HADMÉRNÖK

XII. Évfolyam 1. különszám – 2017. július

AZ ELEKTRONIKAI FELDERÍTÉS KORSZERŰ ESZKÖZEI: FELÜGYELET NÉLKÜLI SZENZORHÁLÓZATOK

NOVEL TECHNIQUES IN THE ELECTRONIC SURVEILLANCE: UNATTENDED GROUND SENSORS

BOGNÁR Eszter Katalin

(ORCID: 0000-0002-3697-7871)

bognarek@uni-nke.hu

Absztrakt

A felügyelet nélküli szenzorhálózatok a katonai művelet számára pontos, időszerű és helyhez kötött felderítési adatokat biztosító rendszerek. A harctéren elhelyezett kisméretű infravörös, akusztikus, mágneses és szeizmikus érzékelők az adatgyűjtés jelenleg elérhető egyik legkorszerűbb eszközei, napjaink és a jövő hadviselésének nélkülözhetetlen kellékei. Alkalmazásuk hatalmas potenciált jelent a szemben álló féllel szembeni információs fölény kivívásában, ugyanakkor teljesen flexibilis, önszerveződő és biztonságos rendszerek kialakítása számos megoldandó feladatot is magában rejt. A cikk célja a témában fellelhető hazai és nemzetközi szakirodalom alapján áttekinteni a felügyelet nélküli szenzorhálózatok tervezésének és működésének alapjait, az üzemeltetés során fellépő technológiai és biztonsági kihívásokat, a REMBASS és az Elbit Treasures rendszerén keresztül ismertetni a jelenleg elérhető képességeket és fejlesztési irányokat.

Kulcsszavak: *vezeték nélküli szenzorhálózatok, katonai szenzorok, felügyelet nélküli szenzorhálózatok*

Abstract

Unattended ground sensors (UGS) are systems to provide accurate, timely and location based reconnaissance data for military operations. These small infrared, acoustic, magnetic and seismic sensors are one of the latest technologies of data collection on the battlefield and are essential parts of today's and future army. The application of these systems has enormous potential in gaining information superiority against the enemy, but challenges engineers to design fully flexible, self-organizing, and security proved systems. Based on the available literature, the aim of this article is to give an overview about the design and operation of UGS networks together with the technology and security related challenges. Focused on the REMBASS and Elbit's Treasures systems the currently available capabilities and directions for future research are introduced.

Keywords: *wireless sensor networks (WSN) unattended networked sensors, military sensors, unattended ground sensors (UGS)*

A kézirat benyújtásának dátuma (Date of the submission): 2017.05.25.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.06.27.

BEVEZETÉS

Vezeték nélküli szenzorhálózat alatt több száz, vagy akár több ezer hálózatba kapcsolt érzékelőt értünk, melyek összehangolt működésük révén alkalmasak egy adott terület vagy objektum monitorozására. A technológia rohamos fejlődésének köszönhetően ma már rendkívül kisméretű, olcsó szenzorok gyártására van lehetőség, melyek szinte bárhova telepíthetőek. Sokoldalú felhasználhatóságuknak köszönhetően széles körben elterjedtek mind a civil szférában (pl.: egészségügy, a gyártás-monitorozás, környezetvédelem), mind a honvédelemben, az elektronikai felderítés egyik legkorszerűbb megoldását kínálva.

A modern hadseregek felderítési képességeinek fejlesztése kapcsán mindenképpen figyelmet kell fordítani a felügyelet nélküli szenzorhálózatok nyújtotta lehetőségekre. A cikk célja, hogy a fellelhető releváns szakirodalom összefoglaló elemzésével ismertesse a szenzorhálózatok harctéri alkalmazhatóságának előnyeit és korlátait, igazolja létjogosultságukat a 21. századi hadviselésben, valamint rámutasson a jelenlegi rendszerek kapcsán megjelenő mérnöki kihívásokra, felvázolva a lehetséges fejlesztési irányokat. Az első részben ismertetésre kerül a szenzorhálózatok helye és szerepe a modernkori hadviselés rendszerében, majd a cikk összefoglalja a szenzorhálózatok legfontosabb jellemzőit és a velük szemben támasztott követelményeket, alkalmazásuk korlátait, majd a biztonságra fókuszálva bemutatja a rendszerek főbb sérülékenységeit.

INFORMÁCIÓS HADVISELÉS A 21. SZÁZADBAN

Az információs kor technikai vívmányainak köszönhetően számos változás következett be a hadügy területén. A korábban földön, vízen, levegőben zajló háborúk új dimenzióval, az információs hadszíntérrel bővültek, melyben a szemben álló felek információs fölényért folytatott küzdelme zajlik különböző információs műveletek által. Előtérbe kerültek az információ megszerzését és annak hatékony, valós idejű feldolgozását lehetővé tévő korszerű technológiák.

A felderítéssel szemben támasztott alapvető követelmény a megfelelő mennyiségű és minőségű információ, megfelelő helyre és időben történő továbbítása, mely csak egy egységes, nagymértékben automatizált, a technológiai lehetőségeket maximálisan kihasználó korszerű felderítő és adatelosztó rendszerben képzelhető el, ahol egy közös számítógépes hálózatban helyezkednek el az adatgyűjtést végző szenzorok és berendezések, valamint ugyanitt történik meg az adatok feldolgozása, értékelése és szétosztása. [1]

A modern hadseregek információs rendszerei esetében tehát nélkülözhetetlenné vált a hálózatközpontú megközelítés: az adatgyűjtés eszközeit és az adatfeldolgozást megvalósító szolgáltatásokat egy számítógépes hálózat alapú, komplex rendszerbe kell integrálni, mely által lehetővé válik: [2]

- a valós idejű kommunikáció a szenzorok, döntéshozók és a harcoló alakulatok között;
- a valós időben történő adatgyűjtés a környezetről és harctevékenységekről, az információ minden platformra történő továbbítása, vizualizációja és értékelése;
- a decentralizált vezetés és irányítás, amelyben minden döntéshozó hozzáfér és felhasználhatja az összes rendelkezésre álló releváns, időszerű adatot.

Mindezek által jelentősen növelhető a hadsereg ISTAR[1] képessége.

Az ISTAR egyre szélesebb körben elterjedt katonai terminológia, mely az AJP-2.711 [3] doktrína alapján Gulyás Attila fordításában a következőképpen definiált:

„Az ISTAR egy olyan eljárás, mely összekapcsolja (integrálja) a megfigyelő, a felderítő és a célokról adatot szerző (célfelderítő) rendszereket, valamint érzékelőket a műveletek és a csapásmérő eszközök irányítása érdekében. Magában foglalja az információgyűjtést, a műveleti és felderítő információk menedzsmentjét, helyzetjelentést, illetve helyzetértékelést biztosít a parancsnok és törzse részére a hadműveletek vezetése és a célmegjelölő eljárások támogatása érdekében. A műveleti felderítő tevékenység integrálja és szinkronizálja a tervezést, a felderítő eszközök és érzékelők alkalmazását, az információ feldolgozását és felhasználását, valamint a célmegjelölő és tájékoztató rendszereket közvetlenül támogatva a folyamatban lévő és jövőbeli műveleteket." [4]

A műveletekben a felderítő támogatás tehát az ISTAR-koncepció mentén szerveződik, mely központi koordinációval integrálja a felderítő, hírszerző és célmeghatározó eszközöket. [5]

A megfelelő ISTAR képességek birtokában, az automatikus és folyamatos információfeldolgozás és továbbítás révén a következő képességekre tehető szer: [6]

- a támadások hatékonyabb felismerése;
- az információs rendszerek közötti átjárhatóság biztosítása;
- a hatékonyabb helyzetfelismerés;
- a veszteségek csökkentése;
- a kölcsönös együttműködés és támogatás;
- a harci képességek növelése.

A fenti képességek nélkülözhetetlen a sikeres harcászati, hadműveleti tevékenységek végrehajtásához.

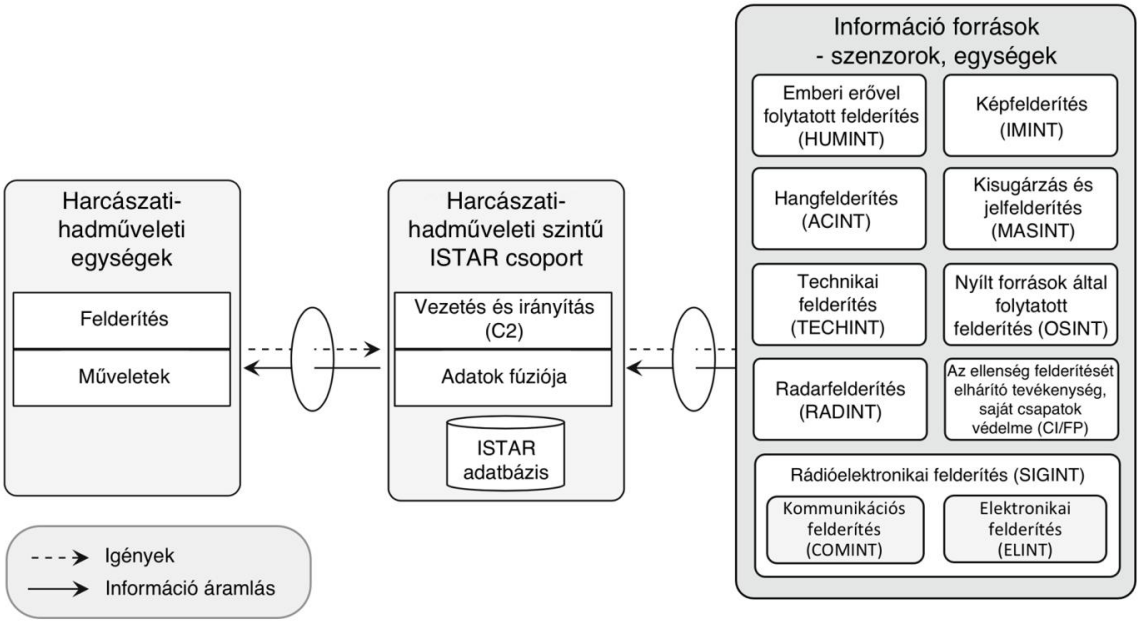
Az ISTAR információforrásai sokfélék lehetnek: [5]

- emberi erővel folytatott felderítés (HUMINT[2]);
- képfelderítés (IMINT[3]);
- rádióelektronikai felderítés (SIGINT[4]);
- rádiófelderítés (COMINT[5]);
- rációtechnikai felderítés (ELINT[6]);
- hangfelderítés (ACINT[7]);
- kisugárzás és jelfelderítés (MASINT[8]);
- radarfelderítés (RADINT[9]);
- technikai felderítés (TECHINT[10]);

[1] ISTAR: Intelligence, Surveillance, Target Acquisition and Reconnaissance – Felderítő, megfigyelő és célmeghatározó rendszer
[2] HUMINT: Human Intelligence
[3] IMINT: Imagery Intelligence
[4] SIGINT: Signal Intelligence
[5] COMINT: Communication Intelligence
[6] ELINT: Electronic Intelligence
[7] ACINT: Acoustic Intelligence
[8] MASINT: Measurements Intelligence
[9] RADINT: Radar Intelligence

- nyílt források által folytatott felderítés (OSINT[11]);
- az ellenség felderítését elhárító tevékenység, saját csapatok védelme (CI/FP[12]).

Az 1. ábra bemutatja az ISTAR információ forrásait és az információ áramlását a rendszerben.



1. ábra *Az ISTAR információ forrásai és az információ áramlása* (a szerző szerkesztése [6] alapján)

A különböző felderítési fajtákat különböző hordozóeszközökről alkalmazhatják. A felderítés történhet pl. repülőgépről, pilóta nélküli repülőgépekről (UAV[13]), földi állomásokról, műholdakról. A felügyelet nélküli szenzorhálózatok szintén a felderítés egyik platformját képezik, melyben különböző MASINT szenzorok (pl.: szeizmikus, termikus, akusztikus, mágneses stb.) helyezkednek el.

SZENZORHÁLÓZATOK A HARCTÉREN

A szenzorhálózatok létrejöttéhez elengedhetetlenek voltak az elmúlt évek technológiai vívmányai. Az adatátvitel fejlődése révén egyre megbízhatóbb, és nagyobb sebességű kommunikációs kapcsolat alakítható ki a számítógépek között vezetékes vagy vezeték nélküli megoldásokkal. A mikro-elektromechanikus (MEMS[14]) rendszerek megjelenésének köszönhetően egyre kisebb méretű és költséghatékonyan előállítható érzékelőket gyártanak, az akkumulátor technológia fejlődésének köszönhetően egyre nagyobb energia- és teljesítménysűrűségű megoldások láttak napvilágot. Ennek köszönhetően elterjedtek mind a civil, mind a védelmi szférában is a vezeték nélküli szenzorhálózatok, mint az elektronikai felderítés modern eszközei.

---

[10] TECHINT: Technical Intelligence
[11] OSINT: Open Source Intelligence
[12] CI/FP: Counterintelligence and Force Protection
[13] UAV: Unmanned Arial Vehicle
[14] MEMS: Microelectromechanical systems – mikro-elektromechanikus rendszer

A szenzorok kis méretüknek köszönhetően szinte bárhova elhelyezhetőek, ezért széles körben alkalmazzák őket. Telepíthetőek földön, vízen, levegőben, vagy akár katonák harci felszerelésének részeként is szolgálhatnak, integrálva az adatgyűjtő katonát a felderítő-hírszerző rendszerbe. [8] Több szenzor hálózatba kötésével pedig nagy területi lefedettség, több, akár eltérő forrásból származó fuzionált adatgyűjtés valósítható. Cikkem további részében a földi telepítésű felügyelet nélküli szenzorhálózatokra fókuszálok.

A szenzorhálózatok az ISTAR számára szolgáltatott adatokkal támogatják a harctér minél pontosabb vizualizációját, ellátva a parancsnokot a harctér aktuális körülményeire vonatkozó információval (saját és ellenséges csapatok helyzete, időjárási körülmények, földrajzi viszonyok), biztosítva számára a döntéshozatal alapjául szolgáló megfelelő mennyiségű, minőségű és időszerű információt. [9]

A felügyelet nélküli szenzorhálózatok szintén nagy előnye, hogy az információforráshoz közel, emberi erő bevetése és veszélyeztetése nélkül képesek a folyamatos, felügyelet nélküli adatszolgáltatásra, elősegítve a katonák életének megóvását és a felderítési hatékonyság nagymértékű növelését.

A szenzorok és szenzorhálózatok felépítése és működése

A felügyelet nélküli szenzorhálózatokat csomópontok (szenzor node) alkotják, melyek egymással vezeték nélküli (wireless) kapcsolattal kommunikálnak, a külvilág felé pedig egy speciális node, az átjáró (gateway) biztosítja a kapcsolatot.

A vezeték nélküli kapcsolat nagy előnye, hogy kellő mobilitást biztosít, gyorsabban telepíthető, ezen kívül kevésbé infrastruktúrafüggő, melyek mind megfontolandó szempontok harctéri körülmények között. [6] A továbbiakban ismertetem a szenzorok és a szenzorok alkotta hálózat felépítésének és működésének alapjait.

Szenzorok

A szenzorok a következő alkotóelemekből épülnek fel: beépített feldolgozóegység, különböző fedélzeti érzékelő egységek (akusztikus, szeizmikus, infravörös, mágneses, optikai, nyomás, kémiai, biológiai, nukleáris, mechanikus, termikus), tároló kapacitás, vezeték nélküli hálózati adapter, mely biztosítja a kapcsolatot a többi node-dal, valamit beépített GPS vevő, mely a GIS[15] adatokhoz történő hozzáférést lehetővé téve pontos és friss helyinformációval látja el a szenzort. [10]

A szenzorok GIS adatbázisokhoz való hozzáférése több szempontból is fontos kritérium. A szenzorokat nagyon sokszor ad hoc telepítik, például pilóta nélküli repülőgépekről szórják a monitorozandó területre, a pontos helyinformáció alapján a szenzorok képesek lesznek a beállításaik finom hangolására az aktuális környezeti viszonyoknak megfelelően. [11] A GIS adatok emellett szintén nélkülözhetetlenek a különböző szenzorok által szolgáltatott adatok fúziója során.

Szenzorhálózatok

A hálózat felépítése, szerkezete, a benne található elemek tulajdonságai jelentős szereppel bírnak a biztonságos és megbízható kommunikáció kivitelezésében. A node-ok esetében a legfontosabb tulajdonságok közé az akkumulátor élettartama, aktuális energiaszintje, a szenzorok típusa és a kommunikációt biztosító vezeték nélküli adóvevő hatótávolsága tartoznak. [12] A szárazföldi harcászati felderítés során az optimális működést ezen kívül nagymértékben befolyásolják a terep meteorológiai, geológiai viszonyai, főként a különböző hőmérséklet, csapadékmennyiség, köd, páratartalom, valamint a domborzati feltételek. [13]

[15] GIS: Geographic Information System – földrajzi információs rendszer

A hardver elemek mellett jelentős szerep jut az azokat működtető szoftverre is: vezérli a hálózat kiépítését, menedzseli a különböző útvonalválasztó protokollokat, az adatok gyűjtését, tárolását és továbbítását. [14] A szenzorokon futó operációs rendszer tekintetében fontos szempont az esemény alapú, moduláris programozás lehetősége, mindezt ráadásul a szenzorok nyújtotta korlátozott erőforrásokon megvalósítva. A fenti kritériumoknak eleget téve a vezeték nélküli hálózatok ajánlott operációs rendszere a TinyOS[16], valamint a hozzá tartozó NesC programozási nyelv, mely a C nyelv egy speciális változata. [15]

A node-ok alkotta hálózat kialakítása több módon történhet, melyet az 1. táblázat foglal össze.

Előre definiált hálózat	**Ad-hoc hálózat**	**Mozgó node-okkal rendelkező hálózat**
A node-ok helye és szerepe, valamint a hálózat topológiája előre eltervezett. pl.: kézi telepítésű szenzorhálózatok	A node-ok helye, hatásköre nincs előre meghatározva, telepítés után, általában automatikusan kerül kialakításra. pl.: UAV-ról „leszórt” szenzorhálózatok	A node-ok helye telepítés után is változhat. Pl.: szenzorokkal felszerelt járműkonvoj, UAV-k alkotta szenzorhálózat

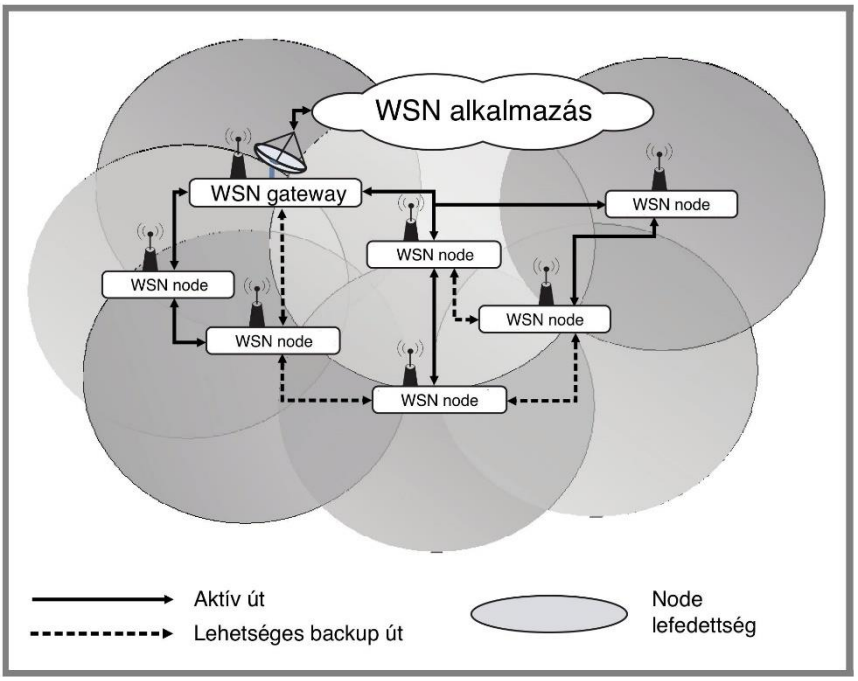
1. táblázat Szenzorhálózatok szerkezete. (a szerző szerkesztése [12] alapján)

A hálózatban a szenzorok a környezet fizikai állapotváltozásait detektálják, mely lehet hőmérséklet, nyomás, hang, szeizmikus mozgás, különböző frekvenciatartományú és hullámhosszú rádió-mágneses hullámok. A mért értéken ezután a szenzor feldolgozó egysége elő feldolgozást végezhet vagy továbbítja az adatot a szomszédos node vagy az átjáró (gateway) felé. Az egymással kapcsolatban álló szenzorok általában egy átjárón keresztül kommunikálnak a külvilágban található feldolgozó központtal. Az átjárónak fontos szerep jut, hiszen a node-ok a kis méret, olcsó előállítás és élettartamra vonatkozó megszorítások miatt csak korlátozott tárhellyel, számítási kapacitással és energiával rendelkeznek, rajtuk komplex, számításigényes algoritmusokat nem lehet futtatni.

A gateway feladata a különböző szenzorokból származó adatok fúzióját és feldolgozását, valamint eljuttatását a felhasználás helyére. Ez megvalósulhat folyamatos, közel valós idejű, nagy hatótávolságú vezeték nélküli (wireless) vagy műholdas kapcsolat használatával, vagy aszinkron adatátvitellel a terület felett elhaladó pilóta nélküli repülőgépekre való feltöltéssel. Az átjáró ezen kívül általában nagyobb tárhellyel rendelkezve biztosítja az adatok hosszabb távú megőrzését, biztonsági mentését. A szenzorok tehát egymással és az átjáróval kommunikálnak, az átjáró pedig kapcsolatot biztosít a külvilág felé, ahol egy alkalmazáson keresztül valósul meg a hálózat felügyelete és az adatok értékelése, vizualizációja. [16][17]

A 2. ábra a vezeték nélküli szenzorhálózatok (WSN) általános felépítése és működése látható.

[16] TinyOS és NesC: https://github.com/tinyos



2. ábra Szenzorhálózatok tipikus felépítése és működése. (a szerző fordítása [15] alapján)

A szenzorhálózatokkal szemben támasztott követelmények

Különösen harctéri feltételek mellett, a felügyelet nélküli szenzorhálózatokkal szemben számos követelmény fogalmazódott meg, melyek közül [9][16][18] alapján a legfontosabbak:

- passzív működés;
- önszerveződés, skálázhatóság, flexibilitás;
- alacsony költség, kis méret;
- könnyű telepíthetőség;
- nagy területi lefedettség;
- ellenállóság a környezeti feltételeknek;
- távoli felügyelet, közbeavatkozás, átprogramozhatóság;
- kielégítő élettartam;
- megbízható kommunikáció titkosított adatátvitellel;
- védelem az illetéktelen hozzáférés, adatmanipuláció ellen;
- hibatűrés, adatvesztés elleni védelem;
- adatok relevanciája, időszerűsége;
- rejtettség, nehezen észrevehetőség.

A fentiek alapján látható, hogy rendkívül fontos a hálózatok költséghatékony, gyors, automatikus telepítése és működése a monitorozandó környezetben, ugyanakkor lehetővé kell tenni azok távoli menedzselését. Nagy területi lefedettséget kell biztosítani nehezen észrevehető, kisméretű szenzorokkal, valamint megfelelő energiaforrással, energia hatékony protokollok alkalmazásával biztosítani a hálózatok hosszabb ideig történő felhasználását.

Mindemellett a rendszert és a benne tárolt adatokat védeni kell minden káros eseménytől, legyen az fizikai behatás (pl.: lopás, környezeti csapások, elektromágneses zavarok) vagy egyéb káros tevékenység (pl.: üzenetek illegális lehallgatása, módosítása).

Adatok fúziós feldolgozása

Az optimálisan működő szenzorhálózatoknak biztosítani kell több, párhuzamosan történő esemény egyértelmű, pontos azonosítását a harctéren, az adatok összevetését a szomszédos csomópontokkal, majd a különböző objektumok és események megfelelő osztályozását. Egyetlen node nem képes a harctéri objektumok pontos azonosítására és követésére. A különböző pozícióban és frekvencia tartományban működő érzékelők által szolgáltatott adatok összevetésével és elemzésével azonban jelentősen csökkenthető a hibák száma és növelhető a rendszer felderítő képessége. Nélkülözhetetlen tehát a hatékony adatfúzió és elemzés, mely elősegíti, hogy az adatok több forrásból származva kerüljenek feldolgozásra, csökkentve a mérési pontatlanságok, torzulások késleltetett kommunikáció, zavarások okozta ellenhatásokat. A különböző alkalmazások közötti interoperatibilitás megvalósítása érdekében közös formátumra és sztenderdekre van szükség a szenzor adatokra és kommunikációs csatorna használatára vonatkozóan. [2][16][20]

Működési korlátok

Az előző fejezetben ismertetett optimális működés megvalósításának számos korlátja van, mely a szenzorhálózatot alkotó elemek és az adatátvitelre használt vezeték nélküli kapcsolat karakterisztikájából ered. A továbbiakban Walters et al. munkája [19] alapján a legjelentősebb működési korlátok kerülnek bemutatásra.

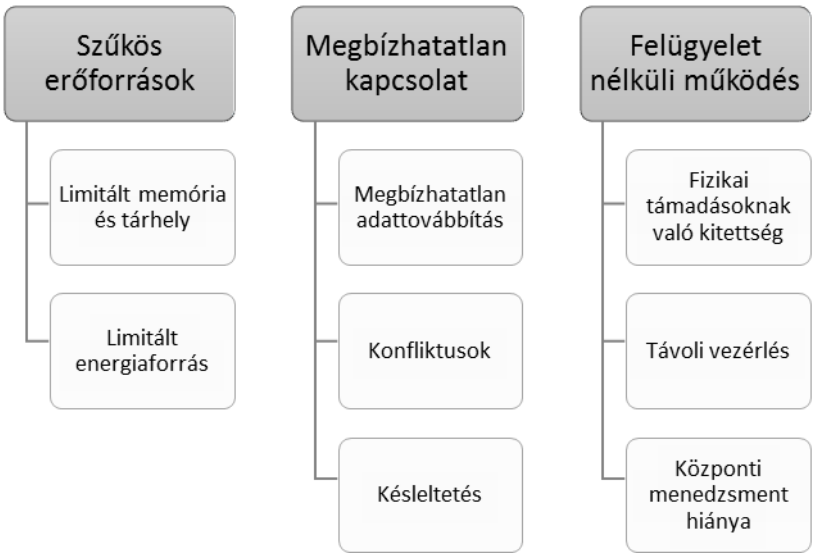
Az egyik legnagyobb korlátot az jelenti, hogy a szenzorok kis méretük és olcsóságuk miatt csak limitált erőforrásokkal rendelkeznek, amely memória, tárhely, számítási kapacitás és energia igényes műveletek esetén komoly problémát okoz. Az adatok feldolgozását, biztonsági szolgáltatásokat stb. megvalósító programokat ennek megfelelően a lehető legjobban optimalizálva kell elkészíteni a megszorítások figyelembe vételével. Nagy előrelépést jelent a szenzorok energiaszükségletét napelemmel biztosító megoldások elterjedése.

Egy újabb korlátot jelent a kommunikációra használt vezeték nélküli hálózati kapcsolat természete. A hálózatban történő adattovábbításra a gyors adatátvitel prioritása miatt legtöbbször UDP[17]-t használnak, mely gyors, összeköttetés nélküli, csomag (datagram) alapú adattovábbítást tesz lehetővé a hálózatba kapcsolt node-ok között. A protokoll előnye a gyorsaság, ugyanakkor nem garantált a csomagok megérkezése, azok elveszhetnek, többszöröződhetnek, mely biztonsági problémákat vet fel, valamint nehezíti az észlelt adatok feldolgozását. A vezeték nélküli hálózatban emellett számolni kell a csomagtovábbítás során fellépő konfliktusokkal. Több node-on áthaladó (multihop) adatfolyam esetén akár jelentős késleltetés is lehet az adattovábbításban, mely szintén nehezíti az adatok összevetését és elemzését.

A megszorítások harmadik csoportját a felügyelet nélküli működés okozta korlátok képezik. Ide tartoznak a különböző környezeti hatások, fizikai támadások, mely a felügyelet nélküli, harctéri körülmények között elhelyezett szenzorokat fokozottan veszélyezteti. Mivel a szenzorok a hálózatot vezérlő központtól távol helyezkednek el, nincs lehetőség a meghibásodott eszközök cseréjére, az akkumulátorok töltésére, az eszközökön végzett esetleges káros célú módosítások észlelésére. A problémára megoldást nyújthat a szenzorokba épített öntesztelési lehetőség (BIST[18]), mellyel távolról is pontos képet kaphatunk a készülék állapotáról: az esetleges meghibásodások felismerhetőek, helyük azonosítható. [25]

[17] UDP: User Datagram Protocol
[18] BIST: Built-In Self-Test

Hátrányként említhető még, hogy a vezeték nélküli hálózatok legtöbbször elosztott rendszerek. A központi vezérlés hiánya habár növeli a hálózatok flexibilitását, egy hosszú időre magára hagyott hálózat működése során már problémát okozhat. A fent említett működési korlátok összefoglalása a 3. ábra látható.



3. ábra *Szenzorhálózatok működési korlátai* (saját szerkesztés)

A felügyelet nélküli szenzorhálózatok biztonsági kérdései

A felügyelet nélküli szenzorhálózatok biztonsági kérdéseivel számos publikáció foglalkozik, a fejezet Nagy, [7] Winkler et al., [16] Buttyán és Hubaux [21] tanulmányai alapján röviden ismerteti a rendszerek biztonságára vonatkozó főbb jellemzőket.

A rendszerek biztonsága a különösen értékes, a parancsnoki döntéshozatal alapjául szolgáló felderítési adatok esetén rendkívül fontos kérdés. A felügyelet nélküli szenzorhálózatokon tárolt és továbbított kritikus fontosságú információk esetében ezért nélkülözhetetlen az információbiztonság alapelveinek (bizalmasság, sértetlenség, rendelkezésre állás, hitelesség) teljes körű megvalósítása. Az előző fejezetben ismertetett a felügyelet nélküli szenzorhálózatok működését korlátozó tényezők azonban jelentősen megnehezítik a feladatot. A szenzorok korlátozott erőforrásai, a vezeték nélküli hálózat megbízhatatlan adattovábbítása, valamint a rendszerek közvetlen felügyeletének hiánya korlátozza a biztonság növelését elősegítő megoldások létrehozását. Habár a vezeték nélküli szenzorhálózatok biztonságának növelésére számos megoldás létezik, azok implementálása során mindig figyelembe kell venni a rendszerekre jellemző szűkös erőforrások képezte korlátokat.

A hálózatokat veszélyeztető jelentősebb támadások és az ellenük való védekezés lehetőségei a teljesség igénye nélkül a következőek:

- *Lehallgatás (Eavesdropping):* A lehetőség arra, hogy az ellenség elfogjon és dekódoljon üzeneteket a szenzorhálózatok eszközei között. A támadás elleni védelem megoldható az elérhető civil kriptográfiai megoldásokkal.
- *Hamisítás (Spoofing):* Annak lehetősége, hogy egy idegen csomópont legitim csomópontként viselkedve módosíthassa a hálózat adatcseréjét. A problémára különböző kriptográfiai autentikációs mechanizmusok alkalmazhatóak.
- *Túlterheléses támadás (Denial of Service):* A rendszer kérésekkel való túlterhelése, amely ennek következtében lelassul, és nem tudja a funkcióját a megfelelő színvonalon ellátni Az olcsó adóvevők jelenleg nem rendelkeznek robusztus

zavarás elleni védelemmel, ezzel a szenzorhálózatokat védtelenné teszik az ilyen irányú támadásokkal szemben.

- *Geolokalizáció:* Lehetőség a csomópontok földrajzi pozíciójának meghatározására az eszközökből érkező jelek detektálása révén. A hálózatban az átvitelek számának és hosszának minimalizálása csökkenti annak a valószínűségét, hogy egy támadó detektálja, vagy lokalizálja a szenzorhálózatot. Az optimalizáció a megfelelő protokoll kiválasztásával és tervezéssel biztosítható. Mindezek ellenére nem kizárható annak a veszélye, hogy az átvitelt észlelje az ellenség, különösen akkor, ha a szenzorhálózat létezését már gyanítja az adott földrajzi területen.
- *Fizikai kompromittáció:* Az ellenség információt nyerhet ki a megtalált és elfogott szenzor csomópontból. A kompromittáció ellen egyszerű mechanizmusokkal lehet védekezni pl.: olyan megoldásokkal, melyek illetéktelen hozzáférés esetén törlik a rendszermemóriából az érzékeny információkat. Ezek kipróbált és tesztelt megoldások a fizikai ellenálló képesség javítására.

Napjaink modern rendszerei

A világon számos különböző típusú felügyelet nélküli érzékelő rendszer van jelenleg is használatban. Ezek közül a továbbiakban a REMBASS II és TREASURES rendszerek kerülnek bemutatásra.

REMBASS II (L3 Technologies Inc.) [22]

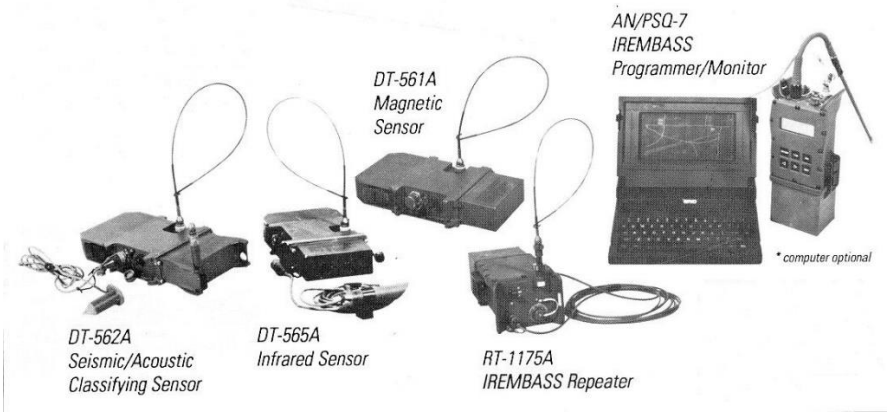
Az Amerikai Egyesült Államokban széles körben alkalmazott felderítő rendszer az AN/GSR-8 (REMBASSII). A rendszer alkalmas célobjektumok azonosítására, osztályozására és az emberek, járművek mozgásirányának detektálása.

A rendszer háromféle szenzort tartalmaz:

- szeizmikus/akusztikus;
- passzív infravörös (PIR[19]);
- mágneses.

A szenzorok közötti kommunikáció és adattovábbítás kis valószínűséggel detektálható (LPI/LPD[20]) kapcsolaton keresztül, nyílt interfész használatával valósul meg, így más típusú szenzorok is könnyen integrálhatóak a rendszerbe. A kommunikációs csatorna hatótávolsága 15 km, de ismétlőkkel akár 150 km is lehet.

A 4. ábra a REMBASS rendszer alkotóelemei láthatóak.



4. ábra *A REMBASS rendszer alkotóelemei [23]*

[19] PIR: Passive Infrared
[20] LPI/LPD: Low Probability of Intercept/Low Probability of detection

Elbit „Treasures" (Elbit Systems Ltd.) [24]

Az Elbit Systems Ltd. „Treasures" rendszere meglehetősen új fejlesztés, valós időben detektálja, osztályozza és követi a személyeket vagy járműveket. A rendszer többféle típusú, kisméretű szenzort tartalmaz, melyeket úgy terveztek, hogy extrém időjárási körülményeknek is ellenálljanak, alacsony legyen az energiaszükségletük, lehetővé téve, hogy a szenzorok felügyelet nélkül, hosszú ideig működhessenek.

A rendszer kompatibilis más gyártók szenzorjaival és könnyen integrálható egyéb C4I rendszerekkel.

A különböző érzékelési tartományban működő szenzorok között ad-hoc, önszerveződő speciális kommunikációs protokollokkal megvalósított hálózat van. A szenzorok figyelmeztetései kézi rádióra érkeznek a Treasures saját kommunikációs protokollját használva.

A rendszer a következő szenzortípusokat tartalmazza:

- *SAND*[21]: Intelligens, különböző terepen alkalmazható szenzorhálózat: látóhatáron kívüli érzékelésre is képes szenzorhálózat, alkalmas emberek és járművek detektálására. A szenzorok élettartama években mérhető;
- *OCEAN*: Szeizmikus/akusztikus multi-detektor, az emberek és járművek azonosítása mellett iránydetektálásra is képes, a szeizmikus-akusztikus adatok fúziója révén pontosabb célobjektum-azonosításra képes kevesebb téves riasztás mellett;
- *MID*[22]: Kis méretű éjjel/nappali (színes CCD és hő kamera), mely fejlett képfelismerő és videó-mozgásdetektálást megvalósító algoritmusokkal ellátott. A szenzorok keskenysávú UHF[23] hálózaton keresztül automatikusan továbbítják a célobjektummal korreláló optikai és hőkamerás képeket;
- *CHAMELEON 2*: Éjjel/nappal látó videó és hőkamera, forgatható állványra szerelhető, így nagy lefedettségű és képfelbontású megfigyelést tesz lehetővé. Szélessávú kapcsolaton keresztül továbbítja a videókat;
- *MTR*[24]: Kis méretű taktikai radar. Szabadalmaztatott, ultra alacsony fogyasztású, napenergiát használó szenzor. Egy kibocsátó egységet használ, mely horizontális és vertikális irányú lefedettséget is biztosít;
- *TALOS*: Nagyobb méretű felügyelet nélküli radar. Napenergiát használ, több kibocsátó egységgel rendelkezik, így minden irányból lefedettséget biztosít, többszáz méterről is képes detektálni a célobjektumokat;
- *„Pearls of Wisdom"*: Miniatűr, rejtett, felügyelet nélküli földi érzékelők, a rendszert jelenleg az amerikai hadsereg is teszteli.

A Treasures rendszer szenzorjait az 5. ábra szemlélteti:

[21] SAND: Smart All-terrain Networked Detectors
[22] MID: Miniature Imaging Device
[23] UHF: Ultra High Frequency - 300 MHz to 3 GHz közötti frekvencia
[24] MTR: Miniature Tactical Radar

5. ábra *A Treasures rendszer alkotóelemei* (saját szerkesztés)

KÖVETKEZTETÉSEK

A cikk a fellelhető releváns szakirodalom összefoglaló elemzésével ismertette a szenzorhálózatok harctéri alkalmazhatóságának előnyeit és korlátait. A témában íródott számos publikáció tanulmányozása alapján kijelenthető, hogy a felügyelet nélküli szenzorhálózatok a 21. század modern hadseregének nélkülözhetetlen kellékei, a felderítés egyik legkorszerűbb eszközei. Alkalmazásuk sikeresen integrálható a hadsereg ISTAR folyamataiba, igazolva, hogy a modern hadseregek felderítési képességeinek fejlesztése kapcsán mindenképpen figyelmet kell fordítani a felügyelet nélküli szenzorhálózatok nyújtotta lehetőségekre.

A szenzorhálózatok jellemzőinek vizsgálata alapján megállapítható, hogy habár a bennük rejlő potenciál óriási, sok esetben kompromisszumot kell kötni a rendszerek biztonsága, illetve a működéssel szemben támasztott elvárások terén. A problémát az olcsó, kisméretű szenzorok limitált erőforrásai, valamint a vezeték nélküli hálózati kapcsolat korlátai jelentik, mely számos elvárt funkció megvalósítását gátolja, legyen szó az adatok hatékony továbbításáról, feldolgozásáról vagy a számítógépes támadások elleni védelemről.

A technológiai fejlődés megállíthatatlan, a jövőben a szenzorok mérete és előállítási költsége tovább csökken majd és több száz vagy akár ezer érzékelőből álló rendszerek kerülnek kialakításra. A cikkben ismertetett problémák ugyanakkor még megoldásra várnak, a komplexebb hálózatok esetében pedig még komolyabb kihívást jelentenek majd a jövőben. Ezek alapján mindenképpen fontos a jelenlegi rendszerek hiányosságainak tanulmányozása és olyan eljárások kutatása (pl.: energia hatékony és biztonságos útvonal választási stratégiák, továbbfejlesztett kriptográfiai algoritmusok, elosztott adatfeldolgozáson alapuló megoldások), melyek a szenzorhálózatokra jellemző szűkös erőforrások nyújtotta feltételek mellett is maradéktalanul el tudják látni a funkciójukat.

A bemutatott REMBASS és Treasures rendszerek példáján látható, hogy egy rendkívül gyorsan fejlődő területről van szó, hiszen a korszerűbb Treasures esetén már számos újítás megjelenik. Nagy előrelépést jelent a szenzorok élettartamának növekedését hozó napelemes megoldások alkalmazása. A további fejlesztések a fúziós adatfeldolgozásra, képfelismerést és mozgásérzékelést megvalósító algoritmusokra koncentrálnak, lehetővé téve a minél nagyobb lefedettségű, minél pontosabb célobjektum azonosítást, kisebb számú hamis riasztás mellett.

FELHASZNÁLT IRODALOM

[1] KOVÁCS L.: *Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben*. Budapest: ZMNE, 2003. (PhD értekezés)

[2] HAIG ZS.: *Network-Centric Warfare and sensor fusion*. AARMS, 2 2 (2003), 245–256.

[3] NATO AJP-2.7 Allied Joint Doctrine for Reconnaissance and Surveillance.

[4] GULYÁS A.: *A nemzetközi különleges erők felderítő támogatása*. Hadmérnök, VII 3 (2012), 131–144.

[5] HAIG ZS., KOVÁCS L., VÁNYA L., VASS S.: *Elektronikai hadviselés*. Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[6] WINKLER, M., STREET, M., TUCHS, K. D., WRONA, K.: *Wireless Sensor Networks for Military Purposes*. In. FILIPPINE, D., Autonomous Sensor Networks. 365–394. Berlin: Springer Berlin Heidelberg, 2013.

[7] NAGY D.: *Kriptográfiai kihívások a vezeték nélküli szenzorhálózatokban*. Hadmérnök, XI 1 (2016), 183–194.

[8] BALOGH P.: *Elektronikai felderítő eszközök: szenzorok, mint a katona egyéni felszerelésének részei*. Hadmérnök, VII 3 (2012), 100–113.

[9] HAIG ZS.: *Networked unattended ground sensors for battlefield visualization*. AARMS, 3 3 (2004), 387–399.

[10] CHONG, C-Y., KUMAR, S.: *Sensor networks: evolution, opportunities, and challenges*. Proceedings of the IEEE, 91 8 (2003), 1247–1256.

[11] NAGY D.: *Possible uses of geographical information systems in wireless network systems of future*. Hadmérnök, X 5 (2015), 234–243.

[12] NAGY T. I.: *Hálózati réteg a szenzorhálózatokban*. Hadmérnök, VII 3 (2012), 123–130.

[13] NAGY T. I.: *Szenzorhálózatokkal szemben támasztott terepi követelmények*. Hadmérnök, VII 1 (2012), 202–213.

[14] NAGY T. I.: *A felügyelet nélküli szenzorhálózatok és a programozási nyelvek kapcsolata*. Hadmérnök, IV 4 (2009), 303–311.

[15] KARL, H., WILLIG, A.: *Protocols and Architectures for Wireless Sensor Networks*. West Sussex: John Wiley & Sons, 2005.

[16] WINKLER, M., TUCHS, K. D., HUGHES, K., BARCLAY, G.: *Theoretical and Practical aspects of military wireless sensor networks. Journal of Telecommunications and Information Technology*, 2 1 (2008), 37–45.

[17] ARORA, A., DUTTA, P., BAPAT, S., KULATHUMANI, V., ZHANG, H., NAIK, V., MITTAL, V., CAO, H., DEMIRBAS, M., GOUDA, M., CHOI, Y., HERMAN, T., KULKARNI, S., ARUMUNGAM, U., NESTERENKO, M., VORA, A., MIYASHITA, M.: *A Line in the Sand: A Wireless Sensor Network for Target Detection, Classification, and Tracking*. Journal Computer Networks: The International Journal of Computer and Telecommunication Networking, Special issue: Military communications systems and technologies, 46 5 (2004), 605–634.

[18] AKYILDIZ, I. F., STUNTEBECK, E. P.: *Wireless underground sensor networks: Research challenges.* Ad Hoc Networks, 4 6 (2006), 669–686.

[19] WALTERS, J. P., LIANG, Z., SHI, W., CHAUDHARI, V.: *Wireless sensor network security: A survey*. In. XIAO, Y., Security in Distributed, Grid, Mobile, and Pervasive Computing. 466–508. Boston: Auerbach Publications, 2007.

[20] BUZÁSI T.: *Jelfeldolgozás a haditechnikában. Harctéri szenzorok jelének kiértékelése*. Repüléstudományi Közlemények, 17 Különszám – Repüléstudományi konferencia (2005).

[21] BUTTYÁN L., HUBAUX J.-P.: *Security and Cooperation in Wireless Networks*. Cambridge: Cambridge University Press, 2008.

[22] REMBASS II UGS: http://www2.l-3com.com/cs-east/pdf/rembassii.pdf, (A letöltés dátuma: 2017. 05. 05.)

[23] REMBASS UGS: https://fas.org/man/dod-101/sys/land/rembass.htm, (A letöltés dátuma: 2017. 05. 05.)

[24] Treasures UGS: http://elbitsystems.com/media/TREASURES.pdf, (A letöltés dátuma: 2017. 05. 05.)

[25] MOLNÁR ZS.: *A terepi elektronikai rendszerek beépített öntesztelési lehetőségei*, Hadmérnök, III 4 (2008), 154-164.