SECRET

SECurity of Railways against Electromagnetic aTtacks

Grant Agreement number: 285136

Funding Scheme: Collaborative project

Start date of the contract: 01/08/2012

Project website address: http://www.secret-project.eu

Deliverable D 4.5

Validation of the Implementation through Use-Case

Submission date: October 2015

Deliverable on Dynamic Protection System

Date: 24/08/2013

Distribution: All partners

Manager: Trialog

Document details:

Title	Validation of the Implementation through Use-Case
Work package	WP4
Date	05/06/2015
Author(s)	E Jacob (EHU), C Pinedo (EHU), C Gransart (IFSTTAR), A Kung (TRIALOG), M Sall (TRIALOG)
Responsible Partner	Trialog
Document Code	SEC-WP4-D45-Validation of the Implementation through Use-Case - V6
Version	1.0
Status	Final

Dissemination level:

Project co-funded by the European Commission within the Seventh Framework Programme

PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission) Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document history:

Revision	Date	Authors	Description
0.1	05/06/2015	EHU IFSTTAR TRIALOG	Creation of the document. Contribution from EHU, IFSTTAR and Trialog
0.2	13/10/2015	ALSTOM	Description of use case 2
0.3	14/10/2015	EHU	Description of use case 1
0.4	15/10/2015	TRIALOG	Integration of contributions. Conclusion section

Table of content

1 Executive summary

This deliverable focuses on the validation of Secret architecture for communication resilience (specified in D4.1 and D4.2, simulated in D4.3 and implemented in D4.4) through use case implementations.

Two use cases are implemented: use case 1 based on mainstream components and two communication means, WiFi and WiMax; use case 2, based on railways system components and on two communication means, 3G and WiFi

These use cases are described and results from the implementation are analyzed. It is concluded that the use case implementation results are consistent with simulation results (D4.3). They therefore validate the secret architecture for resilient communication from an implementation viewpoint.

2 Introduction

2.1 Content of Deliverable

The purpose of this deliverable is (1) to present the two use cases chosen to implement the Secret architecture for resilient communication under EM attack.

This deliverable completes the WP4 series of deliverables:

- D4.1 Preliminary specification of the dynamic protection system. It presents an overview of the protection system and gives a brief description of the components of the protection system.
- D4.2 Final specification of the dynamic protection system. It presents a final and complete view of the resilient architecture in order to face EM attacks. It served as the basis for the implementation of the resilient architecture.
- D4.3 Simulation and assessment results of dynamic protection system. In order to understand and predict the behavior of the protection system, this deliverable has modelled all the components of this protection system with all their interactions and dependencies. Simulations have been made which gave good results.
- D4.4 Implementation of the dynamic protection system. This implementation followed the architecture specified in D4.2.
- D4.5 Validation of the implementation through use-case.

The deliverable is structure as follows:

- Section 2 presents the architecture for resilient communication as well as an introduction to the two use cases
- Section 3 presents use case 1
- Section 4 presents use case 2
- Section 5 concludes

2.2 SECRET Architecture Components for Resilient Communication

A detailed specification of the SECRET architecture for resilient communication. This section highlights the main components which need to be implemented in the use cases.

The Resilient Communication Architecture (RCA) in the train is composed of the following main components (see Figure 1):

- Health/Attack Manager (HAM)
- Acquisition System Analyser (ASA)
- Sensors connected to the ASA
- Multipath Communication Manager (MCM)
- Several communication devices behind the MCM

The first three components are part of what has been called the protection subsystem (see figure below). The role of this subsystem is to continuously monitor the overall network for detecting EM attacks performed on the network. The two remaining components are part of the MCM. The role of this second subsystem is to provide resilient communications between trains and the command center located at the ground.

HAMs are further subdivided into categories according to their roles:

- Train Health/Attack Management
- Trackside Health/Attack Management
- Central Health/Attack Management

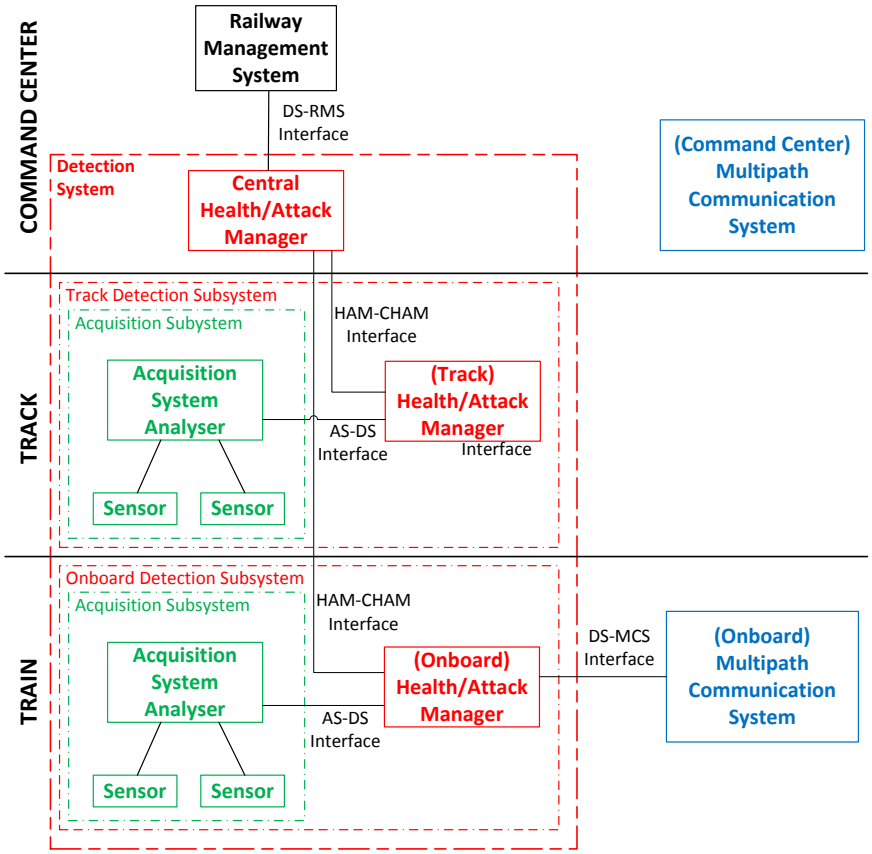


Figure 1: SECRET resilience components

2.3 Introduction to Use Cases

The SECRET work plan initially focused on a single use case that would be used to demonstrate the complete resilient communication architecture. During the project, concern was raised on the fact that the demonstration would not be based on actual railways systems. The project has consequently decided to focus on two use cases:

- Use-case 1 focuses on a complete resilient communication architecture. To this end mainstream (PC centric) components are used and redundant communication is based on WiFi and WiMax.
- Use-case 2 focuses on the flexibility of the architecture and its use in actual railways system components (e.g Alstom netbox equipment), with redundant communication based on 3G and WiFi.

3 Implementation of Use Case 1

3.1 Functional description

The objective of this use case is to test and validate the complete resilient communication architecture defined in the SECRET project. Thus, this use case makes use of all the components of the architecture which consists of: the Acquisition System Analyser (ASA), the Detection System (DS) and the Multipath Communication System (MCS).

The sensors and algorithms developed for the ASA inside the train will try to detect EMIs and inform the Health/Attack Manager (HAM) of the DS. This HAM, based on the information provided by the ASA, will perform actions on the MCS if required. These actions would imply the reconfiguration of the Multipath Communication Manager (MCM) depending on the current traffic policy applied in the MCM and the type of EMIs suffered in order to overcome the EMIs. Finally, the MCM would apply the communication changes requested by HAM.

The use-case is composed of a video camera on a simulated trackside which sends a streaming HTTP video over the air to a simulated train. The train is equipped with a monitor to display the video in real-time.

The scheme of this use case is detailed in the next Figure 2.

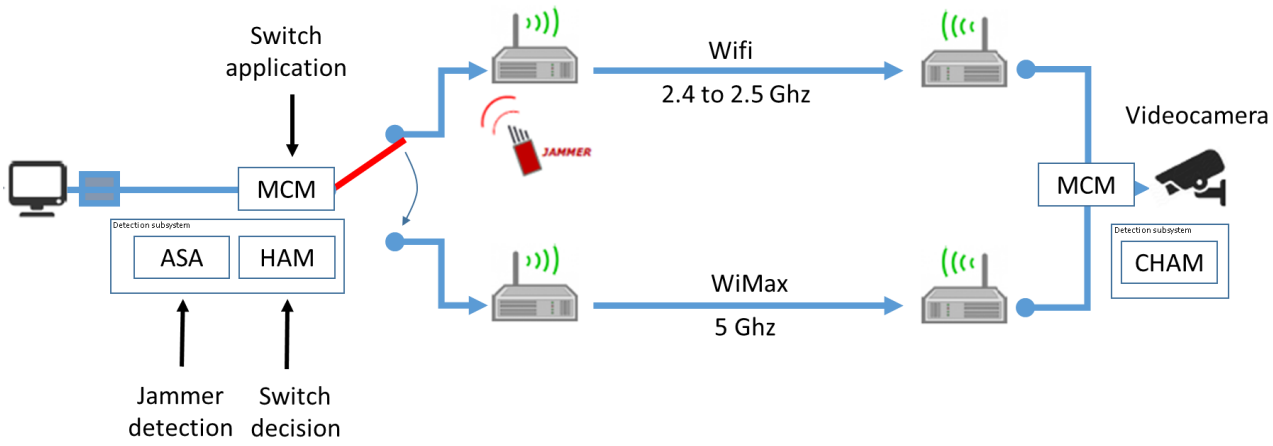


Figure 2: Diagram of the use-case 1.

Two wireless communication technologies have been chosen for the use case, which have different operating frequencies to provide robustness against EM attacks launched at different frequency ranges. The first and default technology is a Wifi connection whose operating frequency is between 2.4 and 2.5 Ghz. The second technology is a WiMax connection at 5 Ghz.

The communication interfaces of the train are managed by the Multipath Communication Manager (MCM) located on the train. The MCM can apply different values to the interfaces and bring them up and down. Furthermore, thanks to the implementation of Multipath-TCP it is possible to provide soft vertical handoffs and use simultaneously multiple interfaces to transmit TCP traffic. However, other kinds of traffic (UDP or ICMP) can't benefit from this multipath protocol.

Figure 3: Train communication device that implements HAM and MCM (with WiFi and WiMAX interfaces); and have Ethernet wired connections to receive information from the sensors of the train.

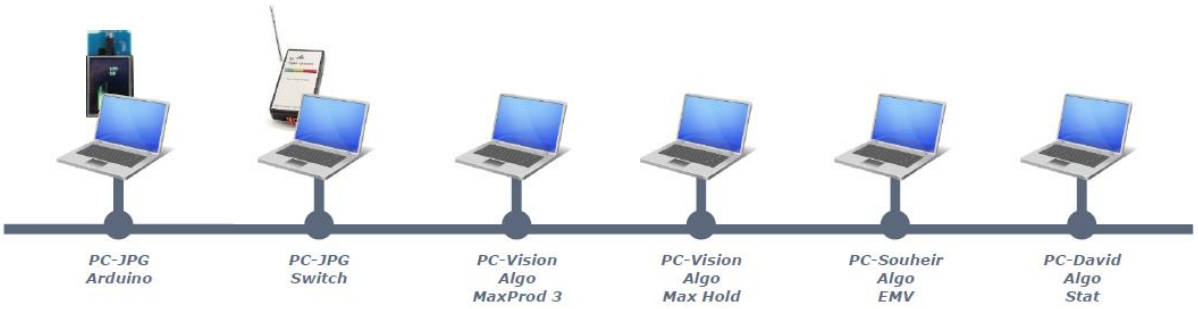
On ground, there is another MCM behind WiFi and WiMAX base stations. However, this MCM is only used to finish the MPTCP traffic of the train and translate the MPTCP to TCP and vice versa. This MCM is not controlled by any HAM and does not govern dynamically the behaviour of the WiFi and WiMAX base stations.

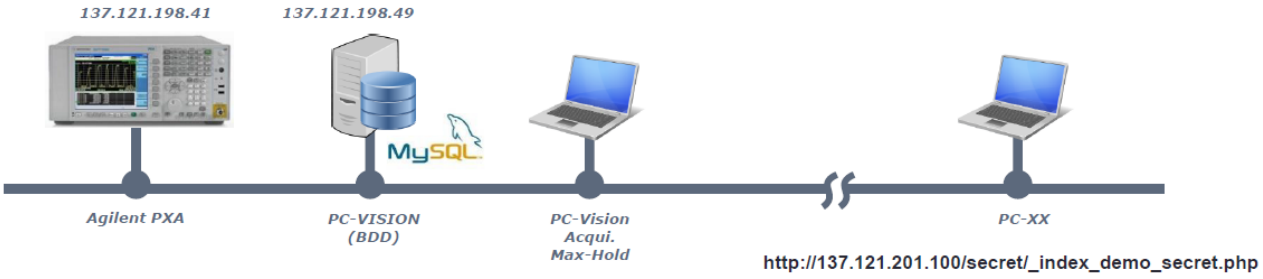
Figure 4: Ground part of the testbed: WiFi Access Point, WiMAX Base Station and communication device where ground MCM and CHAM is developed.

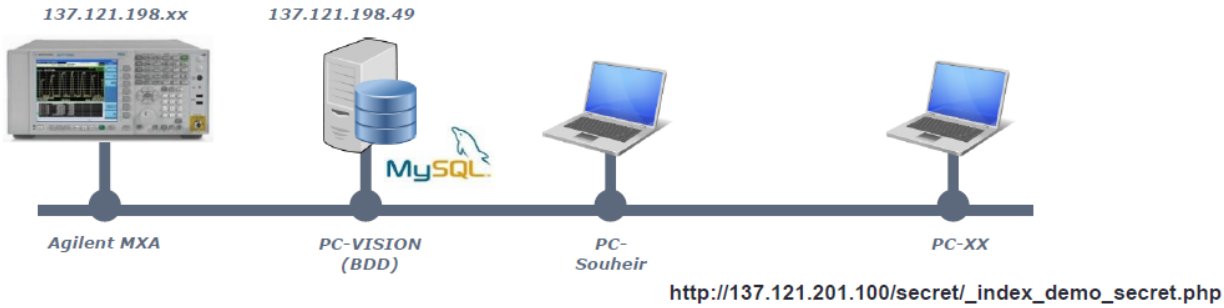
The Detection System is connected to the Acquisition System Analyser (ASA). The ASA is strongly linked with a HAM located in the train and one Central Health/Attack Manager (CHAM) on ground. The HAM of the train requests that the MCM modifies the communications based on the EM attacks reported to the HAM by the sensors of the Acquisition System Analyser deployed along the train. In fact, the HAM applies different traffic policies in the MCM, which can be changed during the operation. On the other hand, the CHAM is located on ground and receives the EM attack reports of the remote HAMs.

The full set of detectors presented in the deliverable D3.4 has been setup for the demonstrator. A description of these detectors is presented in the deliverable D3.4. A bunch of algorithms has been implemented. They analyse the spectrum and store their results in a database. See figure below.

For each of these algorithms, a class has been implemented in the ASA. Each class reads this database periodically. According to the current values and historical information (sliding window on data), it determines if the communication is under attack or not. When a jammer is detected by the ASA, the HAM is informed and then the HAM requests the MCM to execute a countermeasure. This action depends on the policy in place within the HAM. Several policies have been implemented and are described in the next section.







3.2 Description of Traffic Policies

When the MCM is configured in auto mode, it applies a default configuration to the wireless interfaces. However, when the MCM of the train is in managed mode, it allows the HAM to directly configure the wireless interfaces dynamically. Up to three parameters can be configured per interface in managed mode:

- Interface mode: down or up.

- Interface metric: the metric value for the IP routes that are learned through this interface. If the same IP route is learned from multiple interfaces, the interface with the lowest metric value is the preferred one for those IP routes.
- MPTCP mode: disabled, active or backup mode.

Consequently, there are a lot of possible combinations of the previous values for the two interfaces of the use case. However, to simplify the management of the interfaces and to reduce the number of possible and useful configurations the concept of traffic policies is used. The traffic policies are based in three main concepts: number of interfaces simultaneously activated in the MCM, HAM interaction, and MPTCP functionality.

Number of interfaces simultaneously activated on the MCM	HAM interaction	MPTCP functionality
One	No	Disabled
	Yes	Disabled
		Enabled
Multiple	No	Disabled
		Active Backup (mix of active/backup interfaces)
		Load Balancing (all backup interfaces)
		Replication (all active interfaces)
	Yes	Disabled
		Active Backup (mix of active/backup interfaces)
		Load Balancing (all backup interfaces)
		Replication (all active interfaces)

Table 1: Concepts to define traffic policies for the MCM.

In D4.4 up to five traffic policies were described. These were selected as an example set of static and dynamic traffic policies. However, considering the Table 1 even more traffic policies can be defined.

The first term to consider to define the traffic policy is the number of interfaces that are going to be enabled simultaneously. If only one interface is going to be enabled simultaneously, the HAM interaction can be interesting to bring interfaces up and down depending on events such as the EM attacks. Otherwise, in case of problems with the activated interface, the HAM can't activate the other interfaces. Apart from the HAM interaction, MPTCP functionality might be required to provide soft vertical handovers between interfaces for MPTCP/TCP connections (the MPTPC/TCP connection is not lost when there is a change of the wireless interface activated).

If there are multiple interfaces simultaneously enabled in the MCM, there are more options. MPTCP is not only useful to provide soft vertical handovers between interfaces, but also to send data in different ways through all the enabled interfaces. Thus, the MPTCP redundant scheduler developed for the SECRET Project allows active-backup, load-balancing and replication traffic transmissions. The active-backup behaviour is obtained when one interface is configured as active and the other as backup. The load-balancing behaviour is obtained when all interfaces are configured in backup mode. Finally, the replication behaviour is obtained when all interfaces are configured as active interfaces.

For this use-case, we have selected the most interesting traffic policies to face EM attacks dynamically with the help of the HAM:

- Switching traffic policy.
- Active-backup traffic policy.
- Replication traffic policy.

These traffic policies are explained in detail in the following sections.

Switching traffic policy

The HAM only activates one interface at a time with MPTCP enabled (active mode). If there are events affecting the enabled interface, the HAM selects other interface to bring up and it also brings the old interface down.

One advantage of this policy is that it uses interfaces very efficiently because only one is activated at a time. However, it depends heavily on the HAM and the jammer detection capabilities of the AS to function properly.

Thanks to this policy, TCP traffic (translated to MPTCP traffic by the MCM) benefits from soft handovers when there is an interface switch, that is, the already established TCP connections are maintained. However, other protocols such as UDP and ICMP suffer hard handovers.

Active-backup traffic policy

The HAM enables all the available interfaces. One of the interfaces is the main interface and the rest are configured as backup interfaces.

Backup interfaces are only used if they are required. But they have some residual traffic even when there is no necessity to use them because TCP backup subflows are pre-established. The advantage of this procedure is that switching from one interface to another one is faster. The TCP connections (translated to MPTCP connections by the MCM) use automatically the backup interfaces even without the intervention of the HAM when there are problems with the primary interface. However, to establish new TCP connections or to use other transport protocols such as UDP or ICMP through the backup interfaces there is a dynamic reconfiguration of the backup interfaces required by the HAM.

Thanks to this policy, TCP traffic (translated to MPTCP traffic by the MCM) benefits from soft handovers when there is an interface switch, i.e., the already established TCP connections are maintained. In contrast, other protocols such as UDP and ICMP suffer hard handovers.

Replication traffic policy

The HAM enables all the available interfaces and set them as active interfaces for MPTCP. According to the redundant scheduler developed in the SECRET Project, this involves that traffic is going to be replicated through all the available interfaces. In other words, the same information is going to be sent through all the available interfaces.

This scheduler provides better delay and jitter because if there is any problem in one interface the data has been already sent or received through other interfaces, which avoids the retransmissions and so the delay and jitter introduced by them.

The HAM is necessary in order to set always the appropriate interface with the lowest metric, because this interface is essential to establish new TCP connections (translated to

MPTCP connections by the MCM) and for the rest of IP traffic (UDP or ICMP for instance). If the interface with the lowest metric is suffering from a bad connectivity, this implies problems for the establishment of new TCP connections and for the non-TCP IP traffic.

As in the previous traffic policies, TCP traffic (translated to MPTCP traffic by the MCM) benefits from soft handovers when there is an interface switch but no other transport protocols.

3.3 Configuration of Traffic Policies

In this section, the selected three traffic policies are configured specifically for this use case. This involves that there are two wireless interfaces available in the MCM: one WiFi interface and one WiMAX interface. The preferred interface is the WiFi interface and the WiMAX interface is used in different ways depending on the traffic policy to provide more resilience against problems in the WiFi interface.

Switching traffic policy

This traffic policy is applied for the WiFi and WIMAX interfaces of the MCM. The WiFi interface is the preferred interface and the WIMAX is the backup one. Thus, initially the HAM configures MCM with the WiFi interface enabled and the WIMAX interface disabled as it is shown in Table 2.

WiFi interface (main & active interface)	WiMAX interface (disabled)
interface_mode=enabled interface_metric= 100 mptcp_mode=enabled	interface_mode=disabled interface_metric=101 mptcp_mode=enabled

Table 2: Initial configuration for the switching traffic policy.

When there is an attack or problem that affects the WiFi connection, the HAM decides to switch from the WiFi connection to the WIMAX one. The configuration to apply it is shown in Table 3.

WiFi interface (disabled)	WiMAX interface (main & active interface)
interface_mode=disabled interface_metric= 100 mptcp_mode=enabled	interface_mode=enabled interface_metric=101 mptcp_mode=enabled

Table 3: Reconfiguration for the switching traffic policy to face EM attack on WiFi interface.

Finally, when the problems in the WiFi interface finishes, the initial configuration detailed in Table 2 is applied by the HAM in the MCM again.

Active-backup traffic policy

Initially, the HAM applies this traffic policy by bringing up the WiFi and the WiMAX wireless interfaces. Since the WiFi interface is the preferred connection whereas the WiMAX interfaces is the backup one, the WiFi interface is configured with a lower metric than the WiMAX interface and the WiFi interface is an active interface for MPTCP while the WiMAX interface is a backup interface for MPTCP. This configuration is summarized in the Table 4.

WiFi interface (main & active interface)	WiMAX interface (backup interface)
interface_mode=enabled	interface_mode=enabled

interface_metric= 100 mptcp_mode=enabled	interface_metric=101 mptcp_mode=backup

Table 4: Initial configuration for the active-backup traffic policy.

When there is an attack in the preferred WiFi interface, the metric of one of the backup interfaces must be improved to begin to use that interface when it is required to establish new TCP connections and to send other transport traffic such as UDP or ICMP. In the use case the WiMAX interface is reconfigured with a better metric than the WiFi interface as shown in Table 5.

WiMAX interface (new main & backup interface)
interface_mode=enabled interface_metric=99 mptcp_mode=backup

Table 5: Reconfiguration for the active-backup traffic policy to face EM attack on WiFi interface.

When the attack finishes, only the backup interface modified must be reconfigure by HAM with the default configuration. This is show in Table 6.

WiMAX interface (only backup interface again)
interface_mode=enabled interface_metric=101 mptcp_mode=backup

Table 6: Reconfiguration for the active-backup traffic policy to recover initial behaviour.

Replication traffic policy

The initial configuration to apply in the MCM by the HAM is quite similar to the configuration applied to the active-backup previous traffic policy. WiFi and WiMAX interfaces are configured to be enabled, with MPTCP configured in active mode and with a preferred metric in the WiFi interface (see Table 7).

WiFi interface (main & active interface)	WiMAX interface (active interface)
interface_mode=enabled interface_metric= 100 mptcp_mode=enabled	interface_mode=enabled interface_metric=101 mptcp_mode=enabled

Table 7: Initial configuration for the replication traffic policy.

When an EM attack is detected on the WiFi interface, the HAM must set the WiMAX interface with a preferred metric value as shown in Table 8.

WiMAX interface (new main & active interface)
interface_mode=enabled interface_metric=99 mptcp_mode=enabled

Table 8: Reconfiguration for the replication to face EM attack on the WiFi interface.

Later, when the HAM realized that there is no EM attack on the WiFi interface, it must set again the preferred metric value in the WiFi interface and therefore it increases the value of the metric parameter of the WiMAX interface (see Table 9).

WiMAX interface (only active interface again)
interface_mode=enabled interface_metric=101 mptcp_mode=enabled

Table 9: Reconfiguration for the replication traffic policy to recover the initial behaviour.

3.4 Attack description

The use case consists in a video streaming HTTP connection already established between the train and ground using the default wireless interface, the WiFi interface, at T0. Then, one jammer begins to disturb the WiFi frequency band and affecting the communication at T1 until T5.

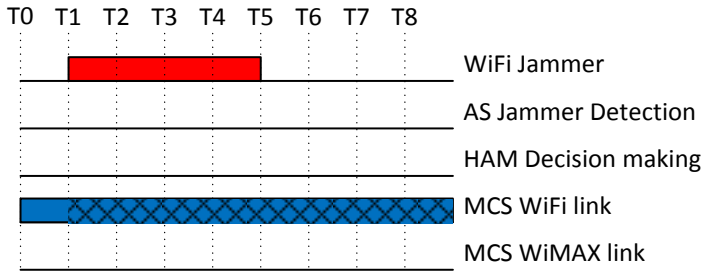


Figure 5: Timing diagram for the use-case.

Depending on the traffic policy configured by the HAM in the MCM, the resilient communication architecture faces the EM attack differently. Without the resilient communication architecture, this attack can imply the loss of communication between T1-T5 and the need to establish again the video streaming connection after T5.

3.5 Impact Traffic Policies on Attack

In this section we apply the attack to the three traffic policies and verify the impact of the attack in every case.

Switching traffic policy

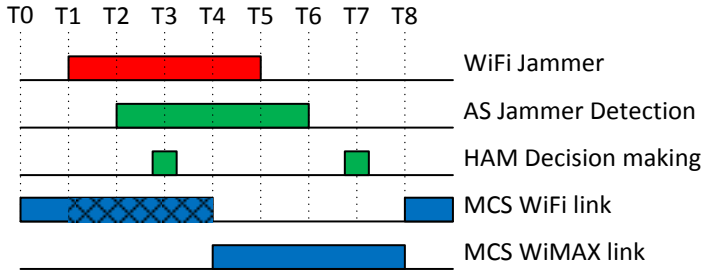


Figure 6: Timing diagram for the switching traffic policy.

At T0 there is a video streaming HTTP service already established between the train and ground using the WiFi interface. The WiFi jammer begins at T1 but it is not detected by sensors until T2. The HAM processes the information and takes the decision to switch from WiFi to WiMAX interface at T3. The WiFi interface is brought down and the WiMAX interface is finally brought up at T4.

Thus, depending on the power of the Jammer the WiFi connection can have a significant BER (Bit Error Rate) or even be down from T1 to T4.

Finally, when the jammer is aware that the jammer attack has finished, it decides to change the communication from WiMAX to WiFi again at T7 and it doesn't happen until T8.

This traffic policy is efficient because the redundant connection (WiMAX connection) is only used when it is required and it is down the rest of the time. However, there is a huge dependency on the HAM because the switching decision is taken by the HAM.If the HAM decides not to switch the communication is not restored. Furthermore, even with a proper HAM, there could be a significant loss of communication time from T1 to T4. The connection is maintained but the video is frozen several seconds but once switched to WiMAX connection it continues.

One key point to improve the switching from one interface to another is the order of bringing interfaces up and down.

If the HAM decides to switch from WiFi to WiMAX, firstly it will bring down the WiFi interface and then it will bring the WiMAX connection up. During, this switch there is a brief loss of communication time (the video freezes). That is shown in the next real measurements:

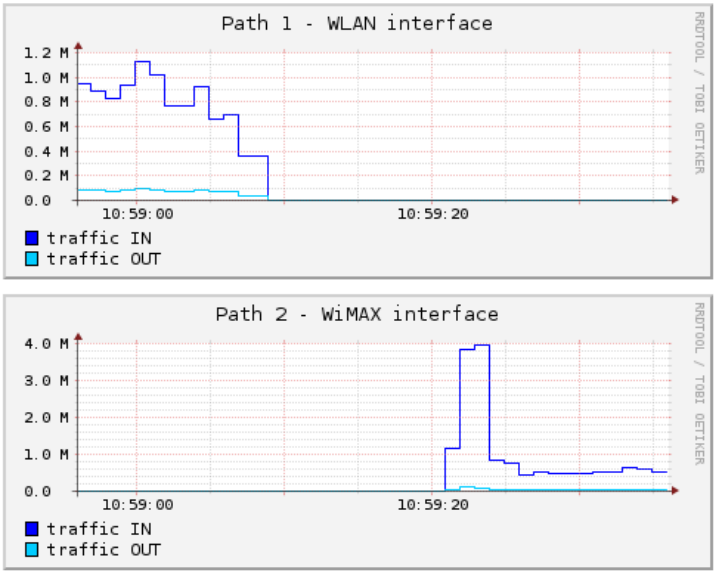


Figure 7: Traffic Bringing WiMAX down and then bringing WiFi up.

Although the video communication is maintained thanks to the vertical handover capabilities of MPTCP, this loss of communication time depends on the specifics of the wireless technology used. For example, in order to bring one WiMAX connection up, the interface needs to connect to the WiMAX network, perform an authentication process, obtain one IP address from the DHCP service and then the interface is considered to be ready to send data. This procedure differs from one wireless technology to another and it may imply more or less time, but in any case a significant amount of time (a couple of seconds).

In any case, the video connection is maintained and when the WiMAX connection is finally ready there is a peak of transmission due to the buffered data pending to be transmitted.

One improvement to this approach is to firstly bring the WiMAX interface up and then bring the WiFi interface down. Thanks to MPTCP and to the redundant scheduler developed for the SECRET project, during the brief time both interfaces are up simultaneously they send the same data and so there is no video freezing. This is confirmed because of the absence of any traffic peak when the WiMAX interface is activated due to any buffered and not already sent data.

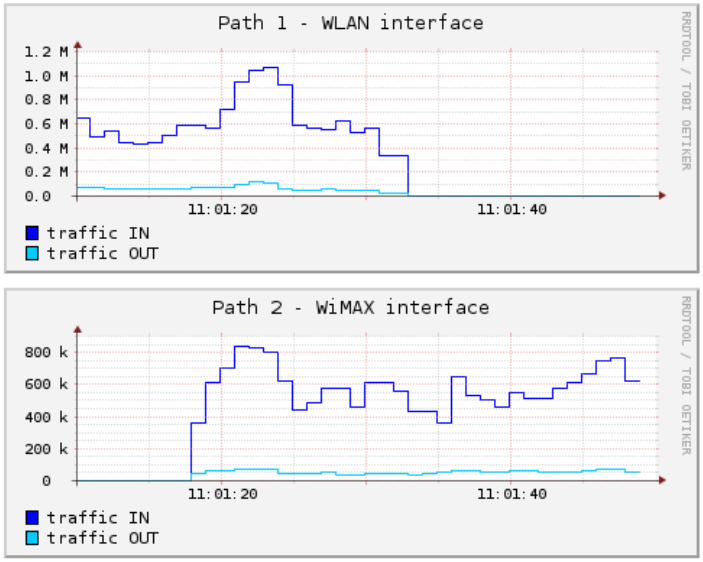


Figure 8: Traffic Bringing WiFi up and then bringing WiMAX down.

Active-backup traffic policy

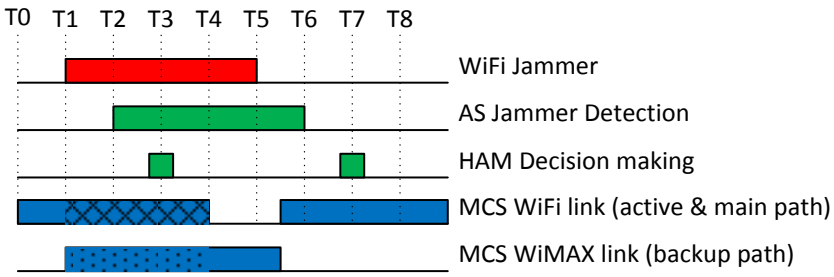


Figure 9: Timing diagram for the active-backup traffic policy.

To perform the tests with this traffic policy at T0 the video streaming connection is established through the WiFi interface. It is interesting to verify that in fact there is some traffic in the backup interface because the WiMAX interface is enabled and MPTCP establishes backup TCP subflows for the ongoing connections that will be used in case of failover (see Figure 10).

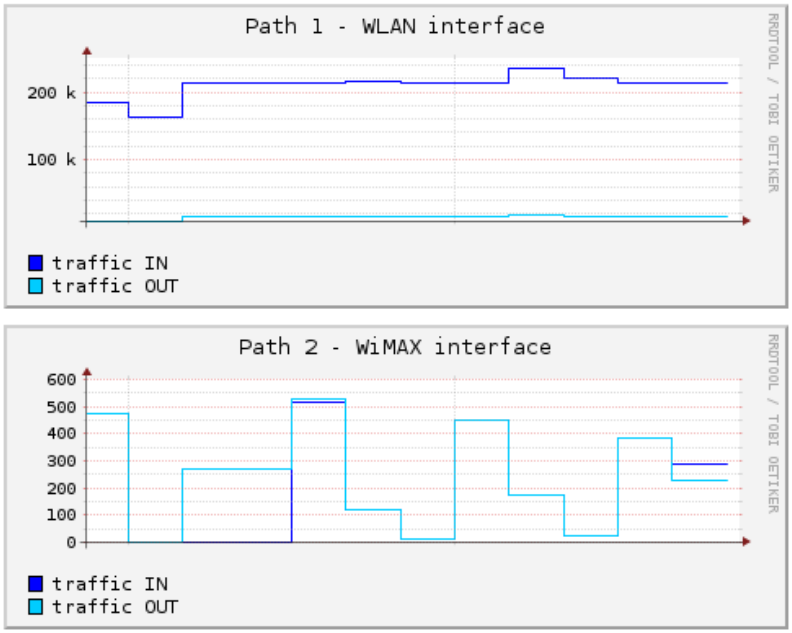


Figure 10: Video traffic in the WiFi interface and minimal traffic in WiMAX interface due to MPTCP backup TCP subflow.

At T1 the WiFi jammer starts to jam the WiFi connection, but the sensors detect the attack at T2 and the HAM receives the information and makes decision at T3. However, thanks to this traffic policy if there are problems transmitting data of the video streaming service through the WiFi connection, the backup connection, the WiMAX connection, is used automatically without waiting the response of the HAM at T4. So, the video streaming connection continues using the WiMAX connection if required without any gap in the video playback.

Depending on the power of the WiFi jammer there could be two different cases:

- If the jammer is not so powerful, the WiFi connection is not broken but the Bit Error Rate (BER) increases significantly. This produces bit errors in the transmitted data package so that it must be re-transmitted. Apart from being re-transmitted via the original WiFi connection (mandatory due to the behaviour of the TCP protocol), the re-transmission of the data package is also scheduled in the WiMAX connection thanks to MPTCP.
- If the jammer is very powerful, the WiFi connection is lost. So the video streaming connection switches directly to the backup connection in order to continue sending the data because the primary connection is down.

The tests were performed in the laboratory with a jammer that brought the WiFi interface totally down. We could verify how immediately the WiFi connection is brought down the data is sent through the WiMAX interface because the interface is already enabled with a backup subflow established. In Figure 11, we can see how at T1 when jammer tears the WiFi interface down, the video traffic is automatically sent through the WiMAX interface without waiting the reaction of HAM at T4.

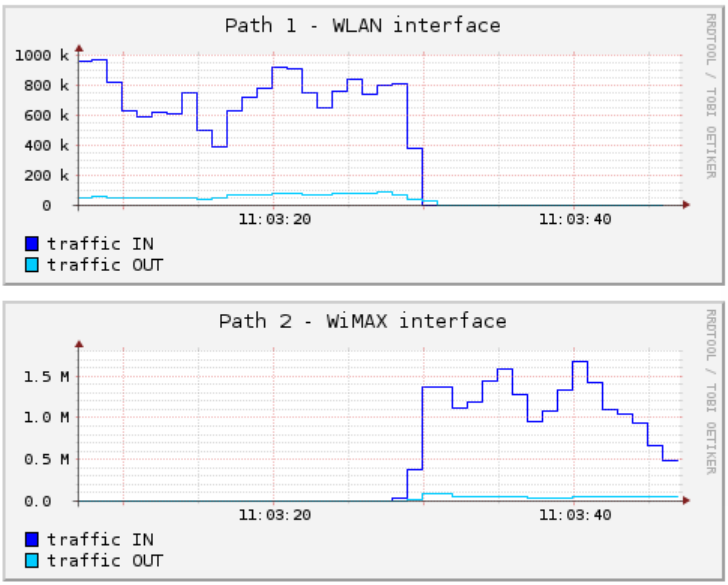


Figure 11: Behaviour at T1, video traffic automatically switches from WLAN to WiMAX on WiFi attack.

Later, at T4, the HAM realized that there is a problem with the current WiFi connection and sets the preferred metric for the WiMAX connection. This is important if the WiFi connection is still up because the new TCP connections (converted to MPTCP connections) and other transport protocols would be using this jammed interface instead of one not affected by the attack. So, from T1 to T4 there could be a problem with new TCP connections and non-TCP traffic that it is solved by the HAM definitely at T4.

Similarly, when the jammer stops at T5 the WiFi connection is recovered a bit later (after link setup, authentication procedures, etc.) and the switching from the WiMAX to the WiFi interface is performed before the HAM is aware at T7 and without requiring its intervention as it is shown in Figure 12.

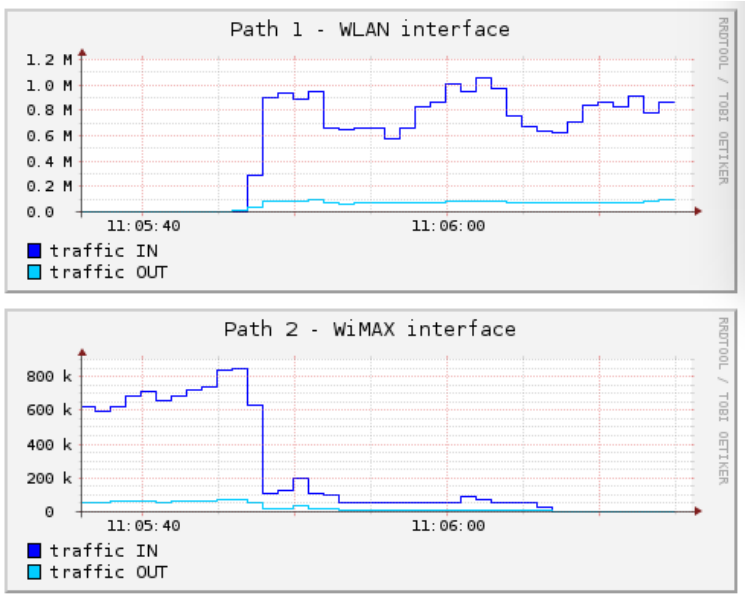


Figure 12: Behaviour between T5-T6, video traffic automatically switches from WiMAX to WLAN interface once WLAN interface is recovered.

Finally the HAM at T7 re-establish the WiFi connection as the preferred connection to establish new TCP connections and to be used by non-TCP traffic such as UDP and ICMP.

Replication traffic policy

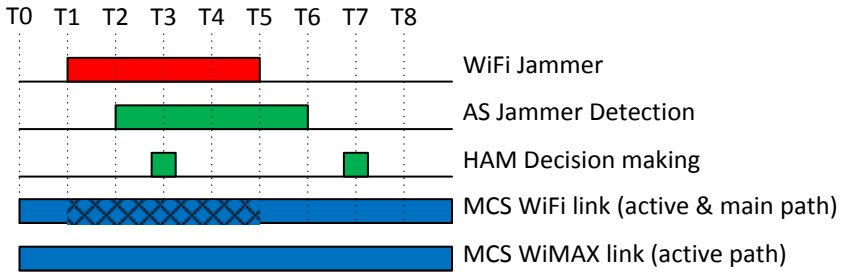


Figure 13: Timing diagram for the replication traffic policy.

At T0 there is a video streaming connection established between the train and ground and due to the use of this traffic policy the data is replicated through the WiFi and WiMAX interfaces as it is shown in Figure 14.

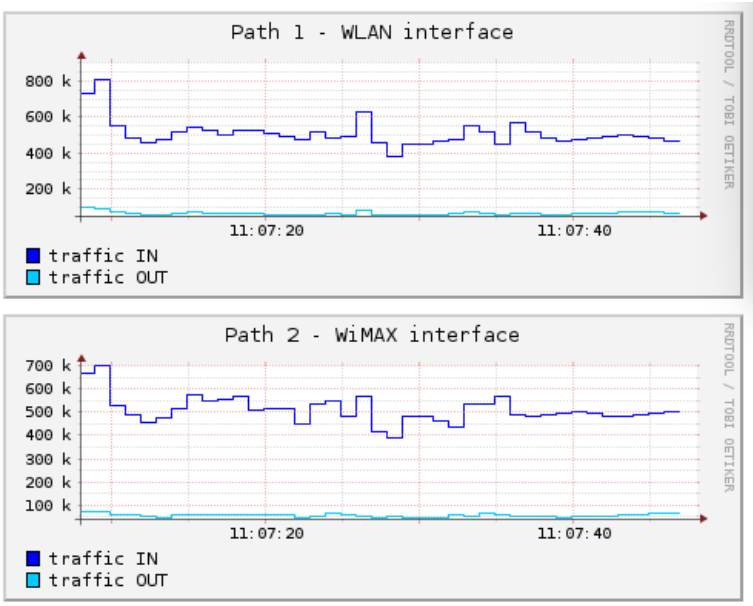


Figure 14: The video streaming connection is established and data is replicated through all the interfaces at T0.

At T1 when the jammer begins the WiFi interface is teared down and the video data is only sent through the WiMAX interface. The video reproduction continues smoothly without being affected by the WiFi jammer (see Figure 15).

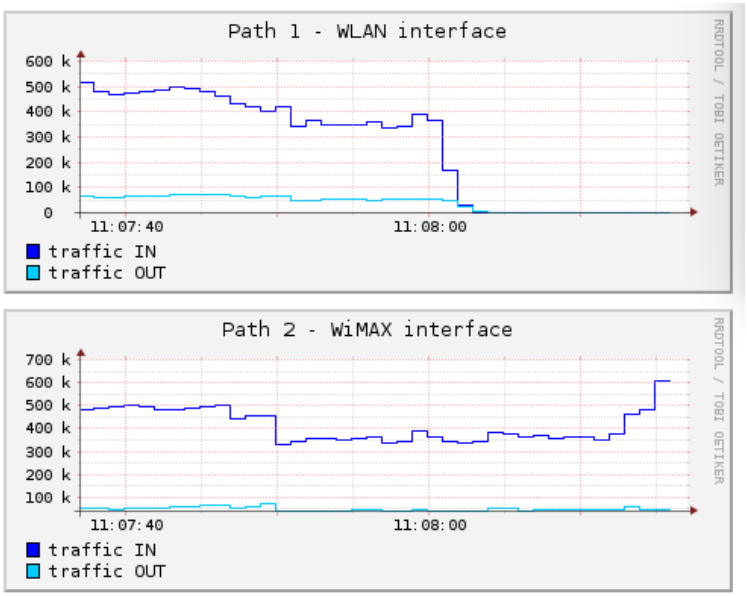


Figure 15: The WiFi connection is teared down by the jammer at T1 but the video transmission continues through the WiMAX connection.

This traffic policy provides a packet delivery with better delay and jitter than the previous traffic policies because the packets are sent through the WiMAX connection without waiting if a re-transmission is required or not. Thus, this traffic policy could be of interest in very noisy scenarios or even to protect traffic very sensitive to delay and jitter such as ETCS traffic.

If the HAM realized that there is an attack at T4, it will change the interface priority so that the WiMAX interface would be the preferred interface. If the WiFi interface was teared down by the WiFi attack, this is not necessary. However, if the WiFi interface was still up at T4, it is a noisy interface and the new TCP connections and other non-TCP traffic is suffering a very noisy link since T1. Thus, from T4 on, new TCP connections can be established and other traffic such as UDP or ICMP stops suffering a very high BER because they begin to use the WiMAX interface.

The jammer stops at T5 and once the WiFi link is ready again (link establishment, authentication and IP address configuration) traffic replication begins automatically again through the WiFi interface, see Figure 16, without waiting for the HAM intervention at T7.

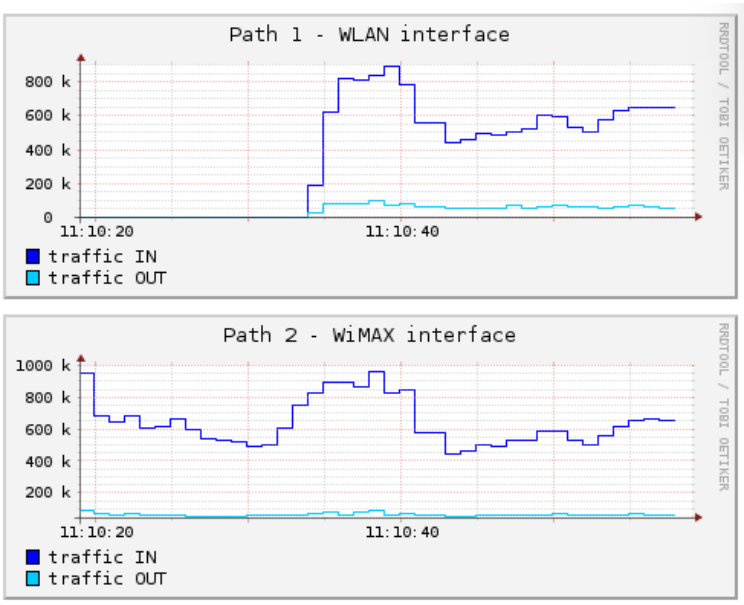


Figure 16: Traffic replication begins automatically at WLAN interface just a bit later than T5 when the WLAN link is ready again.

The HAM requires more time to realise that the jammer ended and at T7 it establishes the WiFi connection again as the preferred interface for new TCP connections and for the rest of the IP traffic. This is applied by the MCM almost instantly at T8.

Comparison of Traffic Policies

Table 10 presents a comparison of the results obtained for the three traffic policies of the MCM in this use case. What it is remarkable is the flexibility provided by the MCM to consider different traffic policies depending on the requirements defined such as efficient resource usage or a quick recovery under attack. Furthermore, the traffic policy does not need to be statically configured and could be dynamically changed by the HAM. For instance, it would be possible to initially apply the switching traffic policy and when there is a general EM attack affecting all the interfaces the HAM might decide to move towards a replication traffic policy.

Traffic Policy	Resource Usage	TCP (MPTPC) handoff	Non-TCP handoff	Attack Reaction at T1 (time reaction important to overcome the communication problem)		Attack Recovery at T5 (time reaction not so important to recover original behaviour)	
				TCP (MPTCP) handoff time	Non-TCP handoff time	TCP (MPTCP) handoff time	Non-TCP handoff time
Switching	Efficient	Soft	Hard	T4* (bring up interface)	T4* (bring up interface)	T8* (bring up interface)	T8* (bring up interface)
Active-backup	Less Efficient	Soft	Hard	~ T1 (depending of the RTO of the attacked interface)	T4** (interface already up)	T5 + time to recover the link in the attacked interface	T8** (interface already up)
Replication	Intensive	Soft	Hard	T1 (instantly)	T4** (interface already up)	T5 + time to recover the link in the attack interface	T8** (interface already up)

Table 10: Comparison of results obtained with the different traffic policies in use case 1.

4 Implementation of Use Case 2

4.1 Functional Description

The aim of use case 2 was to implement a vertical roaming solution between available interfaces of a connecting train radio device (Alstom Netox) and to use it for improving resilience of the communication between train and ground.

- If one channel is jammed and the handoff algorithm detects it, it will automatically switch to another communication system
- If a jamming is detected on one communication channel by an external system, this will be taken into account by the handoff algorithm and it will force the switching to another communication system or at least decrease the preference of the jammed channel.

Two software components have been implemented on the Alstom Netbox: a Vertical Handoff algorithm (SEAMO) and a Mobile IP solution (open HIP) in order to manage the communication flows of an application running between the train and the ground.

The SeaMo Vertical Handoff algorithm is an implementation of seamless handoffs across heterogeneous wireless access networks. SeaMo uses a fuzzy logic based decision algorithm to decide when to handoff.

The main advantage of this algorithm is that it is able to take any other information into account beside classical network information parameters. So jamming detection can be easily introduced as an important parameter independent from its format (yes/no, probability,...).

All technical information of the implementation architecture of SeaMo can be found here :

> *Rafiq, M.; Kumar, S.; Kammar, N.; Prasad, G.; Garge, G.K.S.; Anand, S.V.R.; Hegde, M.; , "A Vertical Handoff decision scheme for end-to-end QoS in heterogeneous networks: An implementation on a mobile IP test bed," Communications (NCC), 2011 NationalConference on , vol., no., pp.1-5, 28-30 Jan. 2011*

The jamming detection equipment is connected to a HAM module implemented in the Netbox. It relays the information to the SeaMo vertical roaming module. If jamming information is received from the detector, a vertical handoff is processed in order to maintain the link between Netbox and the trackside server.

The HAM presented here is different from the one developed for use case 1.

This local version of HAM implemented on the NETBOX provides a waiting time of three seconds of jamming alert before the decision making and the switching from the active link to the alternative one. The aim of this procedure is to avoid a hysteresis operating mode which can switch too quickly between the communication links.

Concerning the communication between the train and the ground, the Mobile HIP (Hardware independent address) function provides a virtual IP address to all devices allowing them to address themselves independently of the real IP network. In our case, the streaming client can contact the streaming server without any information of the real IP addresses of the devices, or the channel (Wi-Fi or 3G) used for the transmission.

The Netbox implementation of HIP is the openhip solution.

More information can be found here: *http://openhip.sourceforge.net*

In order to use the Netbox as close as possible to a real implementation, 3G and Wi-Fi networks were used.

3G Communication from the train to the ground is implemented through a standard public telecommunication operator (PROXIMUS 3G Belgian operator). Wi-fi is implemented through a classical access point using standard 802.11 b/g at 2.4GHz.

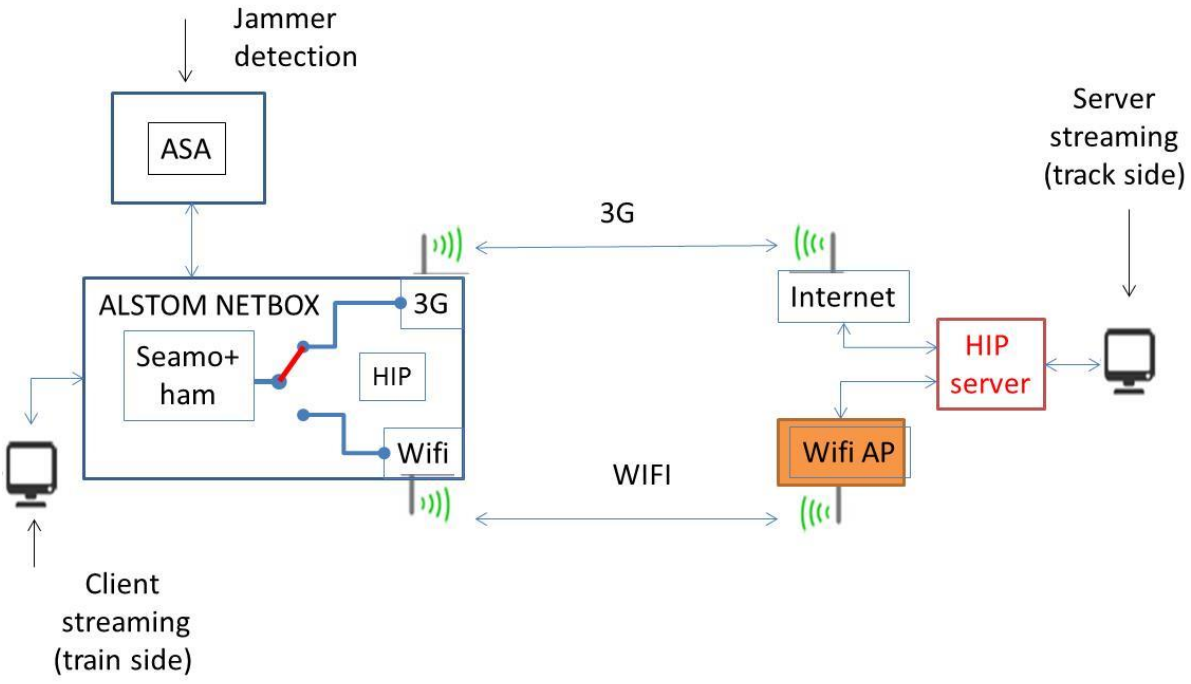


Figure 17: Diagram of the use-case 2.

4.2 Attack Description

See IFSTTAR attack scenarios (Deliverable D3.4)

4.3 Validation Approach

All packet traffic and process debug information have been logged and performance were analysed in-line and off-line. These parameters are process events, packet losses, latency,... as well as qualitative impressions of the received audio and video steams (freeze, pixelization, glitches,...).

The results are provided in Deliverable D3.4.

4.4 Evaluation

The results are coherent with the theoretical expectations - with one notable exception.

As implemented, a new connection is activated when jamming is detected and any unused channel is deactivated when it is not used. This implies that when a jamming condition is detected, the NETBOX activates a new link and the first process is to negotiate its access with the access point (Wi-Fi) or the Telecommunication operator (3G).

In Wi-Fi, this only takes a few seconds but for 3G, especially in “rush hours”, we have observed that several authentication trials must be performed before obtaining a connection. This may take up to XXX sec. time – which may be definitely too long in critical attack situations.

In both cases, and mainly in 3G, several improvements can be made in order to reduce the time gap between actually switching from one channel to the other:

1) Maintain the channel connection, even if it is not used for the communication:

This will be particularly efficient with 3G network since this is the channel where this problem is more important. The drawback is of course that the related communication will probably also increase. For Wi-Fi, this is less useful since the Wi-Fi zone is “local” and the authentication process more efficient.

2) Anticipate the connection:

The idea will be to initiate the authentication when a first jamming detection occurs. The 3G session initiation process can be launched before jamming confirmation (realized in order to avoid false positive event). If there is a confirmation of the jamming, the process and the vertical roaming will take place more rapidly. If it was false information, the process is stopped and the 3G channel is not used.

3) Cooperate with the telecom operator in order to prioritize the connectivity of the NETBOX device. This kind of prioritization, based on the SIM card user profile for example, should be realizable.

These three solutions could improve the switching process with a gain of a few tens of seconds during rush hours.

Another improvement could also attend the Mobile IP solution which is open-HIP in our test bed. As it was implemented, the authentication and encryption mechanism is completely renewed at each channel switching. An improvement could be to simplify this re-authentication between two systems that have already been connected through HIP.

We also detect that after stopping jamming of a 3G communication, latency stays rather important (sometimes a few seconds). This seems to come from the telecommunication operator process and could also be investigated.

5 Results and conclusions

5.1 Simulation Validation

Figure 18 shows typical results displayed by the simulation system developed in the project and described in deliverable D4.3. The SyMo/Ready modelling and simulation tool (developed by Fraunhofer IAIS was used) to allow for agent-based modelling. Each single aspect (attack detection, communication interfaces) was modelled. The overall system behaviour was described using an abstraction layer dealing with system states and communication. A concrete railways system model was also realised to allow the analysis of an attack in a given sector. Parameters of the simulation were attack position (inside a train, outside at different track sector), strength of attack, duration of attack.

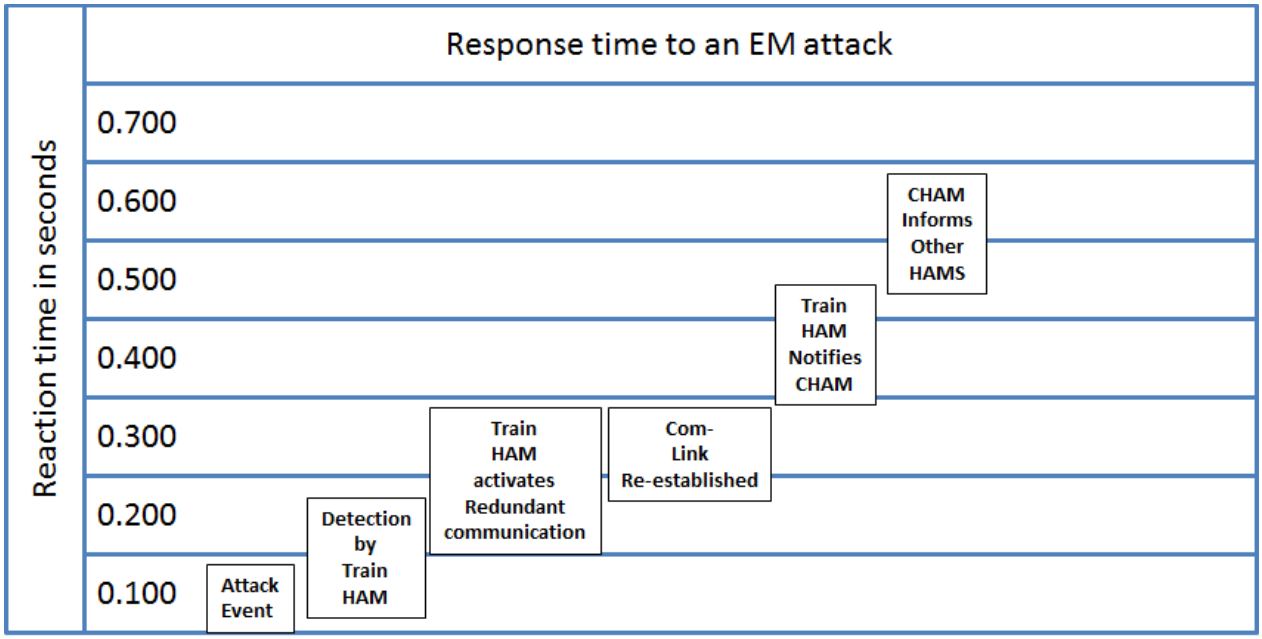


Figure 18: Response time with Simulator

The simulation that under different conditions and scenario, the railways communication is resilient against EM attacks.

5.2 Use Case 1 Validation

In the use-case 1 we applied different traffic policies in the MCM to overcome the attack. Depending on the traffic policy applied the response to the attack differs.

Figure 19 shows the results of an attack detection in use case 1 when the switching traffic policy is used. In this case, the communication is recovered thanks to the HAM interaction.

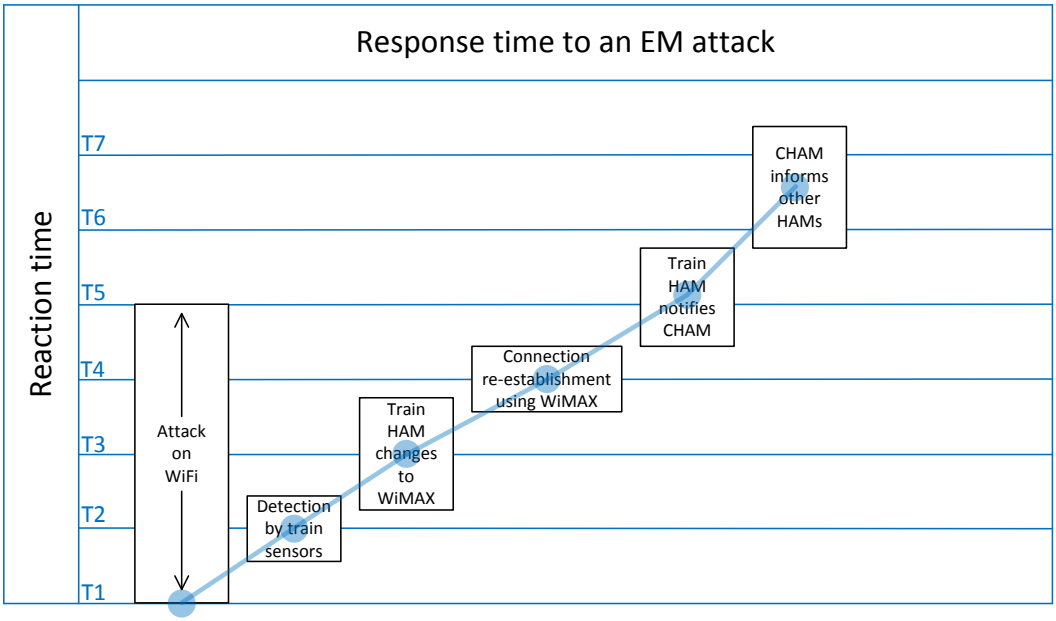


Figure 19: Response time to an EM attack with switching traffic policy.

Figure 20 show the response time to the attack when the active-backup traffic policy is applied. Thanks to this policy, already established TCP (or MPTCP) connections are moved to WiMAX almost instantly with a minimum delay related with the RTO of the TCP connection in the WiFi interface. However, to allow new TCP connections and the non-TCP traffic the HAM must set the WiMAX interface as the preferred interface.

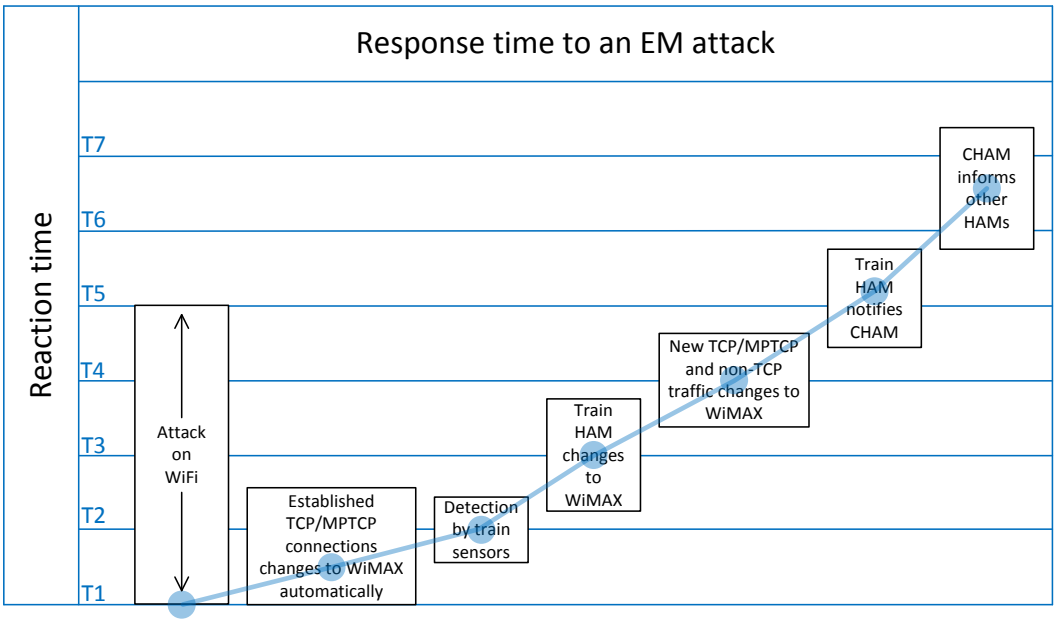


Figure 20: Response time to an EM attack with active-backup traffic policy.

Finally, Figure 21 shows the response time to face an EM attack when the replication traffic policy is applied. In this case, the TCP (or MPTCP) established connections are not affected by the jammer because the information is already being sent duplicate through

the WiMAX interface. However, for new TCP (or MPTCP) connections and non-TCP traffic the HAM must set the WiMAX interface as the preferred one.

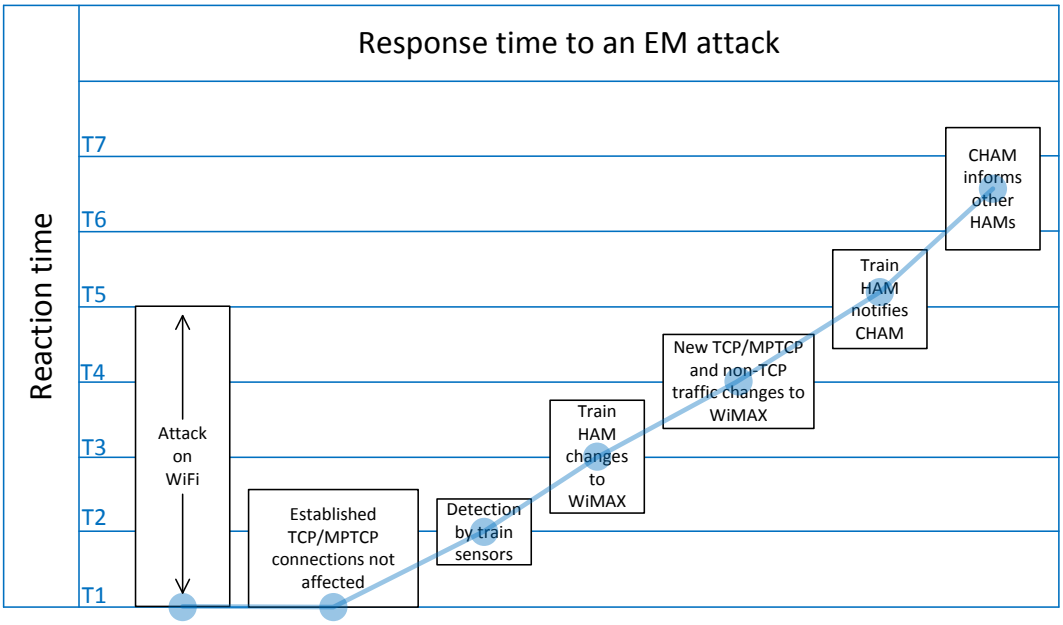


Figure 21: Response time to an EM attack with replication traffic policy.

In conclusion, the MCM with the help of the HAM provides multiple ways of facing and recovering from one EM attack and they can be selected depending on the requirements for a specific type of traffic. For example, for a critical traffic like ERTMS it could be advisable to use the replication traffic policy to guarantee a good communication less prone to interferences, whereas for a less critical application the switching traffic policy could be enough. Furthermore, the HAM could move from one traffic policy to another one and, for instance, initially apply a conservative traffic policy to preserve communication resources and when needed apply a more aggressive traffic policy such as the replication policy.

5.3 Use Case 2 Validation

Figure 22 shows the results of an attack detection in use case 2. This second use case as described earlier investigates an Alstom Netbox. The communication links are WIFI and 3G. We present here the scenario when the initial link is the 3G that switches to the WIFI when jamming is detected. The scenario provides a video streaming by a 3G link from the server to the client (from the track to the on-board).At a certain time the jammer is switched on. Figure 22 describes the different states of this procedure.

The setting is the following:

- Using detectors previously developed on WP 3 associated with a simplified local HAM
- For the Health Attack Manager, we use the SEAMO switching from one link to the other (see $4.1).

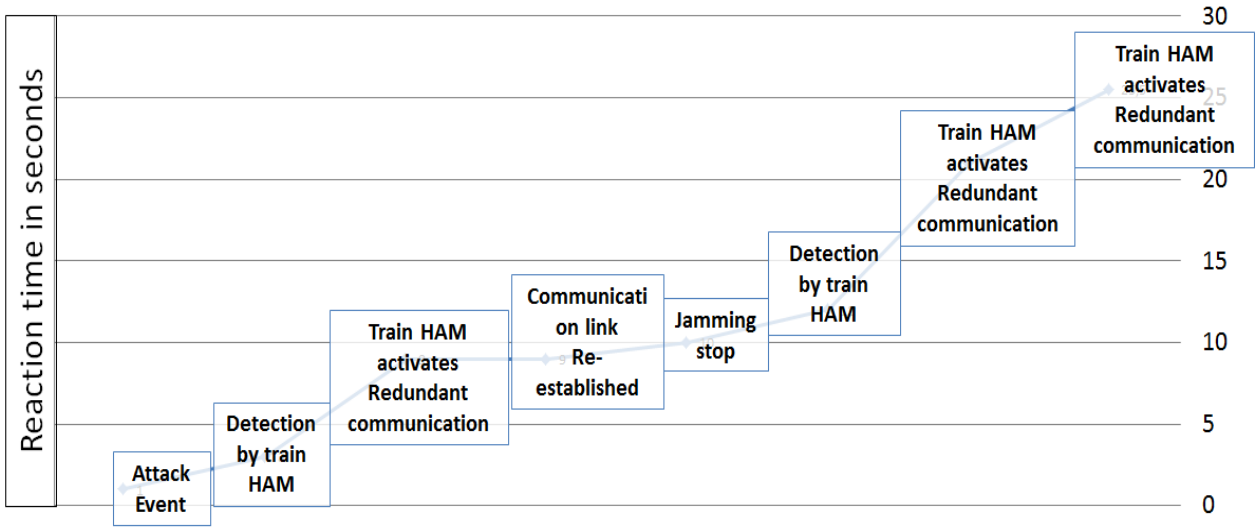


Figure 22: Response time with Use case 2

The system reaction procedure is described in details as follows:

Scenario 1: Switch on the radio jammer

- The jamming equipment is switched on when communication is on 3G. About 2 seconds later the detector sensors discover the presence of jamming;
- This information is delivered to the specific version of HAM implement in the Netbox. At this moment the decision is taken to switch from 3G to WIFI.
- A wait time is needed when the 3G link is interrupted and when the WiFi link is started, this waiting time corresponds to the association time requested to access the WiFi network.

Scenario 2: Switch off the radio jammer

- All the sensors indicate that there is no more jamming affecting the 3G band.
- The Netbox (HAM, SeaMo, HIP) decides to switch back from WiFi to 3G.
- During this switching operation we are losing the communication (no data transfer). This corresponds to the re-association time requested to access the 3G network that depends on the 3G operator (Proximus in our case).

The conclusion is that despite the loss of communication durations, the presented results prove the efficiency of real time sensors and the HAM based switching of communication channel.