# RFID ADATBIZTONSÁG

Csikós Sándor – Sárosi József – Czifra György

**Absztrakt:** A „rádiófrekvenciás azonosítás” (RFID) technológiákat már a II. világháború óta alkalmazzák. A technológia lényege, hogy legalább az egyik felet azonosítsa. A negyedik ipari forradalomban ez a technológia talán a legjobb jelölt az okos termékek megvalósítására. Ez az új használati kör új biztonsági feladatokat jelent, amik megoldásra várnak. Ilyenek például az adat biztonság és adat integritás biztosítása. Ebben a cikkben az RFID technológiákon ismert támadások és a lehetséges védelmi módszerek kerülnek bemutatásra.

**Abstract:** Radio frequency identification (RFID) technologies have been in use since world war II. The purpose of this technology is to identify at least one of the participants. In the fourth industrial revolution this technology is the best contender to create smart products. This new field of use brings forth new challenges that must be solved. Such as securing data security and data integrity. In this article I will present the known attacks on RFID technologies and the potential defences against them.

*Kulcsszavak:* RFID, biztonság, adat integritás

*Keywords:* RFID, security, data integrity

## 1. Bevezetés

A „rádiófrekvenciás azonosítás” (RFID) technológia alatt olyan rádiófrekvenciás kommunikációt értünk, aminek a célja a résztvevők legalább egyikének azonosítása. A technológia első alkalmazása a Brit Királyi Légierő Identification Friend or Foe (IFF) adóvevője volt 1939-ben, itt repülőgépek azonosítására használták fel. A civil szférában az első alkalmazásig várni kellett az 1980-as évekig, amikor autópálya használati díjak automatikus beszedésére alkalmazták elsőként Norvégiában, majd az Amerikai Egyesült Államokban. Az 1990-es években kezdtek kialakulni a napjainkban is ismeretes RFID szabványok, mivel egyre több gyártó lépett a piacra saját rendszerének implementációjával. Manapság ez a technológia része mindennapi életünknek Az alkalmazási területek felölelik a logisztikát, beléptetést és fizetést. Az üzletekben a termékeken RFID jelölőket helyeznek el, amik riasztást váltanak ki, amikor a bejáratnál lévő olvasók közelében áthalad és előtte a fizetés során nem lett deaktiválva. Fizetéskor paypass-os bankkártyát használhatunk, amely ugyanezt a technológiát használja, csomagjainkat RFID jelölők azonosíthatják az automatikus csomagválogató központokban, beléptető rendszereknél RFID technológiát tartalmazó okos kártyák azonosíthatják a személyeket (Landt, 2005; Sziklai et al., 2007). A negyedik ipari forradalomban az egyik legalkalmasabb technológia lehet az okos termékek nyomkövetésének megoldására. Okos termékeknek (Smart Product) nevezünk olyan termékeket, amelyek magukkal hordozzák gyártási folyamatuk lépéseit, életciklusuk adatait. Egy ilyen termék képes az őt megmunkáló berendezéssel közölni, hogy milyen technológiai paramétereket és beállításokat kell alkalmazni a munka elvégzése során. Egy idealizált gyártósoron az érkező okos termék a szerelési és megmunkálási paramétereit, mint például a szorítási erő, szín, hőkezelési hőmérséklet, stb. közli a megmunkáló, aktuális feladatot végrehajtó egységgel. Az ilyen okos termék menet közben akár a

DOI: 10.14232/jtgf.2020.3-4.133-138

megrendelő kérésére módosítható, így például a szín megváltoztatható, ha még nem jutott a festő állomáshoz (Gilchrist, 2016). Fontos megemlíteni, hogy az okos termék nem kell, hogy tartalmazza az összes említett információt, minimális esetben csak azonosítania kell magát a terméknek és ez alapján egy központi adatbázisból kiolvashatók a termékhez kapcsolt adatok. Ez a módszer lényegesen eltérő biztonsági problémákat vet fel, melyet egy külön cikkben érdemes elemezni. Az ilyen széleskörűen és univerzálisan alkalmazott technológia új támadási felületeket hoz magával. Mi akadályozhat meg egy illetéktelen személyt, hogy az okos termékből kiolvassa a legyártásához szükséges információkat? Hogyan lehet megakadályozni, hogy valaki felülírja a termék gyártásához tartozó űrtartalmat, hosszokat, hőmérsékleteket és ennek következtében félig- vagy túltöltött, esetleg eltérő méretű selejtes darabokat gyártsunk? Valós a veszély, hogy egy illetéktelen beavatkozás a selejtes terméken túl a gyártósorra is kihatással lesz, robbanást vagy tüzet, egyéb anyagi kárt okozhat, vagy természeti katasztrófát, nagymértékű környezetszennyezést is kiválthat, akár emberéletet is kiolthat.

## 2. RFID rendszerek felépítése

Egy tipikus RFID rendszer 3 elemből épül fel:

- Adóvevő (Tag)
- Olvasó (Interrogator)
- Feldolgozó szerver

Az adóvevő, más néven tag tartalmaz egy mikrovezérlőt és egy meghatározott frekvenciára hangolt antennát. Amikor a behangolt gerjesztési frekvencián az antenna jelet kap, a tag válaszol a képességeinek megfelelően. A válasz elhangolja az antennát, ami visszaszórást eredményez, ezt az olvasó érzékelni tudja. Három fajta taget különböztetünk meg: passzív, szemi-passzív és aktív (Kleist, 2004), ezek felépítését az *1. ábra* szemlélteti. A tárolt adatok módosíthatósága szempontjából létezik egyszer és többször írható tag is.

A passzív tagek nem rendelkeznek energiaforrással, így nem képesek maguktól jelet küldeni. Energiaforrásként a gerjesztési frekvencián lévő jelet használják fel és csak az olvasó által kiadott elektromágneses térben működnek. Hatótávjuk így a három fajta tag közül a legkisebb, nehezen működnek zajos környezetekben, viszont egyszerű felépítésük miatt az előállításuk a legolcsóbb. A legegyszerűbb passzív az 1 bites tag, ezek csak jelenlétükről nyújtanak információt. Ilyeneket láthatunk az üzletekben a termékeken, ezeket vásárláskor az eladók eltávolítják vagy kisütik.

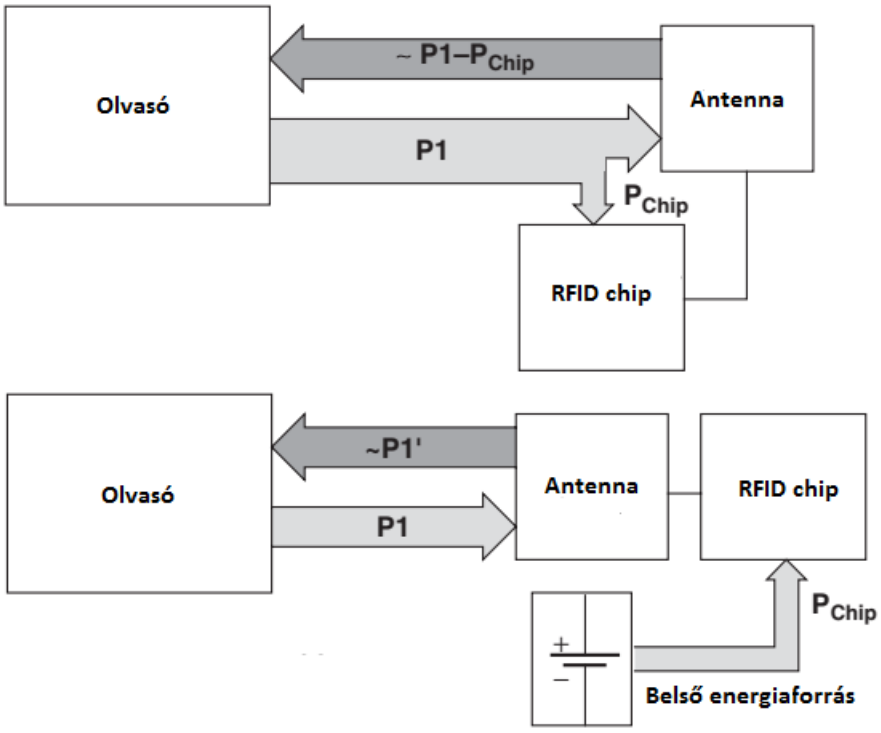
A szemi-passzív tagek hasonló felépítéssel rendelkeznek, mint a passzívak. A lényeges különbség az, hogy nekik van energiaforrásuk. Ezt a taghez kötött egyéb rendszerek táplálására használják, így kiterjeszthető a működési távolságuk. Mivel a gerjesztő jel egésze visszaküldhető, nem használódik el energiájának egy része a belső működésre. Ilyen elven működött az eredeti IFF is.

Az aktív tagek rendelkeznek saját energiaforrással, így a hatótávjuk a legnagyobb a felsoroltak közül. Nem képesek magas frekvenciájú jelek kiadására, így a kommunikációjuk során az olvasó jelét visszaszórják.

Az olvasó feladata a gerjesztő jel kiadása, ezzel energiával látja el a taget a kommunikációra. Választ a tagtől visszaszórás formájában fogad, ami a kiküldött gerjesztő jel modulációja. A választ továbbítja a feldolgozó szervernek. Az alkalmazott szabványos frekvenciákat az *1. táblázat* tartalmazza.

A feldolgozó szerver az olvasótól kapott információt fogadja és a beállított módon cselekszik. Ez a bolti alkalmazásoknál egy riasztás elindítása, amikor az olvasó jelzi egy tag jelenlétét.

*1. ábra:* **Passzív (felül), szemi-passzív és aktív (alul) taget alkalmazó rendszerek.**




Forrás: Finkenzeller (2010)

*1. táblázat:* **Szabványos RFID frekvenciák**

| Frekvencia | Alkalmazható távolság | Szabványszám |
|---|---|---|
| 135 KHz | 10 cm | ISO/IEC 18000-2 |
| 13,56 MHz | 70 cm | ISO/IEC 18000-3 |
| 860-960 MHz | 5 m | ISO/IEC 18000-6 |
| 2,45 GHz | 1 m | ISO/IEC 18000-4 |

Forrás: Finkenzeller (2010)

## 3. RFID támadási és védekezési módszerek

Az RFID tageken végrehajtható támadásokat két csoportra bonthatjuk: adatvédelmi és biztonsági. Adatvédelmi fenyegetések alatt olyan támadásokat értünk, ahol a támadó megpróbál információt szerezni, más néven hallgatózik. Biztonsági fenyegetésnek olyan támadásokat tekintünk, amelyeknél a támadó lemásolja az egyik fél viselkedését, hogy elérje céljait (RFID Security, 2016). Néha nem egyértelmű, melyik kategóriába soroljunk egy támadást, mivel a végkifejlettől függően a módszer mindkét kategóriába sorolható. Egy másik osztályozás a támadások végkimenetelét figyelembe véve: passzív lehallgatás, aktív üzenetbeiktatás, zavarás (Sziklai et al., 2007). Következzen néhány támadási lehetőség és a szakirodalomban található védekezési módszerek:

Lehallgatás: mivel az RFID vezeték nélkül kommunikál, az adatfolyam lehallgatható. A támadó messzebb is lehet, feltéve, hogy erősebb antennával rendelkezik. Az egyetlen ismert védekezési forma a lehallgatás ellen a küldött adatok titkosítása, viszont mivel az RFID chip viszonylag gyenge erőforrásokkal rendelkezik, ez a megoldás nem minden esetben használható.

Üzenet korrupció: egy üzenetküldést meghiúsíthat a támadó, ebben az esetben a tag elküldi az adatot, de az nem érkezik meg az olvasóhoz épségben a támadó beiktatott jele miatt. Mivel ez a beavatkozás energiatöbblet eredményez, detektálható lesz és így kivédhető.

Üzenetmódosítás: ez a támadás hasonlít az előzőhöz egy lényeges eltéréssel: a támadó beavatkozása módosítja az üzenet tartalmát egy másik, az eredetitől eltérő érvényes üzenetre. Védekezés az ilyenfajta támadások ellen az adatsebesség módosításával valósítható meg, 106 kbaud-os adatsebesség megakadályozza az adatok módosítását aktív módban használt tageknél. Ez a mód viszont megnöveli a lehallgatás lehetőségét. Egy másik módszer a védekezésre egy biztonságos kommunikációs csatorna használata.

Üzenet beiktatás: a tag és az olvasó közötti kommunikációba beszúrhat a támadó egy érvényes üzenetet. Ha a támadó helyesen időzít, akkor minden adat átmegy a többlet adattal együtt, ellenkező esetben a támadás átalakul üzenet-korrupcióvá. Ilyen támadás akkor lehetséges, amikor a felek lassan reagálnak és időt adnak a támadónak. Ha késleltetés nélkül azonnal válaszolunk, akkor nem hagyunk a támadásra lehetőséget. Egy másik módszer a védekezésre egy biztonságos kommunikációs csatorna használata.

Közbeékelődéses támadás: ennél a módszernél a támadó sikeresen becsapja mindkét felet és elhiteti velük, hogy egymással kommunikálnak, miközben valójában minden adat a támadón keresztül megy át – ő dönti el, hogy melyik adatcsomag fog átmenni és milyen tartalommal. Egy ilyen támadás sikerességéhez a két fél közé kell fizikailag férkőzni, ez jóformán kivitelezhetetlen, ha a felek elég közel vannak egymáshoz (Chattha, 2014).

## 4. RFID adatok sérülése

Az RFID tagek EEPROM memóriája érzékeny az elektromágneses zajokra és ionizáló sugárzásra, a megfelelő frekvenciájú zavaró jel elnyomhatja az olvasó üzenetét vagy akár túl is terhelheti a *tag*-et. Ezeket a hibákat két csoportba sorolhatjuk: *hard error* és *soft error*. *Hard error* esetén nem csak a memória, hanem a vezérlő is sérül, ilyenkor az írás és az olvasás ellehetetlenül. *Soft error* esetén a *tag* memóriájában tárolt adatok sérülnek meg, de a vezérlő ép marad. Bár a kommunikáció helyességét ellenőrizhetjük, ebben az esetben a memóriában tárolt adat változik meg, amit a kommunikációban felhasznált CRC-vel nem tudunk ellenőrizni. Az ilyen esetekben hibadetektáló, valamint hibajavító kódokban érdemes tárolni a tageken az adatot. Ezekkel a kódokkal olyan szintű redundanciát viszünk be a rendszerbe, ami garantáltan érzékelhetővé teszi az adatok módosítását. A legegyszerűbb ilyen redundancia minden bit két biten való tárolása (0→01; 1→10), ami bár megfelezi a tag memóriáját, de az EEPROM kialakításából adódik, hogy ionizáló sugárzás esetén csak a logikai magas érték változhat át alacsonyra, fordított eset nem valósulhat meg. A dekódolásnál így csak a 00 kombinációkat kell figyelni, hogy észrevegyük a hibát. Ezzel a módszerrel csak detektálni tudjuk a hibát, viszont nem tudjuk az eredeti adatot visszaállítani (Teraura et al., 2013). Bizonyos alkalmazásokban ez elég is, mivel detektált hiba esetén csak kicseréljük a sérült adatot tartalmazó taget. Hibajavító kódolások használatával maximalizálhatjuk egy *tag* élettartamát. Ha feltételezhetünk egy maximális számú *(n) soft errort*, ami után már *hard error* következik be, megalkothatunk egy olyan tökéletes kódot, ami ki tud javítani *n* számú *soft errort* és jelezni tud ettől több hibát is abban az esetben, ha a feltételezésünk helytelen és *n*-nél több *soft error* bekövetkezése után is képes a rendszer *hard error* nélkül működni.

## 5. Következtetések

Az RFID technológiák kifejlesztésük óta életünk számos területére bekerültek és sok alkalmazási területen megkönnyítették a munkát. Mint minden új és fejlett technológia esetében a saját veszélyeivel számolnunk kell, melyek közül a legjelentősebbek a támadó által végrehajtott adat – manipulálások, a sugárzás és elektromágneses zaj által okozott *soft,* illetve *hard errorok*. A támadásokat elsősorban detektálnunk kell, a hibákat – ha lehet, helyreállítani. Közismert, hogy az elektromágneses zajok hibákat okozhatnak RFID tagekben, de eddig nem ismert ennek mértéke. Tervem olyan mérést végrehajtani, ami feltérképezi ezt az összefüggést, ami alapján megtervezhető egy hibajavító kód a feltételezett maximális számú *soft error* kijavítására.

## Irodalomjegyzék

Chattha, N. A. (2014): NFC – Vulnerabilities and Defense. In: *Conference on Information Assurance and Cyber Security (CIACS)*. IEEE. Raalpindi, Pakisztán, 35–38. https://doi.org/10.1109/CIACS.2014.6861328

Finkenzeller, K. (2010): *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication.* Wiley, Wiltshire.

Gilchrist, A. (2016): *Industry 4.0*. Apress, Berkeley California. https://doi.org/10.1007/978-1-4842-2047-4

Kleist, R. A. (szerk.) (2004): *RFID Labeling: Smart Labeling Concepts & Applications for the Consumer Packaged Goods Supply Chain*. Printronix, Irvine Califorfnia.

Landt, J. (2005): The History of RFID. *IEEE Potentials*, 24 (4): 8–11. https://doi.org/10.1109/MP.2005.1549751

Sziklai P., Nagy D., Ligeti P. (2007): Rádiófrekvenciás azonosítás és biztonság. *Magyar Tudomány*, 167 (7): 904.

RFID Security (2016): Springer Science+Business Media, New York, New York.

Teraura, N., Ito, K., Takahashi, N., Sakurai, K. (2013): The Development of Radiation-Resistant RF Tags for Use at Nuclear Power Plants. In: *Volume 1: Plant Operations, Maintenance, Engineering, Modifications, Life Cycle and Balance of Plant; Nuclear Fuel and Materials; Radiation Protection and Nuclear Technology Applications*. ASME, Csengtu, Kína, p. V001T01A043. https://doi.org/10.1115/ICONE21-16605