Ványa László

A MŰHOLDAS HELYMEGHATÁROZÓ RENDSZEREK ELEKTRONIKAI HADVISELÉSI KÉRDÉSEI

A globális műholdas helymeghatározó rendszerek mind járműbe épített, mind kézi hordozható vevőkészülékei ki vannak téve az elektronikai zavarásnak (a műholdas jelek teljesítményben való elnyomásának) és a spoofing technikának (amikor a vevőkészülék helytelen pozíciót számít ki a zavarás miatt). Jelen írás célja, hogy áttekintse az elektronikai hadviselés három fő területét a globális helymeghatározó rendszerek szempontjából. A cikk bemutat néhány eljárást a műholdas helymeghatározó rendszerek elleni fenyegetésre, majd néhány eszközt és eljárást a támadásuk detektálására és védelmükre.

Kulcsszavak: *Műholdas navigációs rendszerek, zavarás, spoofing, elektronikai hadviselés, GPS szimulátor*

BEVEZETÉS

Az elektronikai hadviselés célpontjai között mindig is jelentős helyet foglaltak el a navigációs célú berendezések. A fizikai pusztítás mellett speciálisan erre a célra épített zavaró berendezések alkalmazásával lehetővé vált a szofisztikált zavarás létrehozása, amely működése nem nyilvánvaló azonnal, hiszen nem az a cél, hogy látványosan megszűnjön a szolgáltatás, hanem az, hogy hihetően megtévessze a kezelőt, meghamisítsa a mérési adatokat, meghiúsítsa a feladat végrehajtását, vagy olyan mértékű pontatlanságot vigyen bele, amely jelentősen csökkenti az elvárt eredményt.

Ilyen speciálisan erre a célra kifejlesztett berendezés volt a TACAN harcászati légi navigációs rendszer ellen épített R-388 típusú orosz gyártmányú zavaró állomás (NATO kód: STOVE PIPE), amelyről egy korábbi cikkben részletesen esett szó [1]. Ugyancsak ebben az írásban található néhány olyan zavaró berendezés, amely a napjainkban rendkívül széles körben elterjedt globális műholdas helymeghatározó rendszereket (Global Positioning Systems - GPS) vagy más használatos elnevezéssel, a GNSS – Global Navigation Satellite Systems – globális műholdas navigációs rendszereket képesek zavarni, a jelfeldolgozásban őket akadályozni, így meghiúsítani a rájuk épülő szolgáltatásokat.

Jelen írás az elektronikai hadviselés hagyományos hármas felosztása szerint tárgyalja a műholdas helymeghatározó (navigációs) rendszerek kérdését. Külön megvizsgáljuk az elektronikai megfigyelés (Electronic Surveillance – ES), az elektronikai támadás (Electronic Attack – EA) és az elektronikai védelem (Electronic Defence – ED)[1] releváns vonatkozásait a teljesség igénye nélkül, néhány példán keresztül.

[1] A felosztás megnevezései az érvényben lévő Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína 2. kiadás szerinti felosztásnak felelnek meg. [2]

A MŰHOLDAS NAVIGÁCIÓS RENDSZEREK ÉS AZ ELEKTRONIKAI MEGFIGYELÉS

Talán furcsának tűnhetne, ha azt mondanánk, hogy mivel a globális műholdas navigációs rendszerek nemzetközileg szabványosított, pontosan ismert és védett frekvenciákon dolgoznak, nincs mit megfigyelni rajtuk. Ez a kijelentés első közelítésben, például az ellátottsági mérések, a szolgáltatás folytonossági vizsgálatok kivételével helytálló is lenne. Az elektronikai megfigyelésnek esetükben azonban más lesz a célja. Mégpedig az, hogy a rendszereket érő interferenciákat, szándékos zavartatásokat észleljük több okból is.

Az egyik oldalról a hagyományos polgári zavarkivizsgálási, zavarelhárítási tevékenységek során az egyes nemzetek erre hivatott szervezetei[2] hivatalból kell, hogy keressék az ilyen zavarforrásokat és tegyék meg a szükséges lépéseket a zavartatás megszüntetése érdekében. A másik oldal a katonai, nemzetbiztonsági, esetleg terror elhárítási célú zavarforrás felkutatás, amely a katonai műveletek során, vagy még békeidőszakban kutatja a zavarok forrásait, hiszen a repülésbiztonság, a navigációs eszközökre épülő rendkívül sokféle szolgáltatás üzemének a fenntartása biztonsági probléma. Az [1] írásban példaként bemutatott olcsón beszerezhető eszközök és a katonai kivitelű zavaró berendezések a szolgáltatások leállását képesek elérni, ezt a hatást a kezelők közvetlenül észlelik is, okát azonban saját eszközeikkel nem tudják megállapítani.

Az ilyen „nyers erővel”, működő eszközök detektálására, majd a pozícióik bemérésére speciális eszközök szükségesek. Ezeket interferencia detektoroknak nevezik. Az 1. képen egy Spirent[3] gyártmányú eszköz látható.

1. kép Spirent GSS100D GPS/GNSS interferencia detektor [3]

Működése során folyamatosan monitorozza a GPS/GNSS rendszerek frekvenciasávjait. Idegen, zavaró jelek megjelenésekor azokat rögzíti, osztályozza és lehetővé teszi, hogy későbbi vizsgálatok során azokat laborkörülmények között újra elő lehessen állítani további elemzésre. Az eszközzel rendelkező jogosult felhasználók számára e-mail formában üzenetet küld zavarforrások észleléséről és a korábbi mérési eredményeket központi adatbázisban tárolva, hozzáférést biztosít

[2] Magyarországon a Nemzeti Média és Hírközlési Hatóság - NMHH
[3] A Spirent cég az Egyesült Királyságban található

számukra. Az elemzés során meg tudja különböztetni az „egyszerű” zavarokat a megtévesztő célú, ún. spoofing módszerrel üzemelő zavaró berendezések jeleitől, amely során a vevőkészülékek olyan valósnak tűnő jeleket dolgoznak fel, amelyek a kezelő számára észrevétlenül a pozícióadatokat hamisítják meg. Ezt a „spoofing detektor” üzemnek nevezik, amely csak szándékos zavarási folyamatban, speciális eljárás alkalmazásával jöhet létre [3].

A spoofing módszer lényege, hogy a valódi műholdak jeleinek megfelelő, de más pozícióadatokat eredményező jeleket sugároznak a vevőkészülékeknek, így amennyiben azok ráállnak ezen jelek feldolgozására, akkor a hamis helyadatok miatt az eredeti útvonaltervhez igyekeznek módosítani pl. a repülési irányt és letérnek az eredeti feladatról. Ha pl. a programozott leszállás helyszínét „eltolják”, akkor a leszállás a hamis adatok alapján akár a szembenálló félnek kedvező helyen is megvalósulhat. 2011. december 4-én egy RQ-170 Sentinel típusú amerikai UAV-t minden valószínűség szerint ezzel a módszerrel térített el és szállított le Irán [4][5].

Az elfojtó zavarok és a spoofing mellett van egy harmadik eljárás is, amelyet „meaconing”-nak neveznek. Ennek az a lényege, hogy a valódi műholdjeleket rögzítik, majd bizonyos idő elteltével újra kisugározzák, ezzel hamisítva meg a méréseket.

Kiemelten fontos tehát a spoofing és a meaconing detektálása, hiszen a műholdas helymeghatározó rendszer mellett más navigációs eszközt is kell a fedélzeten alkalmazni, így már az is jelentős információ, ha a megtévesztés jeleinek eredményeképpen a folyamatból a műholdas helymeghatározó eszközt kizárják és másra térnek át.

Az elektronikai megfigyelés, más szóval – felderítés körébe sorolható a működő zavaró berendezések felkutatása, helyzetük meghatározása, hogy utána ki lehessen iktatni őket. A Stanford University szerzői kollektívája a GPS World folyóiratban publikált írásában egy ilyen speciálisan GNSS zavaró berendezések felkutatására tervezett eszközt mutatott be [6]. (2. kép)

2. kép. GPS zavaró berendezést kereső oktokopter [6]

A fejlesztési program neve: JAGER - Jammer Acquisition with GPS Exploration & Reconnaissance. A cél, egy repülőtér nagyságú területen működő zavarforrás mintegy 30 m-es pontossággal, 15 percen belüli megtalálása. A hordozó eszköz egy 11 kg maximális össztömegű, 1,2

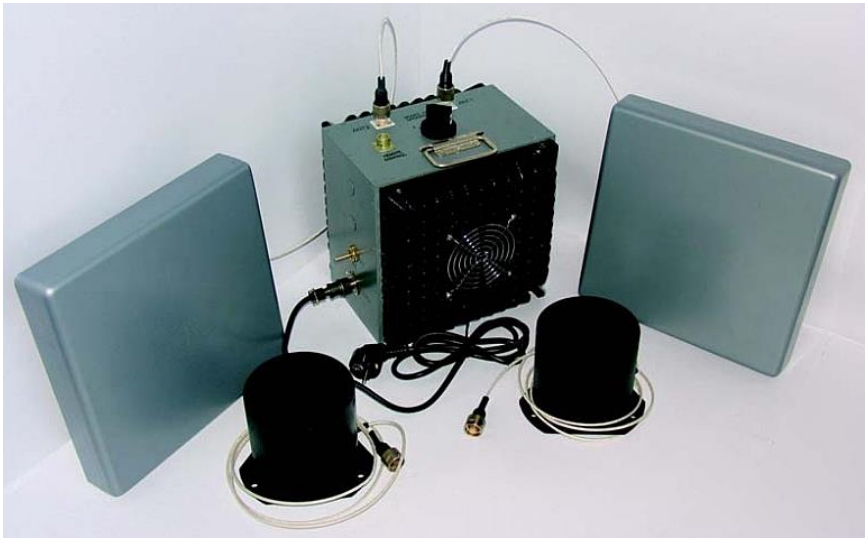
m átmérőjű oktokopter[4], amely legnagyobb sebessége eléri a 20 m/s (72 km/h) sebességet és a repülési ideje mintegy 30 min. A feladat megoldására mintegy 5 kg tömegű hasznos teher hordozására van mód.

Mivel az eszköz rendeltetése szerint a műholdas navigációs rendszert zavaró berendezés felkutatására szolgál, a tipikus alkalmazási környezetben a műholdas navigációs rendszer tehát nem használható, ezért egy speciális fedélzeti APNT (Alternative Position, Navigation and Timing – alternatív helyzet, navigáció és idő) eszköz került kifejlesztésre.

A zavaró eszköz helymeghatározására egy irányított antennával végzett maximumkeresési eljárás szolgál, amely lényege egyszerűen az, hogy a repülés során a GPS frekvenciasávjában észlelt kisugárzás jelszintje alapján az autopilot rendszer a nagyobb jelszint irányába való fordulásra ad utasítást.

A MŰHOLDAS NAVIGÁCIÓS RENDSZEREK ÉS AZ ELEKTRONIKAI TÁMADÁS

A szakirodalmi forrásokban a műholdas navigációs berendezések zavarásáról esik a legtöbb szó. A mintegy 20 000 km távolság miatt a vehető jelteljesítmény igen alacsony, ezért a földi (UAV fedélzeti) zavaró eszközök már viszonylag kis teljesítmény, néhány W mellett is hatékony, nagy hatótávolságú zavarjeleket produkálnak. A jelek kódolásának javításával, a zavarhatékonyságot sikerült is csökkenteniük a fejlesztőknek, de még így is igen sérülékenyek a vevőkészülékek, különösen azok a polgári eszközök, amelyek nem rendelkeznek speciális védelmi algoritmusokkal. Példaképpen a 3. képen látható egy orosz gyártmányú, nagyteljesítményű, mobil eszközbe építhető zavaró berendezés.



3. kép A orosz Aviakonversiya GNSS zavaró berendezése [7]

Ezeket az eszközöket alkalmazták például a 2003-as iraki hadműveletekben az ún. intelligens bombák (US JDAMS) és más GPS-t alkalmazó rendszerek ellen. A nagyteljesítményű változat

[4] Nyolc légcsavaros, helyből felszállni képes repülő eszköz.

20 W teljesítmény mellett mintegy 150 km, a kisteljesítményű változat 2–3 W teljesítménnyel mintegy 50 km zavarási zónát biztosít. A védelmi eljárások, mint a CRPA antenna, vagy az aktív nullázásos technikák hatékonyan csökkentik a zavarás hatótávolságát [7].

Rendszeresnek mondható a Dél-koreai – amerikai gyakorlatok, repülések navigációs eszközeinek zavarása Észak-Koreából, ahogy erről a világsajtó is rendszeresen beszámol [8].

Anélkül, hogy további ilyen „brute force" zavaróeszközöket sorolnánk, a továbbiakban egy talán továbbgondolásra alkalmas lehetőségről essen szó. A LabSat cég által épített GPS szimulátor (4. kép) lehetséges alkalmazásain lenne érdemes elgondolkodni.

4. kép A LabSat GPS Simulator készüléke [9]

A készülék eredetileg a GPS, GLONASS, BEIDOU és GALILEO rendszerek jeleinek elektronikus rögzítésére, tárolására és később valós, navigációs rádiófrekvenciás jelek formájában való lejátszására készült. A navigációs jelek felvételekor lehetőség van videofelvételek rögzítésére, amelyek később visszajátszhatók, és a haladás sebességének függvényében adja a műholdak navigációs jeleit is. Ezeket a szolgáltatásokat járműfejlesztőknek, jármű navigációs szoftverek készítőinek dolgozták ki, mert sokkal költséghatékonyabban és kényelmesebben megoldható a program írása laboratóriumi körülmények között, mint az úton haladó gépkocsiban.

Érdemes lenne részletesebb vizsgálat alá vetni az ilyen képességű, szolgáltatású berendezéseket, mert egyrészt ezekre építve új működési elvű elektronikai hadviselési berendezések fejleszthetők, másrészt a lehetőségek feltérképezése közelebb vihet a hasonló működési elvű berendezések elleni védelemhez, ami jelentősen csökkenthetné a védelem folyamatos lemaradását a támadó technikákhoz képest.

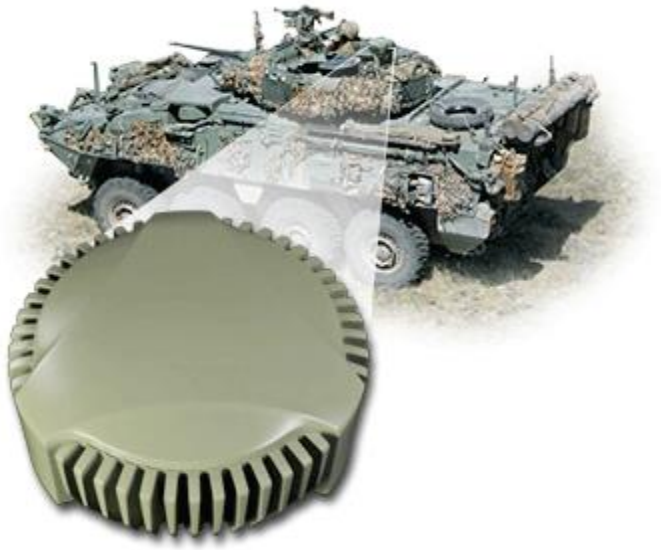
A MŰHOLDAS NAVIGÁCIÓS RENDSZEREK ÉS AZ ELEKTRONIKAI VÉDELEM

Az elektronikai megfigyeléssel foglalkozó részben már érintettük, hogy a saját navigációs eszközök védelme érdekében lehetséges a zavarok műszeres észlelése és akár a kezelők figyelemfelhívása, akár a működtető programokba való rutinok beépítése, amikor is ezekre a zavarokra való reakcióképpen megváltoztatják pl. a működtető programok algoritmusait.

A továbbiakban először olyan eszközökről lesz szó, amelyeket pl. harcjárművekre lehet telepíteni és valamilyen speciális megoldással támogatják a zavarás elleni védekezést. A NovAtel cég GAJT® 710ML[5] típusjelű antennája bármely járműre utólag is felszerelhető [10]. (5. kép) Főbb jellemzői:

[5] GAJT – GPS Anti Jam Technology ® NovAtel védett márkaneve

1. 7 antenna elemmel 6 független nullirányt hozhat létre;
2. a GPS L1, L2 frekvenciákon egyidőben működik;
3. M-kód előkészített;
4. egyszerű telepíthetőség;
5. bármely GPS vevőhöz vagy jármű navigációs eszközhöz kompatibilis;
6. méretei: átmérő – 290 mm, magasság – 120 mm, tömeg – 7,5 kg.



5. kép NovAtel GAJT® 710ML antennarendszere [10]

Működésének lényege az, hogy az antennaelemek jeleit a fázisvezérelt rácsantennákhoz hasonlóan komplex erősítőtagokon keresztül vezetjük a jelösszegzőre, amivel egyrészről az antenna karakterisztikája változtatható, másrészről ezt kihasználva, az iránykarakterisztika egyes irányaiba minimumhelyek, nullahelyek hozhatók létre. Ez teszi lehetővé, hogy a zavaró jelforrásokat kiszűrjék. A zavarszűrés mértéke eléri a 40 dB-t.

Természetes, hogy a kézi hordozható navigációs vevőkészülékek, vagy akár a kisméretű automatizált járművek esetén ilyen megoldások nem alkalmazhatók. A katonai célú és a P/Y kódot is alkalmazó vevőkészülékek a polgári eszközöknél védettebbek, ugyanakkor a spoofing, vagy akár a meaconing ellen így sem biztosítható a teljes védelem. Más megoldásokat kell tehát keresni.

A Vulnerability Assessment Team, Los Alamos National Laboratory által publikált [11] módszerek egyfajta statisztikai megfigyelésen alapulnak, amelyek lényege az, hogy a vevőkészülékek a tipikusan alacsony teljesítményű – mintegy –160 dBW jelszintű jelekhez képest a zavaró berendezésektől jelentősen nagyobb jeleket vesznek. Már ez önmagában is figyelmeztethet a zavarásra. Ha a valós műholdjeleket egymással összevetjük, azt tapasztalhatjuk, hogy a vett jelszintek eltérőek, amíg a hamis jelek forrásától származó „műholdjelek” pontosan azonos szintűek.

Bonyolultabb, de nem megoldhatatlan az az eljárás sem, hogy a műholdak konstellációjának szabályossága alapján a pillanatnyi vett műhold azonosítókat összevetik az elvárt azonosítókkal és a zavarás során megváltozó, megjelenő „idegen” műholdak jelenléte riaszthatja a kezelőket.

A műhold szimulátorok további gyengesége, hogy az egyes hamis „műholdak” közötti időparaméterek felismerhetően eltérnek a valódi időzítési adatoktól, így megkülönböztethetővé válnak a spoofing adó jelei.

További kiegészítő módszer lehet az, hogy az adott jármű haladását regisztráló más rendszer adataival folyamatosan összevetésre kerülnek a GPS által szolgáltatott adatok és amennyiben egyszer csak jelentős eltérés, kiugró különbség jelentkezik az előre kalkulált és a GPS-től kapott adatok között, akkor az ismét riasztást válthat ki.

BEFEJEZÉS

A műholdas helymeghatározó rendszerekre épülő infrastruktúrák folyamatosan bővülnek, a képességeikre alapozott szolgáltatások egyre szélesebb körbe, egyre olcsóbb eszközökbe kerülnek beépítésre. Ez a ma már alapvetően megbízhatónak minősülő technikai vívmány azonban mind a rossz szándékú szolgáltatás megszakításos támadásoknak, mind a hamisításoknak ki van téve és ezek technikai megvalósítása sem igényel jelentős erőforrásokat. Ezért fontos annak ismerete, hogy milyen módszerek, eljárások és eszközök milyen problémák előidézésére alkalmasak, illetve, hogy milyen lehetőségek vannak azok jelzésére, hatásuk csökkentésére vagy akár megszüntetésére.

Véleményem szerint néhány éven belül a forgalomba kerülő GNSS eszközök alapszolgáltatása lesz a zavartatás indikálása, a kezelők figyelmének felhívása a jelek hamisításának észlelésére, a műholdak konstellációjában észlelt eltérések kijelzése. A beépített algoritmusok és tesztek jóval szofisztikáltabb értesítéseket fognak adni, mint a mai*: „A műholdak vétele megszűnt!”* üzenet. *„Újratervezés!”*

FELHASZNÁLT IRODALOM

[1] VÁNYA LÁSZLÓ: Navigációs berendezések zavarása és megtévesztése. Repüléstudományi Közlemények, Szolnok, XXVII. évf. 2015. 2. szám, pp. 7-16. (online) url: http://www.repulestudomany.hu/folyoirat/2015_2/2015-2-01-0189-Vanya_Laszlo.pdf

[2] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína 2. kiadás. A Magyar Honvédség kiadványa 2014.

[3] Detecting and Protecting Against GPS Cyberthreats. (online) url: http://www.spirent.com/Assets/WP/WP-Detecting-Protecting-Against-GPS-Cyberthreats (2016.03.11.)

[4] VÁNYA LÁSZLÓ: Kérdések és válaszok a szupertitkos RQ-170 iráni kézre kerüléséről. Repüléstudományi Közlemények, Szolnok, 24:(2) pp. 634-641. (2012) (online) url: http://www.repulestudomany.hu/kulonszamok/2012_cikkek/52_Vanya_Laszlo.pdf (2016.03.11.)

[5] WIKIPEDIA THE FREE ENCYCLOPEDIA: Iran–U.S. RQ-170 incident. (online), url: https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident (2016.03.11.)

[6] JAMES SPICER, ADRIEN PERKINS, LOUIS DRESSEL, MARK JAMES, YU-HSUAN CHEN, SHERMAN LO , DAVID S. DE LORENZO, PER ENGE: Jammer hunting with UAV. (online): http://gpsworld.com/jammer-hunting-with-a-uav/ (2016.03.11.)

[7] DR. CARLO KOPP: Air Defence System Defensive Aids. Technical Report APA-TR-2009-0604. (online) url: http://www.ausairpower.net/APA-SAM-DefAids.html#mozTocId158380 (2016.03.11.)

[8] GPS World staff: Massive GPS Jamming Attack by North Korea. (online) url: http://gpsworld.com/massive-gps-jamming-attack-by-north-korea/ (2016.03.11.)

[9] LABSAT 3 GPS SIMULATOR (online) url: http://www.labsat.co.uk/index.php/en/products/labsat-3

[10] GAJT® 710ML (online) url: http://www.novatel.com/products/gnss-antennas/gajt-anti-jam-antennas/gajt/ (2016.03.15.)

[11] JON S. WARNER, ROGER G. JOHNSTON: GPS Spoofing Countermeasures. (online) url: http://perma-link.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-6163 (2016.03.11.)

ELECTRONIC WARFARE ASPECTS OF SATELLITE NAVIGATION SYSTEMS

The Global Navigation Satellite Systems – GNSS vehicle mounted and handheld receivers are vulnerable to jamming (overpowering GNSS signals) and spoofing (making GNSS receivers to calculate false position). The main aim of this article to overview three parts of electronic warfare in terms of global satellite navigation systems. This article outlines some methods of the threats to GNSS and presents some methods and devices for detection of jamming and defence GNSS systems.

Keywords: *GNSS, jamming, spoofing, electronic warfare, GPS simulator*

Dr. VÁNYA László (PhD)	Dr. VÁNYA László (PhD)
egyetemi docens	Associate professor
Nemzeti Közszolgálati Egyetem	National University of Public Service
Hadtudományi és Honvédtisztképző Kar	Faculty of Military Science and Officer Training
Katonai Üzemeltető Intézet	Institute of Military Maintenance
Elektronikai Hadviselés Tanszék	Department of Electronic Warfare
vanya.laszlo@uni-nke.hu	vanya.laszlo@uni-nke.hu
orcid.org/0000-0001-5472-7190	orcid.org/0000-0001-5472-7190

http://www.repulestudomany.hu/folyoirat/2016_2/2016-2-09-0308_Vanya_Laszlo.pdf