HADMÉRNÖK
VÉDELMI ELEKTRONIKA, INFORMATIKA, KOMMUNIKÁCIÓ

14. évfolyam (2019) 3. szám 101–111.
DOI: 10.32567/hm.2019.3.9

Károly Krisztián[1]

LoRaWAN-technológia felhasználási lehetőségei a katonai alkalmazások tükrében

Application Opportunities of LoRaWAN in the Point of Military Deploying

Napjaink automatizálási trendjeinek köszönhetően előtérbe kerültek az emberi beavatkozást nem igénylő, úgynevezett gép-gép kommunikációt (M2M) lebonyolító távközlési megoldások. Ilyen kommunikációs eljárás a LoRaWAN-technológia is, amely Chirp moduláció segítségével képes csillag topológiájú hálózatokba szervezni szenzorainkat, akár viszonylag nagyobb területek lefedése mellett is.
Kutatásomban a LoRaWAN-technológia katonai felhasználási lehetőségeit vizsgálom. Feltárom a technológia katonai szempontból előnyös tulajdonságait, valamint az alkalmazhatóság korlátait.

Kulcsszavak: LoRaWAN, LPWAN, szenzor, Chirp

Gratitude to today's automation trends the machine to machine (M2M) technologies came into the scene. Based on their specified characteristics they do not require any human intervention. The LoRaWAN technology is one of them and it is based on Chirp modulation. It is able to organise and re-organise the applied sensors into star topology network covering wide operational areas.
My intention is to present the most likely courses of actions of LoRaWAN's military applications pointing out the advantages and disadvantages with focus on the military deployability.

Keywords: LoRaWAN, LPWAN, sensor, Chirp

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: krisztian.karoly@mil.hu, ORCID: https://orcid.org/0000-0002-5835-7980

Bevezetés

Napjainkban robbanásszerű növekedést figyelhetünk meg az IoT[2]-alapú megoldások területén. Az ezeket kiszolgáló eszközök képesek emberi beavatkozás nélkül, akár nagyméretű hálózatokba integráltan kommunikálni egymással, ezáltal megvalósítva a gép – gép (M2M[3]) interakciót. Az Ericsson vállalat elemzése alapján [1: 16.] 2017-ben 7,5 milliárd db mobiltelefon és 1,6 milliárd db PC/laptop/tablet volt használatban, míg 2022-re várhatóan az előbbiek száma 8,6 milliárd db-ra, az utóbbiaké pedig 1,7 milliárd db-ra növekszik majd. Eközben 2017-ben a nagy területet lefedő hálózatokba (WAN[4]) szervezett IoT-eszközök száma 0,8 milliárd db (ebből 0,7 milliárd mobilhálózati), míg a rövid hatótávolságú hálózatokba szervezett IoT-eszközök száma 6,2 milliárd db volt. Ezeken a területeken 2023-ra 17–30%-os éves növekedést prognosztizálnak, azaz addigra várhatóan a WAN-hálózatokba szervezett IoT-eszközök száma eléri majd a 4,1 milliárd db-ot (ebből 3,5 milliárd mobilhálózati), a rövid hatótávolságú hálózatokba szervezett IoT-eszközök száma pedig 15,7 milliárd db-ra növekszik. Az előrejelzések alapján megállapítható tehát, hogy 2023-ra várhatóan közel kétszer annyi IoT-eszköz lesz használatban, mint telefon vagy számítógép.

Természetesen a hálózatba integrált infokommunikációs eszközök piacának ilyen irányú átrendeződése a katonai szektorra is hatással lehet. Az autonóm szenzorhálózatok alkalmazása révén rövid idő alatt, nagy mennyiségű adatot csatornázhatunk be különböző rendszereinkbe, amelyekből célszoftverek segítségével olyan információkat nyerhetünk ki, amelyek nagyban képesek támogatni a parancsnokokat és törzseiket a minél reálisabb helyzetismeret (SA[5]) kialakításában. Mindez a vezetési fölény jelenleginél lényegesen rövidebb idő alatt történő kivívásának lehetőségét hordozhatja magában.

A rövid hatótávolságú IoT-hálózatok kommunikációs protokolljai közé tartozik az IEEE 802.15.1 Bluetooth [2], az IEEE 802.15.4 ZigBee [3], és ezen IoT-hálózatokat támogatja az IEEE 802.11 Wifi [4] szabvány is. A Bluetooth és Wifi technológiák köztudottan széles körű szakirodalommal rendelkeznek, a Zigbee technológia katonai alkalmazhatóságával kapcsolatban egy korábbi publikációmban foglalkoztam [5]. A nagy területeket lefedő IoT-hálózatok terén kiemelkedők az LPWAN[6]-megoldások [6], amelyeket kritikus energiaigényű szenzorhálózatoknál érdemes alkalmazni, és alacsony adatrátát biztosítanak. Mint azt az előbb említett Ericsson-felmérésből is láthattuk, a legnagyobb darabszámú fejlődést a mobilhálózati megoldásoktól várhatjuk, ilyen az NB-IoT[7] is [6: 10–14.]. E technológia alkalmazásának kritérium-feltétele a 3G/4G/5G mobilhálózati lefedettség, amely a katonai műveletek során számos esetben nem biztosítható. További LPWAN-technológiák a LoRaWAN[8], a Sigfox, Wi-SUN Alliance FAN[9] technológiák [6], amelyek közül a LoRaWAN kommunikációs eljárást vizsgálom

[2] Internet of Things – dolgok internete.
[3] Machine to machnine – gép és gép közötti kommunikáció.
[4] Wide Area Network – nagy kiterjedésű hálózat.
[5] Situational Awareness – helyzetismeret.
[6] Low-Power Wide Area Network – alacsony energiaigényű nagykiterjedésű hálózat.
[7] Narrow-Band IoT – keskeny sávú IoT kommunikációs protokoll.
[8] Long Range Wide Area Network – nagy hatótávolságú és nagy területet lefedő hálózat.
[9] Field Area Network – földfelszíni hálózat.

a katonai alkalmazhatóság szempontjából számos előnyös tulajdonsága miatt, többek között az önálló infrastruktúra lehetősége, és Chirp modulációs eljárás miatt.

Fontos megemlíteni, hogy a LoRaWAN-technológiát többek között már sikerrel alkalmazták környezetbiztonsági, klímaváltozási kutatások során [7], ahol nagy kiterjedésű telekommunikációs infrastruktúra nélküli területeket fedtek le. E példa mentén érdekes lehet a LoRaWAN alkalmazásának megvizsgálása a Nemzeti Közszolgálati Egyetem egyéb kutatási területein is, mint például a klímaváltozás hazai hatásainak nyomon követése során, például a csapadékmennyiségek és intenzitások tekintetében [8], [9], [10], [11].

Kutatási célkitűzésem a LoRaWAN-technológia katonai alkalmazhatóságának behatárolása, az esetleges korlátok feltárása, és ezekre megoldási javaslatok megfogalmazása.

A LoRaWAN-technológia

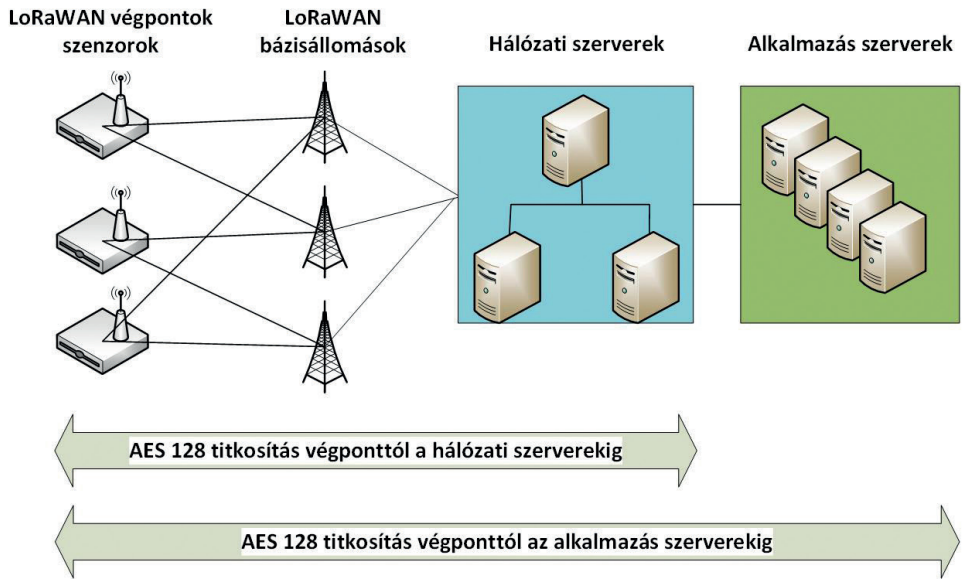
A Semtech cég fejlesztette ki [12] eredetileg a LoRa[10]-technológia alapjait, amely az OSI[11]-modell szerinti fizikai- (L1[12]) és adatkapcsolati rétegbeli (L2[13]) ajánlásokat fogalmaz meg. A technológia fizikai rétegbeli specifikációit szokás még LoRaPHY-ként is emlegetni. A LoRaWAN-protokollkészlet már a LoRa-végpontok (node-ok) hálózatszervezési kérdéseivel foglalkozik, adatkapcsolati- (L2) és hálózati rétegbeli (L3[14]) definíciókat rögzít, ugyanakkor szűkíti a fizikai réteg egyes paramétereit. Jó példa erre, hogy LoRaWAN alkalmazása esetén 125 kHz, 250 kHz és 500 kHz-es sávszélességű csatornákkal tervezhetünk, míg az eredeti LoRa esetén lehetőség van akár 25 kHz-es csatornák kialakítására is. A LoRaWAN szigorúbb szabályozási keretei annak a gyakorlati felismerésnek köszönhetők, hogy a kisebb sávszélesség sokkal pontosabb oszcillátorokat követel meg a végpontoknál, amelyek aránytalanul megdrágítanák ezen node-ok előállítási költségeit [13], [14], [15]. További különbség, hogy LoRa-kapcsolat alatt többségében pont-pont összeköttetéseket értünk, míg LoRaWAN esetében csillagtopológiájú hálózatokról beszélhetünk.

A LoRa Európában a 868 Mhz-es rádióengedély nélkül használható ISM[15]-sávban működik, 25 mW maximális adóteljesítmény mellett 0,1–1% adáskitöltési tényezővel. A LoRa-technológia fizikai rétegét tekintve, úgynevezett „LoRa modulációt" alkalmaz, amely egy speciálisan kialakított Chirp szórt spektrumú (CSS[16]) modulációs technika. A szinuszos hullámformájú jelet lineáris frekvenciamodulációval (LFM[17]) modulálják, amely a Chirp-jelet eredményezi. Ennek a modulációnak köszönhetően rövid idő alatt, keskeny sávszélességen, minimális energiafelhasználás mellett vihetők át a továbbításra szánt adatok. Ez az eljárás olyan szenzorhálózati megoldásoknak kedvez, ahol a szenzor

[10] Long Range – nagy hatótávolságú.
[11] Open Systems Interconnection Reference Model – nyílt rendszerek összekapcsolása referenciamodellje.
[12] Layer 1 – 1. réteg.
[13] Layer 2 – 2. réteg.
[14] Layer 3 – 3. réteg.
[15] Industrial, Scientific and Medical – ipari, tudományos és orvosi.
[16] Chirp Spread Spectrum – Chirp szórt spektrumú moduláció.
[17] Linear Frequency Modulation – lineáris frekvenciamoduláció.

teljes élettartama alatt csak minimális szintű kommunikációra van szükség, például éveken keresztül történő napi néhány alkalommal történő adatközlés esetén [13].

A Chirp-modulációnak köszönhetően –137 dBm vevőérzékenység, és –19 dB jel-zaj viszony (SNR[18]) mellett képes a kapcsolat fenntartására, amely rendkívül jó zavarállóságot biztosít a rendszernek [13]. A LoRaWAN alapvetően csillagtopológiájú hálózatok kialakítását teszi lehetővé, amelyet az 1. ábrán láthatunk.



1. ábra

LoRaWAN hálózat részei, multicsomópontú csillagtopológiába szervezve

(a szerző szerkesztése [15: 168.] alapján)

A szenzoroktól begyűjtött adatokat a LoRaWAN-végpontok a bázisállomások (átjárók) felé továbbítják, amelyek TCP/IP[19] hálózatokra csatolják ki az adatokat. A bázisállomásoktól a hálózati szervereken keresztül jutnak el az adatok az alkalmazásszerverekig. A LoRaWAN-technológia kétszintű titkosítást biztosít a rendszernek, egyrészt a végponttól AES[20] 128-cal titkosított adatfolyamon jut el az információ a hálózati szerverekig, azonban, hogy a hálózati szolgáltatásokat biztosítók ne lássanak bele a kommunikációba, a végpont-alkalmazás szerverkapcsolat is kaphat egy AES-128-as titkosítást [13], [14] (lásd 1. ábra).

A LoRaWAN-technológia kétirányú kommunikációt biztosít végpont és átjáró között. Az „A" osztályú eszközök vételi időablakai csak rövid időre vannak nyitva. Ehhez képest a „B" osztályú eszközök extra vételi időablakokat nyitnak meg a vételi periódusokban. A „C" osztályú eszközök az adásidejüket leszámítva szinte folyamatosan

[18] Signal-Noise Ratio – jel-zaj viszony.
[19] Transmission Control Protocol/Internet Protocol – átviteli vezérlő protokoll/internetprotokoll.
[20] Advanced Encryption Standard – továbbfejlesztett titkosítási szabvány.

vételen vannak, így minimálisra csökkentve a rendszer késleltetését, azonban ezzel energiafelhasználásuk lényegesen magasabb az „A" osztályú eszközökénél.

A katonai alkalmazás korlátai

A katonai felhasználás szempontjából a LoRaWAN számos kedvező tulajdonsága ellenére csak bizonyos korlátozásokkal alkalmazható.

Az első kihívás a bázisállomás-végpont klasszikus csillagtopológiájú elrendezéséből adódhat, ahol egy bázisállomáshoz kapcsolódhat több száz vagy akár ezer végpont is. Ez esetben a kritikus csomópontok működésének akadályozásával (akár pusztításával) darabjaira eshet szét a hálózat. Ez a kockázat részben kompenzálható, amennyiben a bázisállomások lefedettségi területét úgy alakítjuk ki, hogy egy végpont akár több bázisállomáshoz is képes legyen kapcsolódni. Ezt a multicsomópontú csillagtopológiás kialakítást is szemlélteti az 1. ábra.

Megítélésem szerint a másik fő kihívást az ISM-sávú frekvenciahasználat jelenti. Amint azt az afganisztáni példák is mutatták [16], a 868–869 MHz-es sávban működő például egyszerű kapu-távirányítón alapuló rádióvezérelt improvizált robbanóeszközök (RC-IED[21]), komoly biztonsági problémát jelentettek a szövetséges erőknek. Az erők megóvása érdekében a szövetséges csapatok aktív zavaró-berendezéseket (jammereket) helyeztek el többek között a járművekben, vagy háti hordozható verzióban a gyalogos kisalegységeknél. A rádiófrekvenciás erőforrások tervezése során figyelembe kell tehát venni, hogy a jelzett frekvenciasávot akár az ellenséges akár a szövetséges csapatok is alkalmazhatják, illetve zavarhatják. Az adott frekvencia ellenség általi felhasználása adott esetben nagyobb fenyegetettséget jelenthet, mint amennyi előnnyel járnak a szenzorhálózatokból nyert adatok, így egy felelős parancsnok e sáv elektronikai úton történő korlátozását rendeli el [17: 233.]. Bár korábban említettem a LoRaWAN-technológia kimagasló zavartűrő-képességét, adott alkalmazási körülmények között (például távolság- és terepviszonyok) mindenképpen mérési eredményekkel kell róla meggyőződnünk, hogy például az üzemi sávban működő aktív zavaró-berendezés, milyen mértékben korlátozza a LoRaWAN-eszközök kommunikációját, illetve a közeli térben való üzemeltetés milyen EMC[22]-problémákat okozhat. Ugyanakkor annak érdekében, hogy mégis igénybe lehessen venni egy ilyen rendszer által biztosított, előnyös tulajdonságokkal rendelkező szolgáltatásokat, egy praktikus megoldás lehet, ha a LoRaWAN működési frekvenciatartományt, olyan sávra is kiterjesztjük (vagy áthelyezzük), amelyet a későbbiekben nem szükséges korlátoznunk. (Természetesen különböző adaptív rádiófrekvenciás megoldásokkal lehetőség lenne olyan rendszerek kialakítására is, amelyek rugalmasan, autonóm módon képesek alkalmazkodni akár egy folyamatosan változó elektromágneses környezetben is, ugyanakkor ezek a megoldások lényegesen bonyolultabb hardver- és szoftvertechnikákat igényelnek, amelyek integrációja nagyságrendekkel növelné meg a fajlagos költségeket.)

[21] Radio Controlled Improvised Explosive Device.
[22] Electromagnetic Compatibility – Elektromágneses Kompatibilitás.

Kitekintésként megjegyezném, hogy a bevezetőben említett NB-IoT-technológiánál is fennáll a fenti sávhasználati korlát, mert az a mobilhálózati frekvenciákon működik, amelyet az afganisztáni példából láthatóan [16] is szintén előszeretettel alkalmazott a szembenálló fél. Így az említett kihívás várhatóan az LPWAN-technológiák döntő többségét érintheti. Azonban mivel az NB-IoT-technológia frekvenciaallokációjának megváltoztatása lényegesen nagyobb problémát jelentene (hiszen itt pont a mobilhálózatok által biztosított infrastruktúrán van a fókusz), ez egy újabb érvet jelenthet egy módosított LoRaWAN-technológia katonai alkalmazása mellett az alacsony energiaigényű szenzorhálózatok kommunikációs vonalainak biztosítása területén.

Bár elsőre merésznek tűnhet a frekvenciaallokáció megváltoztatásának gondolata, szeretnék kiemelni egy honi innovációt, amelyet a Bonn Hungary Elektronikai Kft. – Óbudai Egyetem – Budapesti Műszaki Egyetem közösen valósított meg [18]. A kutatás során Chirp-modulációs csatornákat alakítottak ki drónok vezérlésére sávszélesség-takarékossági szempontok figyelembevétele mellett. A megvalósult fejlesztés végeredményének kedvező tulajdonságai alapján kijelenthető, hogy a hazai ipar is képes akár a LoRaWAN-technológián alapuló, továbbfejlesztett katonai szenzorhálózati célú kommunikációs megoldások fejlesztésére, előállítására.

Felmerülhet a kérdés, hogy a kétszintű AES-128-as titkosítással védett szenzoradatok kielégítik-e a katonai alkalmazás követelményeit? Megítélésem szerint a szenzorhálózatok egyes nodejai által továbbított adatokhoz való hozzáférés – azok jellege miatt – önmagában nem sok információt hordoz, míg a teljes forgalom (százas–ezres nagyságrendű alacsony sugárzási intenzitású forgalmi csatorna) felderítése és ellenőrzése a rádióspektrumban aránytalanul nagy erőfeszítést, illetve erőforrásokat igényelne, ilyen szempontból ez a titkosítási eljárás megfelelő szintű védelmet jelenthet. Lényegesen magasabb kockázatot jelent az alkalmazásszerveren tárolt, feldolgozott információkhoz való hozzáférés lehetősége, így annak támadása elleni védelemre nagyobb hangsúlyt kell fektetni. A nagyobb problémát megítélésem szerint nem a lehallgatás, hanem a LoRa-csatornák zavarása/elnyomása jelentheti, amely esetén visszatérünk a frekvenciaallokáció problémaköréhez, amivel korábban már foglalkoztam.

A katonai felhasználás lehetőségei

A LoRaWAN-technológia valós műveleti körülmények között történő alkalmazása előtt szükséges megvizsgálni az esetleges ellenséges elektronikai hadviselési tevékenységek által jelentett kockázatokat, és ennek függvényében dönteni, hogy milyen struktúrában, műszaki specifikációban alkalmazzuk a technológiát (például az előzőkben említett allokáció). A LoRaWAN általánosságban felhasználható WAN – MAN[23] kiterjedésű szenzorhálózatok rádiófrekvenciás átviteli útjaként. Ilyenek lehetnek például a határzárak vagy demilitarizált övezetek elektronikai védelmi rendszerei, de különböző objektum- vagy táborfelügyeleti, illetve védelmi megoldások esetén is lehet létjogosultsága a technológia alkalmazásának. Adott területen egy rendszeren belül

[23] Metropolitan Area Network – Nagyvárosi Kiterjedésű Hálózat.

akár többféle szenzort (például nyitásérzékelőket, szakadásjelzőket, infrakapukat) is köthetünk egy LoRaWAN-végpontra ezzel optimalizálva a hálózati erőforrásokat, de a feladat függvényében a technológia lehetőséget biztosít lényegesen komplexebb, többszintű, és/vagy redundáns megoldások kialakítására is.

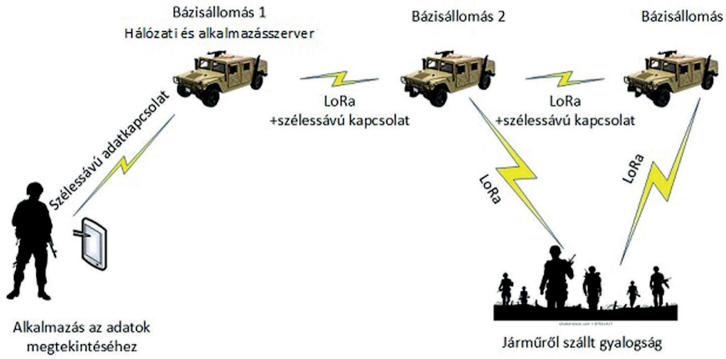
További lehetőségként jelentkezik a katonai objektumok, laktanyák, repülőterek, adótornyok stb. IoT-eszközei kommunikációs igényeinek kiszolgálása, akár fő-, akár tartalék adatátviteli útvonalként. Ilyen szenzorhálózati megoldások lehetnek például különböző infrastrukturális (épületgépészeti, villamos, hulladékkezelési) rendszerek visszajelzései, vezérlése, illetve elektronikai vagyonvédelmi jelzőeszközök, riasztási rendszerek átviteli vonalai. A robosztus hálózatszervezés támogatása érdekében lehetőség nyílik a korábbi elterjedten használt vezetékes és GSM-átviteli eljárásokat (amennyiben szükséges) kiegészíteni, kritikus erőforrások esetén NB-IoT, ZigBee, LoRaWAN stb. megoldásokkal tartalékútvonalakat kiépíteni.

A LoRaWAN felhasználási trendjeit napjainkban vizsgálva [19] azt tapasztalhatjuk, hogy megjelentek a geolokális pozíció megosztását célzó felhasználások, amelyekben a GNSS[24]-vevők által előállított pozícióadatokat LoRaWAN-hálózatokon keresztül osztják meg az alkalmazásszerverekkel. A vonatkozó NATO-ajánlások [20] értelmében a helyzetismeret információk továbbításának földi eszközre telepített terminál esetén 5 percenként, vagy 800 méterenként kell megtörténnie, míg légi járművek esetén – alapvetően a lényegesen nagyobb sebesség miatt – percenként, vagy 2300 méterenként kell frissülniük az információknak. Ezeknek a követelményeknek a LoRaWAN műszaki specifikációja és tulajdonságai alapján képes megfelelni. Ugyanakkor azt is szükséges megjegyezni, hogy a rendszer által kicsatolt adatok nem felelnek meg a vonatkozó NATO-szabályzók adatformátumának [21], [22], [23], [24], [25], amit az alkalmazásszerverek szintjén mindenképpen orvosolni szükséges, amennyiben egyéb hálózatok felé [26], [27] kívánjuk publikálni adatainkat.

E vezérfonal mentén egy újabb területen is megnyílik a felhasználás lehetősége, mégpedig a kisebb méretű és hatótávolságú drónok forgalmának egységes légtérbe történő biztonságos integrációja során. Egy LoRaWAN alapú megoldás képes lehet megfelelni akár egy nagyforgalmú városi légtér egységes forgalomirányítási rendszerében való alkalmazással szemben támasztott követelményeknek azáltal, hogy biztosítja a robosztus, megbízható kétirányú kommunikáció lehetőségét a pilóta nélküli légi járművek, és a légi irányítás rendszere között (például nyomkövetés, illetve biztonsági protokollok végrehajtása során a járművek vezérlésébe történő beavatkozás lehetősége) [28], [29], [30].

Az alábbi példában egy menetoszlop LoRaWAN-szenzorhálózattal történő támogatásának lehetőségét mutatjuk be, amelyet a 2. ábra szemléltet.

[24] Global Navigational Satellite System – Globális Műholdas Navigációs Rendszer.



2. ábra

Menetoszlop szenzorhálózati kommunikációjának támogatása LoRaWAN-technológiával

[a szerző szerkesztése]

Az ábrán a gép- és harcjárművek feltöltöttségi adatait, hadrafoghatóságát (például üzemanyagfogyás, lőszerfogyás, toronyfegyver csőhőmérséklet, keréknyomás stb.) szenzorhálózati úton monitorozzuk. Ennek egyik leghatékonyabb módja, ha a szükséges adatokat a járművek CAN[25]-buszrendszeréből nyerjük ki és csatoljuk a LoRa-végpontra. Az egyéb szenzorokat a szükség szerint csoportosíthatjuk, és így rendelhetjük őket egyéb LoRa-végpontokhoz. Modulrendszerben a deszantállomány is kaphat LoRaWAN-nodeokat annak érdekében, hogy geolokális adataikat a jármű elhagyását követően is nyomon lehessen követni. Ezeket az adatokat a LoRaWAN-átjárók gyűjtik össze. A bázisállomásokat a menetoszlopon belül célszerű járművekre telepíteni, és közöttük szélessávú vezeték nélküli rádiókapcsolatot [31] létesíteni, hogy képesek legyenek megosztani a hálózati szerver irányába a begyűjtött adatokat. Több átjáró telepítésével képesek vagyunk a korábban említett multicsomópontú csillagtopológiájú hálózat kialakítására is. Ezáltal, ha egyes átjárók kiesnek a hálózatból (például műszaki meghibásodás vagy lemarad a jármű) a hatókörön belül lévő szenzorok adatai továbbra is monitorozhatók. A hálózati és alkalmazásszervereket célszerű az oszlopparancsnok járművébe telepíteni. Innen a szerverről kliensalkalmazáson keresztül (például tableten) adatok kérhetők le (vezetékes vagy vezeték nélküli úton) a menetoszlopról.

Következtetések

Kutatásom során a LoRaWAN-technológia lehetséges katonai alkalmazásának lehetőségeit vizsgáltam. A publikációm bevezetésében felvázolt elemzés alapján néhány éven belül jelentős átalakulások várhatók a hálózatba kapcsolt információtechnológiai eszközeink területén. Az IoT-eszközök robbanásszerű terjedésével párhuzamosan, várhatóan megjelenik katonai felhasználásuk is. A LoRaWAN-technológia Layer 1–3 szintű

[25] Car Area Network – Jármű Kiterjedésű Hálózat.

működésének elemzését követően analizáltam a katonai alkalmazás szempontjából előnyös tulajdonságokat, úgymint a LoRa-moduláció, a kiemelkedő energetikai mérleg, a kedvező vételi jel-zaj viszony, valamint az önálló infrastruktúra lehetősége. Mindemellett feltártam a katonai felhasználás szempontjából lehetséges korlátokat is, úgymint a csillagpontos topológia sebezhetősége, vagy az ISM-sávú működés. A csillagtopológiából eredő kihívások az átjárók számának növelésével és a lefedettségi területek átlapolásával kompenzálhatók. Az ISM-sáv használatából eredő esetleges fenyegetettségek feltárása további kutatásokat indukál. Megítélésem szerint katonai szempontból a későbbiekben mindenképpen szükséges előzetes mérésekkel bizonyítani, hogy a LoRaWAN-technológia képes lehet-e vagy képessé tehető-e a szándékos zavarás káros hatása kockázatának csökkentésére a különböző ellenséges elektronikai hadviselési tevékenységek mellett történő megbízható üzemelésre, illetve megfelel-e a katonai alkalmazásból eredő kiberbiztonsági [32], [33] követelményeknek.

Mindezen elemzésen túlmenően beazonosítottam a LoRaWAN-technológia lehetséges katonai felhasználási területeit. A kutatás következő lépéseként javasolt a felállított modellek életképességének gyakorlati úton történő bizonyítása, mérések, kísérletek útján.

A kutatás az Emberi Erőforrások Minisztériuma ÚNKP-18-3-IV-NKE-27 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

The research is supported by the ÚNKP-18-3-IV-NKE-27 New National Excellence Program of the Ministry of Human Capacities.

Hivatkozások

[1] F. Jejdling, *Ericsson Mobility Report.* Svédország, Stockholm: Ericsson, június, 2018. [Online]. Elérhető: www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf (Letöltve: 2019. 05. 05.)

[2] IEEE, „802.15.1-2002 – *IEEE Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN – Specific Requirements – Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)*," June 14, 2002. [Online]. Elérhető: https://ieeexplore.ieee.org/document/1016473 (Letöltve: 2019. 05. 05.)

[3] Zigbee szövetség hivatalos honlapja, Zigbee Alliance, Elérhető: www.zigbee.org/ (Letöltve: 2019. 05. 05.)

[4] AZ IEEE WLAN munkacsoportjának hivatalos honlapja, Elérhető: www.ieee802.org/11/# (Letöltve: 2019. 05. 05.)

[5] K. Károly, „Szenzorhálózatok adatainak integrálási lehetőségei a perspektivikus erőkövetési rendszerekbe, különös tekintettel az egyéni egészségügyi adatokra," *Hadmérnök,* 14. évf. 1. sz. pp. 260–270, 2019.

[6] RFC 8376, S. Farell, „*Low-Power Wide Area Network (LPWAN) Overview*," IETF, Trinity College Dublin, p. 43, 2018. május, [Online]. Elérhető: https://tools.ietf.org/html/rfc8376 (Letöltve: 2019. 05. 05.)

[7] N. Hisham, N. Ibrahim, A. R. Ibrahim, I. Mat, A. N. Harun, és G. Witjaksono, „LoRaWAN in Climate Monitoring in Advance Precision Agriculture System," In: Proc. 2018 International Conference on Intelligent and Advanced System (ICIAS), Kuala Lumpur, Malajzia, 2018. DOI: https://doi.org/10.1109/ICIAS.2018.8540598
[8] R. Kirovné Rácz, „Magyarország hidrológiai eredetű katasztrófaveszélyeztettsége 2017. szeptembertől 2018. januárig az extrém mennyiségű és intenzitású csapadékhullás tükrében," *Hadtudományi Szemle,* 11. évf. 2. sz. pp. 252–267, 2018.
[9] R. Rácz, „The economical aspects of the climate change," *AARMS,* vol. 9, no. 1, pp. 153–157, 2010.
[10] B. Lóderer és R. Rácz, „A klímaváltozás és annak következményeire való felkészülés lehetséges jövőbeni aspektusai," *Hadtudományi Szemle,* 4. évf. 3. sz. pp. 91–98, 2011.
[11] R. Rácz, „The function of the system of national defence and disaster management in the disaster management structure," *AARMS,* vol. 10, no. 1, pp. 173–181, 2011.
[12] A Semtech cég hivatalos weboldala, Elérhető: www.semtech.com/lora (Letöltve: 2019. 05. 09.)
[13] T. Holman, B. Márkus, oktatóanyag, „LoRaWAN workshop," ChipCAD Kft. Budapest, február 21. 2019.
[14] T. Holman, „A LoRaWAN technológia hazai bevezetésének tapasztalatai," *Magyar Elektronika,* 35. évf. 9. sz. pp. 42–44, 2018.
[15] T. Holman, B. Márkus, és A. Gnandt, „LoRaWAN technológia 2019", in *Rádiótechnika Évkönyve 2019,* F. Békei szerk. Budapest: Rádióvilág Kft., pp. 168–171.
[16] A. Gulyás, „The Radio Controlled Improvised Explosive Device (RCIED) threat in Afghanistan," *AARMS,* vol. 12, no. 1, pp. 9–23, 2013.
[17] Zs. Haig, L. Kovács, L. Ványa, és S. Vass, *Elektronikai hadviselés.* Budapest: NKE-HHK, 2014, p. 271.
[18] Z. Belső, K. Elek, I. Koller, és Gy. Mikó, „Magyar fejlesztésű korszerű kommunikációs rendszer mobil alkalmazásokra," Elektronet.hu, 2012. 04.18, [Online]. Elérhető: www.elektro-net.hu/konstruktor/3594-magyar-fejlesztesu-korszeru-kommunikacios-rendszer-mobil-alkalmazasokra (Letöltve: 2019. 05. 08.)
[19] B. Márkus és T. Holman, „Építsünk együtt nyílt LoRaWAN hálózatot!", in: *Rádiótechnika Évkönyve 2017,* Budapest: Rádióvilág Kft., pp. 191–196.
[20] NATO STANAG 5500, "Concept of NATO Message Text Formatting System," (CONFORMETS) -ADATP-3 (A), 2. Nov. 2010.
[21] A. Gulyás, „Gondolatok az adatátviteli rendszerek fejlődéséről," *Seregszemle,* 15. évf. 2. sz. pp. 162–188, 2017.
[22] A. Gulyás, „Kognitív üzemmódok katonai alkalmazása," *Seregszemle,* 14. évf. 1. sz. pp. 59–75, 2016.
[23] A. Gulyás, „Szabványosított hullámforma azonosításra (1. rész)," *Seregszemle,* 16. évf. 1. sz. pp. 160–172, 2018.
[24] A. Gulyás, „Szabványosított hullámforma azonosításra (2. rész)," *Seregszemle,* 16. évf. 2. sz. pp. 146–154, 2018.
[25] A. Gulyás, „Szoftvervezérelt rádiók azonosító jelsorozatai," *Seregszemle,* 11. évf. 4. sz. pp. 56–81, 2013.

[26] Sz. Jobbágy, „A Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata," *Hadmérnök,* 12. évf. 3. sz. pp. 223–236, 2017.
[27] A. Gulyás, "Force Tracking System in SOF applications," *AARMS,* vol. 8, no. 4, pp. 601–617, 2009.
[28] A. Németh, „UAV-k alkalmazása a közfeladatok ellátása során I," *Hadmérnök,* 13. évf. 2. sz. pp. 37–60, 2018.
[29] A. Németh, „UAV-k alkalmazása a közfeladatok ellátása során II," *Hadmérnök,* 13. évf. 3. sz. pp. 68–86, 2018.
[30] B. Márkus, S. Jeszenszky, „Repülős LoRaWAN teszt Magyarországon," micromite.chipcad.org [Online]. Elérhető: http://micromite.chipcad.org/home/repuelos-lorawan-teszt-magyarorszagon (Letöltve: 2019. 05. 12.)
[31] A. Németh, A. Horváth, és A. Gulyás, „Ultra wideband data channels for special operations forces," *Hadmérnök,* vol. 8, no. 1. pp. 154–165, 2013.
[32] D. Dévai, "The U.S. Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace (Part 1)," *AARMS,* vol. 18, no. 1. pp. 39–57. 2019. DOI: https://doi.org/10.32565/aarms.2019.3 [Online]. Elérhető: https://folyoiratok.uni-nke.hu/document/nkeszolgaltato-uni-nke-hu/AARMS_2019_01_03_Dora-DeVAI1.pdf (Letöltve: 2019. 06. 23.)
[33] D. Dévai, "The U.S. Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace (Part 2)," *AARMS,* vol. 18, no. 1. pp. 59–77. 2019. DOI: https://doi.org/10.32565/aarms.2019.4 Elérhető: https://folyoiratok.uni-nke.hu/document/nkeszolgaltato-uni-nke-hu/AARMS_2019_01_03_Dora-DeVAI1.pdf (Letöltve: 2019. 06. 23.)