Towards a resilient railway communication network against electromagnetic attacks

Marc Heddebaut, Souheir Mili, David Sodoyer, Eduardo Jacob, Marina Aguado, Christian Pinedo Zamalloa, Igor Lopez, Virginie Deniau

Towards a resilient railway communication network against electromagnetic attacks

Marc Heddebaut[a], Souheir Mili[a], David Sodoyer[a], Eduardo Jacob[b], Marina Aguado[b], Christian Pinedo Zamalloa[b], Igor Lopez[b] and Virginie Deniau[a*]

[a]*Univ. Lille Nord de France, Lille, France*
IFSTTAR, COSYS, LEOST, Villeneuve d'Ascq, France
[b]*Univ. of the Basque Country (UPV-EHU), Bilbao, Spain*

Abstract

Due to its widespread deployment and its relative ease of access, the rail infrastructure constitutes an attractive target for potential attacks. These attacks could have extended economic and security consequences. Recently, considerable efforts have been dedicated to develop an interoperable Pan-European railway traffic management system. To create the conditions of interoperability, the system is well documented and the relevant information is widely and easily available. Radio equipment are used at different levels of the system. Some of these are likely to be disturbed by malicious actions involving jammers. In this context, the "SECRET" European project aims to develop innovative solutions to improve the resilience of these interoperable radio systems. This article explores several research aspects of the project. The first part analyzes the railway infrastructure and the potential risks of electromagnetic attacks that may occur. The next section explores some of the conditions that can inhibit ground to train radio. To mitigate the impact of these jamming systems, a resilient communication architecture is analyzed in the last section.

Keywords: Railway; radio; attack; jammer; architecture; resilience

Résumé

En raison de son déploiement très vaste et de sa relative facilité d'accès, l'infrastructure ferroviaire apparait susceptible de subir d'éventuelles attaques. Celles-ci pourraient avoir des conséquences significatives sur l'économie ainsi qu'en termes de sécurité. Ces dernières années, des efforts considérables ont été déployés en vue de développer un système de gestion du trafic ferroviaire paneuropéen interopérable. Ce systèmes sont de ce fait bien documentés et leurs caractéristiques sont également largement diffusées et disponibles. Des communications radio de différentes natures sont largement employées pour gérer ce trafic ferroviaire. Dans ce contexte, le projet européen «SECRET» vise à développer des solutions innovantes afin d'améliorer la résilience électromagnétique des systèmes radio ferroviaires. Cet article explore différents aspects de recherche du projet. Une première partie analyse l'infrastructure ferroviaire et les risques d'attaques électromagnétiques. La section suivante explore certaines des conditions qui peuvent inhiber la radio sol-train. Afin de contrer ces systèmes de brouillage, une architecture de communication résiliente est analysée en dernière section.

Mots-clé: Transport ferroviaire ; radio ; attaque ; brouilleur ; architecture ; résilience

* Corresponding author information: Tel.: 33 3 20 43 89 91; fax: 33 3 20 43 83 97.
E-mail address: virginie.deniau@ifsttar.fr.

1. Introduction

The terrorism threat to European citizens has been constantly elevated for several years. This threat also concerns rail transportation and its associated infrastructure which provide mass transport. Both rail operation and its infrastructure are recognized as critical priorities because of the economic and security impacts of terrorist attacks (loss of service, destruction of vehicles, and destruction of infrastructure…). Extended consequences on the surrounding businesses are also expected, as well as the impaired reputation of the railway as a safe and secure transport system. Indeed, the railway is an attractive target for security attacks, because of its familiarity, ease of access and openness. The attacks carried out on the French railway infrastructure in November 2008 involving metal bars on the catenaries which caused delays for 160 TGVs, Eurostar and Thalys (coordinated attacks that targeted four different rail lines on the French Railway network) showed that more subtle actions than bombings can be carried out by terrorists: the terrorists can base their action methods on the vulnerabilities of technologies employed. Equally, electromagnetic (EM) terrorism is based on a similar approach, as it consists in failing equipment or devices which serve the efficiency and safety of railway transport systems.

The European railway network constitutes a mass transport system which includes a large number of telecommunication, command-control, electronic and computer systems and subsystems potentially vulnerable to intentional electromagnetic interferences (IEMI). Generally, electromagnetic interferences (EMI) can act on wireless communications, on wired networks and on electronic and computer components and systems. They can have three main effects:

- Destruction of the electronic components;
- jamming information transmitted and, thus, impeding communication between two components;
- modifying the information transmitted and, thus, enabling or disabling certain functions unexpectedly.

Considering the current evolution of the European rail network which is based on the deployment of the GSM-Railway communication system to transmit the signalling information between the control-centres and the trains, the first feared effect is the jamming of communication signals. Indeed, the jamming of wireless communication signals can be easily implemented in comparison to other techniques aiming to modifying the carried information. However, today, the real consequences of such attacks on the whole railway network are not well-known.

Consequently, the European project SECRET (SECurity of Railways against Electromagnetic aTtacks) aims to assess the real risks concerning EM attacks on rail networks, to identify areas for strengthening and to develop a detection and management system for EM attacks that is integrated into the rail infrastructure, making it an architecture resilient to any EM attack. Obviously, to be in agreement with the current evolution of the European railway network, the architecture has to be adapted to interoperability needs associated with the current harmonization process of the European railway network.

Knowing that, within the railway, information exchanges between trains and the infrastructure are necessarily provided by wireless links, it is, therefore, impossible to protect such information from EM attacks with conventional shields, filters or other topological solutions. Thus, it becomes necessary to provide a dynamic solution based on the detection of the EM attack and on the redundancy of communication solutions to ensure that the correct information reaches the recipient (infrastructure or train) in an adequate amount of time.

This research article is structured as follows. Section 2 underpins the potential risk that EM attacks may introduce in railway operation: our research motivation. Section 3 determines the different railway radio communication subject to electromagnetic attacks and focuses our research on a specific target scenario: the GSM-R communication link. Next, we identify current jamming systems and measure their effectiveness to disturb GSM-R communication. Based on real measurements, we also provide a necessary baseline of EM behaviour characterization for normal GSM-R radio operation in the railway scenario. Once, we identify the target communication to be protected, the attack scenario and the effect of the EM attack in the GSM-R communication link, section 4 describes the resilient railway communication network able to react in real time to this attack scenario. The proposed architecture is grounded on two major concepts: a Detection System, which

will use of the detection techniques of GSM-R attacks detailed in the section 3 among others, and a Multipath Communication System, which will strengthen the connections between trains and trackside.

2. EM attacks and railway network

EM attacks consist of intentionally generated EM signals in order to induce EM disturbances on electronic, computer or communication components. A definition of Intentional Electromagnetic Interferences (IEMI) is given by the International Electrotechnical Commission (IEC) as "intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems thus, disrupting, confusing, or damaging these systems for terrorist or criminal purposes."

In general, we can assume that EM attacks involving sufficiently high-level power interference can produce permanent damages to electronic equipment, and that lower power level EM interferences can mainly impact the quality of wireless transmissions.

In the case of EM attacks on railways, a large number of components of railway infrastructure can be affected: control-command systems (track switches, barrier crossing, traffic signal light...), spot communication systems for detection (track circuits, eurobalise, euroloop), continuous communication systems (local train radio systems, GSM-Railway). Consequently, the railway infrastructure is an effective potential victim of electromagnetism terrorism. According to the systems or subsystems attacked and to the nature of the intentional interferences, the consequences on the individuals, the structures and the materials can significantly vary.

Moreover, the deployment of ERTMS (European Rail Traffic Management System) not only homogenizes the technologies to manage the trains over the European territory, but also the vulnerability points to EM interferences. Some examples can be set up in the context of the harmonization of systems and rules due to interoperability requirements for all operational domains in the rail transportation in Europe (operation, control, management, maintenance…). These include the strategy to reduce the number of control centres of the track switches in Europe that will rely on interlocking remote controlled systems in order to activate switches. Thus, if a terrorist is designing an intentional EM emissions device capable of disrupting management systems for rail infrastructure in Berlin, for instance, the same device will have the same attack capacity in all European cities. This will cause immediate economic consequences and possibly more…. Harmonization thus facilitates the implementation of organized and simultaneous EM attacks.

The easiness of implementation of an EM attack will notably depend on the accessibility of the required devices to generate a given EM attack signal. Today, with the proliferation of the telecommunication applications, it is really easy to obtain equipment providing relatively low-level power interference able to jam wireless communication signals. Consequently, in SECRET, the priority is given to the study of the potential impacts of low power interference sources, such as jammers, on wireless railway communication systems.

Meanwhile, the technologies and frequencies employed in the railway field can be similar to technologies and frequencies used for applications available to the general public. Indeed, the railway no longer develops technology "owners" but adapts general public technologies. This increases the vulnerability of the railway because it is easy to obtain emission devices capable of disrupting rail technologies. With a relatively low basic knowledge of electronics and the performance of electronic components and antennas available on the open market, these emission devices can be combined with amplifiers to increase the capacity of EM attacks.

Given the potential vulnerability of the railway network and the ease of implementation of such EM attacks, we chose to work on an integrated solution to ERTMS offering the capability of detecting EM attack situations and engaging appropriate responses to maintain the security and capability of the railway network.

3. Detection of EM attack signals

3.1. Critical railway radio targets

A preliminary step of this study was to determine the potential radio interface targets for electromagnetic threats and malicious attacks. They are mainly related to the use of the GSM-Railway (GSM-R) for train to ground communication, the use of GNSS/GPS satellite navigation received signals for the train odometry system and the Eurobalise/Balise Transmission Module for spot communication. TETRA, Terrestrial Trunked Radio, which was

also considered many years ago for ground to train radio communication, is also a potential target. TETRA is currently used by some railway operators for railway and depot communication and also for railway security applications. This paper will concentrate on GSM-R.

3.2. GSM-R presentation

GSM-R is a standard communication platform for railways. It is a strategic communication system focused on the interoperability between European railway infrastructures. By the end of 2016, 56 countries in five continents should have operational GSM-R networks. Its specifications are widely disseminated. Europe is leading GSM-R implementation in 11 countries (Austria, Belgium, Czech Republic, France, Germany, Italy, the Netherlands, Norway, Spain, Sweden and Switzerland). In 2011, GSM-R deployment provided coverage of about 30% of the European railway network with 68,000 km in operation; 156,000 km are planned to be covered (70% of the European railway network). The main objectives of GSM-R are to replace analogical radio communication and to provide a unique data transmission solution for ERTMS/ETCS (European Rail Traffic Management System / European Train Control System) level 2 and level 3.

GSM-R is an evolution of public GSM dedicated to railway application. Therefore, GSM-R has similar characteristics to those of public GSM system. GSM-R functionality is built on standards and recommendations supported by mainly two organizations, ETSI (European Telecommunications Standards Institute) and UIC (Union Internationale des Chemins de fer, International Union of Railways). ETSI technical committee RT (Railway Telecommunications) is responsible for those aspects of Global System for Mobile communications standardization which are specific to Railway (GSM-R) and Private Mobile Radio (PMR) operations. UIC specifies through its EIRENE (European Integrated Railway Radio Enhanced Network) project, a digital radio standard for the European railways. It forms part of the specification for technical interoperability.

GSM-R performances are guaranteed for high-speed conditions (up to 500 km/h). A common European frequency band is allocated to GSM-R below the frequencies of the public GSM standard. The allocated frequency bands are for the uplink: 876 MHz - 880 MHz and for the downlink: 921 MHz - 925 MHz. As represented in figure 1, GSM-R has its own cellular network installed along the track designed to provide a minimum level of received power > -95 dBm anywhere along the track. This is a mandatory requirement coming from the EIRENE specifications. This represents a limited level of power with the potential of being jammed.

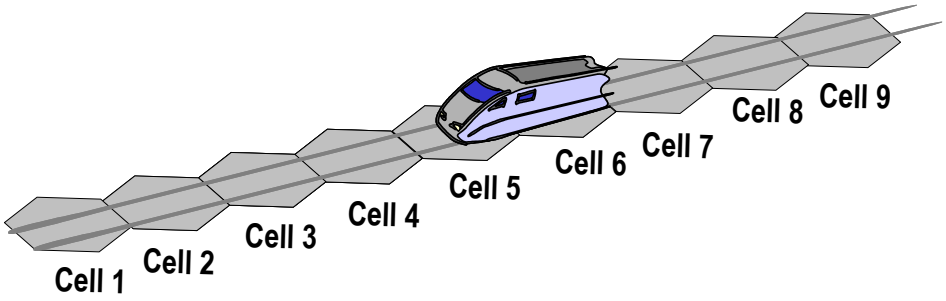

Figure 1: Cells deployed along a GSM-R network

3.3. Existing jamming systems

A study was carried out regarding existing jammers. Five classes of jammers were identified, noted A to E (RABC, 2001):

- Type ‘A’ devices ‘jammers’: These devices hold several independent oscillators transmitting ‘jamming signals’ disturbing and making impossible the establishment of the communications, blocking the frequencies used by mobile communication equipment.
- Type ‘B’ devices ‘intelligent cellular disablers’: These devices do not transmit interfering signals but work as detectors. So, when they detect signals in quite areas, they send a signal to inform the base station to interrupt the communication.
- Type ‘C’ devices ‘intelligent beacon disablers’ : These devices work on the control channels as ‘beacons’, they control mobile devices located in a quiet area by sending instructions to disable ringer or disable its operation.

- Type 'D' devices 'Direct Receive and Transmit Jammers': These devices operate as a small independent base station. The jammer is predominantly in receiving mode and will choose intelligently interaction and blocking the cell phone if it is within close proximity of the jammer.
- Type "E" devices 'EMI Shield – Passive Jamming': These jamming solutions consist in suppressing electromagnetic signals by using the properties of the Faraday cages. The Faraday cage essentially blocks, or greatly attenuates, all electromagnetic signals entering or leaving the cage.

In this presentation, we shall only consider type 'A' jammers. The next step of this study was to determine the effectiveness of these particular jammers.

3.4. Jamming effectiveness

To evaluate the effectiveness of any particular type 'A' jammer, a dedicated test bench was set up. It is presented in figure 1. A GSM-R communication is established in laboratory using a base transceiver station (BTS) emulator (CMU) and GSM-R train mobile equipment. Using combiners, a supplementary radio signal is injected in the radiofrequency link generating different jamming waveforms, at different power levels. A spectrum analyzer is used to visualize these waveform frequency occupancies (Mili et al., 2013).

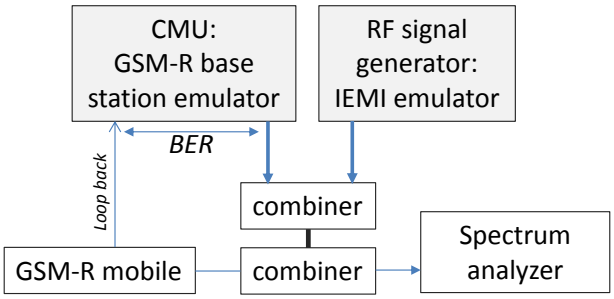

Figure 2: Test bench for the evaluation of jamming effectiveness

Using this test bench, the jamming effectiveness could be examined. Table 1 presents some results obtained with this set-up.

Table 1. Impact of a jammer on radio communication

P_GSM-R (dBm)	P_JAM (dBm)	BER *Pure sinusoïdal jammer*	BER *FM mod 75 kHz dev. jammer*
-38	-36	*Loss of comm.*	*No connexion*
-38	-37	12.6	*No connexion*
-38	-38	5.6	*No connexion*
-38	-40	2.1	14.7
-38	-42	0.8	7.8
-38	-44	0.2	2.7
-38	-46	0.1	0.6
-38	-48	0.06	0.2
-38	-50	0.02	0.04

In the first column, a constant -38 dBm GSM-R level is delivered to the input of the mobile GSM-R receiver. This represents a comfortable level of operation, as compared to the -95 dBm minimum level requested by the EIRENE specifications. The second column indicates the variable continuous wave jamming power injected at the input of the GSM-R mobile receiver. This jamming signal is centred in the GSM-R communication channel. The third column shows the resulting measured bit error rate (BER) in the case of a pure sinusoidal jammer. The last column indicates the results obtained with FM modulated jamming signals. We obtain that:

- When the received GSM-R power is of the same order of magnitude as the power received from the jammer then, the communication is perturbed or interrupted.

- A 6 dB difference (or more) between the two power levels greatly reduces the impact of the jammer.
- A pure sine wave centered on the GSM-R channel has less impact than a wider bandwidth FM modulated jamming signal.

We conclude that limited power jammers can effectively affect GSM-R communication.

The next step of the study was to evaluate "normal" EM environments in order to be able to then detect "jammed" electromagnetic conditions. Therefore, it was decided to perform electromagnetic environment measurements in different critical railway environments i.e. in stations, along railway tracks and in trains. Figure 3 represents one typical result of spectral measurements performed in a railway station (on the left side, a 3D representation: frequency, time, and received power and, on the right side, the equivalent waterfall representation).

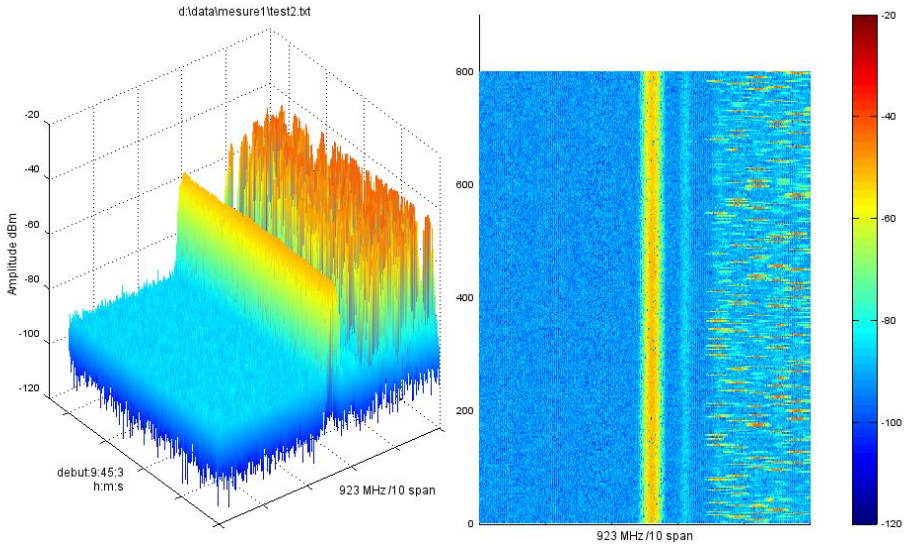

Figure 3: GSM-R downlink frequencies - span = 10 MHz (on a station platform).

The results presented cover a bandwidth of 10 MHz. As stated before, the GSM-R band occupies the 4 MHz central part of this 10 MHz band. A single GSM-R beacon channel, providing strong radio coverage of the station, is received in the GSM-R band; Line of Sight (LOS) of the corresponding GSM-R BTS antenna is nearly possible from this measurement location. Another, weaker, GSM-R BTS signal is also discernible higher in frequency, corresponding to a farther GSM-R BTS. The upper part of the band is fairly busy due to the number of cellular phone users in the station and its surroundings. The lower part of the monitored band is free of activity at the particular time of this recording.

After determining "normal" electromagnetic ambient conditions, sensors shall be installed in order to detect potential attacks. They will use possible discrepancies between the observed electromagnetic environments and the recorded "normal" electromagnetic environments. Sensor outputs deliver data to an optimized communication architecture providing the capability to react against these attacks.

4. A resilient communication architecture against EM attacks

This section describes the proposed resilient railway communication architecture able to detect and react against an EM or jamming attack similar to those described in section 3 and, consequently, able to manage the disruption of the train-trackside communication.

As previously introduced in section 3, ERTMS Levels 2 and 3 require a permanent communication path between trackside and the train so that the Radio Block Centre (RBC) can signal the train. All the possible communication paths between the trackside and the train rely on wireless communication technologies, at least

in a certain section of the communication path. Up to four wireless technologies are defined in the current specifications of ERTMS: GSM-R, Eurobalise, Euroloop and Radio-infill. The usage and importance of the previous technologies depends on the ERTMS Level deployed in the track.

Facing the impossibility to absolutely guarantee wireless communication between trackside and the train during EM attacks, due to the open-air interface inherent features, the aim of the proposed resilient architecture is to provide a flexible architecture that will provide multiple ways to make more resilient trackside-train communications depending on, on the one hand, on the ERTMS deployment and, on the other hand, on the security level the management staff wishes.

The architecture is based on two main concepts: detection of EM attacks and a more resilient wireless communication path. These two main concepts are the basis of the resilient architecture that consists of two subsystems: the Detection System (DS) and the Multipath Communication System (MCS) presented in figure 5.

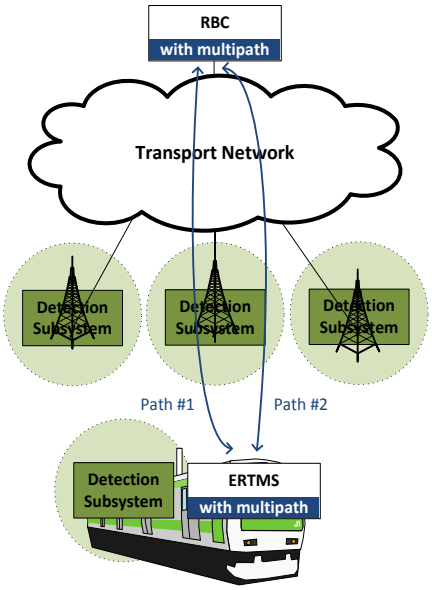

Figure 5: Detection System (DS) and Multipath Communication System (MCS) for the resilient architecture

Firstly, based on the data sent by the sensors, the DS allows the detection in real time of the EM attacks that occur in the railway infrastructure. Thus, the management staff can be provided with accurate information which allows them to anticipate a loss scenario of connectivity in certain sections of the trackside exposed to an EM attack or, in the worst case scenario, resolve quickly if the loss of communication with a train is due to an EM attack or due to a different reason (lack of power, hardware failure, …). The availability of this information for the railway management staff is crucial to perform the suitable actions in order to restore communications and normal operation. Given the information, management staff could deploy manual reactive actions or even, depending on the railway management system, automatic reactive actions.
Secondly, the MCS aims to provide multiple paths of communication between the RBC and the train in order to maintain the ETCS session of ERTMS Level 2 or Level 3, even if one or several paths fail. This implies the requirement of deploying an end-to-end multipath solution between the RBC and the on-board ERTMS located in the train.

The resilience level provided by MCS will depend on the dissimilarity level of the established paths, especially the wireless sections, which are the most sensitive to EM attack. Thus, the use of different wireless access technologies or, even better, frequencies would be desirable.

Finally, deploying the DS and the MCS together is of great interest because both subsystems are complementary. On the one hand, the DS might provide useful information to the MCS in order to change the active interface in case an attack that affects the current active interface is being performed. Thus, the MCS might change the communication paths based on the information provided by the DS. On the other hand, the DS could profit from the more resilient communication provided by the MCS to increase the resiliency of the communication between the trackside detection subsystem and the on-board detection subsystem located in the train.

4.1. The Detection System (DS) architecture

The main aim of the Detection System (DS) is to detect EM attacks that are performed in the protected infrastructure and, thus, be able to react to overcome them. The DS presents a geographically distributed architecture composed of one Central Health/Attack Manager (CHAM) that would be generally located at the command centre, and multiple detection subsystems distributed along the track and inside trains. Figure 6 presents this architecture.

The CHAM is the main element of the DS. It consolidates the information provided by its detection subsystem with regard to the information EM attacks and, thus, it provides a complete view of the EM state of the railway infrastructure. The CHAM also eases the centralized management of the detection subsystems.

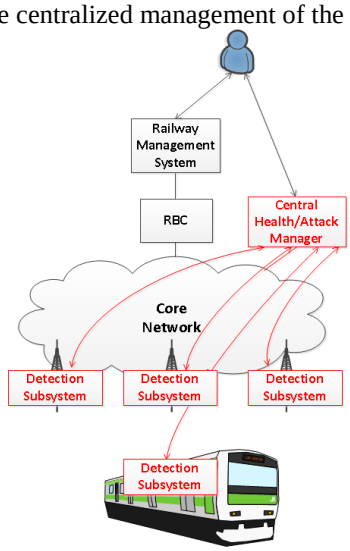

Figure 6: Architecture of Detection System (DS)

The detection subsystems are autonomous systems, governed by a local Health/Attack Manager (HAM), which is responsible for the detection of EM attacks in a specific geographical area and for carrying out the pertinent actions when EM attacks are detected. These subsystems may be deployed along the track or in the trains.

Inside each detection subsystem, sensors are deployed to feed with information regarding EM attacks the HAM that governs the local detection subsystem. Different types of sensors may be deployed; and the information provided by the sensors and the processing requirement of that information varies depending on the type of sensor used. For example, it can be the radio frequency signal received by an electromagnetic sensor or even information from upper layers like the latency, bit error rate or number of retransmissions.

In order to deploy sensors for detecting EM attacks inside GSM-R frequency bands with the processing algorithms proposed in section 3, two categories of electromagnetic sensor can be used. A first category considers sensors or inputs that provide access to information inside the GSM-R receiver situated in the train or at ground level, at different stages along the receiving chain. This allows us to collect information before/after different filters in the GSM-R receiver. This approach requires the modification of the existing equipment in order to collect the necessary analogue data. A second category considers a sensor independent of the GSM-R equipment, receiving the same radiofrequency signals as those effectively received by the railway equipment, by sharing the electromagnetic signals received by the train or ground BTS antenna.

Regarding the actions performed when an EM attack is discovered, they may depend on the current configuration of the detection subsystem:

- Discard the EM attack.
- Report the information about the EM attack to the CHAM in order to inform the railway management staff.
- In case of availability of a Multipath Communication System (MCS), change the communications

configuration of the MCS to adapt communications to the on-going EM attack.

4.2 Multipath Communication System (MCS) architecture

The aim of the Multipath Communication System (MCS) is to offer redundant communication paths between the Radio Block Centre (RBC) and the train. Figure 7 presents the architecture of this multipath communication system. The current ERTMS specification is based on circuit-switching technology which involves the use of a reserved channel. This supposes an inefficient use of the limited spectrum resources of GSM-R that would be increased in the case of performing a multipath technology on it. In addition, the deployment of a multipath communication system involves a modification of communication protocols or the application layer. In the case of an application level proposal, this would require a substantial modification of the ETCS equipment, which have already been certified by the industry to fulfil the strict requirements of the SIL4 standard. Thus, all modifications should focus on communication protocols.

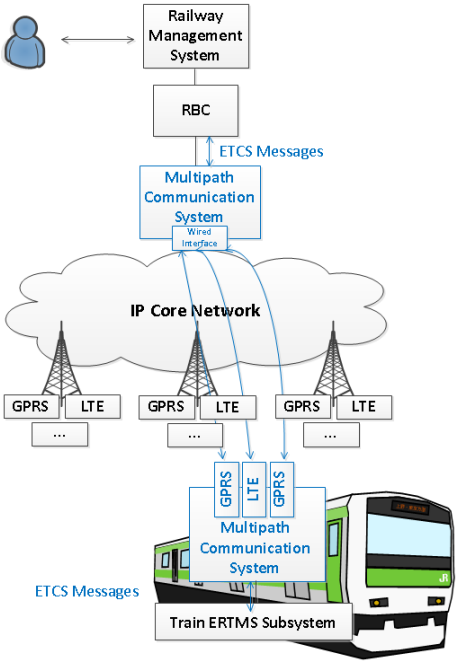

Figure 7: Architecture of the Multipath Communication System

Nowadays, the industry is considering the migration of the ERTMS from GSM-R towards new wireless access technologies due to the end of support of GSM technology in 2020 and the inefficient use of the spectrum of this technology (Ruesche et al., 2008), (Sniady et al., 2012). All new proposals, such as GPRS and LTE, are based on packet switching technologies (UIC, 2012), (Tentea, 2011) and TCP/IP protocol stack. This migration to TCP/IP protocols allows us to apply different multipath strategies, which are already used in IP networks, and the packet-switching technologies provide a more efficient resource usage.

Taking all this into account, the MCS proposal has been designed to cover the scenarios of railway communications that will be deployed in the near future. And, thus, the MCS will only consider TCP/IP as a communication protocol stack. In order to take full advantage of MCS, trains need to be multihomed or, in other words trains need to have two or more IP interfaces. This brings into focus the necessity to study protocols (Gladisch et al., 2012) like HIP, SHIM6, MPTCP or, SCTP. The availability of Software Defined Networking technologies which make a clear separation between data path and signalling control planes and the availability of several protocols, such as OpenFlow and ForCES, present the possibility to use a technology agnostic mechanism to control the MCS. It is important to remark that the MCS is unaware of the wireless technologies used, which provides a great flexibility (WiMAX (Aguado et al., 2013), LTE (Tingting et al., 2010), Tetra-IP…). Depending on the number and type of interfaces the communication will be more reliable against EM attacks. Indeed, in order to provide a better resilience against EM attacks it would be advisable to deploy multiple interfaces using different technologies that ideally use different range of frequencies. However, the use of

multiple interfaces of the same technology may be also useful as a fallback solution against eventual equipment failures.
Thanks to the MCS, the ETCS application of the RBC and train are unaware of the multiple paths since underlying networking protocols manage them transparently to offer a more robust and efficient data transport service to the upper layers of the network stack. This is a great advantage, because no change in the ETCS application protocol is required.

5. Conclusion

The railway is an attractive target for security attacks, because of its familiarity, ease of access and openness. Among the potential security attacks, electromagnetic terrorism aims at failing equipment or devices which serve the efficiency and safety of the railway transport system. This paper has presented some work performed on the SECurity of Railways against Electromagnetic aTtacks FP7 project aiming to assess the real risks concerning EM attacks on rail networks. It has concentrated on the ground to train communication by presenting the impact of a low-power jammer on this communication. Elements regarding the development of a detection system able to discriminate jamming signals from "normal" electromagnetic railway environmental conditions were also discussed. Finally, using this input, the resilient architecture discussed offers an improved resilience against EM attacks in order to protect wireless communications between trackside and trains principally. The proposed architecture provides a dynamic protection solution combining resilient communication architecture with a resilient health and attack management subsystem.

Acknowledgements

The research leading to these results has received funding from the European Community's Framework Program FP7/2007-2013 under grant agreement n°"285136".

References

Mansson, D., Thottappillil, R., Bäckström, M., & Lundén, O. (2008). Vulnerability of European Rail Traffic Management System to Radiated Intentional EMI. *IEEE Transactions on Electromagnetic Compatibility*, 50,. 101 - 109.

Mobile and personal communications committee of the Radio Advisory Board of Canada (2001). Use of jammer disabler devices for blocking PCS cellular and related services. In *http://www.meshcode.ca/PROJECTS/telefire/MK_jamming_laws_canada_01pub3.pdf*

Mili, S., Sodoyer D., Deniau V., Heddebaut, M., Philippe, H., Canavero, F. (2013). Recognition process of jamming signals superimposed on GSM-R radiocommunications. In *Proceedings of the EMC Europe 2013*.

S. F. Ruesche S.F. , Steuer J. & Jobmann K. (2008). The European Switch. Packet-Switched Approach to a Train Control System. *IEEE Vehicular Technology Magazine*.

Sniady A., & Soler J. (2012). An overview of GSM-R technology and its shortcomings. *In 12th International Conference on ITS Telecommunications (ITST)*, 626 - 629.

UIC GSM-R Projects 2010-2012 (2012). GSM-R Network Management, Frequency management. In *http://www.uic.org/spip.php?article429*

2011-EU-60013-S (2011). Facilitating and speeding up ERTMS deployment. In *http://tentea.ec.europa.eu*.

Gladisch A., Daher R., & Tavangarian D. (2012). Survey on Mobility and Multihoming in Future Internet. *Wireless Personal Communications*, 1 - 37.

Aguado M., Onandi O., Agustin P., Higuero M., & Taquet E. (2008). "WiMax on rails". *IEEE Vehicular Technology Magazine*, 3, 47,56.

Tingting G., Bin S. (2010). A high-speed railway mobile communication system based on LTE. In *International Conference On Electronics and Information Engineering (ICEIE)*, 1, 414 - 417.