Egungo trenbideen komunikazio-sistemen erronka: segurtasuna

(The chanllenge of current railway communication systems: security)

Irene Arsuaga Oria, Nerea Toledo Gandarias*

I2T Taldea, Bilboko Ingeniaritza Eskola (UPV/EHU)

* iarsuaga005@ehu.eus

DOI: 10.1387/ekaia.19687

Jasoa: 2018-05-14 Onartua: 2018-06-19

Laburpena: Trenbide-sistemak asko aldatu dira azken urteotan komunikazio-teknologia berrien sorkuntzarekin batera. Europan, trenbide-sare bakarra izateko nahiarekin, ERTMS (European Rail Traffic Management System) sistema sortu zen, elkarrekiko bateragarriak ez ziren Europako herrialdeetako kudeaketa-sistema estandar ezberdinak ordezteko. Baina sistema berria sortzearekin batera, segurtasunaren inguruko hainbat erronka berri ere sortu ziren; izan ere, ERTMS aurreko sistema itxi eta ezezagunak protokolo ireki eta teknologia ezagunez ordeztu ziren. Ondorioz, aurrerapausoak eman diren arren, oraindik ere hutsune nabarmenak daude segurtasunaren arloan.

Hitz gakoak: trenbideak, babes-segurtasuna, prebentzio-segurtasuna, ERTMS.

Abstract: Railway systems have evolved considerably in the last years with the adoption of new communication technologies. Aiming to achieve a single European railway network, the European Rail Traffic Management System (ERTMS) was created to substitute the multiple and non-interoperable national railway communication standards. But with the creation of the new system, new challenges in security were created; in fact, closed and unkown systems were replaced by open protocols and known technologies. Therefore, even if improvements have been done, there are still gaps to cover in the field of security.

Keywords: railway, security, safety, ERTMS.

1. **SARRERA**

Trenen seinalizaziorako komunikazio-sistemek eboluzio handia izan dute azken urteotan. Orain dela urte batzuk arte, herrialde bakoitzak bere seinalizazio-sistema propioa erabiltzen zuen, baina horrek arazoak sortzen zituen hainbat herrialdetan zehar mugitzen ziren trenetan. Ondorioz, Europako lurraldeetan operatzeko modu ezberdinak egonik, trenen merkatu komun bat izateko nahiak agerian utzi zuen herrialde guztientzako bateragarria den kudeaketarako sistema berri baten beharra. Horrela, pasa den mendeko laurogeiko hamarkadan, Europako trenen elkarteek kudeaketa-sistema bati buruzko ikerketa hasi zuten, eta horrela, ERTMS (European Rail Traffic Management System) sistema sortu zuten [1]. Sistema hori trenen kontrolerako lurraldeetako estandar ezberdinak ordezteko sortu zen.

Baina ERTMS sistema sortzeak industriarako eta bidaiarientzako onurak ekarri bazituen ere, hainbat erronka berri ere azaleratu zituen. Izan ere, trenbideetako azpiegiturak sistema itxietan oinarrituta egon ziren ordura arte, eta horrenbestez, euren segurtasuna sistemen isolamenduan eta erabilitako teknologien ezagutzarik ezean oinarritzen zen.

Baina printzipio horiek ez dira bateragarriak ERTMSren sorrerarekin; hain zuzen, ERTMS sistema irekietan eta protokolo zein teknologia ezagunen erabileran oinarritzen da. Horren ondorioz, trenbideetako segurtasuna bermatzeko, ezinbestekoa da prozedura berriak definitu eta inplementatzea.

ERTMS komunikazioak irrati bidezkoak dira; hortaz, hari gabeko sistemak erabiltzen dira, RBCtik (Radio Block Centre) —trenen operazioa kudeatzen duen entitatea— trenei agindu ezberdinak bidaltzeko. Gaur egun arte, GSM-R (Global System for Mobile Railways) hari gabeko komunikazio-teknologia erabili da, trenbideetarako garatutako GSM sistema orokorraren bertsio espezifiko bat.

Komunikazioetan segurtasuna bermatzeko, GSM-R sareak hainbat segurtasun-ezaugarri finkatu behar ditu. Alde batetik, igorritako datuen konfidentzialtasuna bermatu behar du. Gainera, trenek agindu faltsuak jasotzen ez dituztela ziurtatzeko, mezuen osotasuna bermatu behar du; hau da, trenak mezua jaso baino lehen erasotzaile batek aldatu ez duela bermatu behar du. Azkenik, komunikazio-sarearen erabilgarritasuna ere ziurtatu behar du. Beraz, sareak CIA (Confidentiality, Integrity, Availability) triada garantizatu behar du: Konfidentzialtasuna, Osotasuna eta Erabilgarritasuna. CIA triada erakunde bateko segurtasun-politikak gidatzeko eredua izan ohi da, segurtasun-ezaugarri kritikoenak errepresentatzen dituena.

Kasu honetan, trenean bertan bidaiatzen duten pertsonen segurtasuna denez kontu kritikoena, CIA triadako osotasuna kontsideratzen da segurtasun-mekanismo garrantzitsuena.

Hori horrela izanik, komunikazio-sareen osotasuna bermatzeko, bi kriptografia-sistema erabiltzen dira komunikazio-geruza[1] bakoitzean: A5/1 kriptografia-sistema erabiltzen da GSMn, eta EuroRadio protokoloa aplikazio mailan. Baina bi segurtasun-mekanismo horiek ahultasunak dituztela frogatu da [2-5].

Ondoko ataletan honakoak aztertuko ditugu: bigarren atalean ERTMS sistema azaltzen da; ondoren, hirugarren atalean ERTMS sistemako segurtasun mekanismoak deskribatzen dira; laugarren atalean ERTMS sistemaren segurtasunari dagozkion arazoak esplikatzen dira; gero, bosgarren atalean ondorio nagusiak azpimarratzen dira; eta bukatzeko, seigarren atalean testuan zehar dauden siglen esanahiak azaltzen dira, bai ingelesez, baita euskaraz ere.

2. **ERTMS**

ERTMS bi azpisistema hauek osatzen dute: (1) ETCS (European Train Control System) seinalizaziorako eta (2) GSM-R komunikaziorako.

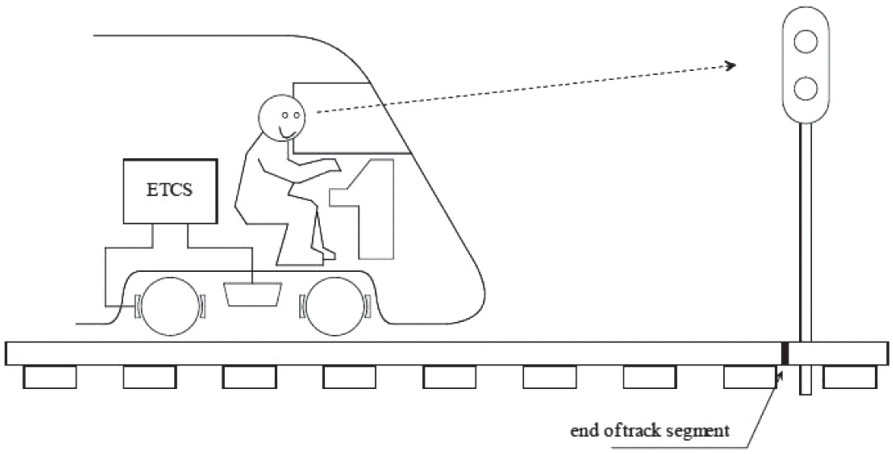
2.1. **ETCS**

Dagoeneko kokatuta dauden trenbideetan edota linea berrietan lan egiten duten seinalizazio-ekipamendu ezberdinetara egokitzeko, hainbat konfigurazio eskaintzen ditu ETCS sistemak. Hain zuzen, bost maila desberdintzen dira, horietako bakoitzak bere automatizazio-maila eskaintzen duela. ERTMS eta ETCSren operatzeko modua Subset-026 v.3.4.0 arauan [6] azaltzen da.

ETCS 0 maila

Tren zaharren eta ETCS sistema duten trenen arteko trantsizio egokia bermatzeko definitzen da maila hau; izan ere, hemen kokatzen dira ETCS ekipamendua duten baina linea zaharretan dabiltzan trenak. Ondorioz, maila honetan trenek mezuak GSM-R bidez jaso beharrean, lineako seinaleen bitartez jasotzen dituzte. Maila honetako operatzeko modua 1. irudian ikus daiteke.

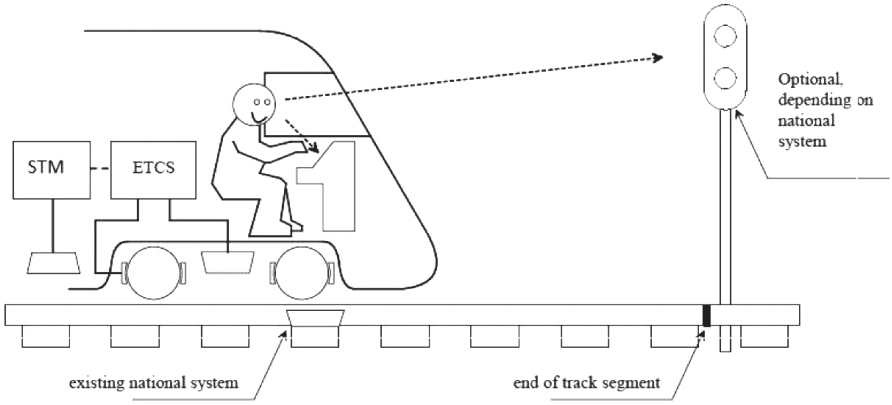
[1] Sistemen arteko komunikazioetarako informatika eta telekomunikazioetan erabiltzen diren protokoloak hainbat modutan bana daitezke, OSI (Open System Interconnection) ereduaren banaketa izanik ezagunena. Eredu horren arabera, komunikazio-protokoloak geruza ezberdinetan banatzen dira.



1. irudia. ETCS 0 maila, [6]tik hartua.

ETCS NTC (National Train Control) maila

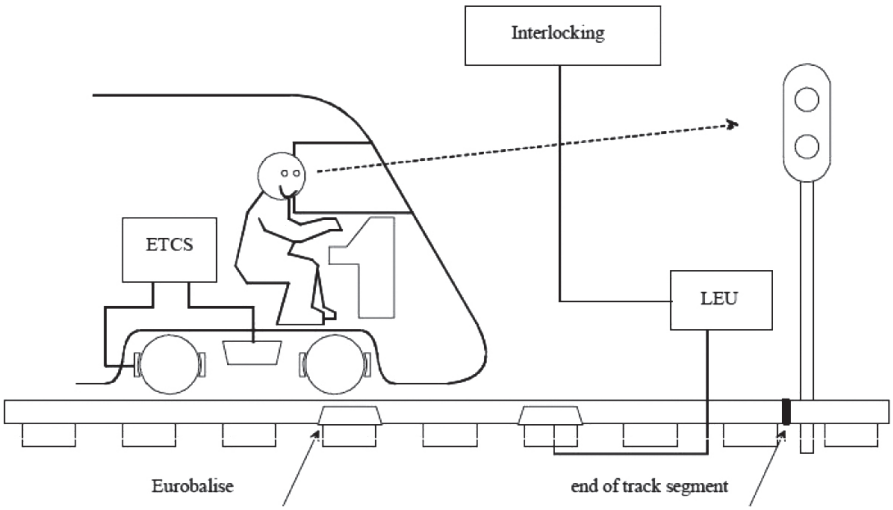
Bigarren maila hau ETCSdun trenek erabiltzen dute. ETCS NTC mailaren bitartez sistema nazionalek euren trenen kontrola egiten dute trenbide nazionaletan. Maila honetako trenek STM (Specific Transmission Module) gailua dute, zeinak herrialde bakoitzeko sistemaren eta ETCS ekipamenduaren interfaze moduan lan egiten duen. Maila honetako operatzeko modua 2. irudian ikus daiteke.



2. irudia. ETCS NTC maila, [6]n oinarritua.

ETCS 1 maila

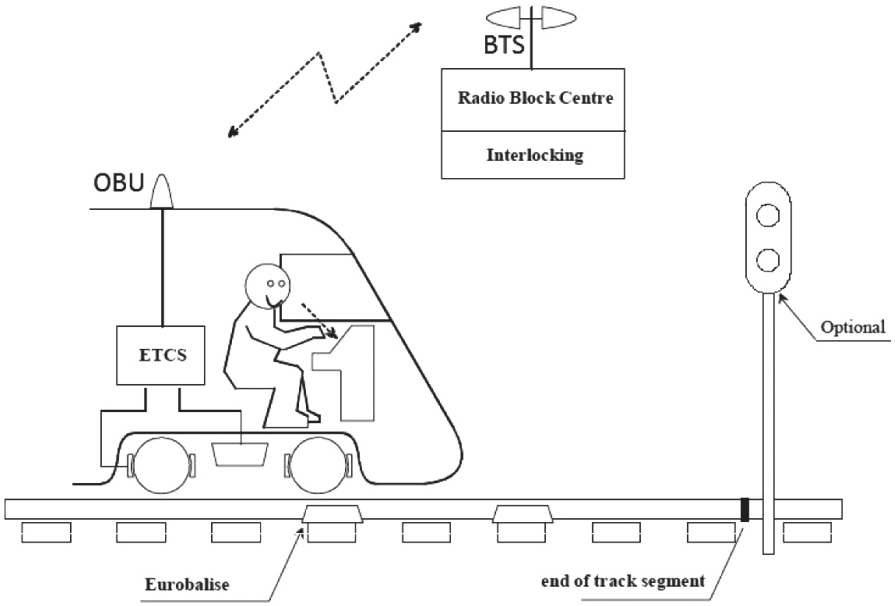
Maila honetan ETCS sistema ohiko seinalizazio-ekipamenduaren gainean ezartzen da. Trenaren kokalekua ohiko trenbideko gailuen bitartez jasotzen da, eta horrek informazioa *interlocking* ari bidaltzen dio, LEU (Lineside Electronic Unit) ekipoaren bitartez. *Interlocking* a trenaren kontrolaz arduratzen den ekipoa da. Bestalde, trenaren eta trenbidearen arteko datuak *eurobalise* n bitartez bidaltzen dira, horiek trenbidean kokatutako aparatuak izanik. Maila honetako operazio-modua 3. irudian ikusten da.



3. irudia. ETCS 1 maila, [6]tik hartua.

ETCS 2 maila

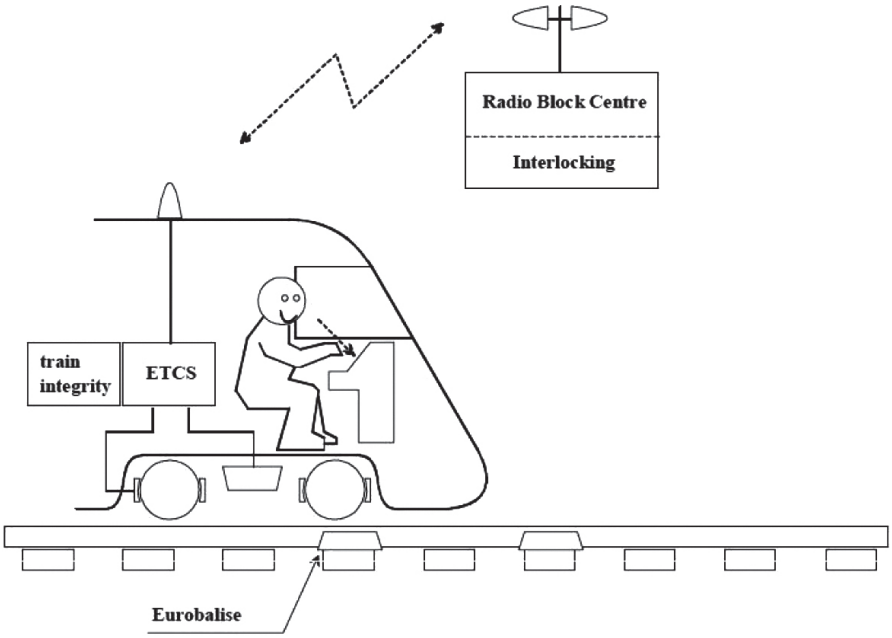
Aplikazio-maila honetan GSM-R komunikazio-teknologia erabiltzen da RBCaren eta trenaren arteko datuen trukerako; trenbidean zehar kokaturiko BTSak (Base Transceiver Station) treneko OBUarekin (On Board Unit) komunikatzen dira. Hala eta guztiz ere, seinalizazio-funtzio guztiak ez dira teknologia horren bitartez betetzen; trenaren kokalekua oraindik ere trenbideko gailuen bitartez jasotzen da. Beraz, ETCS sistemen irismenetik kanpo dago funtzio hori. ETCS 2 mailaren operazioa 4. irudian azaltzen da.



4. irudia. ETCS 2 maila, [6]n oinarritua.

ETCS 3 maila

Bukatzeko, aplikazio-maila honetan, ETCS sistemaren funtzio guztiak betetzen dira. Izan ere, maila honetan GSM-R sarea erabiltzen da, bai RBCaren eta trenaren arteko datuen trukerako, bai trenaren kokalekuaren informazioa jasotzeko. Halaber, maila honetan *eurobalise* ak trenbidean mantentzen dira, baina horien funtzioa trenaren erreferentziazko kokapena lortzea baino ez da. Azken maila honetako operatzeko modua 5. irudian azaltzen da.



5. irudia. ETCS 3 maila, [6]tik hartua.

2.2. **GSM-R**

Aurretik esandako moduan, GSM-R sistema erabiltzen da trenaren eta trenbidearen arteko komunikaziorako. Hain zuzen, [1] liburuak azaltzen duenez, ERTMS sistema diseinatzen ari ziren garaian, operazio komertzialean produktuak eskuragarri zituen sistema bakarra zen GSM sistema, baina hala ere, ez zituen betetzen trenetarako zerbitzu eraginkorra emateko beharrezkoak diren eskakizun guztiak. Ondorioz, ezaugarri funtzional zehatz batzuk gehitu zizkieten GSMko espezifikazioei, GSM-900 bandan, hau da, 900 MHz inguruko bandan trenen erabilerarako maiztasun jakin batzuk erreserbatzea, besteak beste.

3. **ERTMS SISTEMAREN SEGURTASUNA**

Segurtasun hitzak ingelesez bi adiera ditu: *safety* eta *security*. Bi hitz horiek industriako kontrol-sistemetan kontzeptu ezberdinak definitzeko erabiltzen dira. Alde batetik, *safety* hitza ustekabeko gertaeren prebentzio-sistemetarako erabiltzen da. Horrela, *safety* hitza istripuak ekiditeko neurriekin lotzen da. Bestalde, *security* berariazko kalteei aurre egiteko babesekin lotzen da. Bi terminoak definituta, *safety* hitza prebentzio-segurtasuna terminoarekin erabiliko da eta *security* hitza babes-segurtasun terminoarekin.

Trenbideen ingurunean lan handia egin da prebentzio-segurtasuna bermatzeko, honako artikulu hauetan ikus daitekeen moduan: [7, 8]. Baina babes-segurtasuna eskakizun berria da, eta hori bermatzeko ikerketan ahaleginak egin badira ere [5, 9, 11, 12], oraindik ere lan handia behar du. Gainera, prebentzio-segurtasuna bermatzeko erabiltzen diren arriskuen probabilitateetan oinarritutako analisiak ez dira baliagarriak babes-segurtasuna bermatzeko, ezin baita jakin erasotzaile batek noiz aurkituko dituen sistemaren ahultasunak.

Horrela, atal honetan azalduko diren ERTMS sistemaren segurtasun-mekanismoak eta hurrengo ataleko segurtasun-arazoek trenen babes-segurtasunari egingo diete erreferentzia.

Aurretik aipatu den moduan, datuak GSM-R bidez transmititzen diren ETCS sistemaren operazio-mailetan (ETCS 2 eta 3 mailetan, alegia) bi segurtasun-mekanismo erabiltzen dira: A5/1 GSM-Rrako eta EuroRadio ETCSrako.

Lehena, A5/1 izenekoa, datuak fluxuan[2] kodetzen dituen zifratze-algoritmoa da, eta GSM sareei pribatutasuna emateko sortu zuten. Zehazki, 64 biteko gako batekin hasieratzen den sekuentzia-zenbaki baten bitartez, algoritmoak 114 biteko gakoa sortzen du. Gako horrek eta informazioa duten 114 bitek XOR eragiketa[3] egiten dute eta eragiketaren emaitza mezu zifratua da.

Bestalde, EuroRadio protokoloa ERTMS sistemaren Subset-037 v.3.1.0 arauan [10] azaltzen da. Lau gako erabiltzen dira ERTMSko entitateen arteko komunikazioetan. Horietatik hiru KMC (Key Management Centre) entitateak sortzen ditu: KTRANS, K-KMC eta KMAC gakoak alegia. Laugarrena, aldiz, KSMAC izenekoa, KMAC gakoaren bitartez sortzen da eta komunikazioa osatzen duten entitateen artean erabakitzen den saio-

[2] Datuak fluxuan kodetzen direla esaten da, informazio-bitak denbora errealean zifratzen direnean; hau da, multzo finkoetan banatu gabe.

[3] XOR eragiketa 2 biten arteko eragiketa da. Horietako baten balioa 1ekoa denean soilik da eragiketaren emaitza 1ekoa.

gakoa da. Bestalde, KTRANS eta K-KMC gakoak garraio-gakoak dira, ERTMSko entitate ez-berdinetara KMAC gakoaren banaketa segurua egiteko erabiltzen direnak. Banaketa hori *off-line* eran egiten denez, beharrezkoa da gizakien esku-hartzea.

KSMAC saio-gakoa lortzeko, hiru mezu trukatzen dira komunikazioa osatzen duten ERTMS entitateen artean. Mezu horien bitartez, bi entitateak elkarrekiko autentifikatzen dira, KSMAC saio-gakoa sortzearekin batera. TDES (Triple Data Encryption Standard) motako gakoa da KSMAC saio-gakoa. TDES algoritmoak hiru aldiz egiten du bloke bidezko zifratze simetrikoa. Ondorioz, KSMAC saio-gakoa hiru azpigakoz osatzen da, ondoko berdintzak osatuz: KSMAC = $K_S = \{K_{S1}, K_{S2}, K_{S3}\}$. Gako horiek lortzeko, ausazko bi zenbaki (entitate bakoitzak bat sortzen du) eta aurretik *off-line* moduan jasotako KMAC gakoa erabiltzen dira.

4. **ERTMS SISTEMAREN SEGURTASUN-ARAZOAK**

Aurreko atalean ikusitako moduan, ERTMS sistemak A5/1 algoritmoan eta Euro-Radio protokoloan oinarritzen du bere segurtasuna. A5/1 algoritmoa 1987. urtean sortu zen eta EuroRadio protokoloa oinarritutako TDES algoritmoa, 1998an. Biak orain bizpahiru hamarkada sortuak izanik, horien segurtasuna zalantzan jarri duten hainbat lan argitaratu dira.

Alde batetik, A5/1 algoritmoari dagokionez, hasiera batean segurua zela jotzen bazen ere, hurrengo urteetan haren segurtasuna auzitan jarri zuten hainbat eraso argitaratu ziren: [2] 2000an, [3] 2003an eta [4] 2006an. Izatez, gaur egun A5/1 algoritmoaz zifratutako mezuak deszifratzeko taulak eskuragarri daude Interneten[4]. Ondorioz, erabat hautsita dago algoritmo honen segurtasuna.

Bestalde, EuroRadio protokoloaren segurtasuna ere zalantzan jarri da beraren ahultasunak deskribatzen dituzten hainbat artikuluren bitartez. Adibidez, [5] artikuluan Euro-Radio protokoloaren ProVerif[5] erremintaren bitarteko analisia egin da. Erreminta horrek automatikoki frogatzen ditu protokolo kriptografikoen segurtasun-ezaugarriak. Analisi horretan, hainbat ahultasun azaltzen dira, hala nola lehentasun handiko mezuak entitateen autentifikaziorik gabe sarean sartzeko aukera eta sesioa hasteko fasean denbora-zigilurik (*time-stamp*) ez erabiltzea. Horien ondorioz, mezuak errepikatzeko aukera sortzen da.

Aurrekoez gain, [11] artikuluan EuroRadio protokoloaren bestelako ahultasunak deskribatzen dira, bereziki KMAC kodea *off-line* banatzearen

[4] http://drive.google.com/drive/folders/0B-8F5I-fE6lFQk1HY1pTWGJyM3M

[5] http://prosecco.gforge.inria.fr/personal/bblanche/proverif/

ondorioz sortzen diren ahultasunak. Izan ere, banaketa hori *off-line* egitearen ondorioz, beharrezkoa da banaketan gizakien esku-hartzea, lehen esandako moduan. Hori dela eta, nahiz eta izatez KMAC gako ezberdin bat sortu beharko litzatekeen bi entitateen komunikazio bakoitzerako, zenbait operadorek prozesua sinplifikatzea erabaki dute, komunikazio askotan KMAC gako berdina erabiliz. Hori eginda, handitu egiten da erasoren bat jasateko probabilitatea. Izan ere, KMAC lortzeko helburuarekin erasoa sesioa hasteko fasean egingo balitz, entitate ezberdinek gako bera izanda, sistema osoaren segurtasuna jarriko litzateke arriskuan; erasotzaile batek beste tren baten identitatea hartu ahalko luke, beste sesio bat hasteko faseren batean.

Gainera, [12] artikuluan azaltzen den ERTMSko segurtasunaren analisian ondorioztatzen da EuroRadio protokoloa ez dela segurua datu-kantitate handi eta komunikazio-sesio luzeetarako.

ERTMSk dituen segurtasun-arazo teorikoak aztertzeaz gain, trenbideetan azken urteotako trenen seinalizazioari eragin dien zibererasoen azterketa ere egin da. Azterketa horren bitartez, segurtasun-arazo horiek sortzen dituzten ahultasunak errealitatean ustiatzea posible dela ikusi da. Zibererasoen bilduma 1. taulan ikus daiteke.

1. taula. Trenbideetako azken urteotako zibererasoak.

Herrialdea	Urtea	Azalpena
Polonia	2008	Etxean eginiko transmisore baten bitartez, errailetako kommutagailuak manipulatu eta trenak norabidez aldatu zituen gazte batek. Dozena bat pertsona zauritu ziren istripuaren ondorioz.
Ameriketako Estatu Batuak	2011	Zibererasoen bitartez ipar-mendebaldeko trenbideen seinalizazioa eta trafikoa eten zuten bi egunez.
Ukraina	2015	BlackEnergy troiarraren[6] bidezko erasoa egin zuten.
Japonia	2015	Gizarte-ingeniaritzaren bitarteko *phishing*-eraso bat garatu zuten.
Erresuma Batua	2015	Ziberespioitza-operazioak eragin zituzten herrialdeko trenbide-sisteman.
Hego Korea	2016	Hilabete askotan zehar Seulgo metroko hainbat terminal erasotu zituzten.
Ameriketako Estatu Batuak	2016	San Frantziskoko tranbia-sisteman Ransomware erasoa[7] eragin zuten.
Alemania	2017	WannaCry Ransomware erasoa eragin zuten Alemaniako hainbat tren-, tranbia- eta autobus-zerbitzu kudeatzen dituen enpresan.

[6] Erabilgarritasunaren aurkako erasoa egiten du.

[7] Software gaiztoa, biktimaren sistema digitaleko datuak zifratzen ditu eta horiek desblokeatzeko erreskatea eskatu.

Ez da ezaguna taulako erasoak azaldu berritako A5/1 eta EuroRadio protokoloen ahultasunen ustiapenetan oinarritzen diren, baina hala ere, trenbideetako segurtasun beharren adierazle dira.

Bestalde, Alemanian 2015. urtean hainbat auditoretza egin ziren trenbideen sektorean. Horietan, sistemaren zenbait akats azaleratu ziren: babes falta erabiltzaileen autentifikazioan, sistema eragile zaharrak, hurruneko sarbideetarako pasahitz ez seguruak, etab.

Beste zenbait ikuskaritzak ETCS 2 eta 3 mailen eta GSM-R hari gabeko komunikazio-protokoloa erabiltzearen ahultasunak ere nabarmendu zituen. Eraso posibleen artean datuak baimenik gabeko dekodetzea, SIM (Subscriber Identity Module) txartelak klonatzea, mezuen blokeoa eta *jamming* erasoa[8] identifikatu zituzten.

5. **ONDORIOAK**

Aurreko atalean deskribatutako segurtasun-arazoak eta horiek sor ditzaketen eraso larrien azterketa eginda, nabaria da oraindik ere handia dela trenbide-sistemetan babes- segurtasuna bermatzeko egin beharreko lana. Hori horrela izanik, lan horiek garatzeko berrikuntza eta ikerkuntza bide egokien gisa ikusten dira.

ERTMS sistemen komunikazioetan ahultasunak bilatzeko *pentesting* —metodoen erabilera gomendatzen da, esate baterako. Metodo horien bitartez, sistemen ahultasunak bila— tzeaz gain, ahultasun horiek ustiatzeko probabilitate eta aukera ere aztertzen dira. Horrela, metodoaren emaitzaren arabera jakingo da identifikatutako ahultasunak ustiatzea posible den ala ez. Informazio horrekin ondorioztatuko da ahultasunak murrizteko segurtasun-neurriak eta erasoen inpaktua lausotzeko teknikak aplikatzea beharrezkoa den ala ez.

Bestalde, ERTMS sistemaren segurtasun-arazoak konpontzeko, beraren segurtasuna ebaluatzen duen metodologia baten estandarizazioa egitea ere gomendatzen da. Izan ere, gaur egun oraindik ez dago Europan trenbide-sistemen zibersegurtasun-ebaluazioa egiten duen metodologia komunik. Mota horretako metodologiak hainbat onura ekarriko lizkioke trenbide-sistemari, adibidez, Europan ERTMS sistema bateratua izanda herrialde guztietan segurtasuna bermatzeko neurri eta teknologien ezarpen komuna.

[8] Sistemako errekurtsoen desaktibatzea edota asetzea eragiten du *jamming* erasoak.

6. **SIGLAK**

Testuan zehar azaldutako siglen esanahia azaltzen da 2. taulan.

2. taula. Siglen esanahia.

Sigla	Ingelesez	Euskarazko baliokidetza
BTS	Base Transceiver Station	Oinarri Estazio
CIA	Confidentiality Integrity Availability	Konfidentzialtasuna-Osotasuna-Erabilgarritasuna
ERTMS	European Rail Traffic Management System	Europako Trenen Zirkulaziorako Kudeake- ta Sistema
ETCS	European Train Control System	Europako Trenen Kontrol Sistema
GSM-R	Global System for Mobile Railways	Trenbideetako Komunikazio Mugikorretako Sistema Orokorra
KMC	Key Management Centre	Gakoen Kudeaketa Zentroa
LEU	Lineside Electronic Unit	Lineako Unitate Elektronikoa
NTC	National Train Control	Trenen Kontrol Nazionala
OBU	On Board Unit	Tren Unitatea
OSI	Open System Interconnection	Sistema Irekien Interkonexioa
RBC	Radio Block Centre	Irrati bidezko Blokeo Zentroa
SIM	Subscriber Identity Module	Abonatuaren Identifikazio Txartela
STM	Speciffic Transmission Module	Transmisio Espezifikorako Modulua
TDES	Triple Data Encryption Standard	Datu Kodetze Estandar Hirukoitza

7. **BIBLIOGRAFIA**

[1] UIC PETER WINTER. 2009. *Compendium on ERTMS*. Eurorail press. Hamburg.

[2] BIHAM, ELI eta DUNKELMAN, ORR. 2000. <Cryptanalysis of the A5/1 GSM Stream Cipher>. *Progress in Cryptology —INDOCRYPT 2000*. 43-51.

[3] BARKAN, ELAD; BIHAM, ELI eta KELLER NATHAN. 2003. <Instant Ciphertext- Only Cryptanalysis of GSM Encrypted Communication>. *Advances in Cryptology - CRYPTO 2003*. 600-616.

[4] BARKAN, ELAD eta BIHAM, ELI. 2006. <Conditional Estimators: An Effective Attack on A5/1>. *Selected Areas in Cryptography*. 1-19.

[5] JOERI DE RUITER, R. J. T. eta CHOTHIA, T. 2016. <A formal security analysis of ERTMS train to trackside protocols>. *Reliability, Safety and Security of Railway Systems - Modelling, Analysis, Verification and Certification*. 53-68.

[6] U. SUBSET-026-2. <ERTMS/ETCS system requirements specification, Chapter 2, Basic System Description>. tech. rep., 2014.

[7] FAIVRE, A.; LAPITRE, A.; LANUSSE, A.; PERIN, M.; RANGRA, S.; SALLAK, M. eta SCHN, W. 2015. <Two methods for modeling and verification of safety properties of railway infrastructures>. *2015 International Conference on Industrial Engineering and Systems Management (IESM)*. 48-54.

[8] FRANEKOV, M.; RSTOCNY, K.; JANOTA, A. eta CHRTIANSKY, P. 2011. <Safety analysis of cryptography mechanisms used in GSM for railway>. *Annals of the Faculty of Engineering Hunedoara*. **9**. 207-212.

[9] VALDIVIA, L. J.; ADIN, I.; ARRIZABALAGA, S.; ANORGA, J. eta MENDIZABAL, J. 2018. <Cybersecurity - the forgotten issue in railways: Security can be woven into safety designs>. *IEEE Vehicular Technology Magazine*. **99**. 48-55.

[10] U. SUBSET-037. <EuroRadio FIS>. tech. rep., 2014.

[11] LOPEZ, I. eta AGUADO, M. 2015. <Cyber security analysis of the European Train Control System>. *IEEE Communication Magazine*. **53**. 110-116.

[12] CHOTHIA, TOM; ORDEAN, MIHAI; DE RUITER, JOERI eta THOMAS, RICHARD J. 2017. <An Attack Against Message Authentication in the ERTMS Train to Trackside Communication Protocols>. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. 743-756.