyezéséhez. A következő kategóriában már az engedélyezés távirányítóval történik, így a tolvajnak nem elég egyszerűen kifigyelni a rejtett kapcsoló helyét. Ennél fejlettebbek a GSM és GPS modullal rendelkező eszközök, melyek a riasztási eseményt és a GPS pozíciójukat GSM hálózaton továbbítják. A legfejlettebb szolgáltatások esetén szerveres informatikai háttér rendszer egészíti ki az autóriasztót.

A. Elektronikus GPS-GSM alapú védelem, szerverszolgáltatások

A GPS-GSM riasztók piacán kezdetben flottakövetés funkció miatt jelentek meg a szerveralkalmazások, azonban a GSM jelzavarók elleni védekezés miatt a szerverfelügyelet fontossága előtérbe került. Ha az autó folyamatosan (pl. fél percenként) kommunikál egy szerverrel, akkor egy GSM zavaró bekapcsolása esetén a szerver azonnali értesítést tud küldeni a tulajdonosnak a jel megszakadásáról.

A szerverszolgáltatások elterjedésével megjelentek a kiegészítő diagnosztikai funkciók, mint például a raktérhőmérséklet figyelése, a guminyomás mérése és ezen adatok szerverre továbbítása. A szerver pedig különböző eseményekre riasztásokat tud küldeni az illetékes munkatársaknak, tulajdonosnak.

B. Elektronikus védelmi rendszerek beszerelése

Az utólagos védelmi rendszerek beszerelésekor fontos szempont a szerelési idő, és a jármű roncsolás-mentes, szakszerű megbontása, mindamellett, hogy a készülékeket a lehető legjobban el kell rejteni. Ehhez nyújt nagy segítséget, ha a védelmi rendszer távirányítóján kívül a rendszer kiegészítő elemei is - például egy hőmérő modul - vezeték nélkül kommunikálnak egymással, így nincs szükség a plusz kábelezés miatt további burkolatelemek megbontására és a készülék felderítése is jóval nehezebb, mert nem vezetnek felé típusidegen kábelek.

A vezeték nélküli kommunikáció viszont más működési és biztonságtechnikai kérdéseket vet fel, mint a jel lehallgatása, ismétlése, vagy zavaró jel esetén a kommunikáció megszakadása.

A lehallgatás ellen az elterjedt, szabványos, banki szintű titkosítási eljárások, mint például TLS (*Transport Layer Security*), AES256 (*Advanced Encryption Standard*) alkalmazhatóak.

A jelismétlés egy könnyen kijátszható biztonsági rés még ugrókódos távirányítók alkalmazása esetén is [5]. Az ugrókódos távirányító lényege, hogy a jelismétlés megakadályozása céljából minden gombnyomásra újabb kódot generál, a gépjárműbe épített vevő pedig a kódokat a generálás sorrendjében fogadja csak el, egy kódot csak egyszer. A kijátszás módja a következő: A tolvaj az autó riasztójának élesítésekor egy speciális készülékkel veszi az ugrókódos távirányító által adott kódot, miközben rádió impulzusokkal zavarja az autó vételét. Mivel a gépjármű tulajdonosnak egy gombnyomásra nem sikerült élesítenie a riasztót, ezért még egyszer megnyomja a gombot. A zavaró eszköz ekkor veszi a második kódot is (közben ismét zavarva az autót a vételben), de rögtön ezt követően visszajátssza az először kapott kódot, így a gépjárművédelmi rendszer élesedik. A gépjármű tulajdonos távozása után pedig a tolvaj a készülékkel lejátszhatja a másodszorra kapott kódot, mellyel a gépjárművédelmi rendszer hatástalanodik. Ijesztő módon ez a speciális hacker eszköz is alacsony áron kapható kereskedelmi forgalomban, és használata nem igényel szaktudást. A jel ismétlés azonban megakadályozható

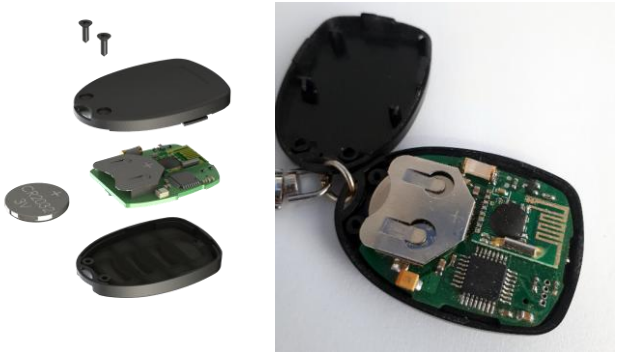
kétirányú kommunikáció esetén úgy, ha az autó először titkosított időt tartalmazó kódot küld a távirányítónak, melyet a távirányító további titkosítás után visszaküld az autónak. A kommunikációban ekkor titkosítva szerepel a másodperc pontos időpont, így a jel nem visszajátszható és nem is módosítható.

Bár a rádiós kapcsolatok zavarása nehezíthető, de teljesen nem megakadályozható. A fentebb bemutatott nagy teljesítményű RF jammer eszköz mindenképpen blokkolja egy gombelemmel működő távirányító kommunikációját, ezért olyan helyen alkalmazható az RF kommunikáció, ahol a kapcsolat megszakadása nem okozhat biztonsági problémát. Például egy autó távirányító esetén a zavarással csak annyit érhetne el a tolvaj, hogy a tulajdonos sem lenne képes elindítani az autót, de nem lenne képes hatástalanítani a riasztót.

C. Többcsatornás vezeték nélküli kommunikáció

A rádiójeleket nem szándékosan is zavarják más rádiófrekvenciás eszközök. A zavarást csatornaváltással lehetséges kiküszöbölni, így olyan rádiós modulok alkalmazhatók, amelyek sok eltérő frekvenciájú, beállítható csatornán képesek adni és venni. Az eltérő kommunikációs csomópontok, un. node-ok pedig azonos időtől függő algoritmus szerint váltanak csatornát, ha elveszítik a kommunikációt a többi node-al. Ezzel a megoldással széles frekvenciasávon lehetséges a kommunikáció, aminek a zavarása és lehallgatása is nehezebb feladat. Az algoritmikus frekvencia váltás legnagyobb előnye továbbá, hogy a kulcsnélküli autóknál használt jelismétlők ellen védelmet jelent.

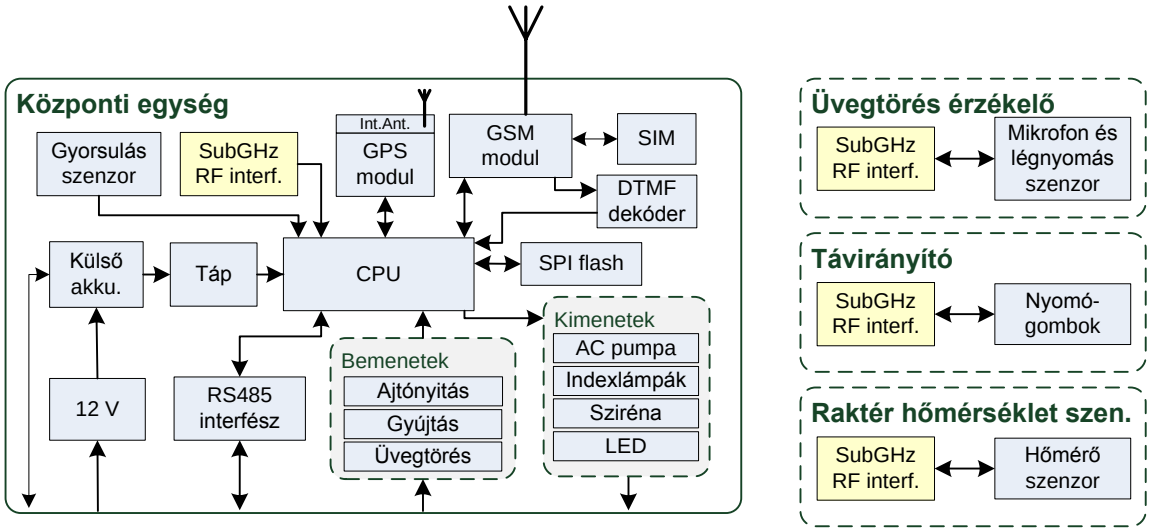
A fejlesztés során, egy 72 csatornán RF kommunikációs modult választottuk, amely elég kisméretű ahhoz, hogy egy kézi távirányítóban is elférjen. Az elkészült távirányító 3D modellje és fényképe a 4. ábrán látható.



4. ábra Többcsatornás vezeték nélküli kommunikációt megvalósító távirányító

Az áramkörön található az RF modul mellett egy processzor és egy speciális, rezgésérzékelő szenzor is. Utóbbi szerepe, hogy az egyébként folyamatosan kommunikáló távirányító elalszik nyugalmi állapotban. Ezzel növelve a biztonságot, mert egy szögre akasztott kulcs egyáltalán nem kommunikál. Ha viszont a járműtulajdonos zsebében van, akkor kommunikációra készen áll az autóval, meghagyva a kulcs nélküli nyitás kényelmét.

Az autóban található többi különálló egység, mint a központi egység, a különálló üvegtörés érzékelő vagy a raktérhőmérséklet szenzor is felszerelhető a rádiós modullal, melynek révén könnyen beszerelhetővé válik a berendezés. A központi egység és a hozzá rádiós interfészen kapcsolódó modulok blokkdiagramja az 5. ábrán látható.



5. ábra A gépjárművédelmi berendezés központi egysége és a hozzá kapcsolódó modulok

A központi egység mozgatórugója egy 16-bites RISC utasításkészletű processzor, mely kapcsolatban van minden belső egységgel, mint a GSM kommunikációért felelős modullal vagy a GPS-el.

A központi egységben található egy gyorsulásszenzor, mely az autó megemelését érzékeli. A szenzor jele idővel és hőmérsékletingadozással folyamatosan kúszik, e miatt a viszonyítási pontot egy erősebb rekurzív szűrő adja, amelyet

egy kisebb ablakú mozgó átlag szűrő értékéhez hasonlít a processzor, kiszűrve a pillanatnyi rezgéseket.

A GSM modul jelfeldolgozásában szerepet játszik egy un. DTMF dekóder, amely a telefonálás közben lenyomott gombok eltérő frekvencián sípoló hangjából állapítja meg, hogy a felhasználó mely gombot nyomta le a telefonos menürendszer kezelése közben.

A processzorhoz kapcsolódik egy SPI interfészen kommunikáló külső flash memória, melyben a kapcsolat megszakadása esetén két napi útvonal információ is megőrizhető, így a GPRS kommunikáció helyreállása után folyamatos nyomvonal látható a térképen.

A készülék energia menedzsment része támogatja másodlagos akkumulátor bekötését is, amely táppal látja el a védelmi berendezést az autó fő akkumulátorának kiszerelése esetén is.

A kommunikációs interfészek közt helyet kapott egy RS485 busz, amelyre csatlakoztatható sofőrazonosításra használt RFID olvasó. A bementek érzékelik az ajtó-, gépháztető-, és csomagtér nyitását, a gyújtás ráadását, és harmadik forrásból származó egyéb szenzorok jeleit, mint például ultrahangos mozgásérzékelő.

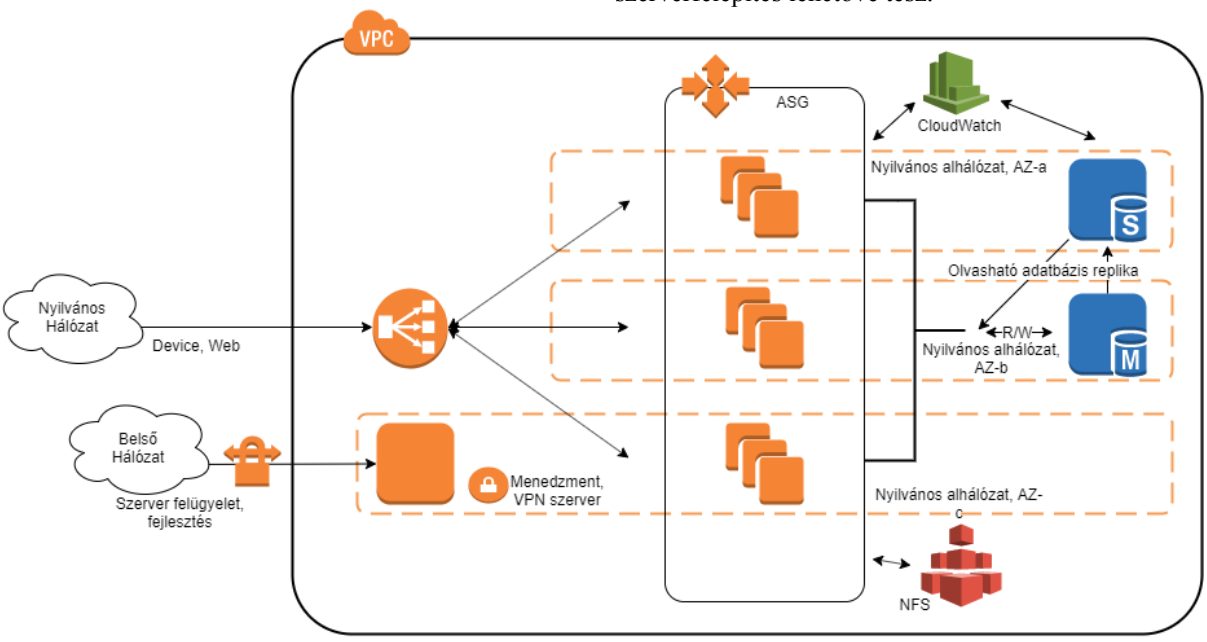
A kimenetek kezelik a gépjármű irányjelzőit, a motor működésének megszakításához az üzemanyag-szivattyút (köznapi nevén AC pumpát), egy szirénét, valamint egy visszajelző LED-et, ami informál a berendezés élesített állapotáról.

III. Felhő alapú GPS-GSM szerverszolgáltatások biztonsága

Az RF jammer-rel blokkolt kommunikáció esetén az egyetlen lehetőség, ha szerverek észlelik a megszakadt kommunikációt és értesítik az ügyfelet, így az ügyfélnek van lehetősége a gépjárművét ellenőrizni még mielőtt a tolvaj a riasztó felderítést és kiszerelést elvégezhetné, mely időigényes folyamat. Ebben az esetben kulcs fontosságú, hogy a szerverek teljes megbízhatósággal működjenek, amikor a lopási kísérlet történik.

Tradicionális szerver felépítés (monolitikus szerver architektúra) esetén a szoftverek egyetlen szervergépen futnak. Megbízhatóbb szerverek esetén a szerver egy adatcenterben van, ahol az áram és internet ellátás viszonylag biztonságos, mégis a szoftver frissítések, router konfiguráció módosítások, esetleges hardver problémák időszakosan elérhetetlenné teszik a szervert.

Felhő alapú rendszerek esetén a feldolgozás több virtuális gépen történhet párhuzamosan [6]. A virtuális gépek fizikailag is különböző adatcenterekben vannak, egymástól távol. Az adatok 5-8 merevlemezen tárolódnak, fizikailag is több helyen. Ilyen rendszerben a szoftver frissítések virtuális szerverenként egyenként elvégezhetőek, míg a többi szerver a rendszer szüneteltetése nélkül végzi a feladatát. Így a hardver problémákból és frissítésekből adódó szolgáltatás kiesések ideje egy megfelelően felépített felhő alapú szerver megoldás esetén töredéke ahhoz, mint amit egy hagyományos szerverfelépítés lehetővé tesz.



6. ábra Geo-redundáns IoT rendszer egyszerűsített blokk diagrammja.

A 6. ábrán láthatóak az informatikai rendszer egyenként is redundáns építőelemei. Az eszközök és weboldal felöl érkező adatokat Load Balancer továbbítja automatikusan skálázódó virtuális szerverek felé. Az elosztott szerverek között a tárolást hálózati meghajtó biztosítja. Az adatbázis rendelkezik egy replikával is, mely az adatbázis szerver hibája esetén automatikusan átveszi a szerepét. Ilyen esetben automatikusan egy újabb replika indul a redundancia visszaállítására.

IV. Összefoglaló

A gépjárművédelmi rendszerek fejlesztése kapcsán feltártuk a gépjárművek feltörésének és elindításának gyakori módjait, majd ezeket figyelembe véve választottuk meg a konstrukciós megoldásokat. Bemutattunk egy több csatornát és banki szintű titkosítást alkalmazó rádiós kommunikációt, amely védelmet jelent a jelismétlővel történő autólopások ellen. A kifejlesztett nagy biztonságú, felhő alapú szerverinfrastruktúra hatékony védelmet jelent a jelzavaróval történő autólopások ellen. Az informatikai rendszer több mint húszezer jármű követése mellett teljesíti az e-útdíj rendszer szigorú SLA és IT biztonsági auditok követelményeit.

Köszönetnyilvánítás

A fejlesztés a VEKOP 2.1.7-15-2016-00626 számú pályázat finanszírozásával valósult meg. A projekt az Európai Unió támogatásával valósult meg.

Irodalomjegyzék

[1] Turbodecoder honlapja: https://turbodecoder.com/turbo-decoder-locksmith-tools-car-unlocking-picking/

[2] VIN to PIN adatbázis honlap: https://www.weboctopus.nl/ipc/vin2pin.php

[3] Daniel S. Fowler, „Keyless Entry Theft with Range Extender Devices”, TekEye, 2017.11.28. https://tekeye.uk/automotive/cyber-security/keyless-entry-theft-with-range-extender

[4] Lisa Vaas, „RFID repeater used to steal Mercedes with keys locked inside a house”, Naked Security, 2019.12.01, https://nakedsecurity.sophos.com/2017/12/01/rfid-repeater-used-to-steal-mercedes-with-keys-locked-inside-a-house/

[5] Samy Kamkar, defcon-23, https://www.rtl-sdr.com/bypassing-rolling-code-systems-codegrabbing-rolljam/

[6] Jeff Barr, Attila Narin, and Jinesh Varia, „Building Fault-Tolerant Applications on AWS”, https://d0.awsstatic.com/whitepapers/aws-building-fault-tolerant-applications.pdf