Hadtudományi Szemle
17. évfolyam (2024) 2. szám 85–102. • DOI: 10.32563/HSZ.2024.2.8

Hevesi Judit Ildikó,[1] Haig Zsolt[2]

A folyamatos glükózmonitorozó rendszer katonai környezetben való alkalmazhatósága és sebezhetősége

Applicability of a Continuous Glucose Monitoring System in a Military Environment and its Vulnerability

Absztrakt

A cukorbetegségben szenvedők száma folyamatosan növekszik, ez pedig a katonai szolgálatot ellátókat is egyre nagyobb mértékben érinti. A vércukorszint aktuális ismerete és nyomon követése alapvető fontosságú az extrém magas és alacsony vércukorértékek elkerülésében. A diabétesz kezelésében ma már elérhetők olyan új technológiák, amelyek jó lehetőséget nyújtanak abban, hogy a diabéteszes katonák igénybe vehetők legyenek különböző katonai feladatokban. A tanulmány egy ilyen új szenzortechnológiát, a folyamatos glükózmonitorozásra alkalmas szenzorrendszert tárgyalja. Bemutatja a cukorbetegség és az egészségi alkalmasság összefüggéseit, elemezi a szenzorrendszer alkalmazási lehetőségeit, előnyeit, esetleges hátrányait, kitérve a katonai környezet sajátosságaira. A katonai környezetből adódóan vizsgálja a rendszer sebezhetőségét, a vele szemben alkalmazható fenyegetéseket.

Kulcsszavak: diabétesz, egészségi alkalmasság, glükózmonitorozás, szenzor, Bluetooth LE sebezhetőség

[1] Rendelésvezető főorvos, Észak-Pesti Centrumkórház-Honvédkórház Szakrendelő Intézet Diabetológia Szakrendelés, e-mail: hevesi.judit0607@gmail.com

[2] Egyetemi tanár, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Elektronikai Hadviselés Tanszék, e-mail: haig.zsolt@uni-nke.hu

Abstract

The number of people suffering from diabetes is constantly increasing, and this also affects those who serve in the military. Actual knowledge of blood sugar levels is essential to avoiding extremely high and low blood sugar values. New technologies are now available for the treatment of diabetes, which offers a good opportunity for soldiers with diabetes to be deployed for various military missions. This paper discusses one such new sensor technology, the continuous glucose monitoring system. The study presents the connections between diabetes and health fitness, analyses the application possibilities, advantages, and possible disadvantages of the sensor system, focusing on the specifics of its use in the military environment. Due to the military environment, the study examines the vulnerability of the system and the threats that can be applied against it.

Keywords: diabetes, health fitness, glucose monitoring, sensor, Bluetooth LE vulnerability

Bevezetés

A cukorbetegség *(diabetes mellitus)* globális előfordulása folyamatosan nő, és az abban szenvedők száma világszerte járványos méreteket ölt. A globális betegszám a 20–79 éves korosztályban 2030-ra már akár a 643 millió főt is elérheti.[3]

A diabétesznek több típusa ismert, a kialakulás szerinti csoportosítás alapján a betegek legnagyobb része – mintegy 90%-a – a 2-es típusba (Type-2 Diabetes Mellitus – T2DM) tartozik, amelyre inkább a felnőttkori kialakulás jellemző. Létrejöttének oka a hasnyálmirigy által termelt inzulinhormon hatásának az elmaradása vagy elégtelensége. A kezelésének alapja a megfelelő életmód, ami fokozott fizikai munkavégzést és adekvát étrend alkalmazását jelenti. Emellett gyógyszeres kezelésre is szükség van, a T2DM-ben használható készítmények palettája rendkívül széles.

A betegek kisebb hányadánál, közel 10%-uk esetén beszélünk 1-es típusú megbetegedésről (Type-1 Diabetes Mellitus – T1DM), amelynél a betegség kialakulásának oka az inzulint termelő sejtek elpusztulása, aminek következtében abszolút inzulinhiány alakul ki. Az ebben a változatban szenvedő betegek vércukorszint-csökkentő terápiája csak az inzulin lehet, amely az ő esetükben az életben maradáshoz szükséges.

A diabétesz globális előfordulásának növekedése érinti a Magyar Honvédség kötelékében szolgálókat is, akiknek az egészségi alkalmasság tekintetében szigorú feltételeknek kell megfelelniük. Az ő esetükben rendkívül jelentős szerepe van a fizikai és mentális állapotot befolyásoló extrém magas vagy alacsony vércukorértékek elkerülésének. Ez az önmenedzselés célja, legfőbb eszköze pedig a vércukorszint aktuális ismerete. E célból a betegek alkalmazhatják az ujjbegyből történő vércukorszint-önellenőrzést (*self monitoring of blood glucose* – SMBG, újabb elnevezéssel *blood glucose monitoring* – BGM), valamint a bőr alá behelyezett érzékelőt magában foglaló folyamatos szöveti glükózmonitorozó rendszert (*continuous glucose monitoring system* – CGMS).

[3] International Diabetes Federation 2021: 11–19.

A CGMS új technológiaként jó lehetőséget teremthet arra, hogy a rövid távú szövődmények, mint az extrém magas és alacsony vércukorértékek, kordában tarthatók legyenek, így például a diabéteszes katonák a korábbiaknál nagyobb biztonsággal igénybe vehetők különböző katonai feladatokban, esetleg missziós küldetésekben is alkalmazhatók lehetnek.

A vezeték nélküli beültetett egészségügyi eszközök elterjedésével (mint például a CGMS) növekszik az aggodalom, hogy illetéktelenek átvehetik ezen eszközök felett az irányítást, manipulálhatják az egészségügyi adatokat, vagy drasztikusabb esetben súlyos, akár halálos kimenetelű folyamatokat indíthatnak el. Jelenleg ugyan nem ismertek olyan incidensek, amelyek arra utalnának, hogy a betegeket orvosi eszközükön keresztül érték volna fenyegetések. A problémát azonban jól mutatja, hogy Dick Cheney volt amerikai alelnök egykor attól tartott, hogy a terroristák a szívéhez közel beültetett defibrillátorral[4] megölhetik őt. Emiatt 2007-ben azt egy olyan eszközre cserélték le, amelynek nem volt vezeték nélküli vezérlőeleme, amihez illetéktelenek hozzáférhettek volna.[5]

Azóta is számos kutatás lát napvilágot arról, hogy hogyan lehet feltörni vezeték nélküli egészségügyi eszközöket. 2011-ben például egy Las Vegas-i biztonsági konferencián egy 150 méterrel távolabb elhelyezett inzulinpumpát tudtak kikapcsolni, illetve inzulintúladagolást előidézni.[6] A vezeték nélküli beültetett egészségügyi eszközök elterjedésével nő a reális esélye annak, hogy ezeken keresztül a betegek ki vannak téve fenyegetéseknek. Különösen indokolt az aggodalom a magas vezetői pozíciókban lévő személyek, így akár katonai vezetők esetében. Az ilyen fenyegetések eredménye lehet a mért adatok jogosulatlan felhasználása, nyilvánosságra hozatala, kompromittálása, módosítása vagy az eszköz funkcióvesztése.

A vázolt tudományos probléma alapján a tanulmány célja ismertetni a cukorbetegség és az egészségügyi alkalmasság összefüggéseit, elemezni a CGMS alkalmazási lehetőségeit, előnyeit, esetleges hátrányait, kitérve a katonai környezet sajátosságaira. További célul tűztük ki, hogy megvizsgáljuk a CGMS sebezhetőségét, és néhány módszer bemutatásával alátámasszuk a fenyegetés valós jellegét.

Cukorbetegség melletti katonai alkalmasság kérdése

A cukorbetegség mint krónikus kórállapot nem feltétlenül zárja ki a katonai szolgálat folytatását, de a fizikális és pszichés állapotra hatva sajátos foglalkozási kihívásokkal jár. A Magyar Honvédség kötelékébe tartozók egészségi alkalmasságának feltételeit rendeletek és utasítások rögzítik.[7] Diabétesz fennálltakor a minősítés nem a cukorbetegség típusától, hanem elsősorban a kezelés formájától és a betegség kimenetelét is meghatározó hosszú távú szövődmények súlyosságától függ.

[4] A mellkas falába beültetett eszköz, amely életveszélyes szívritmuszavar esetén elektromos impulzusokat leadva visszaállítja a normál ritmust.
[5] Daily Mail Reporter 2013.
[6] Klonoff 2015.
[7] 2012. évi CCV. törvény; 9/2013. (VIII. 12.) HM rendelet; 10/2015. (VII. 30.) HM rendelet.

A diabétesz rövid távú (akut) szövődményei az extrém magas (hiperglikémia) és alacsony vércukorérték (hipoglikémia) kialakulásával kapcsolatosak, amelyek az általuk okozott panaszokkal és tünetekkel nemcsak befolyásolják a munkateljesítményt, hanem életveszélyes állapotot is teremthetnek. Egészséges egyénekben a vércukorszintet a szervezet szigorúan szabályozza, körülbelül 3,9–7,8 mmol/l között. A 7,0 mmol/l vagy afeletti éhomi[8] és a 11,1 mmol/l vagy afeletti étkezéstől független random értékek a cukorbetegség diagnosztikai kritériumát jelentik.[9] A normál tartományon kívül eső vércukorértékekre adott reakciók vércukor-értékhatára és intenzitása egyénfüggő. Heterogén ideg- és elmezavar tünetei jelentkezhetnek koncentrációs nehézséggel, érzelmi és kognitív zavarral, az akaratlagos mozgást befolyásoló motoros rendellenességekkel, súlyosabb esetben beszűkült tudatállapot, eszméletvesztés és kóma is kialakulhat. A hirtelen kialakuló magas vércukorszintet is megérezheti a beteg szédülésre, látászavarra, fáradékonyságra stb. panaszkodva, de a tartósan magas érték már komplex anyagcserezavart okoz. Kiváltó okként étrendi hiba, a terápia elégtelensége, fertőző betegségek, baleset stb. szerepelhet.[10] A váratlanul kialakuló hipoglikémia (3,9 mmol/l vagy az alatti vércukorszint) veszélyesebb. A kezelés mellékhatásaként alakul ki elsősorban inzulinterápia alkalmazása esetén, de bizonyos szájon át alkalmazható vércukorszint-csökkentő készítmények is hajlamosítanak a létrejöttére.[11] A közvetlen ok lehet nagyobb dózisú inzulin mellett fokozott fizikai munkavégzés vagy diétahiba. A betegek leggyakoribb okként az inzulin beadása után valamilyen váratlan esemény miatti kimaradt étkezést szokták megemlíteni. A kezdeti tünetek (fokozott verejtékezés, kézremegés, koncentrációs nehézség stb.) észlelésekor fokozott szénhidrátbevitellel a súlyosabb, már külső segítséget igénylő állapot megelőzhető. Hosszabb betegségtartam és gyakori hipoglikémiás epizódok mellett előfordulhat, hogy a szervezet kevésbé reagál az alacsony vércukorértékre, és ennek eredményeként nem jelentkeznek a típusos tünetek, panaszok. Ebben az esetben bevezető tünetek hiányában a beteg nem tud idejében beavatkozni, és az addig jó állapotban lévő személynél hirtelen jelentkezik a potenciálisan életveszélyes tudatzavar.[12]

A hipoglikémia kialakulása nemcsak a személyes egészséget befolyásolhatja, hanem jelentős hatással lehet a katonai tevékenységekre is, hiszen a koncentráció, az ítélő- és a döntéshozatali képesség elvesztése kritikus helyzetet teremthet.

A magyar jogszabályok alapján a csak inzulinnal kezelhető T1DM fennállása foglalkozás-egészségügyi szempontból alkalmatlansággal vagy bizonyos esetekben beosztási, munkaköri, illetve fegyvernemi korlátozásokkal jár, leggyakrabban a katonai karrier végét jelenti.[13] A T2DM azonban nem jelent feltétlenül alkalmatlanságot, akár külszolgálat is vállalható mellette. A cukorbetegség minden típusára igaz, hogy a kiszámíthatatlan életmód és az intenzív fizikai követelmények a szénhidrát-anyagcsere labilitását okozzák, ami az akut szövődményekkel életveszélyes helyzeteket teremt, lehetetlenné téve az aktív szolgálatot. A műveleti terület jellemzői, a kiszámíthatatlan

[8] Az utolsó energiafelvételt követően minimum 10 óra elteltével.
[9] Agiostratidou 2017: 1624; A Belügyminisztérium egészségügyi szakmai irányelve a diabetes mellitus kórismézéséről, a cukorbetegek antihyperglykaemiás kezeléséről és gondozásáról felnőttkorban 2023: 1156.
[10] Winkler–Baranyi 2014: 33–38.
[11] Agiostratidou 2017: 1624.
[12] Winkler–Baranyi 2014: 17–20; Yu et al. 2023.
[13] 10/2015. (VII. 30.) HM rendelet.

étkezés, a rendszertelen alvás bármilyen – még a cukorbetegség szintjét el nem érő – szénhidrát-anyagcserezavar esetén is lehetetlenné teszi az életmód kezelését, és jelentős korlátokat szab a gyógyszeres kezelésnek, illetve az önmenedzselésnek. Fokozottan igaz ez a nemzetközi missziós tevékenységekre, ahol egy tengerentúli utazás, az időzónák többszörös megváltoztatása, az extrém időjárás és terepviszony, az esetleg rossz egészségügyi környezet tovább fokozza az anyagcsere-labilitást.[14]

Az önmenedzselés eszköze: a CGMS

A diabétesz kezelésének célja a beteg életminőségének megőrzése és a szövődmények kialakulásának elkerülése, a krónikus szövődmények időben való kitolása. Ennek egyik eszköze a megfelelő glikémiás kontroll, azaz a vércukorértékek megfelelő (terápiás) tartományban tartása. A legújabb amerikai szakmai ajánlás[15] a vércukorszint-csökkentő kezelés hatékonyságának ellenőrzésére az alábbi módszereket javasolja:

- vénás vérvétellel nyert vérmintából laboratóriumi körülmények között meghatározott hemoglobin A1c (HbA1c) érték mérése;[16]
- SMBG alkalmazása;
- CGMS alkalmazásával a tartományban töltött idő (*time in range* – TIR)[17] és az átlagos CGM glükózértékeinek meghatározása.

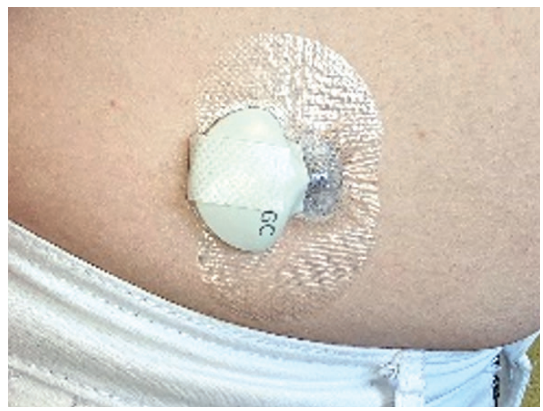
A vércukor-önellenőrzés minden cukorbetegnek javasolt, inzulinkezelés mellett elengedhetetlen, hiszen ez utóbbi esetben az aktuális vércukorszint ismerete a sikeres önmenedzselés feltétele. Az SMBG alkalmazásakor a beteg ujjbegyéből nyert vércsepp tesztcsíkhoz érintése vagy rácseppentése után pár másodpercen belül megjelenik a glükométeren a kapillárisból származó vér glükózkoncentrációja mmol/l vagy mg/dl mértékegységben. Az eljárás hátránya a szúrás, az ebből adódó fertőzésveszély, az összetett feladatsor, az eszközigény és az idő, amely a legkritikusabb tényező a hipoglikémiás rosszullét elhárításakor.

A CGMS áttekintése

A CGMS valós idejű (*real-time,* rtCGMS) típusa a társadalombiztosítási támogatásnak köszönhetően az utóbbi években hazánkban is elterjedt, elsősorban az inzulinnal kezelt betegek körében. Az elérhető készülékek működési elve azonos. A beteg a rendszer érzékelő részét, amely egy vékony, körülbelül 1 cm hosszúságú érzékelőszál, a felkar vagy a has területén a bőr alatti szövetbe helyezi. Ennek a bőr feletti részéhez csatlakoztatandó a távadó, amely egyrészt a szöveti glükózkoncentráció értékét (amely

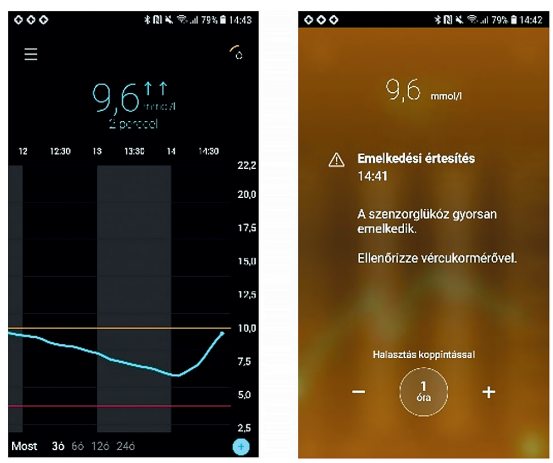
[14] Folaron et al. 2018.
[15] American Diabetes Association Professional Practice Committee 2024.
[16] A HbA1c érték az elmúlt kb. 3 hónap átlagos vércukorértékére enged következtetni.
[17] A TIR azt mutatja meg, hogy a CGMS technikával mért vércukor-koncentrációs értékek az időtartam hány százalékában tartózkodtak a céltartományban (3,9–10,0 mmol/l).

a vénás vércukorértéket tükrözi) típustól függően 2–5 percenként közvetíti a rendszernek, másrészt az érzékelő rész tápegységeként is szolgál (1. ábra).



1. ábra: Guardian Connect távadó a has területén elhelyezve
Forrás: a szerzők felvétele

A távadó bluetooth-kapcsolatban áll a beteg valamilyen okoseszközével, általában okosórával vagy mobiltelefonnal, amelyen megfelelő applikációval a beteg numerikus és grafikus formában követni tudja a vércukorértékét és annak változási irányát és intenzitását. A rendszerben különféle riasztó funkciókat is be lehet állítani, amely a beteget értesíti, ha az érték bizonyos értékhatáron kívülre kerül, vagy ha gyorsan változik (2. ábra).[18]



2. ábra: A Guardian 3 CGMS applikációjának kezdőképernyője mobiltelefonon és a szenzorglükóz érték gyors emelkedési riasztásának megjelenítése
Forrás: a szerzők felvétele

[18] Hevesi 2023.

Ma már mindennapos klinikai gyakorlat T1DM kezelésében olyan folyamatos inzulinadagoló eszköz (inzulinpumpa) alkalmazása, amelyet CGMS-szel integráltak. Ezzel az inzulinkezelés további finomhangolása vált lehetővé, hiszen az inzulinpumpa a szenzor által mért szöveti vércukor-koncentrációhoz igazítja az adagolt inzulin dózisát.

A CGMS alkalmazásának előnye

A CGMS által észlelt szöveti vércukorértékeket felhőalapú rendszerben tárolják, amelyek az interneten keresztül követhetők, letölthetők. Ezzel a szenzortechnika lehetővé teszi a vércukorérték folyamatos, valós idejű monitorozását nemcsak a beteg, hanem a hozzátartozója vagy a kezelőszemélyzet számára is (3. ábra).

3. ábra: A szenzorglükóz értékének megjelenítése, tárolása és megosztása vezeték nélküli kapcsolattal
Forrás: a szerzők szerkesztése

A nagyszámú és rendszeresen hozzáférhető vércukorértékeknek köszönhetően a szénhidrát-anyagcsere objektívebb megismerése elősegíti a terápia optimalizálását, az inzulindózisok finomhangolását. A készülék típusától függő napi 288–1440 vércukorértékből számos statisztikai paramétert is megad a rendszer, amelyek közül többet a mindennapos cukorbeteg-gondozás során is alkalmazunk.[19]

A CGMS használata a riasztó funkcióknak köszönhetően segít megelőzni az extrém magas és alacsony vércukorértékek kialakulását, illetve lehetővé teszi azok felismerését, a gyors reagálást azok elhárítására; és a válaszreakció hatásossága is könnyen ellenőrizhető. Mindezzel a beteg biztonságérzete nőhet, hiszen jobban tud alkalmazkodni az akár szélsőséges élethelyzetekhez is, bátrabban végezhet fizikai munkát, nem kell aggódni az éjszakai extrém vércukorértékek miatt stb., összességében az életminősége

[19] Hevesi 2024.

javul. Az SMBG-hez hasonlítva a szenzor használata egyszerűbb, hiszen az eszközt a típusától függően hetente vagy ritkábban kell cserélni, és nincs szükség ujjbegyszúrásra. Megjegyzendő, hogy a jelenleg Magyarországon elérhető szenzorok egy része a megfelelő analitikai pontosság céljából kalibrációt igényel, ami azt jelenti, hogy a betegeknek napi 1-2 alkalommal SMBG-technikával pontosítani kell.

A CGMS alkalmazásának hátránya

A CGMS alkalmazásának hátrányaként említendő az eszközigény és az anyagi teher, hiszen csak megfelelő szoftververziójú okoseszközön tud problémamentesen működni. A technológia használata némi technikai tudást is feltételez a bluetooth-, illetve internetkapcsolat létrehozásában, az érzékelő beszúrásában, az okoseszköz kezelésében. Habár a CGMS csak minimálisan invazív technika, mégis fertőzésforrás lehet. Az eszköz rögzítéséhez szolgáló tapaszok bőrirritációt okozhatnak, fizikai munkavégzéssel vagy akár pszichés stresszel járó fokozott verejtékezés esetén pedig a rögzítés leválhat. A nagy mennyiségű adat a betegeknek zavaró lehet, negatívummá is válhat azáltal, hogy naponta több alkalommal állítja őket döntéshozás elé, ami megnöveli a kóros válaszreakció lehetőségét. Ez is indokolja, hogy a szenzort használó beteget részletes edukációban kell részesíteni, amely során ki kell térni arra is, hogy mely szenzoradatnál kell feltétlenül beavatkozni (több vagy kevesebb szénhidrátot fogyasztani, csökkenteni vagy növelni a gyors felszívódású szénhidrát mennyiségét, pluszinzulint beadni stb.).

A szenzortechnika használatának gátját jelenti, hogy korlátozottan vízálló, a mágneses tér befolyásolhatja annak működését, és nem tanácsos lézernyaláb útjában sem tartani, illetve különféle képalkotó vizsgálatok – mágneses rezonancia (MRI, MR) vagy komputertomográfia (CT) – során sem javasolt a viselése.

A cikk témája szempontjából kiemelendő, hogy a rendszer rádiófrekvenciás kapcsolaton keresztül kommunikál a beteg okoseszközével, ami jó lehetőséget kínál egy rosszindulatú támadónak, hogy szándékosan korlátozza a CGMS működését, esetleg manipulálja a mért értékeket.

A CGMS használata katonai környezetben

Az amerikai hadsereg egészségügyi központjának kutatói megállapították, hogy például a CGMS használata és a szigorú felkészítés lehetővé teszi, hogy kialakult T1DM mellett a motivált katonák továbbra is aktív szolgálatban maradjanak, illetve akár műveleti területen is részt vegyenek katonai feladatokban.[20] Emiatt egyes haderőkben, mint például az Amerikai Egyesült Államok hadseregében szolgálók körében a cukorbetegség típusától függetlenül támogatott bizonyos CGMS-k használata.[21]

Katonai környezetben a CGMS alkalmazásának számos előnye lehet. Hatékonyabbá tehető a kezelés, amivel javítva a vércukorszint kontrollját, mind az akut, mind a krónikus

[20] Choi–Cucura 2018.
[21] *Diabetic Supplies and Equipment* [é. n.].

szövődmények nagyobb eséllyel előzhetők meg. Segíthet az optimális kondicionálási stratégiáknak megfelelő vércukorérték azonosításában. Az egészségi állapot figyelemmel kísérésével és javításával a szenzortechnika növelheti a betegbiztonságot és az önmenedzselés hatékonyságát, amelyekre a műveletek során kifejezetten szükség van. A szenzor, amelyet a felkaron vagy a has területén helyezünk el, kis méretéből adódóan nem befolyásolja a mozgást, megfelelő rögzítés esetén nem mozdul ki.

Ugyanakkor katonai környezetben, különösen műveleti feladatok végrehajtásakor a CGMS nem csak a cukorbeteg katonák esetében alkalmazható. A technológia jól kapcsolódhat a „digitális katona" koncepcióhoz, amelynek egyik fontos eleme a katona fiziológiai/egészségi állapotának valós idejű, folyamatos monitorozása. A katonán elhelyezhető különböző szenzorok ma már alkalmasak többek között a légzés, a szívműködés, a vérnyomás, a testhőmérséklet, az alvás-ébrenlét ciklus stb. megfigyelésére. A mért paraméterek alapján mind a katona, mind a parancsnok képet kaphat a katona állapotáról (például lehűlés, oxigénhiány, anyagcsereromlás, folyadékhiány, pszichés stressz, kialvatlanság stb.).[22] Ebbe a rendszerbe illeszthető és képességeit kiterjesztheti a CGMS, amellyel akár az egészséges katona vércukorszint-ingadozása is nyomon követhető. Normál szénhidrát-anyagcserés állapot esetén a vércukorszint általában stabil marad, de bizonyos esetekben, mint például tartós éhezésnél, extrém fizikai megterhelés vagy érzelmi stressz hatására, esetleg súlyos fertőző betegség fennállásakor kórosan alacsony vagy magas vércukorértékek is előfordulhatnak. Ebben az esetben a szenzortechnika alkalmas lehet a teljesítmény optimalizálására, valamint változó tápanyag-összetételű ételeknek, illetve a fizikai aktivitást jellemző minőségi és mennyiségi paramétereknek a vércukorszintet befolyásoló egyéni hatásainak elemzésére is.

A félig invazív technológia azonban magában hordozza a fertőzés veszélyét, amely szélsőséges környezeti helyzetben fokozottabb. Ebből a szempontból előnyösebbek lennének a még fejlesztés alatt álló nem invazív vércukormérési eljárások, mint például a spektroszkópia, a bioimpedancia, az optikai koherencia tomográfia stb., amelyek során nem vérmintából történik a vércukor-koncentráció meghatározása.

Katonai környezetben emellett fokozottabban kell számolni a CGMS elleni szándékos fenyegetésekkel, különösen a szenzort használó katonai vezetők körében. Az ilyen jellegű fenyegetések valószínűsége nemcsak a katonák körében merül fel, hanem minden olyan személy esetében is, akik kulcsfontosságú vezetőknek számítanak.

A CGMS ellen alkalmazható fenyegetések

A bevezetésben említett példa szerint, illetve a katonai környezetben való alkalmazhatóság miatt reálisan kell számolnunk a CGMS elleni fenyegetésekkel. A CGMS elleni fenyegetések elméletileg a következők lehetnek:

- az okostelefonra telepített mobilalkalmazás elleni fenyegetések;
- a CGMS érzékelője elleni fenyegetések;
- az érzékelő és az okoseszköz közötti kommunikáció elleni fenyegetések.

[22] Kóródi 2005: 28.

A mobilalkalmazások elleni gyakori fenyegetésnek tekinthetők azok a rosszindulatú programok, amelyek egészségügyi adatokat szivárogtathatnak ki, vagy olyan nem hivatalos CGMS-alkalmazások, amelyek hamis glükózértékeket adnak. Egy kutatás számos olyan, a cukorbetegség kezelésével kapcsolatos rosszindulatú mobilalkalmazást talált, amelyek szándéka nem feltétlenül a beteg egészségének károsítása, hanem elsősorban az anyagi haszonszerzés a motiváció.[23]

A CGMS-szenzor elleni fenyegetés noha elméletileg lehetséges (például az érzékelő manipulálása nem valós vércukorértékek előállítása érdekében), eléggé nehezen kivitelezhető, így a gyakorlatban nem számolunk vele.

A CGMS-szenzor és az okoseszköz közötti, vezeték nélküli kommunikációt a Bluetooth Low Energy (BLE) technológiával valósítják meg. A BLE ellen sokféle támadási formát alkalmazhatnak, amelyeket alapvetően két nagy csoportba lehet sorolni: 1. passzív lehallgatás és 2. aktív ellentevékenység. A passzív lehallgatás során a támadó csupán adatokat kíván megszerezni. A lehallgató ez esetben nem módosítja a mért értékeket, csak hozzáférést szerez a potenciálisan érzékeny információkhoz. Habár a vércukorértékek egészségügyi személyes adatoknak minősülnek, a CGMS esetében ez a kevésbé kritikus támadási forma.

Az aktív ellentevékenység során a támadó szándéka lehet, hogy megakadályozza a távadó és az okoseszköz közti kommunikációt, aminek eredményeként a beteg nem kap folyamatos információt a glükózértékekről. Ezt a fizikai rétegben indított elektronikai zavarással lehet megvalósítani. A másik módszer az adatkapcsolati rétegben alkalmazott úgynevezett közbeékelődéses (*man in the midle* – MITM) támadás, amely a két fél közötti kommunikációt kompromittálva képes a felhasználói adatok manipulálására. Ennek célja lehet, hogy a támadó meghamisítsa a valós mért glükózértékeket, és azokat juttassa el a beteg okoseszközére. Mindkét aktív támadás komoly egészségi kockázatot hordoz. A továbbiakban, a BLE-technológia rövid áttekintése után, a súlyosságukat tekintve e két aktív ellentevékenység kivitelezését elemezzük alaposabban.

A BLE-technológia áttekintése

Mára alapvetően kétféle bluetooth-technológia terjedt el: a Bluetooth Classic és a BLE. A Bluetooth Classic egy kis teljesítményű, vezeték nélküli átviteli technológia, amely a 2,4 GHz-es ISM[24] frekvenciasávban pont-pont kommunikációra szolgál. Mára e technológia a vezeték nélküli hangszórók, fejhallgatók és autós szórakoztatórendszerek szabványos protokolljává vált.[25]

A BLE, mint ahogy az elnevezéséből is kitűnik, egy igen alacsony energiafelhasználású technológia. Létrejöttének és elterjedésének egyik fontos hajtóereje volt az IoT[26] megjelenése és robbanásszerű terjedése az élet minden területén. Az IoT-eszközök többnyire csak időszakos használatot igényelnek, és kisméretű adatállományokat

[23] Apvrille–Lakhani 2019.

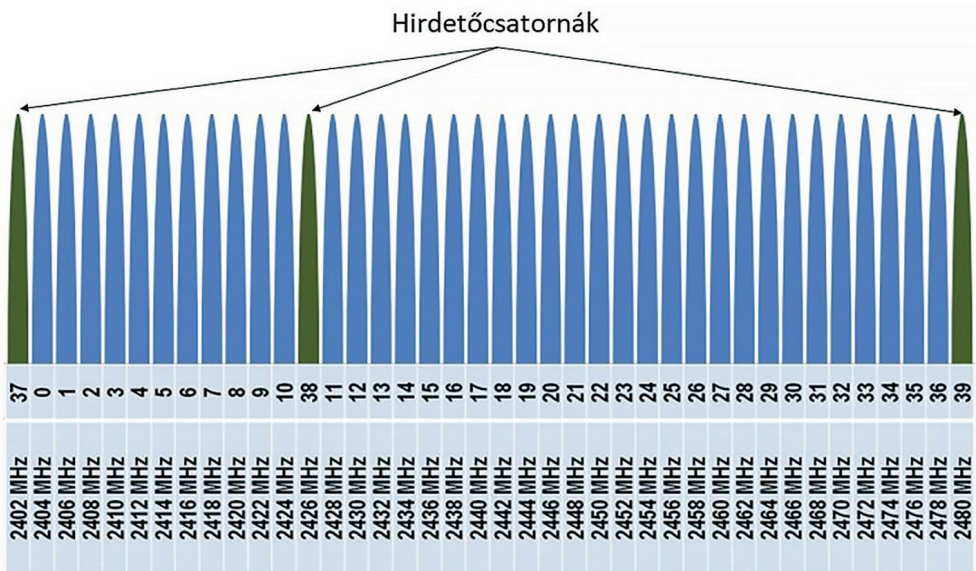
[24] Industrial, Scientific and Medicine – ipari, tudományos és orvosi felhasználású frekvenciasáv, amely nem engedélyköteles, vagyis szabadon felhasználható sáv.

[25] *The Bluetooth® Low Energy Primer* 2023.

[26] Internet of Things – a dolgok internete. A CGMS is egy IoT-eszköznek tekinthető.

továbbítanak alacsony átviteli sebességgel. Ez igaz a CGMS-re is, hiszen itt sincs szükség folyamatos adatkapcsolatra. A szenzor által mért szöveti glükózszintértékek kisméretű adatállományok (néhány 10–100 byte), amelyeket a távadó meghatározott időnként továbbít a beteg okoseszközére.

Ez a technológia szintén a 2,4 GHz-es ISM sávban működik, és 40 csatorna (3 hirdetőcsatorna és 37 adatcsatorna) felhasználását teszi lehetővé (4. ábra). A szabvány szerint a BLE-technológiában a maximális kimeneti teljesítményszintnek 0,01 mW (-20 dBm[27]) és 100 mW (+20 dBm) között kell lennie.[28] A gyakorlatban azonban ennél alacsonyabb teljesítményszinteket mérhetünk egy BLE-hálózatban.



4. ábra: BLE-frekvenciasáv adat- és hirdetőcsatornái
Forrás: Bluetooth LE – Nordic 2020

A bluetooth-kapcsolat megbízhatóságát adaptív frekvenciaugratásos adásmóddal (*frequency hopping spread system* – FHSS) biztosítják. Az FHSS adásmód azt jelenti, hogy az adó- és vevőoldalon szinkronban változtatjuk a vivőfrekvencia pillanatnyi értékét. A BLE frekvenciasávjában (2,402–2,480 GHz) felhasználható vivőfrekvenciák értékét egy álvéletlen kóddal változtatjuk, amelyet a szinkronitás miatt megosztunk az adóval és a vevővel. Az adaptív frekvenciaugratás lehetővé teszi a frekvenciakészletből azon frekvenciák kiválasztását, amelyeken más eszközök nem forgalmaznak, ezzel is csökkentve az interferenciák kialakulását.

A BLE-protokoll biztosítja, hogy a szerverként működő CGMS-szenzor távadója kommunikációs kapcsolatot létesítsen, és továbbítsa a vércukorértékeket egy kliensként csatlakoztatott okoseszköz felé. Ez a kommunikációs eljárás öt lépésből áll:

[27] Logaritmusos teljesítmény-mértékegység, a teljesítmény mértéke 1 mW-ra vonatkoztatva: 1 mW=0 dBm.
[28] *The Bluetooth® Low Energy Primer* 2023.

- a szerver a hirdetőcsatornákon (37, 38, 39) az azonosítóját tartalmazó hirdetőcsomagok adásával jelzi a jelenlétét;
- a kliens ugyanazon csatornákon hirdetőcsomagokat keres, és amennyiben talál, akkor vezeték nélküli kapcsolatot létesít vele;
- a kliens opcionálisan párosítást végezhet a szerverrel egy titkos kulcs megosztásához, ami az adatok titkosítására és hitelesítésére szolgál;
- a kliens hozzáférést kezdeményez a szerveren tárolt adatokhoz;
- a szerver ellenőrzi, hogy a kliensnek van-e joga hozzáférni a kért adatokhoz, és ha igen, a szerver engedélyezi azt.

A szerveren (CGMS-távadón) tárolt vércukorértékek attribútumokba vannak rendezve, és minden egyes attribútumot egyedi azonosítóval látnak el. A szerver minden egyes attribútumhoz meghatározhat egy házirendet, ami leírja, hogy hogyan lehet hozzáférni (csak olvasható, csak írható, vagy írható és olvasható), és milyen biztonsági szint szükséges a hozzáféréshez: 1. biztonság nélkül; 2. csak titkosítással; 3. titkosítással és hitelesítéssel; illetve 4. erős titkosítással és hitelesítéssel. Amikor egy hozzáférési kérelem érkezik az okoseszköztől, a távadó ellenőrzi, hogy az aktuális kapcsolat megfelel-e a biztonsági szintnek, amely a kért attribútum eléréséhez szükséges. Ha nem megfelelő, akkor elutasítja a kérést, és hibaüzenetet küld vissza.

Ha a titkosítás és/vagy a hitelesítés szükséges egy attribútum eléréséhez, abban az esetben párosítás szükséges egy megosztott titkos kulcs generálásához.[29] Mivel a vércukorértékek szenzitív adatoknak minősülnek, azok csak biztonságos adatkapcsolaton keresztül továbbíthatók. Emiatt a CGMS-eknek párosítási kötelezettséget kell előírniuk.

A CGMS BLE-kommunikációjának elektronikai zavarási lehetőségei

Az elektronikai zavarás alapvetően egy katonai területen alkalmazott ellentevékenységi módszer. Mára azonban a civil infokommunikációs technológiák ellen is egyre inkább alkalmazott technikává vált. Így a CGMS-ben használt BLE-kapcsolat is ki van téve a rádiófrekvenciás térből érkező fenyegetéseknek.

A BLE esetében teljességgel ismertek a hálózat paraméterei (frekvencia, teljesítmény, moduláció stb.), amelyek alapján a zavarás megvalósítható. A zavarás minden esetben a vevőponton érzékelhető, így a CGMS esetében az okoseszköz vevője lesz a zavart elszenvedő. A zavarás hatékonynak számít, ha a vevő bemenetén a zavaró jel és a hasznos jel teljesítményének aránya (*jamming to signal ratio* – J/S, zavarási tényező) nagyobb, mint az adott adásmódnak megfelelő zavarási tényező minimális értéke. A BLE esetében a jó zavarvédettséget biztosító frekvenciaugratásos adásmódnak köszönhetően ez akár több 10 dB[30] értéket is megkövetelhet.

[29] Wu et al. 2020.
[30] Két teljesítményszint arányának logaritmikus mértéke.

A kommunikációs rendszerek zavarására különféle zavarjelek alkalmazhatók. A két alapvető zavartípus a célzott és a széles sávú zavar. A célzott zavarás egy egyfrekvenciás zavarási mód, amelynek nagy a teljesítménysűrűsége, de egyszerre csak egy csatornát képes zavarni. A széles sávú zavarás ezzel szemben széles sávon sok csatornát zavar, azonban a teljesítménysűrűsége a sávszélességgel arányosan csökken. Ezek előnyeit ötvözi a csúszó- és a fésűzavarás. A csúszózavarás esetében a vevő vételi sávjában nagy sebességgel csúsztatják a zavarjelet, így az minden egyes időpillanatban nagy teljesítményű kvázi célzott zavarásnak tekinthető. A fésűzavarás esetében pedig az előre meghatározott csatornákra leprogramozott zavaró egy időben több csatornán zavarja a célzott csatornákat. A leghatékonyabb, de egyben a legnehezebben kivitelezhető zavarási mód a követőzavarás, amikor a zavaró követi a frekvenciaugrásokat, és csak azokon zavar.[31]

Elméletileg a CGMS BLE-kommunikációjának zavarására mindegyik megoldás alkalmazható. Ugyanakkor a frekvenciaugratásos adásmód igen nagy fokú zavarvédelmet jelent a keskeny sávú célzott zavarokkal szemben. Voltak ugyan kísérletek intelligens zavarás megvalósítására,[32] amelynek során a címzés dekódolásával és a kommunikáció órajelének megbecsülésével a zavaró a frekvenciaugrásokkal szinkronban sugározza a zavarjeleket. A zavarás sikeréhez azonban a frekvenciaugratás szekvenciájának és órajelének helyes becslésére van szükség, aminek kicsi a valószínűsége. A csúszó- és a követőzavarás szintén nehezen megvalósítható, mivel a gyors frekvenciaugratás miatt rendkívül kevés (néhány tíz µs) idő áll rendelkezésre a zavaró folyamatos áthangolásához, illetve a frekvenciaugrások lekövetéséhez.

A fésűzavarással az adatcsatornák zavarása tulajdonképpen nem igazán értelmezhető, mivel a frekvenciasávban a 40 csatorna közvetlenül egymás mellett helyezkedik el, tehát ez esetben a teljes sávot kell folyamatosan zavarni, ez pedig már a széles sávú zavarásnak tekinthető. Megoldható viszont, hogy fésűzavarással nem mind a 40 csatornát zavarjuk, hanem csak a hirdetőcsatornákat. A hirdetőcsatornák (37, 38, 39) frekvenciája ismert: 2402, 2426 és 2480 MHz, így e frekvenciák zavarása eredményeként a kliens, vagyis a CGMS esetében az okoseszköz nem tudja venni a távadó hirdetőcsomagjait, és a párosítást nem képes elvégezni a két eszköz.

A széles sávú zavarás elegendő teljesítményt feltételezve hatékony támadási technikának tekinthető. Ennek keretében egy viszonylag nagy teljesítményű zavaró jelet sugárzunk ki folyamatosan a BLE teljes 78 MHz széles frekvenciasávjában. A BLE elméleti specifikációjának megfelelve, a gyakorlatban 1–6 mW (0–8 dBm) közötti teljesítménnyel számolhatunk. Ezzel szemben a zavaró eszközök teljesítménye néhány wattól 10–20 W-ig terjedhet. Ez jelentős, akár több tízezerszeres teljesítménykülönbség, ami még a 78 MHz sávszélesség esetén is elegendő J/S teljesítményarányt biztosít a hatékony zavaráshoz.

A zavarás hatására a bluetooth-kapcsolat megszakad a CGMS távadója és az okoseszköz között, illetve a zavarás fennálltáig a kapcsolatlétesítés sem lehetséges. Az okoseszköz nem tudja venni a távadó hirdetőcsomagjait, és a párosítás sem fog megtörténni. Ez a típusú zavarás a gyakorlatban könnyedén kivitelezhető,

[31] Haig et al. 2022.
[32] Köppel 2013.

köszönhetően az SDR-[33] technológia fejlődésének. Emellett kaphatók olyan széles sávú zavaró eszközök, amelyek több frekvenciasávban alkalmasak széles sávú, nagy teljesítményű zavarás megvalósítására.[34] Meg kell jegyezni, hogy ezeknek az eszközöknek a működtetése engedélyköteles, a Nemzeti Média- és Hírközlési Hatóság csak indokolt esetben, ideiglenesen engedélyezi ilyen eszközök rövid idejű bekapcsolását (például nemzetbiztonsági célból).

A szándékos zavarás mellett mindenképpen meg kell említeni a nem szándékos zavarás problémáját. Ez esetben a 2,4 GHz-es sávban működő egyéb eszközök okoznak nem szándékos interferenciát. Habár a BLE-technológia a frekvenciaugratás miatt kevésbé sérülékeny ezen hatásokkal szemben, az ebben a sávban működő egyéb eszközök elleni szándékos zavaró tevékenység (mint például a drónelhárító rendszerekben működő jammerek alkalmazása) ugyanúgy akadályozhatja a működését, mintha az célzottan a CGMS ellen irányulna.

BLE spoofing

A BLE alapvetően a párosítási eljárást alkalmazza az MITM-támadások elleni védelemre. Mindazonáltal a kutatások rámutattak, hogy a párosítási kérelem vagy a válaszüzenetek továbbítása nem biztonságos csatornán keresztül történik. Következésképpen a támadások többsége a párosítási folyamat akadályozására vagy a folyamatba való belépésre összpontosít, ezáltal lehetővé téve a MITM-támadások különféle formáit.[35]

Wu és társainak kutatása azonban az adatkapcsolati rétegben az újracsatlakozási folyamatot vizsgálta.[36] Ez a művelet azután történik meg, ha az eszközök egymás hatótávolságán kívülre, majd újra hatótávolságon belülre kerülnek. Elméletileg amikor a kliens újra csatlakozik a szerverhez, a két eszköznek ellenőriznie kell egymás titkos kulcsait, és ezután csatlakozhatnak újra. A gyakorlatban azonban megállapították, hogy:

- a hitelesítés az eszköz újracsatlakozása során nem kötelező, hanem opcionális;
- a hitelesítés megkerülhető, ha a kliens nem kényszeríti a szervert az adatok hitelesítésére.

Ezek pedig lehetőséget adnak a BLE-hamisítás (*BLE spoofing attack* – BLESA) végrehajtására, aminek során egy, a hatótávolságon belül lévő eszközzel meg lehet kerülni a hitelesítést az újracsatlakozás során.

Mivel a hitelesítés opcionális, a kliens és a szerver az újracsatlakozás során a legalacsonyabb, azaz az 1. *biztonság nélküli szintet* is választhatja. Mivel a kapcsolat biztonsági szintjét minden esetben a szerver határozza meg, a kliens a magasabb biztonsági szintet nem tudja kikényszeríteni. Ez pedig mind a szervert, mind a klienst sebezhetővé teszi a hamisítással szemben. A CGMS esetében ez azt jelenti, hogy a CGMS-távadó határozza meg a hozzáférés-szabályozás szintjét. Ha ez az 1. szint,

[33] *Software defined radio* – szoftvervezérelt rádiótechnológia.
[34] *GSM, GPS, WIFI Blokkolók (Jammer)* [é. n.].
[35] Hlapisi 2016.
[36] Wu et al. 2020.

akkor ebbe a kapcsolatba kívülről, hatótávolságon belül be lehet lépni, és manipulálni lehet a mért értékeket. Védelmi megoldás lehet, ha a CGMS-távadó minden esetben előírja a legalább 2. *csak titkosítással engedélyezett* hozzáférési biztonsági szintet.

A hitelesítés megkerülése során a támadó először azonosítja a szervert, vagyis a CGMS-távadót, majd csatlakozik hozzá, hogy információt (például azonosítókat) szerezzen az attribútumairól. Mivel a BLE-protokoll értelmében bármely eszköz csatlakozhat egy másik BLE-eszközhöz, a támadó könnyen hozzájuthat ezekhez az információkhoz. A hirdetőcsomagok továbbítása egyszerű szövegben történik, így a támadó azonos csomagok sugárzásával és a MAC-címének[37] klónozásával megszemélyesítheti a távadót, és hamisított hirdetőcsomagokat kezd sugározni. A kliens, vagyis az okoseszköz, amikor újra csatlakozni akar a már korábban párosított távadóhoz, akkor a támadó hamisított hirdetőcsomagjait fogja venni, és a támadóval fog kapcsolatot létesíteni. Ekkortól pedig a támadó képes hamis vércukorértékeket küldeni a beteg okoseszközére.

A kutatásban 127 Android-alkalmazást elemeztek,[38] és kimutatták, hogy kétharmaduk, illetve 12-ből 10 valós IoT-eszköz (köztük pulzusmérő is) semmilyen hitelesítést nem alkalmazott az újracsatlakozás során. A Linux (BlueZ), az Android (Fluoride) és az iOS BLE-protokollkészletei mind-mind sebezhetők voltak, míg a Windows-eszközök BLE-protokollkészlete megfelelő védettséget mutatott a BLESA-támadással szemben. Megállapítható tehát, hogy a CGMS, mint sok más egészségmonitorozó eszköz, potenciális célpontja lehet az ilyen típusú fenyegetésnek is.

A CGMS elleni szándékos fenyegetések hatása

Amikor egy valós alacsony vércukorérték helyett a CGMS normál tartományba eső vagy magas glükózértéket jelenít meg, ahhoz vezethet, hogy az egyén ennek tudatában kihagyja az étkezést, bevállal egy nagyobb fizikai munkavégzést, vagy több inzulint ad be, esetleg több gyógyszert vesz be. Mindez akár perceken belül tünetekkel és panaszokkal járó hipoglikémiához vezethet. Fordított esetben viszont, ha a beteg a CGMS-től azt az értesítést kapja, hogy a vércukorértéke alacsony, de valójában az a kórosan magas tartományhoz közelít, vagy azt átlépi, az illető fokozza a szénhidrátbevitelt, ami hiperglikémiához, hosszabb távon egyéb anyagcsere-elváltozásokhoz vezethet. Hasonló helyzeteket teremthet az is, ha a rendszer hamisan azt az információt közli, hogy a vércukorérték meredeken emelkedik vagy csökken.

A hipoglikémia sokkal gyorsabban vezethet olyan állapothoz, amely már idegrendszeri tünetekkel jár, és egy bizonyos érték alatt már csak külső segítséggel tud megoldódni. A kórosan alacsony vércukorérték okozta állapot időbeli lefolyását, intenzitását tekintve sokkal veszélyesebb a kórosan magas értéknél. A hamis adatok az egészségügyi személyzetet is téves útra vezethetik, a valós vércukorértékről pedig csak vérből meghatározott glükózértékkel lehet információt nyerni.

[37] *Media access control* – MAC.
[38] Wu et al. 2020.

Következtetések

Tanulmányunkban megállapítottuk, hogy a CGMS a betegnek nyújtott előnyök mellett segíti az egészségügyi személyzetet a szénhidrát-anyagcsere állapotának objektív megítélésében, a megfelelő vércukorszint-csökkentő terápia kiválasztásában és az inzulinkezelés finomhangolásában.

Más országok haderőiben végzett vizsgálatok eredményei alapján igazoltuk, hogy a CGMS használata esélyt ad arra, hogy a cukorbetegségben szenvedő katonák további aktív szolgálatban maradjanak, illetve akár műveleti területen is részt vegyenek katonai feladatokban. Emellett a szenzortechnika alkalmazható az egészségi alkalmasság megítélésében és a legkedvezőbb kondicionálás megállapításában. További felhasználási lehetőség lehet a digitális katona eszközrendszerében való alkalmazás, amely a katona feladat-végrehajtása során az átfogó egészségi állapotának monitorozását terjesztheti ki.

A kutatás során vizsgáltuk a CGMS sebezhetőségét. Megállapítottuk, hogy a rendszer működéséből adódóan a vezeték nélküli BLE-kapcsolat sérülékenysége kihasználható. Rosszindulatú támadók elektronikai zavarással akadályozhatják a működését, a spoofing technikának köszönhetően pedig hamis vércukorértékeket lehet bevinni.

A szenzor és az okoseszköz közti adatkapcsolat megszakadása a biztonságérzet elvesztésével jár, ami pszichés terhet is jelent az adott szintű katonai vezető számára, ami például a döntési képességeit is negatívan befolyásolhatja. A hamis adatok miatt elmaradt vércukor-korrekciót igénylő beavatkozások, illetve nem adekvát reakciók pedig nemcsak az életét, hanem emiatt akár az egész művelet sikerét is veszélyeztethetik. Mindezek alapján a jelenleg elérhető CGMS-ek katonai környezetben csak korlátozottan alkalmazhatók.

A nagy teljesítményű zavarással szemben megfontolandó a BLE technika kiváltása a néhány cm-es hatótávolságú NFC-kommunikációval,[39] amelynek köszönhetően zavarviszonyok között a J/S arányt tudjuk kedvezően alakítani. Ez esetben a CGMS távadóját és az okoseszközt egymáshoz kell érinteni, vagy legfeljebb 1–2 cm-re kell tenni egymástól az adatátvitelhez. A spoofing elleni védelmet a BLE-protokollkészlet implementációinak javításával és/vagy a BLE-specifikáció frissítésével, a titkosított újrakapcsolódás kötelezővé tételével lehet javítani. A CGMS továbbfejlesztésének iránya egy olyan nem invazív bioszenzor kifejlesztése lehet, amely külső energiaforrás nélkül képes működni, hosszú élettartammal és a jelenleginél biztonságosabb adatkapcsolattal rendelkezik.

Felhasznált irodalom

A Belügyminisztérium egészségügyi szakmai irányelve a diabetes mellitus kórismézéséről, a cukorbetegek antihyperglykaemiás kezeléséről és gondozásáról felnőttkorban (2023). *Egészségügyi Közlöny,* 73(13), 1137–1246. Online: www.kozlonyok.hu/kozlonyok/Kozlonyok/6/PDF/2023/13.pdf

[39] Near Field Communication.

Agiostratidou, Gina et al. (2017): Standardizing Clinically Meaningful Outcome Measures Beyond HbA1c for Type 1 Diabetes: A Consensus Report of the American Association of Clinical Endocrinologists, the American Association of Diabetes Educators, the American Diabetes Association, the Endocrine Society, JDRF International, The Leona M. and Harry B. Helmsley Charitable Trust, the Pediatric Endocrine Society, and the T1D Exchange. *Diabetes Care,* 40(12), 1622–1630. Online: https://doi.org/10.2337/dc17-1624

American Diabetes Association Professional Practice Committee (2024): 6. Glycemic Goals and Hypoglycemia: Standards of Care in Diabetes – 2024. *Diabetes Care,* 47(Supplement_1), S111–S125. Online: https://doi.org/10.2337/dc24-S006

Choi, Sammy Y. – Cucura, John (2018): US Army Soldiers With Type 1 Diabetes Mellitus. *Journal of Diabetes Science and Technology,* 12(4), 854–858. Online: https://doi.org/10.1177/1932296818767700

Folaron, Irene et al. (2018): Effect of Military Deployment on Diabetes Mellitus in Air Force Personnel. *Military Medicine*, 183(11–12), e603–e609. Online: https://doi.org/10.1093/milmed/usy050

Haig Zsolt et al. (2022): Possibilities of Electronic Jamming of WLAN Networks in the Physical Layer. *Hadmérnök,* 17(3), 133–152. Online: https://doi.org/10.32567/hm.2022.3.9

Hevesi Judit Ildikó (2023): A folyamatos szöveti glükózmonitorozó rendszer elérhetősége Magyarországon. *Belügyi Szemle,* 71(12), 2207–2222. Online: https://doi.org/10.38146/BSZ.2023.12.6

Hevesi Judit Ildikó (2024): A szénhidrát-anyagcsere állapot jellemzése a folyamatos szöveti glükózmonitorozó rendszer alkalmazása mellett. *Belügyi Szemle*, 72(1), 75–88. Online: https://doi.org/10.38146/BSZ.2024.1.5

Hlapisi, Nthatisi (2016): Vulnerabilities and Attacks on Bluetooth LE Devices – Reviewing Recent Info. *All About Circuit,* 2016. július 16. Online: www.allaboutcircuits.com/technical-articles/vulnerabilities-and-attacks-on-bluetooth-le-devicesreviewing-recent-info

Klonoff, David C. (2015): Cybersecurity for Connected Diabetes Devices. *Journal of Diabetes Science and Technology,* 9(5), 1143–1147. Online: https://doi.org/10.1177/1932296815583334

Kóródi Gyula (2005): *Az agykoponya lövési sérüléseinek korszerű ellátása szervezési és szakmai szempontok alapján, a NATO tagságunkból fakadó kihívások tükrében.* PhD-értekezés. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola.

Köppel, Steven (2013): *Bluetooth Jamming.* Bachelor's Thesis. ETH Zürich. Online: https://pub.tik.ee.ethz.ch/students/2012-HS/BA-2012-16.pdf

Winkler Gábor – Baranyi Éva (2014): *A cukorbetegség egészségkárosító hatása.* Budapest: SpringMed.

Wu, Jianliang et al. (2020): BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy. *14th USENIX Workshop on Offensive Technologies (WOOT 20),* 2020. augusztus 11. Online: www.usenix.org/system/files/woot20-paper-wu-updated.pdf

Yu, Xiaohui et al. (2023): Prevalence of Impaired Awareness of Hypoglycaemia in People with Diabetes Mellitus: A Systematic Review and Meta-Analysis from 21 Countries and Regions. *Diabetic Medicine,* 40(9), e15129. Online: https://doi.org/10.1111/dme.15129

Internetes források

Apvrille, Axelle – Lakhani, Aamir (2019): Medical IoT for diabetes and cybercrime. *Virus Bulletin International Conference (VB2019),* 2019. október 2–4. Online: www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Apvrille-Lakhani.pdf

Bluetooth LE – Nordic (2020): Understanding Bluetooth LE Advertising. *BeaconZone Blog,* 2020. október 2. Online: www.beaconzone.co.uk/blog/understanding-bluetooth-le-advertising/

Daily Mail Reporter (2013): Dick Cheney Reveals He Feared Terrorists Would Kill Him by Staging Homeland-style Attack on His Pacemaker. *Daily Mail,* 2013. október 19. Online: www.dailymail.co.uk/news/article-2466951/Dick-Cheney-reveals-fearedterrorists-kill-staging-Homeland-style-attack-pacemaker.htm

Diabetic Supplies and Equipment [é. n.]. Online: https://tricare.mil//CoveredServices/IsItCovered/DiabeticSupplies

GSM, GPS, WIFI Blokkolók (Jammer) [é. n.]. Online: https://spyonlineshop.com/termekkategoria/gsm-gps-wifi-blokkolok-jammer

International Diabetes Federation (2021): *IDF Diabetes Atlas.* 10th Edition. Online: https://diabetesatlas.org/idfawp/resource-files/2021/07/IDF_Atlas_10th_Edition_2021.pdf

The Bluetooth® Low Energy Primer (2024). Bluetooth®. Online: www.bluetooth.com/wp-content/uploads/2022/05/the-bluetooth-le-primer-v1.2.0.pdf

Jogszabályok

2012. évi CCV. törvény a honvédek jogállásáról. Online: https://net.jogtar.hu/jogszabaly?docid=A1200205.TV

9/2013. (VIII. 12.) HM rendelet a honvédek jogállásáról szóló 2012. évi CCV. törvény egyes rendelkezéseinek végrehajtásáról. Online: https://net.jogtar.hu/jogszabaly?docid=a1300009.hm

10/2015. (VII. 30.) HM rendelet a katonai szolgálatra való egészségi, pszichikai és fizikai alkalmasságról, valamint a felülvizsgálati eljárásról. Online: https://net.jogtar.hu/jogszabaly?docid=a1500010.hm