PHYS ORG

New detection sensors can help railways cope with EM attacks

July 15 2015

Eleven years ago the Madrid train bombings proved how much European railway security still needed to be improved. But now that rail equipment—like in most other industries—is increasingly standardised and connected, another, more insidious type of offensive has become likely: electromagnetic (EM) attacks. An EU-funded project has developed detection technologies that can help the sector face this new threat.

Did you know that soon, there will be as many connected devices as there are humans on Earth? Five billion of these devices are now in use and this number is expected to reach 25 billion in 2020. Sure, each new type of connected device brings us closer to the advent of smart cities and all of their foreseen benefits. But on the other hand, as recent news has shown, it makes hackers and other tech enthusiasts with bad intentions a growing threat to security.

In the European railway sector for instance, the homogenisation of network technologies and the increasing use of wireless communications has made the scenario of an EM attack very likely. Communication jammers are easy to use and available for anyone to purchase on the Internet, which means that communications could potentially be jammed, with trains being delayed, blocked or even diverted.

To get the sector ready to face this new threat, the SECRET (SECurity of Railways against Electromagnetic aTtacks) project has developed a set of detection sensors capable of identifying EM attacks as they occur, so that rail equipment operators can switch the network to a 'safe mode' immune to the specific type of EM attack being used.

Virginie Deniau, coordinator of SECRET, discusses the likelihood of the EM attack scenario, the devices developed by her team and how the sector will soon need to adapt to this new reality.

How likely would you say is the EM attack scenario?

The definition of an EM attack evolves with the multitude of the applications based on wireless communication technologies. In the past, the EM attacks were based on the generation of high power intentional interferences (Electromagnetic pulse or high-power microwaves) able to disrupt or damage electronic equipment. Today, the functions of this equipment can be triggered by a command or information transmitted by wireless links, which means it is now easier to disrupt the transmitted information and damage the equipment. Such attacks require a less powerful signal which can be generated by mobiles and other discrete devices.

So, from a technological point of view, the likelihood of an attack increases with the vulnerability of the infrastructures. However it is difficult to establish a clear probability because today it is impossible to distinguish a technical failure from an EM attack. EM attacks based on relatively 'low' power signal involve disruptions but no permanent damage.

You mentioned mobile devices. Does that mean anyone is virtually capable of conducting such attacks?

The knowledge of the target is essential to define the means needed to perform an EM attack. Nowadays public communication jammers can easily be bought on the public market but their power and action are limited.

Now if we consider professional or security communication services, specific devices are generally required for such attacks. These devices are usually restricted to the professional market or have to be developed from scratch. While possible, this requires a certain level of skill and knowledge.

However, when these professional applications are supported by public wireless services, they can be disrupted by common jammers. So there is a real issue coming up, and the security and criticality of wireless services have to be seriously considered.

SECRET focuses on railway security. What could be the consequences of EM attacks in this sector?

The main direct risk is a perturbation of rail network traffic. It may be possible to prevent the departure of trains, force train stops and cause significant financial losses and unmanageable situations. However, it is difficult to accurately assess cascading risks, as they depend on the characteristics of each railway network (exploitation, infrastructure, applications, etc.).

Can you tell us more about the tools you developed?

SECRET's vision is that if we are able to detect an EM attack with certainty, we can imagine switching to a safe railway mode perfectly adapted to the situation and allowing operators to regain control. The challenge is therefore to develop fast and reliable detection solutions. With this in mind several solutions have been studied under SECRET. Some could be implemented directly within the communication terminals and other would require dedicated devices but offer the advantage of being able to monitor multiple communication links.

In order to reach resilience, our detection sensors were coupled with an acquisition and decision terminal which was charged with analysing the output of these detection sensors and commanding a reconfigurable telecommunication platform. According to sensors' output, the decision terminal directs the messages to be transmitted towards the communication link that's most resilient to the EM attack. Obviously, such an approach requires the deployment of several communication networks.

When do you expect SECRET's technology to reach the market?

Due to the mobility and the large spectrum of electromagnetic railway environments, the robustness and the total absence of fault of the detection solutions is difficult to demonstrate aboard a train. However, when the train is not moving, SECRET technologies can be really efficient. So we can envisage reaching the market relatively quickly with these technologies to protect train stations or other critical infrastructures.

In parallel, SECRET's technologies can contribute to the evolution of telecommunication standards employed in critical infrastructure. Instead of improving performance in terms of data rate, the standards can evolve to provide real-time information about the quality of services or the presence of jamming signals (intentional or unintentional). They could then provide relevant diagnostics and activate the adequate intervention process.

European railways are already under high economic and security-related pressure. Do you think the sector can bear the extra cost which the implementation of SECRET's solutions would involve?

I think that with this growing threat, it will be necessary to guarantee the resilience of the railway network against such attacks. Usually wireless communication systems only represent a small percentage of the budget of a railway project. However these systems are essential in operational and security plans. EM attacks can have dramatic consequences in terms of cost, and if they are easy to implement, they can also become frequent malicious actions. So a solution against EM attacks should be considered while balancing risks, impacts and investments.

What are your plans now that the project is close to its end?

We would like to test our analysis of EM attacks with other types of attacks such as physical or other cyberattacks. In fact, jamming attacks can easily be employed in support of other malicious actions in order to avoid video or alarm transmissions. As a consequence, the risks analyses have to take into account potentially coupled physical and jamming attacks. We also think that the detection architecture for EM attacks proposed in SECRET should be coupled with other monitoring tools for infrastructure in order get a better grasp of what's happening on the network in real time.

More information: For more information, see SECRET: www.secret-project.eu/

Provided by CORDIS

Citation: New detection sensors can help railways cope with EM attacks (2015, July 15) retrieved 26 April 2024 from https://phys.org/news/2015-07-sensors-railways-cope-em.html