eman ta zabal zazu

Universidad del País Vasco

Euskal Herriko Unibertsitatea

MP-CFM: MPTCP-BASED COMMUNICATION FUNCTIONAL MODULE FOR NEXT GENERATION ERTMS

PhD Thesis presented by

Igor Lopez Orbe

Directed by

Marina Aguado Castrillo

TICRM PhD. Program

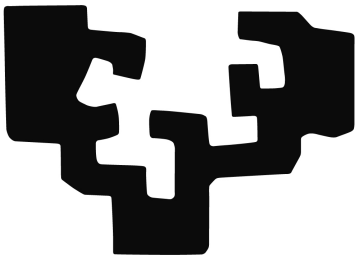
2017

MP-CFM: MPTCP-BASED COMMUNICATION FUNCTIONAL MODULE FOR NEXT GENERATION ERTMS

PHD THESIS PRESENTED BY IGOR LOPEZ ORBE

DIRECTED BY MARINA AGUADO CASTRILLO

eman ta zabal zazu



TICRM PhD. Program

2016-2017 Academic Year

Department of Communications Engineering

Faculty of Engineering of Bilbao

University of the Basque Country

March 2017

ABSTRACT

The European Rail Traffic Management System (ERTMS) was originally designed for the European railways. However, during the last two decades, it has become a de-facto standard for High Speed Railway (HSR) services in most of developing countries.

ERTMS is composed of three main components: 1) the European Train Control System (ETCS) signalling application, 2) Euroradio, which is divided in Safe Functional Module (SFM) and Communication Functional Module (CFM), and 3) the underlying Global System for Mobile Communications-Railway (GSM-R) radio technology used as carrier for data exchange between the train and the Radio Block Centre (RBC) located in ground. The ETCS signalling system supports three main operational Levels. The Level 3 introduces the possibility to operate with moving blocks instead of with fixed blocks. This means that the headway distance between two trains can be adapted reducing it to a minimal safety distance, therefore increasing the capacity of the corridor. This distance can be defined as the addition of the breaking distance and the system signalling delay. Thus, taking into account that the operative of a railway corridor is conditioned by the message transmission delay and reliability, the study of the underlying communication systems plays a key role in the ERTMS evolution. Moreover, a safe operation in ERTMS, from the communication point of view, can be described as a combination of transmission reliability, channel availability, transmission delay and message security.

Linked to this fact, the railway industry is working on the digitalisation and the transition to Internet Protocol (IP) technology of most signalling systems. Aligned with this trend, Union Industry of Signalling (UNISIG) has recently released a new communication model for ERTMS which includes an IP-based operation mode additionally to the Circuit Switching (CS)-based one.

This thesis is aligned with this migration context and it aims to provide a contribution for the definition of the Next Generation ERTMS, increasing the availability, reliability and security, as well as, taking into account the delay as

a basic constrain. There are three main challenges detected to be strengthened in the definition of the communication architecture of the Next Generation European Rail Traffic Management System (NGERTMS): 1) improvement in the survivability against end-to-end channel disruptions; 2) overcome the current limitation of ERTMS in its Packet Switching (PS) mode to operate with High Priority (HP) messages by providing them higher resiliency and lower delay comparing to the regular messages; and 3) the improvement of the security in ERTMS and the increase of the communication availability and reliability with no delay penalisation.

Considering the described concerns, in this thesis we propose a MultiPath TCP (MPTCP)-based communication architecture which overcomes them while keeps the backwards compatibility with the PS-based communication architecture proposed by UNISIG. To the best of our knowledge, this is the first time that a complete communication architecture for the NGERTMS, which overcomes the mentioned shortcomings, is presented. This architecture implements four different Class Services, which correspond to regular and HP messages for two foreseen scenarios; a scenario where the On Board Unit (OBU) and the RBC have multihoming support and a transitional scenario where RBC has multihoming support but the OBU has a single network interface.

With the simulations tests carried out in this thesis we validate the suitability of the proposed communication architecture for the railway domain. Moreover, this validation demonstrates that the proposed architecture has considerably higher robustness against channel disruptions comparing to the UNISIG proposal.

In conclusion, in this thesis we demonstrate that the MPTCP-based communication architecture accomplishes the main features envisaged for the NGERTMS; hence the contributions made in this thesis are a step forward in the process of evolving the European railway signalling system.

LABURPENA

Burdinbide Trafikoa Kudeatzeko Sistema Europarra (ERTMS, bere ingeleseko sigletatik), Europako burdinbideetarako soilik diseinatu zen bere hastapenetan. Hala ere, azkenengo bi hamarkadetan, sistema hau Abiadura Handiko Tren zerbitzuetako nazioarteko de-facto estandarra bihurtu da.

ERTMS sistema hiru azpisistema nagusitan banatuta dago: 1) Burdinbideen Kontrolerako Sistema Europarra (ETCS, bere ingeleseko sigletatik) seinaleztapen aplikazio moduan funtzionatzen duena; Euroradio sistema, aldi berean beste bi azpisistemetan banatuta dagoena, Segurtasunerako Modulu Funtzionala (SFM, bere ingeleseko sigletatik) eta Komunikaziorako Modulu Funtzionala (CFM, bere ingeleseko sigletatik), eta azkenik, GSM-R sistema, mezuak elkartrukatzen dituena Tren Barruko Sistemaren (OBU, bere ingeleseko sigletatik) eta Blokeo- eta Kontrol-Zentroaren (RBC, bere ingeleseko sigletatik) artean. ETCS seinaleztapen sistemak hiru maila ezberdinetan funtziona dezake, bakoitzak ahalbidetutako gaitasunak ezberdinak direlarik. Hirugarren mailan trenen posizioa kontrolatzeko bloke mugikorrak erabiltzea ahalbidetzen du, burdinbidearen bloke finkoak erabili beharrean. Hau horrela izanda, bi trenen arteko distantzia zerbitzuaren segurtasuna bermatzen duen minimo batera gutxitu daiteke, korridorearen kapazitatea handituz. Distantzia hau trenaren balaztatze distantzia eta seinaleztapenen komunikazioen atzerapena konbinatuz zehaztu daiteke. Beraz, esan daiteke erlazio zuzen bat dagoela burdinbidearen kapazitatearen eta komunikazioen atzerapenaren eta fidagarritasunaren artean. Hau dela eta, ERTMS sistemaren komunikazioen hobekuntzaren azterketa, sistema horren garapenean funtsezkoa da. Halaber, ERTMS sistemaren gaineko operazio seguru bat, komunikazioen ikuspuntutik, komunikazio hauen fidagarritasunagatik, komunikazio kanalen erabilgarritasunagatik, komunikazioen atzerapenagatik eta mezuen segurtasunagatik baldintzatuta dago.

Hau guztiarekin lotuta, tren industriak seinaleztapen sistemen digitalizazioan eta IP teknologiarako trantsizioan murgilduta dago. Izan ere,

UNISIG partzuergo industrialak orain dela gutxi komunikazio arkitektura berria argitaratu du ERTMS sistemarentzat, zeinak zirkuitu-kommutazioetan oinarrituta dauden komunikazioekin bakarrik ez, IP teknologian oinarritutako sistemekin ere lan egitea ahalbidetzen duen.

Tesi hau ERTMS sistemaren migrazioarekin lerrokatuta dago eta bere helburua hurrengo belaunaldiko ERTMS (NGERTMS moduan izendatu duguna) sistemaren definizioan laguntzeko asmoarekin, komunikazioen segurtasuna, fidagarritasuna eta erabilgarritasuna bermatuko duen komunikazio arkitektura berria proposatzea da, beti ere mezuen elkartrukearen atzerapena kontuan izanda. Testuinguru honetan, hiru erronka nagusi detektatu dira NGERTMS komunikazioen erresilientzia indartzeko: 1) konexio mozketen aurrean komunikazioen biziraupena hobetzea; 2) egungo IPren gaineko ERTMS arkitekturak, lehentasun handiko mezuekin lan egiteko dituen mugak gainditu, hauei erresilientzia maila altuagoa eta atzerapen baxuagoa bermatuz; eta 3) komunikazioen segurtasuna eta erabilgarritasuna handitu inolako atzerapen kalte-ordainik jasan barik.

Aipatutako erronkak kontutan izanda, tesi honetan MPTCP protokoloan oinarritutako komunikazio arkitektura berria proposatzen da ERTMS sistemarentzat, MP-CFM moduan izendatu dana. Arkitektura honek erronka horiek gainditzea lortzen du, baita IP teknologian oinarritutako ERTMS egungo arkitekturarekin bateragarritasuna bermatzea ere. Momentura arte, hau da lehen aldia erronka hauek gainditzeko kapaza den honelako arkitektura bat plazaratzen dela. Arkitektura honek lau zerbitzu klase mota inplementatzen ditu, bi zerbitzu mota lehentasun handiko mezuentzat eta beste bi lehentasun normaleko mezuentzat. Halaber, horietako bi OBUa eta RBCa interfaze aniztunak diren eszenatokietarako diseinatuak daude, eta beste biak RBCa interfaze aniztuna den, baina OBUa interfaze bakarrekoa den eszenatokietarako. Proposatutako komunikazio arkitektura hau, honetarako espresuki diseinatutako sare simulatzaile baten bitartez, balidatua izan da. Are gehiago, egindako simulazioek frogatzen dute, kanal interferentzien aurrean gure proposamenak, UNISIG plazaratutakoarekin alderatuta, sendotasun askoz handiagoa erakusten duela. Tesi honen emaitzak kontutan izanda, ondorioztatu daiteke MPTCP protokoloan oinarritutako arkitekturak NGERTMSrako guk hasieran finkatutako baldintza zorrotzak

betetzen dituela. Ondorioz, proposamen hau aurrerapauso garrantzitsua da burdinbide seinaleztapenaren garapenaren baitan.

RESUMEN

El Sistema Europeo de Gestión del Tráfico Ferroviario (ERTMS, por sus siglas en inglés), fue originalmente diseñado para los ferrocarriles europeos. Sin embargo, a lo largo de las dos últimas décadas, este sistema se ha convertido en el estándar de-facto para los servicios de Alta Velocidad en la mayoría de países desarrollados.

El sistema ERTMS se compone de tres subsistemas principales: 1) el Sistema de Control Ferroviario Europeo (ETCS, por sus siglas en inglés), que actúa como aplicación de señalización; 2) el sistema Euroradio, que a su vez está dividido en dos subsistemas, el Módulo de Seguridad Funcional (SFM, por sus siglas en inglés), y el Módulo de Comunicación Funcional (CFM, por sus siglas en inglés); y 3) el sistema de comunicaciones subyacente, GSM-R, que transporta la información intercambiada entre el sistema embarcado en el tren (OBU, por sus siglas en inglés) y el Centro de Bloqueo por Radio (RBC, por sus siglas en inglés). El sistema de señalización ETCS soporta tres niveles dependiendo del nivel de prestaciones soportadas. En el nivel 3 se introduce la posibilidad de trabajar con bloques móviles en lugar de bloques fijos definidos en la vía. Esto implica que la distancia de avance entre dos trenes consecutivos puede ser reducida a una distancia mínima en la que se garantice la seguridad del servicio, aumentando por tanto la capacidad del corredor ferroviario. Esta distancia de seguridad viene determinada por la combinación de la distancia de frenado del tren y el retraso de las comunicaciones de señalización. Por lo tanto, se puede afirmar que existe una relación directa entre los retrasos y la confiabilidad de las transmisiones de las aplicaciones de señalización y la capacidad operacional de un corredor ferroviario. Así pues, el estudio y mejora de los sistemas de comunicaciones utilizados en ERTMS juegan un papel clave en la evolución del sistema ERTMS. Asimismo, una operatividad segura en ERTMS, desde el punto de vista de las comunicaciones implicadas en la misma, viene determinada por la confiabilidad de las

comunicaciones, la disponibilidad de sus canales de comunicación, el retraso de las comunicaciones y la seguridad de sus mensajes.

Unido este hecho, la industria ferroviaria ha venido trabajando en la digitalización y la transición al protocolo IP de la mayor parte de los sistemas de señalización. Alineado con esta tendencia, el consorcio industrial UNISIG ha publicado recientemente un nuevo modelo de comunicaciones para ERTMS que incluye la posibilidad, no solo de operar con el sistema tradicional, basado en tecnología de conmutación de circuitos, sino también con un nuevo sistema basado en IP. Esta tesis está alineada con el contexto de migración actual y pretende contribuir a mejorar la disponibilidad, confiabilidad y seguridad de las comunicaciones, tomando como eje fundamental los tiempos de transmisión de los mensajes, con el horizonte puesto en la definición de una próxima generación de ERTMS, definida en esta tesis como NGERTMS. En este contexto, se han detectado tres retos principales para reforzar la resiliencia de la arquitectura de comunicaciones del NGERTMS: 1) mejorar la supervivencia de las comunicaciones ante disrupciones; 2) superar las limitaciones actuales de ERTMS para enviar mensajes de alta prioridad sobre tecnología de conmutación de paquetes, dotando a estos mensajes de un mayor grado de resiliencia y menor latencia respecto a los mensajes ordinarios; y 3) el aumento de la seguridad de las comunicaciones y el incremento de la disponibilidad sin que esto conlleve un incremento en la latencia.

Considerando los desafíos previamente descritos, en esta tesis se propone una arquitectura de comunicaciones basada en el protocolo MPTCP, llamada MP-CFM, que permite superar dichos desafíos, a la par que mantener la retrocompatibilidad con el sistema de comunicaciones basado en conmutación de paquetes recientemente propuesto por UNISIG. Hasta el momento, esta es la primera vez que se propone una arquitectura de comunicaciones completa capaz de abordar los desafíos mencionados anteriormente. Esta arquitectura implementa cuatro tipos de clase de servicio, los cuales son utilizados por los paquetes ordinarios y de alta prioridad para dos escenarios distintos; un escenario en el que ambos extremos, el sistema embarcado o OBU y el RBC, disponen de múltiples interfaces de red; y otro escenario transicional en el cual el RBC sí tiene múltiples interfaces de red pero el OBU solo dispone de una única interfaz. La arquitectura de comunicaciones propuesta para el entorno

ferroviario ha sido validada mediante un entorno de simulación desarrollado para tal efecto. Es más, dichas simulaciones demuestran que la arquitectura propuesta, ante disrupciones de canal, supera con creces en términos de robustez el sistema diseñado por UNISIG. Como conclusión, se puede afirmar que en esta tesis se demuestra que una arquitectura de comunicaciones basada de MPTCP cumple con los exigentes requisitos establecidos para el NGERTMS y por tanto dicha propuesta supone un avance en la evolución del sistema de señalización ferroviario europeo.

ACKNOWLEDGMENTS

A PhD work is similar to a mountain, before arriving to the peak, many partial steps have to be made and in each of these steps you receive the support of many colleagues, without whose help the peak could be hardly reached.

En este sentido mi más sentido agradecimiento a mi directora Marina Aguado quién en todo momento me ha dado el apoyo que necesitaba, motivándome en momentos de desánimo y presionándome positivamente para apuntar siempre un poco más alto. Este agradecimiento lo extiendo al resto de compañeros del grupo de investigación I2T y en especial a Elias y Alaitz, compañeros de batallas en este duro proceso que es el doctorado, quienes además de hacer de psicólogos improvisados, también he compartido y mejorado ideas y propuestas. Tengo que agradecer también a todos aquellos que incondicionalmente me han ayudado desde CAF proporcionándome información y consejo. I am greatly indebted to Marc Antoni, head of the Rail System Department at the UIC for providing me the opportunity to stay at the UIC as invited researcher whereby I learnt a lot about the impact of cyber security in safety services (Merci beaucoup Marc!).

Merci aussi à tous mes amis que j'ai rencontré à Orsay avec qui j'ai ouvert ma tête à nouvelles réalités et manières de penser, en especial a mi "pata" con quién he compartido tantas, tan largas y tan diversas conversaciones y reflexiones a lo largo de estos años, Kankunapac Julio!

Gustatuko litzakit ere eskerrak ematea Zabalduz programaren atzetik egon diran guztiei eta oro har, euskal unibertsitate publiko bat posible egiten daben guztiei, askotan ez baikara konturatzen zenbaterainoko pribilegioa dan gaur egungo munduan ikasteko eskubidea bermatzen dauan unibertsitate publiko bat izatea.

Eta azkenik, eskertuko nahiko neuke nire familiari, beti han egoteagaitik, inolako baldintzarik jarri gabe, beti aurpegi on batekin eta behar neban sostengu moral eta ekonomikoa emateagaitik, zuek gabe hau ez zan posible izango; Ama, Aita, eskerrik asko!

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ERA European Union Agency for Railways

ERTMS European Rail Traffic Management System

NGERTMS Next Generation European Rail Traffic Management System

ETCS European Train Control System

RAMS Reliability, Availability, Maintainability and Safety

EIRENE European Integrated Radio Enhanced Network

SIL Safety Integrity Level

PZB Punktförmige Zugbeeinflussung - Punctiform Train Influencing

AWS/TPWS Automatic Warning System/Train Protection & Warning System

EU European Union

ATP Automatic Train Protection

AWS Automatic Warning Systems

DMI Driver Machine Interface

UNISIG Union Industry of Signalling

CAF Construcciones y Auxiliar de Ferrocarriles

COTS Commercial Off-The-Shelf

HSR High Speed Railway

OBU On Board Unit

RBC Radio Block Centre

DA Destination Address

CFM Communication Functional Module

SFM Safe Functional Module

ALE Adaptation & redundancy management Layer Entity

PDP Packet Data Protocol

APN Access Point Name

HP High Priority

ITU-T Telecommunication Union-Telecommunication Standards Sector

RRE Resilience Requirements for ERTMS

MNOs Mobile Network Operators

GSM Global System for Mobile Communications

GSM-R Global System for Mobile Communications-Railway

LTE Long Term Evolution

GPRS General Packet Radio Service

TETRA Terrestrial Trunked Radio

UMTS Universal Mobile Telephone Service

WiMAX Worldwide Interoperability for Microwave Access

FDD Frequency Division Duplex

TDMA Time Division Multiple Access

GNSS Global Navigation Satellite System

PS Packet Switching

CS Circuit Switching

OSI Open System Interconnection

IP Internet Protocol

TCP Transmission Control Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

IETF Internet Engineering Task Force

RFC Request For Comments

ISP Internet Service Providers

IT Information Technology

DNS Domain Name System

NAT Network Address Translation

WLAN Wireless Local Area Network

AP Access Point

CBTC Communication-Based Train Control

CTMC Continuous Time Markov Chain

RaSTA Rail Safe Transport Application

PRP Parallel Redundancy Protocol

RSTP Rapid Spanning Tree Protocol

DDC Deadline Dependent Coding

MN Mobile Node

CN Corresponding Node

SDN Software-Defined Networking

LIS Locator Identifier Split

MIPv6 Mobile IPv6

MIPv4 Mobile IPv4

PMIPv6 Proxy Mobile IPv6

PMIPv6-MAT Proxy Mobile IPv6 - MAG Address Translation

LMA Local Mobility Anchor

MAG Mobile Access Gateway

FMIPv6 Fast Mobile IPv6 Handover

FBACK Fast Binding Acknowledgement

NAR New Access Router

IPsec Internet Protocol Security

ICMP Internet Control Message Protocol

MCoA Multiple Care-of Address Registration

ILNP Identifier/Locator Network Protocol

IPv6 Internet Protocol version 6

IPv4 Internet Protocol version 4

GLI-Split Global Locator, Local Locator, and Identifier Split

MILSA Mobility and Multihoming supporting Identifier Locator Split Architecture

NEMO Network Mobility

HA Home Agent

CoA Care-of Address

ICMP Internet Control Message Protocol

HIP Host Identity Protocol

RSV RendezVous Server

HIT Host Identity Tag

RANGI Routing Architecture for the Next Generation Internet

HRA Hierarchical Routing Architecture

NIIA Node Identity Internetworking Architecture

Shim6 Site Multihoming by IPv6 Intermediation

REAP Reachability Protocol

ULID Upper-Layer Identifiers

HIT Host Identity Tag

mHIP Multipath Host Identity Protocol

NID Node Identifier

mHIP Multipath Host Identity Protocol

MPTCP MultiPath TCP

SRTT Smoothed Round-Trip Time

RTT Round-Trip Time

SCTP Stream Control Transmission Protocol

CMT Concurrent Multipath Transfer

UDP User Datagram Protocol

MPUDP Multipath UDP

ECCP End-to-end Connection Control Protocol

PERM Practical End-host Multihoming

SACK Selective Acknowledgement

API Application Programming Interface

NC Network Coding

SIP Session Initiation Protocol

SHIP Hybrid SIP and HIP

MIH Media Independent Handover

SIP-NMS SIP Network Mobility Server

IMS IP Multimedia Subsystem

URI Uniform Resource Identifier

MPRTP Multipath Real-time Transport Protocol

MPRTP-AR Multipath Real-Time Transport Protocol Based on Application-Level Relay

RTP Real-time Transport Protocol

RTCP Real-time Control Protocol

MPTS-AR Multipath Transport System based on Application-level Relay

MPTC Multipath Transport Control

SSSN Subflow-Specific Sequence Number

ISP Internet Service Provider

BTS Base Transceiver Station

DSS Data Sequence Signal

PLR Packet Loss Rate

RTO Retransmission Timeout

ABEL Average Burst Error Length

PMR Path Maximum Retransmission

FR Fast Retransmission

ACK Acknowledgement message

MSS Maximum Segment Size

TCP-SF TCP Smart Framing

ER Early Retransmission

NC Network Coding

LT Limited Transmit

F-RTO Forward RTO

DSACK Duplicate Selective Acknowledgement

DACK Delayed Acknowledgement

MTU Maximum Transmission Unit

EWMA Exponential Weighted Moving Average

SITL System-in-the-Loop

TLP Tail Loss Probe

FACK Forward Acknowledgement

OS Operating System

MPLS Multi-Protocol Label Switching

LSR Label Switched Router

LSP Label Switched Path

RSVP Resource Reservation Protocol

LDP Label Distribution Protocol

PCE Path Computation Element

TE Traffic Engineering

QoS Quality of Service

CBC-MAC Cipher Block Chaining-Message Authentication Code

MAC Message Authentication Code

DES Data Encryption Standard

3DES Triple Data Encryption Standard

KMS Key Management System

KMC Key Management Center

DoS Denial of Service

SNR Signal to Noise Ratio

DDoS Distributed Denial of Service

DSRC Dedicated Short Range Communications

TIPHON Telecommunications and Internet Protocol Harmonization Over Networks

ETSI European Telecommunications Standards Institute

TLS Transport Layer Security

PKI Public Key Infrastructure

PSK Pre-Shared Key

ARP Address Resolution Protocol

MITM Man-in-the-middle

ECC Elliptic Curve Cryptography

CA Certification Authority

PTC Positive Train Control

SDH Synchronous Digital Hierarchy

TE Traffic Engineering

OSPF Open Shortest Path First

IGP Interior Gateway Protocols

RRL Resilient Routing Layer

PCE Path Computation Element

SDN Software Define Networking

LER Label Edge Router

LSR Label Switch Router

LSP Label Switched Paths

LDP Label Distribution Protocol

RSVP Resource Reservation Protocol

RTO retransmission timeout

RTT Round-Trip delay Time

RFI Rete Ferroviaria Italiana

PCC Path Computation Client

EPC Evolved Packet Core

RAN Radio Access Network

eNB evolved NodeB

MGEN Multi-Generator

EMI ElectroMagnetic Interference

KPI Key Performance Indicator

MP-CFM MultiPath-Communication Functional Module

SERA Single European Railway Area

Part I

INTRODUCTION AND MOTIVATION

laburpena

Dokumentuaren atal honetan burdinbideen seinaleztapen sistemen garapen historikoaren azterketa egiten da, telegrafoan oinarritutako sistemetatik hasita, gidapen automatikoa ahalbidetzen duten egungo sistema modernoak arte. Gaur egun sistema hauek digitalitalizazio eta IP protokoloranzko migrazio prozesu baten murgilduta daude. Migrazio honek bere eragina du ere ERTMS sistema europarrean, abiadura handiko tren zerbitzuetarako de factoko estandar bihurtu dana. ERTMS hiru bloketan banatuta dago: Segurtasunerako Modulu Funtzionala edo SFM, Komunikaziorako Modulu Funtzionala edo CFM eta ETCS seinaleztapen aplikazioa. Atal honetan egiten den azterketak egungo ERTMSren mugak detektatzea ahalbidetzen digu. Muga horiek, tesi dokumentu honetan aurkezten diren azterketa eta proposamenak egitea bultzatu dute.

resumen

En esta parte del documento se hace un análisis histórico de la evolución de los sistemas de señalización ferroviario, comenzando por los sistemas basados en telégrafos y acabando en los actuales modernos sistemas que permiten la conducción automática. Estos sistemas están actualmente en pleno proceso de digitalización y migración hacia sistemas de comunicaciones basados en IP. Esta migración afecta también al sistema europeo ERTMS que se ha convertido de-facto en el estándar de señalización para servicios de alta velocidad en la mayoría de países del mundo. ERTMS se compone de tres bloques principales: el Modulo Funcional de Seguridad o SFM, el Módulo Funcional de Comunicaciones o CFM y la aplicación de señalización ETCS. El análisis que se realiza en esta parte nos permite detectar los principales límites del actual sistema ERTMS. Dichos límites sirven como motivación para abordar los análisis y propuestas posteriores de este documento de tesis.

1 INTRODUCTION AND CONTEXT

> The major advances in speed of communication and ability to interact took place more than a century ago. The shift from sailing ships to telegraph was far more radical than that from telephone to email!
>
> Noam Chomsky

1.1 INTRODUCTION

Railway systems are key elements of mass transit systems in most of developed countries. Since railway development started in the beginning of the nineteenth century, its deployment has continuously grown until become the backbone of the transportation system in many countries.

These systems have two main features that differ from other transport means; 1) the deterministic path that the vehicle can follow in its travel; 2) the slow braking response of the vehicle due to the mechanical characteristics of steel rails and wheels used as guidance. This feature implies long brake distances that exceed the visibility of the train driver [3].

The knowledge of accurate position of the train in the railway and the reliable communication of braking and moving commands to it are a need for guaranteeing a safety operation. This need of preserving the security of travellers and payload have always justified the use of the state of the art communication technologies in the railway systems, starting with the telegraph

in the nineteenth century and following with current cellular and satellite technologies.

In this chapter we look over the evolution of railway signalling systems emphasising how the communication technology has been adopted for railway signalling purposes. We also present the current challenges for the digitalisation and migration towards IP of the railway signalling and the advantages this migration could provide. Finally, we present how the rest of this thesis document is structured.

1.2 SAFETY REQUIREMENTS OF RAILWAY SYSTEMS

Railway processes involved with the movement of trains, including signalling, are considered safety-related due to the large amount of human lives involved in these operations. Basically, the train must be able to move along the track without risks. To achieve this goal, it is very important to know the accurate position of the train and all track sections in front of the train have to be clear and kept clear until the train has completely passed through them.

This condition is commonly achieve by splitting the railway in fixed or moving blocks in which only one train can be at the same time. The distance of these blocks can be reduced in order to increase the capacity of the railway corridor, as long as the following condition is fulfilled: *the train must be able to perform an emergency break at any moment without risk to crash with the next train in the corridor*. The minimum distance that allows two consecutive trains to operate safely at a desired speed is known as "headway distance".

The norms EN 50126 [4] and IEC 62278 [5] introduce the Reliability, Availability, Maintainability and Safety (RAMS) term for railway. Frequently, this term is extended to RAMS(S) by adding also the security needs of the system.

This norm, defines the availability as: *the ability of a product to be in a state to perform a required function under given conditions at a given instant of time or interval*. The availability is closely related to the reliability, which is defined in the norm IEC 61508 [6] as the probability that an item performs its required function during a time interval. As it can be deduced, the reliability of railway

components, including the ones related to signalling systems, plays a key role for ensuring the availability of the railway operations.

The maintainability is defined in the norm EN 50126 as follow: *the probability that a given active maintenance action, for an item under given conditions of use, can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources*. Thus, the maintenance relies more on the operation policy of the railway operator, which has to define a correct maintenance procedure to repair or replace items when they go out from their available state, that is, when they fail.

An important term in industrial processes and especially in railways is the safety. This term refers to protection of the system against hazardous consequences caused by technical failures and unintentional human mistakes. Many times the security is also introduced for referring the protection against hazardous consequences caused by negligent human actions.

An important requirement in railways is the high availability due to its strong link with safety; the more available the system is, the lower will be the time operating in degraded mode. Equally, a reliable and in-time operation is essential for keeping the railway operation in a safety state. In Figure 1.1 a three-state Markov chain model is illustrated. The default state should be the *Normal* state which represents a full operative safety system. From this state the system can pass to *Degraded Mode* state or to *Unsafe* state. The transition to the first one typically happens due to a hazardous failure of the system. In this state the system keeps working with capacity and service limitations and usually many operations are made manually. Therefore, the *Degraded Mode* state should be avoided as it increase the probability to make dangerous errors that can have critical consequences in terms of economy and human lives, deriving in an *Unsafe* state. To this *Unsafe* state can also be passed directly from *Normal* state but it is unlikely to happen, due to hazards, if the system is designed with safety in mind. However, a security breach could allow an attacker to make it happen. That is why the security and cyber security have such a big importance in railway systems.

Due to the human lives involved, train control systems must fulfil specific requirements regarding to RAMS. These requirements are specified in the

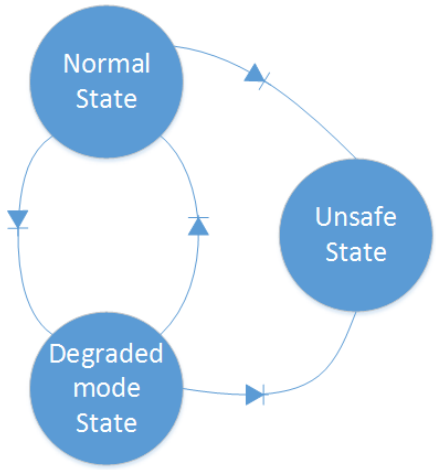


Figure 1.1.: Safety system state machine

railway RAMS standards EN50126 and IEC62278, and they apply to ERTMS [7] to achieve a fault tolerant system with Safety Integrity Level (SIL)-4.

1.3 RAILWAY SIGNALLING SYSTEMS: PRESENT, PAST AND FUTURE

1.3.1 From Telegraph to Control Command Systems

At the very beginning of railways everything was made manually and with no direct communication between stations and trains involved in the procedure. There was no system to track the train location. The relative location of each train was deduced based on the temporal delay in-between two consecutive services. This situation made difficult to increase service frequency in the same corridor in a safe way for passengers and freight.

Little time after the apparition of the electrical telegraph in the market, the first railway-dedicated service was set up in 1839 in the Great Western Railway in England. It permitted nearly instantaneous communication between stations

which were used to dispatch messages to signalmen for setting switches and signals by hand in the track.

Some decades later, the use of the telegraph, together with the appearance of interlocking and electric track circuits, made the automatic track signalling possible. This signalling was able to detect the presence of a train in a track section and automatically display a stop signal in the beginning of the section to be adopted by the incoming train.

As a natural evolution the Automatic Safety Systems, so-called Control Command Systems, emerged allowing to pass information from track to train. These systems are present nowadays in most of railway systems around the world. The communications of these systems can be performed via balises sited along the track, via cable loops or via radio transmissions [8].

These Safety Systems can be classified in two main groups depending on their functions:

Automatic Warning Systems (AWS) - Provides warning if the train exits from protected or *safe* state, e.g. due to the excess of speed or due to the access in a track section without the needed movement authority.

Automatic Train Protection (ATP) - The system calculates continuously the maximum speed of each train for a safe operation and breaks the train automatically if it exits from *safe* state.

Throughout the twentieth century more than fifteen different signalling systems were deployed only in Europe, being the most extended ones the German Punktförmige Zugbeeinflussung - Punctiform Train Influencing (PZB), the Belgian Crocodile and the British Automatic Warning System/Train Protection & Warning System (AWS/TPWS).

Considering these systems were not interoperable between each others, trains operating cross-border services must had multiple signalling equipment installed on board. For pan-European services that involved multiple countries this supposed a significant increase of price and a considerably increase of operational limitations.

1.3.2 Towards a pan-European Railway Signalling System

In order to overcome the incompatibility problem mentioned before, at the end of 90s, the initiative to create a common rail signalling system, the ERTMS, emerged. The ERTMS was backed by the European Union (EU) and envisaged to enhance the cross-border interoperability in Europe. This system is composed of three complementary technical modules: ETCS and GSM-R.

ETCS - This module is the responsible of signalling and traffic control functions. It includes an ATP and a Driver Machine Interface (DMI) that passes to the train driver all line-side information electronically, removing the need of line-side signals that are not visible at high speed operations.

Euroradio - This module is divided in two functional modules, the SFM and the CFM. The SFM is responsible of addressing safety requirements, whereas the CFM provides a complete communication architecture which allows to connect the OBU and the RBC.

GSM-R - This communication module has two main features. On the one hand, it provides a carrier for transmitting ETCS messages between train and track. On the other hand, it provides a unified voice communication service that includes railway specific functionalities such as group calls, dynamic addressing and high-priority emergency calls.

The ERTMS specification is made and upgraded by the UNISIG group which is an industrial consortium composed by the most important companies of the sector, such as Alstom, Ansaldo, Siemens, Thales and Construcciones y Auxiliar de Ferrocarriles (CAF). These specifications are controlled also by the European Union Agency for Railways (ERA) which was created by the EU in 2004.

ERTMS was initially designed for the interconnection of European railway networks. However, during the last years this system has been adopted by many countries outside Europe [9] and it is becoming a global *de facto* standard for high speed railways, being the 46% of deployment contracts from out of Europe [10].

1.3.3 Migration towards IP: Challenges and New perspectives

The adoption of ERTMS in railway corridors has been quite recent. However, the migration of the communication module, GSM-R, towards a more modern technology has been a hot topic during the last years. This idea has been motivated by two main factors; the incoming capacity bottleneck because of the limited data and voice concurrent connection that GSM-R can have in each cell, and the fact that, from 2030 onwards, the Global System for Mobile Communications (GSM) technology will disappear from the commercial telecommunication market. As a first step for updating the communication module, different tests have been carried out over GPRS [11]. The same as GPRS, all potential candidates to substitute GSM-R as communication technology, are based on Transmission Control Protocol/Internet Protocol (TCP/IP) technology. This migration implies the adoption of PS technology where there are not dedicated channels for each user. This fact has the advantage of increasing the capacity with the same spectrum by sharing a common channel among all users, but also potential disadvantages that must be solved, such as the out-of-order packet delivery. Additionally, the adoption of IP-based technology implies the upgrading of the current ERTMS communication protocol stack, as well as its Safety Layer, Euroradio, which is designed to work with CS technology.

In order to promote a planned migration in Europe, the ERA intends nowadays to establish a roadmap to define a new communication solution by 2018 and to start the transition from approximately 2022 [12]. Based on the current trend of the market, the most likely candidate for substituting GSM-R is Long Term Evolution (LTE), a fourth generation technology that is currently being adopted by most of Mobile Network Operators (MNOs) in Europe. However, considering the different evolution pace of the railway and telecommunication markets, for the moment of starting the deployment of LTE in railways, the telecommunication market will be already in the fifth generation technologies, 5G. Therefore, the flexibility to face market changes and technology variation across Europe, a multi-technology policy approach has been presented as the most attractive option [12]. According to [12] this strategy offers the following advantages:

- It allows new/emerging technologies to be introduced over time.

- It offers a future-proof approach for the longer term.
- It allows the use of commercial network bearers with associated potential for cost reduction where appropriate.
- It allows for shared networks in countries where this is viable.
- It allows for private networks in existing spectrum to be retained in areas where this is considered to be the most appropriate option.

In the same way as the migration towards IP-based technologies, the adoption of a new multi-technology paradigm needs for a deep research in order to allow the coexistence and complementary use of multiple technologies by a train, in the same corridor and at the same time.

1.4 STRUCTURE OF THE DOCUMENT

The structure of the rest of this document is divided in the following five parts:

PART 1: INTRODUCTION AND MOTIVATION – Chapter 2 complements the first part of the document. It makes a description in depth of current ERTMS, as well as a critical analysis according to the current perspective and to the upcoming migration towards IP technology. This chapter highlights the shortcomings to be overcome by NGERTMS, which justifies the motivation of the research work of this thesis.

PART 2: STATE OF THE ART – This part is composed of a single chapter, Chapter 3. In this chapter, we analyse the resilience of network communications, understood as the ability to recover from network disruptions, as it encompasses both challenges described above. This analysis of the state of the art is divided in different Open System Interconnection (OSI) layers and for each technology a detailed description is provided followed by a critical analysis of the previously mentioned requirements. Furthermore, using a semi-quantitative analysis of previous requirements, we conclude this chapter identifying the most suitable proposal to be included in the NGERTMS and we highlight the

open points that should be addressed before its inclusion in the NGERTMS's protocol stack.

PART 3: PROPOSAL FOR NEXT GENERATION ERTMS – This part of the document proposes in Chapter 4 a new MPTCP-based communication architecture for the NGERTMS, which improves the survivability against channel disruptions. Moreover, this proposal presents an integral solution which incorporates a differentiated treatment of regular and HP messages in the PS mode. Additionally, in Chapter 5 we evaluate the new security vulnerabilities that could appear with the adoption of MPTCP-based communication architecture and we propose techniques within the state of the art to overcome them. This part of the thesis ends with Chapter 6 that presents a proof-of-concept experiment, which evidences the potentiality of integrating Multi-Protocol Label Switching (MPLS) with MPLS to provide and-to-end path diversity.

PART 4: VALIDATION OF THE PROPOSAL – In this part of the document the validation of the presented proposal is provided. First, in Chapter 7 we explain in detail the simulation framework used for validation purposes. After, in Chapter 8 we present the parametrisation of the proposed new communication architecture for the NGERTMS. Finally, the robustness of the proposal against channel disruptions is presented in Chapter 9. This robustness is validated using as a baseline the current communication architecture proposed by UNISIG.

PART 5: CONCLUSIONS AND DISSEMINATION RESULTS – Last but not least, in this part, Chapter 10 outlines the conclusions resulted from the realisation of this thesis and highlights the future works that may derive from the research work gathered in this document.

2 REVISION OF ERTMS AND THESIS MOTIVATION

> To know what you know
> and what you do not know,
> that is true knowledge.
>
> Confucius

2.1 INTRODUCTION

ERTMS is the current standard ATP system in Europe. Since this system was defined, its deployment has grown constantly, especially in new High Speed lines.

This system was originally attached by design to GSM-R technology. Thus, current ERTMS deployments work over this mobile technology. However, due to the different evolution pace of telecommunication and railway technologies, and despite ERTMS is still considered a modern system, its communication module has already shown its limitations.

Nowadays, the railway industry is working on the digitalisation and the transition to IP technology of most of signalling systems. Aligned with this trend, UNISIG has recently released a new communication model for ERTMS which includes an IP-based operation mode additionally to the CS-based one.

In order to get an accurate view of the weak and strong points of the current ERTMS, in this chapter we make a description in depth as well as a critical analysis according to the current perspective and to the upcoming migration towards IP technology.

We start this analysis by introducing the three main blocks of ERTMS: the GSM-R, the Euroradio (CFM and SFM) and the ETCS application. After, we

define the requirements and constrains associated to the railway domain. This requirements will help to detect the shortcomings of ERTMS and will define a minimum goal to be achieved by the new communication architecture proposed in this thesis work. Afterwards, the ERTMS shortcomings are evaluated for its mobile technology, for its communication module and for its safety module. This chapter ends with a conclusion about the shortcomings that should be overcome which justifies the motivation of the research work of this thesis.

2.2 ARCHITECTURE OF TRAIN MANAGEMENT SYSTEMS

ERTMS is an advanced ATP system composed of three main components, as mentioned in the introduction; ETCS, Euroradio and GSM-R. The ETCS signalling messages are delivered using a data circuit which is dedicated to each train using circuit-switched technology. That way, only the two extremes of the circuit, the RBC and the train, can have access to these messages. In order to ensure the reliability and security of these communications, the Euroradio protocol is provided.

Figure 2.2 illustrates the protocol stack of ERTMS. This architecture is divided in three main functional blocks. In the top the ETCS application that exchange messages between the RBC and the OBU in the train side. This application communicates with the Euroradio SFM which has to protect the integrity and the authentication of exchanges messages. Bellow this safety module, the Euroradio CFM provides end-to-end reliable communications using underlying mobile communication channel, in this case, an end-to-end circuit established through GSM-R network.

In the following sections we will explain the current ERTMS architecture following a bottom-up approach which will start from the Euroradio's CFM and will finish with the ETCS application.

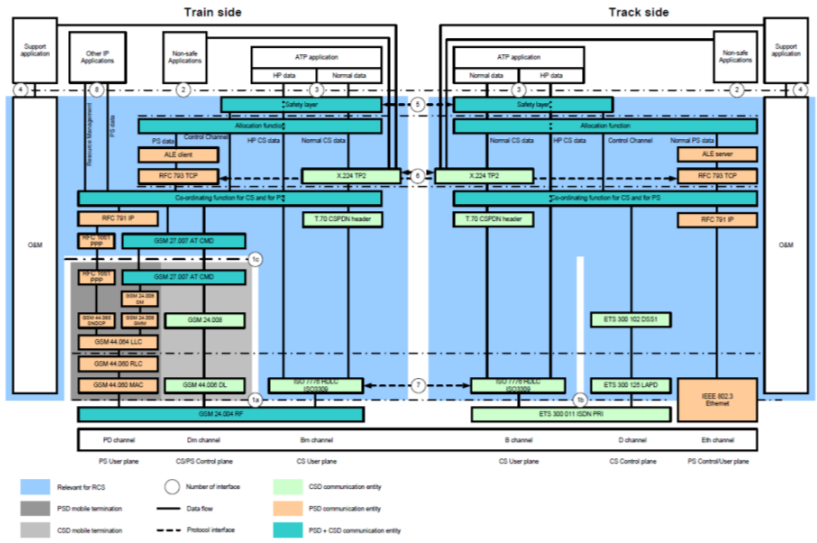


Figure 2.2.: Architecture of ERTMS communication model (Source: Unisig Subset-037 v3.2.0

2.2.1 ERTMS: Communication Functional Module of Euroradio

In this section the protocol stack of the CFM is explained. However there is not only one protocol stack in ERTMS. From the point of view of ERTMS entities involved in the communication, on the one hand, we have the protocol stack used in the RBC-RBC relations, which is based on TCP/IP. On the other hand, we have the protocols stacks used in the OBU-RBC relations, which are two different protocol stacks, one based on CS technology and the other in PS technology. OBU-RBC communication scheme was originally designed only to work over CS technology, using OSI protocols. However, recently a new protocol stack based on TCP/IP has been released, which will be the one used in future deployments and therefore, the reference model taken for this research work.

In the next lines, we will explain in depth the two protocol stacks, which are based on TCP/IP and used for RBC-RBC and OBU-RBC communications.

Communication Functional Module for RBC-RBC Communications

Although the communication between two neighbour RBC, defined in the subset-0.98, is out of scope of this research work, the considerations made in this specification have been used as a basis to define the OBU-RBC communications over TCP/IP. Therefore, it is worth describing the CFM used for these communications.

The CFM for these communications provides the following functions over a non-trusted transmission channel.

- Adaptation between Euroradio Safety Layer and the transport protocol, TCP
- Redundancy to fulfil the availability requirements
- Reliable, transparent and bidirectional transfer of data
- Retransmission of segments, if necessary
- Monitoring of channel availability

The design of the CFM has been made under some assumptions in contrast with the CFM used currently for train-to-ground communications. Within these assumptions it is worth noting the lack of high priority data and explicit flow control. Additionally, the user data is never longer than 1000 bytes.

In this specification, the Euroradio layer keeps the primitives based on Telecommunication Union-Telecommunication Standards Sector (ITU-T) X.224 for communicating with the transport layer. These primitives are not compatible with TCP. Therefore, an ALE that translates these primitives is needed. Additionally to this translation, an address mapping is also needed in order to associate properly the ETCS ID of each RBC with each corresponding IP address. Last but not least, the TCP protocol does not provide redundancy capability. Moreover, a TCP connection can only work with a single interface as its addressing is designed to work with a 4-tuple composed of IP_{source}, $IP_{destination}$, $Port_{source}$ and $Port_{destination}$. Thus, the ALE has to be also able to manage this redundancy, creating multiple TCP connections and managing them transparently for the application layer. These functions, as well as the integration of the ALE in the protocol stack, are illustrated in Figure 2.3.

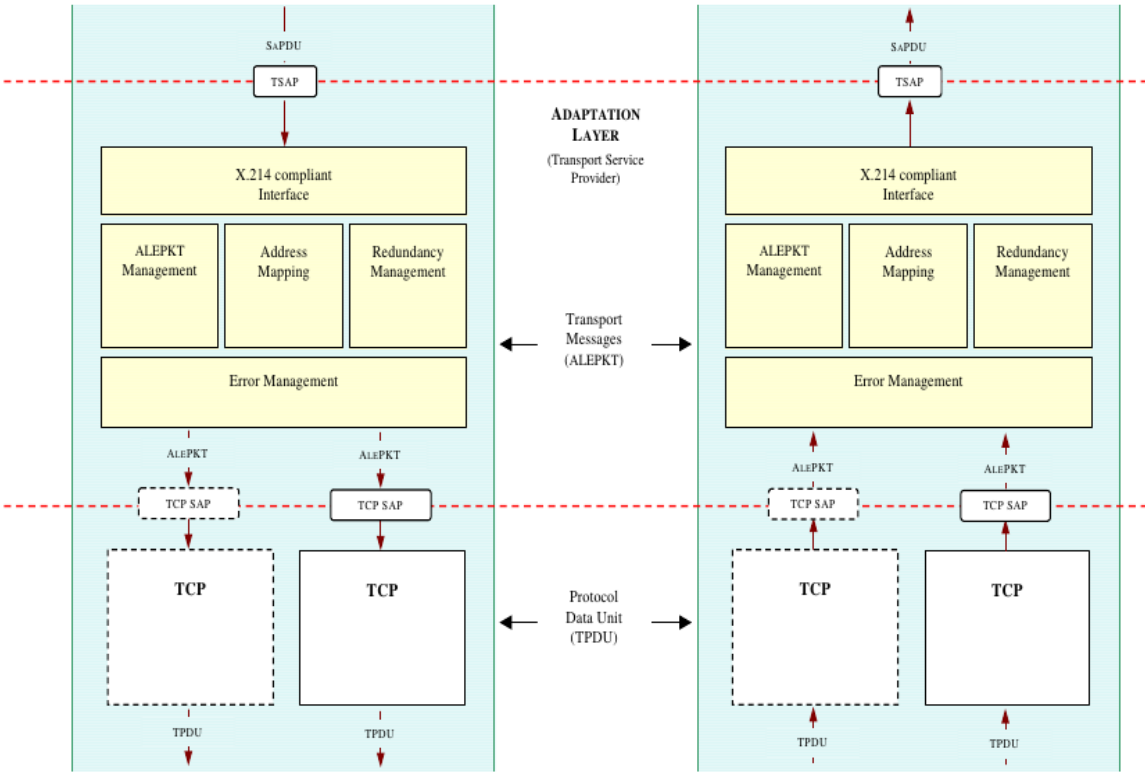


Figure 2.3.: Functions provided by the ALE

The ALE defines two classes of service: **Class A** and **Class D**. Both classes of service differ from each other in the delivery policy performed by the redundancy manager. In both redundancy schemes, two or more physical links can be used, but for our description, the case of only two links is taken into account.

In **Class A**, both links can be used to transfer data, but data packets are transmitted in only one of them each time. In this class, different connections are labelled as "normal" or "redundant". In normal conditions, data is delivered though the "normal" link, whereas the "redundant" one is only used when the "normal" one fails.

In **Class D**, both links are used at the same time for data delivery. Thus, the same transport sequence number is transmitted on both TCP connections. At the receiver side, the ALE layer should detect the same packet reception in both TCP connections and consequently discard the one that arrives later.

Communication Functional Module for OBU-RBC Communications

This section defines the communication protocol stack used in ERTMS over PS technology, which is described in the Subset-037 v3.2.0, but at the time of writing these lines, was not implemented in any railway corridor. It is worth noting that ERTMS was originally designed to work over CS technology. This means that the primitives used by ETCS to interact with the CFM were also designed in that context. Therefore, an abstraction layer to adapt these primitives to the primitives used in TCP/IP is needed.

This primitive translation is made within the ALE. This entity is based on the one presented in the Subset-098 for RBC-RBC. The main functions of the ALE are:

- The adaptation the Euroradio Safety Layer and the TCP layer.
- The establishment and Release of the TCP connection.
- Encapsulation and decapsulation of packets between Safety Layer and TCP stream.
- Monitoring of channel availability.

Comparing to the ALE used between RBC communications, described in Section 2.2.1, the one proposed for OBU-RBC communications lacks in redundancy support. The Subset-037 assumes that the RBC will have multiple network interfaces, that is, the RBC will be multihoming node. However, the OBU will have a single network interface, so the subset assumes that the redundancy cannot be performed as a unique RBC's IP address will be able to be used at the same time by the TCP session. Hence, for these train-to-ground communications, the Class D described in Section 2.2.1 will be used but without redundancy, that is, a regular TCP connection.

Another difference between the PS mode compared to the CS mode is that the first one is not able to handle HP messages, such as the one for commanding

emergency brake to the train. This limitation comes from the fact that these messages in the CS mode are by-passed from the application to the link layer without using any of protocols from safety layer to network layer. However, in PS this bypass cannot be made as the end-to-end connection is not performed as an end-to-end circuit at the link layer. On the contrary, *in PS mode the end-to-end connection is established using two-level addresses, source and destination IP addresses at the network layer, and source and destination TCP ports at transport layer.*

As commented previously, in the PS mode TCP is used as transport layer protocol. *For the parametrisation of the TCP, the Linux implementation is chosen as a reference.* Over this model, a set of parameters have been proposed in the Subset-037 v3.2.0, which is summarised in the Table 9.21. The proposed value for each parameter is based on the Request For Comments (RFC)s related to TCP.

It is worth noting that for the Round-Trip delay Time (RTT) and retransmission timeout (RTO) calculation the Jacobson and Karn algorithms are proposed following the RFC 1122.

For the network layer, this subset establishes that both, the OBU and the RBC must support Internet Protocol version 4 (IPv4), and below this layer, GPRS access technology will be the responsible to provide the wireless connection and set up a dedicated Packet Data Protocol (PDP) context for ETCS.

2.2.2 ERTMS: Safe Functional Module of Euroradio

For ensuring the security of signalling communications, ERTMS adopts the CENELEC standard EN 50159 as a reference for the design of its safety protocol. This standard defines seven security risks that must be faced:

- *Repetition:* an existing message is resent out of its corresponding moment.
- *Deletion:* a message is deleted from the network so that the receiver cannot receive it.
- *Insertion:* a message is inserted into the communication channel by an attacker.
- *Re-sequencing:* the sequence number of a message is intentionally modified.

No.	Mandatory Feature	RFC	Recommended Value
1	Initial RTO	793 & 1122	Minimum RTO
2	Minimum RTO	793 & 1122	4 s
3	Maximum RTO	793 & 1122	10 s
4	Karn and Jacobson's algorithm, with exponential back-off	1122	Standard values
5	TcpMaxConnectRetransmissions	793 & 1122	3
6	TcpMaxDataRetransmissions	793 & 1122	3
7	TcpKeepAliveTime	793 & 1122	12 s
8	TcpKeepAliveInterval	793 & 1122	3 s
9	TcpKeepAliveProbes	793 & 1122	3
10	TcpSack	2018 & 2883	Enabled
11	TcpNoDelay	896	Enabled
12	TCP Push Bit	793	Enabled
13	Max TCP segment size	793	1416 bytes

Table 2.1.: Summary of parametrisation proposed by UNISIG for TCP-based ERTMS: Baseline parametrisation

- *Corruption:* a message is modified resulting in another valid message.
- *Delay:* a message is intentionally delayed by overloading the transmission network.
- *Masquerade:* an attacker performs an identity theft managing to pass as a valid entity of the communication.

The ERTMS faces security risks such as replay attacks and identity theft attacks at different levels [13]. Such risks are counteracted in two main ways. On the one hand, the introduction of timestamps in the ERTMS messages prevents the replay attacks. On the other hand, the authentication and integrity of messages relies on cryptographic algorithms implemented by the Euroradio safety layer.

This layer implements a Cipher Block Chaining-Message Authentication Code (CBC-MAC) for avoiding message insertion, data corruption and masquerading. Other risks detected in the norm EN 50159 are also faced by the ETCS application by introducing timestamps in each message, which are also used for sequencing messages, and end side identifications. Thus, the SFM provides protection against message repetition, deletion, resequencing and delay.

The robustness of the safety layer depends directly to the robustness of the CBC-MAC used and in the key distribution used in this cryptographic mechanism.

Description of Safe session establishment

All communications between the OBU of the train and the RBC are done through a safe session which is established from the beginning of the connection. For each session, a new secret key is generated between two entities involved in the communication, i.e. between the OBU and the RBC. This key, also known as KSMAC or K_S, has 192 bit length and is derived from a key material shared between both entities, KMAC key. The safety session establishment is illustrated in Figure 2.4.

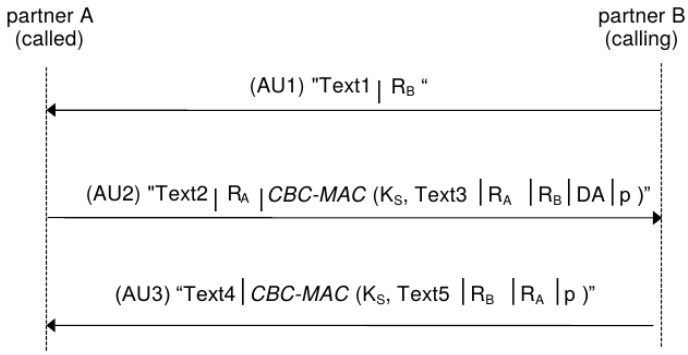


Figure 2.4.: Session establishment of Euroradio Safety protocol

As can be seen, B entity initialises the connection by sending the $text1$ and a random number of 64 bits, R_B. Equally, when A entity response to this message, it responses with the $text2$, another random number of 64 bits, R_A, and the

CBC-MAC for the concatenation of $text3$, R_A, R_B, Destination Address (DA) and a padding, p, with the session key generated from the known KMAC and the both random numbers, K_S. At this stage, B entity has the R_A, the R_B, the $text3$, the DA (its own address) and the K_S, so it can compute de CBC-MAC and generate the session key, K_S, and check that the other side of the communication has received correctly the R_A and that both are using the same K_S.

In order to establish the connection, a third message is sent from B to A, with the CBC-MAC for the concatenation of $text5$, R_B, R_A and a padding, p. Thus, the A entity, as it knows all data to perform the CBC-MAC, can also verify that the B entity has correctly received the R_A and verify that both have generated and are using the same K_S.

All data present in the $text1$, $text2$, $text3$, $text4$ and $text5$ is known for both entities as it is information related with the entities' addresses and the ETCS identification and the message type identifier.

$text1 = "ETY \mid MTI \mid DF \mid SA \mid SaF"$, where SA = calling ETCS ID

$text2 = "ETY|MTI|DF|SA|SaF"$, where SA = responding ETCS ID

$text3 = "l|DA|ETY|MTI|DF|SA|SaF"$, where DA = calling ETCS ID and SA = responding ETCS ID

$text4 = "'000'|MTI|DF"$

$text5 = "l|DA|'000'|MTI|DF"$, where DA = responding ETCS ID

As it has been explained previously, the K_S is generated from the KMAC key and from both random numbers of 64 bits. These two random numbers are split in two blocks of 32 bits for performing the key derivation procedure:

$RA = R_A^L|R_A^R$

$RB = R_B^L|R_B^R$

Equally, the KMAC key is divided in three blocks of 64 bits:

$KMAC = K_{AB} = K_1 \mid K_2 \mid K_3$

The following operations are done in both entities, A and B, for generating the session key, K_S, which is the concatenation of K_{S1}, K_{S2} and K_{S3}.

$K_{S1} := MAC(R_A^L|R_B^L, K_{AB}) = DES(K_3, DES^{-1}(K_2, DES(K_1, R_A^L|R_B^L)))$

$K_{S2} := MAC(R_A^R|R_B^R, K_{AB}) = DES(K_3, DES^{-1}(K_2, DES(K_1, R_A^R|R_B^R)))$

$K_{S3} := MAC(R_A^L|R_B^L, K'_{AB}) = DES(K_1, DES^{-1}(K_2, DES(K_3, R_A^L|R_B^L)))$

With this scheme, both parts, the OBU and the RBC, must know in advance a shared key material, KMAC. In the following lines, we explain how this key material is distributed through all elements involved in a safety connection.

Description of key exchange procedure

The key material used in Euroradio is exchanged through a Key Management System (KMS) protected by different key materials. The ERTMS uses four different keys, which can be categorised in three levels. Table 2.2 summarises this key material, including the entities that make use of each key and their functions.

Key name	Key size	Functions	Entities involved
Level 3:			
K-KMC	384 bits	Encryption, Authentication & Integrity	KMC-KMC
KTRANS	384 bits	Encryption, Authentication & Integrity	KMC-RBC KMC-OBU
Level 2:			
KMAC	192 bits	Authentication & Integrity	OBU-RBC
Level 1:			
KSMAC	192 bits	Authentication & Integrity	OBU-RBC

Table 2.2.: Summary of key material used in ERTMS

The key material in ERTMS is generated by the Key Management Center (KMC), with the exception of KSMACs, which are negotiated for each session between ERTMS entities. Each ERTMS entity must have a valid KMAC shared with other ERTMS entities for establishing safe communication. In order to ensure the secure distribution of KMAC keys from the KMC to ERTMS entities and to other KMCs, transport keys (K-KMC and KTRANS) are used to provide confidentiality, authentication and integrity. Half of the transport key is used for confidentiality by performing Triple Data Encryption Standard (3DES) ciphering

and the other is used for authentication and integrity by calculating a CBC-MAC code.

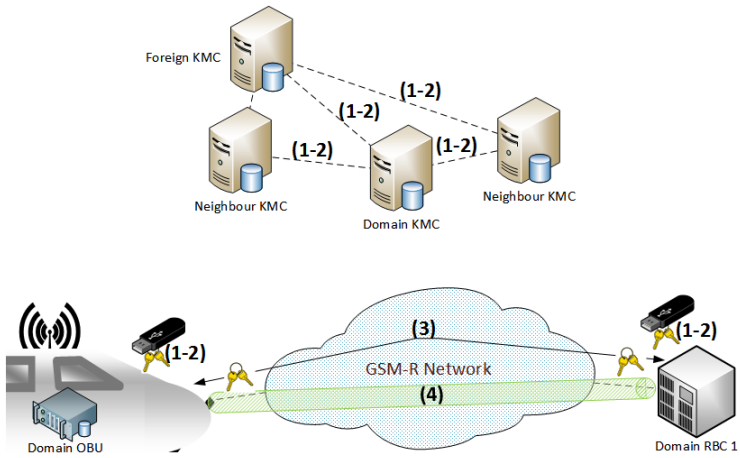


Figure 2.5.: Offline Key distribution system in ERTMS: 1) KTRANS and KKMC keys distribution; 2) KMAC keys distribution; 3) KSMAC derivation from KMAC; 4) safe communication using KSMAC.

The key distribution methodology, illustrated in Figure 2.5, is based on messages defined in Subset-114 of ERTMS specification. These messages can be exchanged using an offline or a new online mode defined in the Subset-137. However, until now, only the offline mode has been carried out, using physical storage devices such as USB sticks or CDROMs. That is, the keys are distributed through manual file distribution process.

In order to guarantee the confidentiality, the authentication and the integrity during the key distribution, the Transport Layer Security (TLS) protocol is chosen in the Subset-137. This protocol is based on ITU-T Recommendation X.509, which means that the proposal fulfils the requirements defined by the European standard EN 50159-2 for safety-related communication in open transmission networks in the railway domain. The authentication can be achieved by two methods, by using a Pre-Shared Key (PSK), named TLS-PSK or by using certificates from a Public Key Infrastructure (PKI), named TLS-PKI. However in the TLS-PSK method, the problem about how to distribute this pre-shared key material remains. Moreover, it would only valid for KMC and KMAC

entities under the same domain. Therefore, the TLS-PKI is preferred, setting aside the TLS-PSK method as fall-back method.

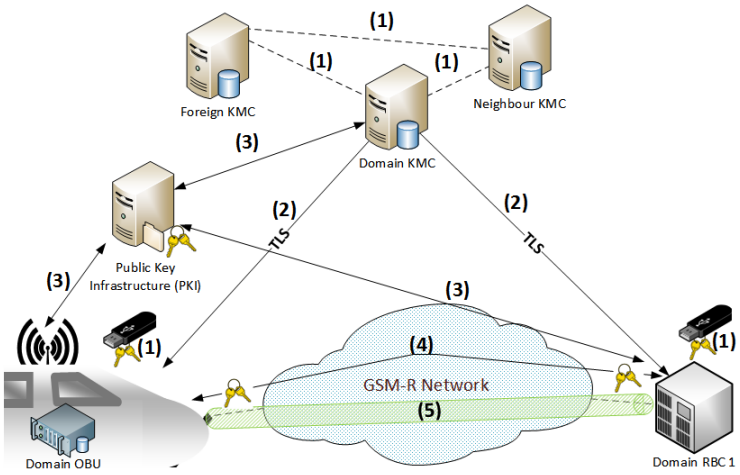


Figure 2.6.: Online Key distribution system in ERTMS: 1) KTRANS and K-KMC are replaced by a private/public key pair; 2) KMAC keys distribution using TLS with the private/public key scheme; 3) the identity of the parties is checked using a public key infrastructure scheme; 4) KSMAC derivation from KMAC; 5) safe communication using KSMAC.

To avoid impact of key distribution procedure on ETCS service, this function is proposed to be carried over a separate GPRS Access Point Name (APN). In fact, the key distribution process and the ETCS are treated independently, performing first the key distribution and then using it in the ETCS service as it is illustrated in Figure 2.6.

2.2.3 ERTMS: ETCS application

Currently the most modern train control systems for high speed services are based on the continuously supervision of the train movement. This is made by frequently comparing the train's current speed against the speed profile assigned to that service in the current position. Therefore, it is necessary for

the train to have the information necessary for this comparison available at any time. Within this information, the following data can be highlighted:

- The current train location in relation with a reference point.
- The current maximum speed at this position.
- The current train position.

In ERTMS the signalling application that allows obtaining this information is ETCS. This application has different operational levels. Depending on the level, different technology is used. In this research work we put the focus on the messages exchanged in the ETCS Levels 2 and 3, which are the ones being deployed in new High Speed Train services and the ones where message exchange relies on wireless access technology.

Three are the main messages used in ETCS to exchange these data: the Movement Authority message, the Position Report message and the Movement Authority Request message.

MOVEMENT AUTHORITY This message is sent using the message number 3 defined in the Subset-026-8. Within these messages the route set for the train, the mode profiles, speed limitations and the information needed to achieve the required safety level is exchanged.

TRAIN POSITION REPORT This message is sent using the message number 136 defined in the Subset-026-8. Within this message the OBU reports its position under different conditions which are: periodically in space or time, when passing over a group of Eurobalises configured for this duty, when mode-change execution happens, at level-change execution and as a consequence of an explicit request from the RBC.

MOVEMENT AUTHORITY REQUEST This message is sent using the message number 132 defined in the Subset-026-8. This message is used by the OBU to explicitly request a Movement Authority to the RBC via the wireless communication channel.

A typical sequence diagram for ETCS Level 2 or 3 is illustrated in Figure 2.7. The Movement Authority and Position Report messages are frequently

exchanged. On the contrary, the Movement Authority Request message is sent by the OBU when it identifies that the train is approaching to the point where the braking curve begins.

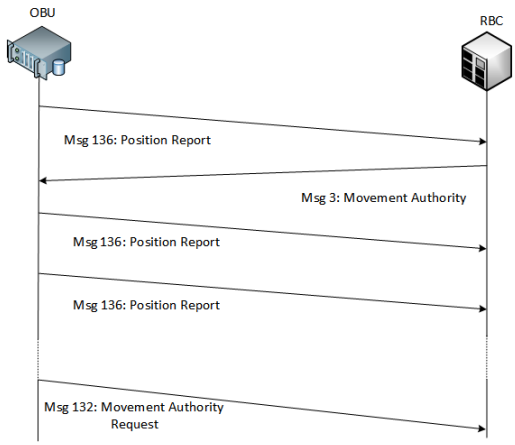


Figure 2.7.: Sequence diagram for ETCS Level 2 or 3

As mentioned before, the information carried by these messages is valid for the current moment. Therefore, these messages have a lifetime during which their information is valid. To guarantee this requirement, during the establishment of the ETCS connection, the OBU sends to the RBC the on-board clock and the RBC sends back an acknowledgement of it. After this moment, both sides are synchronised and ceach message is marked with a timestamp that determines its lifetime.

2.3 COMMUNICATION REQUIREMENTS AND CONSTRAINS IN THE RAILWAY DOMAIN

Communication networks used to carry train signalling have some specific characteristics [14] inherent to the railway context that can be distinguished as follow:

- *Hard delay constrains:* Train signalling systems do not require high data rates, nevertheless most signalling messages, such as the movement authority messages, present a short life-time (message vitality). Longer delays than expected turn the message useless and even dangerous, as it may force the train to stop and consequently affect availability and operational indicators. This delay may not be longer than 500 *ms* to fulfil European Integrated Radio Enhanced Network (EIRENE) requirements over GSM-R. At the moment, the ETCS Quality of Service (QoS) profile of FFFIS for Euroradio version 13.0.0 (Table 2.2, note 4) [15] does not define a maximum transfer delay. However, according to Table 2.3 published by the Danish Railway Company, Banedanmark [1], it is expected to be the same for GPRS .

- *Frequent handovers:* The base stations of the mobile access network are placed along the railway to provide coverage to trains in movement. Trains moving at high speed pass through different coverage areas and consequently perform a sequence of handover processes.

- *Multiple communication networks:* During the last years multiple networks have been deployed along railways [16]. Some of them such as Terrestrial Trunked Radio (TETRA) and GSM-R are rail specific and owned by railway operators. Additionally the deployment of GSM-R has been done in many cases redundantly, providing multiple overlapped cell coverage [17].

- *High security requirements:* These signalling communications have high security requirements because a malicious identity theft could be used to perform an attack that could risk passenger's life.

- *High reliability requirements:* Both ends of the communication link must ensure the correct delivery of signalling messages. Thus, the reliability in implemented protocols must be guaranteed. In GSM-R, network and transport protocols, T.70 and X.224 respectively, are connection oriented and introduce reliability mechanisms. Within X.224, two ways to promote reliability are defined: message reception acknowledgement and retransmission; and splitting and recombining function which allows the simultaneous use of two or more network connections to support the

same transport connection, that is, a multipath strategy. However, this last reliability mechanism is not used in the X.224 deployment of GSM-R, because the system is considered reliable enough with retransmission mechanisms at different protocols. Additionally, this functionality would need multiple channel reservation and this fact would mean a reduction in capacity and availability of the GSM-R network due to the limited spectrum of this technology [17].

QoS Parameter	**Value**
Data integrity (Reliability Class 2):	*Based on GSM 02 60*
• Probability of data loss	$<10^{-4}$
• Probability of data suplication	$<10^{-5}$
• Probability of out-of-sequence data	$<10^{-5}$
• Probability of data corruption	$<10^{-6}$
Data Transfer Delay (Delay Class 1):	*Based on GSM 02 60*
• Mean delay for 128 byte packet	$<0.5\ s$
• 95% of 128 byte packets delayed	$<1.5\ s$
• Mean delay for 1024 byte packet	$<2\ s$
• 95% of 1024 byte packet delayed	$<7\ s$

Table 2.3.: Proposed KPIs for ETCS over GPRS [1]

2.4 ANALYSIS OF THE CURRENT ERTMS

The current communication protocol stack of ERTMS has some limitations and shortcomings that should be overcome in future ERTMS specifications. The upcoming migration towards IP is a good chance to address these limitations by introducing new proposals.

In this section, we differentiate these shortcomings in three main groups: 1) the shortcomings of GSM-R, 2) the design limitations of the current Euroradio

CFM and the limited compatibility with new communication technologies, and 3) the security shortcomings of ERTMS.

2.4.1 Shortcomings of GSM-R/GPRS

There are three main shortcomings of GSM-R; its limited channel capacity, interferences produces by public telcos' networks and the lack of industry support after 2030.

As explained in [18], as GSM-R deploys CS based data transmission, each data connection requires a dedicated channel. Due to the used Frequency Division Duplex (FDD) and Time Division Multiple Access (TDMA) mechanisms the effective capacity of each cell is no higher than 23 simultaneous connections, including voice and data services. As in ETCS each train must have a permanent connection with the RBC, and taking into account that some channels are reserved for voice communications and handover procedures [1], the maximum train number in a junction under the coverage of a single cell is less than 20 [18]. This limitation suppose a bottleneck for railway operations that can hardly overcome without a migration towards another access technology with better spectrum efficiency in order to optimise the currently reserved frequency band for GSM-R ($876 - 880\ MHz$ for the Uplink and $921 - 925\ MHz$ for the Downlink).

The dedicated frequencies of GSM-R suffer from interferences produced by public operators providing services in the 900 MHz band. The intention of public telcos and railway infrastructure managers is to provide as higher and better radio coverage as possible along the track. On the one hand, telcos want to provide voice and data services for travelling passengers. On the other hand, railway managers need correct GSM-R coverage to operate trains services safely. This problem has increased with the popularisation of broadband services over LTE technology [19]. These interference problems have been identified by the ERA and this agency is already working on coexistence strategies [20].

In the telecommunication market, the shortcomings of GSM were noticed long time ago as soon as the data communication needs increased and overtook the voice ones. At that age, GSM was replaced by GPRS first, Universal Mobile Telephone Service (UMTS) after and nowadays by LTE. The railway industry is not unaware of this evolution because the decrease of manufacturers in

the telecommunication market supposes also a lack of competence between them, therefore an increase of production and maintenance costs. Although GSM-R suppliers have guaranteed support to this technology until 2030 [21], the railway industry is already working on the migration towards a new access technology, starting for the definition of ERTMS over GPRS. In fact, the ERA expects to have started the deployment of the replace technology for 2022 [21].

During the last years, predicting the necessity of switching to other access network technologies, multiple academic proposals have been made for substituting GSM-R. From the industrial side, other access technologies have also been tested in railways. The report demanded by the ERA [12] in order to find the most suitable candidate to substitute GSM-R, summarises the possibilities available in the market, as well as previous experiences all around the world.

The most suitable technology to succeed GSM-R as a first step of this migration is GPRS. The suitability for the railway domain has already been demonstrated [11, 12]. The advantage of this technology comparing to other alternatives is that it can use the same frequency bands already reserved for GSM-R and as it introduces better resource managing for data communications it introduces more efficient spectrum use.

However, this migration towards GPRS is not assumed by every country. In Kazakhstan for example [12], TETRA was introduced as communication technology for ERTMS. In the next years the adoption of TETRA is also expected in Finland as underlying technology for ERTMS [22].

In Australia the coexistence of different access networks as carrier for railway signalling has become a reality. This strategy overcomes the lack of coverage in some areas by using commercial cellular UMTS networks [12].

Additionally, many academic works have demonstrate the suitability of 4G technologies, Worldwide Interoperability for Microwave Access (WiMAX) [23] and LTE [24, 25], for the railway domain. These works, in addition to the quick technology evolution, have encouraged industry to think in 4G or even in 5G technologies as a long term technology for the NGERTMS.

All in all, these technologies candidate to replace GSM-R for data transmissions are based on IP technology. Therefore, when talking about NGERTMS, the adaptation of the protocol stack to a full IP-based one is envisaged. Moreover, the adoption of different technologies in different countries or

corridors is more than probable. *Thus, the new ERTMS protocol stack should address the coexistence between different access technologies, as well as the handover between them in a transparent way.*

2.4.2 Design limitations of Euroradio communication module

When Euroradio CFM was designed, the OSI protocol stack was adopted as reference model. Due to this design option, the primitives to connect the CFM and the SFM are designed for the OSI transport layer, ITU-T X.224. The strategy made in CS mode based on implementing specific protocols for railway domain has turned out to be costly and complex [26]. Therefore, *the trend for next generation signalling systems is expected to be the adoption of market standard protocols [21].*

The inclusion of de-facto protocols, i.e. TCP/IP protocol stack needs for an adaptation layer which translates the primitives from X.224 format to TCP/IP format. The addition of adaptation layer involves more processing latency and data overhead due to the addition of headers carrying out the same function. Moreover, although in the new Subset-037 v3.2.0 the adoption of TCP/IP has been made, this subset does not allow the use of other wireless technology than GSM-R or GPRS because the channel requirements established for both, CS mode and PS mode, are based on circuits established by GSM-R of PDP contexts provided by GPRS.

Another design shortcoming in the CS mode comes from the fact that both, data link and transport layers, have similar functions assigned for the same communication context. This is the case of retransmission mechanisms. Although usually data link layer protocols have retransmission mechanisms for providing reliability to the physical channel, this is usually oriented to the device-to-device link protection, whereas the transport retransmission mechanism protect the whole connection from the source to destination. However, in the case of ERTMS, the connection is set up over a virtual circuit from the train to the RBC and therefore the underlying channel protected by the data link layer is also protected by the transport layer. This duplication of functions implies the addition of supplementary timeouts which involves an increase of data transfer latency.

In the PS mode, the existence of multiple network interfaces in the RBC is expected. *However, the management of this multihoming support of the RBC is not detailed in the transition towards IP proposed in the Subset-037 v3.2.0.* Moreover, in this subset, a parametrisation for TCP protocol is proposed. However, these parameters have been taken mainly from RFCs present in the literature that are oriented to the fixed networks. The problem with these parameters is that they are based on the assumption that there are always more data to transmit that the channel can afford, therefore any packet loss is produced by network congestion. That is why congestion control algorithms are proposed for TCP protocol. This assumption can be seen also in the Karn algorithm applied when consecutive retransmission are triggered. For this circumstance, this algorithm, proposes an exponential increment of the timeout time required to wait until the next retransmission. Another case where the adoption of standard parametrisation is not suitable is the values adopted for the Jacobson algorithm which calculates the current Smoothed Round-Trip Time (SRTT) and RTO. These values were calculated originally from extensive tests made in fixed networks where the channel conditions do not change abruptly. However, this is not the case of railway wireless networks where the movement of the mobile node and electromagnetic disturbances produce changes in channel conditions.

2.4.3 Analysis of the Euroradio safety module

This section considers the cyber security threats to current ERTMS security mechanisms based on the taxonomy of cyber attacks on the IT domain presented in the appendix A. This cyber security analysis was already published in the IEEE Communications Magazine in 2015 [13]. It is structured in two parts: the first part reports on those attacks initially considered in the ERTMS design phase, while the second part is concerned with the security threats that were not considered during the ERTMS design phase.

Analysis of ERTMS security mechanisms

The ERTMS faces security risks such as replay attacks and identity theft attacks at different levels. Such risks are counteracted in two main approaches. On the one hand, the introduction of timestamps in the ERTMS messages prevents the

replay attacks. On the other hand, the authentication and integrity of messages relies on cryptographic algorithms implemented by the Euroradio safety layer. Below, we analyse these mechanisms and algorithms in order to identify their strengths and weaknesses.

As mentioned above, to counteract replay attacks, the ERTMS introduces timestamps to sequence the messages. However, this mechanism is not introduced during the session establishment process, making it vulnerable to such attacks. Additionally, since the sequence numbering using timestamps is made at the application layer level, the end-side must decrypt the Message Authentication Code (MAC) provided by Euroradio before checking the validity of the sequence number. This fact can be exploited to perform a flooding attack, resending several valid – but out-of-sequence – messages, which degrades system performance. Preventing such attacks depends on the confidentiality provided by the GSM-R encryption algorithm. However, this algorithm has been already cracked. Moreover, pre-computed key tables – named rainbow tables – are available on the Internet, which allow an attacker to listen and even spoof entities in the same cell of the network. Thus, we can affirm that ERTMS is vulnerable to eavesdropping and replay flooding attacks due to GSM-R weakness and the current ERTMS protocol structure.

From the message integrity and authentication point of view, the potential vulnerability of ERTMS comes from two main factors: the vulnerability of the key material distribution and the weakness of the cryptographic algorithms used.

The key exchange methodology explained in Section 2.2.2 deals with the security of the process. However, the offline process widely used until now, requires personnel to manually deliver the messages from the KMC to the ERTMS entities. Because this process is complex, there is a risk of simplifying it by using the same KMAC for large train fleets. As pointed out in a tender document [27] released by the Danish Railway Company, this fact has security and safety implications, because when many parties share a secret it is no longer a secret. Furthermore, the physical delivery of the key material introduces the possibility of attacks based on social engineering.

With the new online Key Distribution System, the complexity and the cost of distributing all keys for a fleet manually has been reduced. Therefore, the

security risk associated to the use of the same key for all the fleet has also decreased. Moreover, the adoption of TLS with a PKI provides higher protection in the key material distribution comparing with the process defined for the offline mode.

From the point of view of the cryptographic algorithm, critical vulnerabilities of Data Encryption Standard (DES), when it is used to compute CBC-MAC codes, have been already pointed out [28]. As Smith et al have demonstrated, DES is vulnerable to key-collision attacks based on the birthday paradox, which are more efficient than brute force attacks. Additionally, the use of 3DES does not introduce a much higher level of robustness comparing to DES, since it is still vulnerable to meet-in-the-middle attacks [28]. Actually, the real robustness of 3DES is not higher than O(284) if 228 cipher texts are available for the attack. This vulnerability is risky in terms of the authentication provided by the KSMAC. However, higher risk comes from two factors: 1) the fact that multiple trains make use of the same KMAC for a long time, and 2) the possibility of using weak random number generators during the KSMAC derivation. In fact, if the attack is performed against the session establishment with the goal of finding the KMAC, the whole system could be compromised: an attacker could take the identity of one or many trains during subsequent session establishments. As the KSMAC derivation from the KMAC is a public process and the random numbers travel in plain text, the effectiveness of the attack increases considerably.

Once the new online Key Distribution System incorporates TLS-PKI, and knowing that the session key negotiation could be improved from the point of view of security, the question is: why TLS-PKI is not applied also for the safety communication between ERTMS entities instead of using it only for KMAC distribution? Moreover, if ERTMS would communicate each other using TLS-PKI and they have their own certificates, would KMAC keys be necessary?

Security threats not considered by ERTMS

The risks of suffering communications attacks have traditionally been counteracted by isolating the railway networks. Using isolated circuit-switched networks not connected to the open internet and reserved frequency bands; the communication between ERTMS elements has been inaccessible to outsiders.

However, the feasibility of these attacks now requires reconsideration on account of two factors: the popularisation of commercial jammers working in the same band used by GSM-R, and the impending migration of ERTMS towards IP-based cellular technologies [12]. This security risk is common to other vehicular communication technologies, such as Dedicated Short Range Communications (DSRC) [29].

Table 2.4 summarises the potential cyber attacks against ERTMS, their feasibility and mitigation techniques of ERTMS [13] for overcoming them. It also ranks security risks using estimated values for likelihood of occurrence and impact of each attack upon the network. This risk analysis has been done using the Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) methodology published by the European Telecommunications Standards Institute (ETSI).

When compared to the analysis presented in [30] for DSRC, we can conclude that the threat scenario is similar and spoofing threats are also the most critical ones. Unlike [30] we differentiate the feasibility of jamming and flooding attacks and therefore the risk for the first one is critical whereas the risk for the second one is major.

Target	Attack type	Means	Knowledge needed	Detection capability	Mitigation technique specified in ERTMS	Ocurrence likeli-hood	Impact	Risk level
OBU-RBC comms.	Passive	Eaves-dropping	Medium	Low	Dependent on GSM-R robustness	Possible	Low	Minor
	Active	Jamming	Low	High	Not considered	Likely	Medium: force degraded mode	Critical
		Spoofing	High	Medium	Authentication and integrity	Possible	High: wrong driving	Critical
		Flooding replay attacks	High	High	Responsibility of ATP application	Possible	Medium: force degraded mode	Major

Table 2.4.: Review of potential attacks in ERTMS

2.5 SUMMARY AND MOTIVATION

ERTMS protocol stack will need to be updated as soon as a newer radio access technology is adopted as a substitute of GSM-R. Currently ERA is looking for candidate technologies for this replacement, being all of them designed to work with IP. This new communication solution should be ready by 2018 for starting the transition in 2022. Meanwhile, UNISIG has released a new version of the Subset-037 which specifies the adoption of the TCP/IP protocol stack. However, in the current ERTMS specification, in both, CS mode or PS mode, multiple shortcomings that should be overcome have been detected.

On the one hand, in the CFM specification the following shortcomings have been detected:

1. According to the current ERTMS standard regular ETCS traffic and High Priority traffic should be treated differently. However, the bypass strategy followed in the CS mode of ERTMS is not valid for the PS mode, because the connection is not based on a virtual circuit that links the source and the destination.

2. Within the new definition of a protocol stack for NGERTMS, the coexistence of heterogeneous radio coverage in the railway corridors should be taken into account, as well as the future evolution. Moreover, the protocol stack should be independent to the underlying technology, because the different pace of evolution between the railway and telecommunication market will force to address new radio technology migration within the life cycle of the train.

3. The multihoming support of RBCs in the PS, as potential contributor of reliability, is not exploited in any way.

4. The configuration parameters for the TCP protocols chosen were made for fixed networks where channel conditions do not change abruptly. Additionally, these parameters are also select for scenarios where packet losses are provoked by network congestion. This assumption does not fit with the characteristics of the ETCS application: low packet size and long interval time between the deliveries of two consecutive packets.

5. Market standard protocols should be adopted, if possible, and railway specific protocol avoided. The experience with railway specific technology has demonstrated that its reduced market increases its development and maintenance costs, as well as difficult its compatibility with ubiquitous Commercial Off-The-Shelf (COTS) technology.

On the other hand, in the SFM specification the following shortcomings have been detected:

6. The cryptographic algorithms used for safety session between two ERTMS entities, CBC-MAC and 3DES, have been found not robust enough comparing to the current state of the art.

7. The cryptographic algorithms used for safety sessions are fixed and cannot be upgraded without changing all the specification of the Euroradio Safety Layer. These algorithms should be updated according to the security state of the art.

8. The new protocol stack should address the new security risks pointed out in Table 2.4 of Section 2.4.3, specially the protection against jamming attacks.

2.6 GOALS AND CONTRIBUTIONS

Based on the analysis of the current ERTMS system described in this chapter, we envisage that there is a need to re-design ERTMS protocol stack to address the shortcomings explained in the lines above. The main goal of this thesis is to propose a new protocol stack for ERTMS which addresses the detected shortcomings in train-to-ground communications and make the NGERTMS more resilient compared to the current system. The specific goals to be addressed by this research work are enumerated below:

1. Improve the survivability against end-to-end channel disruptions and reduce the latency in ERTMS communications. The faster and more reliable the communication is, the more efficient the train operation will be.

2. A proposal to overcome the current limitation of ERTMS in its PS mode to operate with HP messages by providing them higher resiliency and lower delay comparing to the regular messages.

3. Offer a solution based on standard solutions which will reduce the CAPEX and OPEX by facilitating the adoption of COTS equipment widely used in the telecommunication market.

4. Facilitate the backward compatibility of the proposal with the current system. The migration towards a new proposed protocol stack will be gradual. Therefore, the proposed system should be able to work with the current protocol stack present in the PS mode.

5. Respond to the need of railway operators to provide telecommunication services through different access networks. This thesis aims to provide a communication protocol stack for ERTMS that will allow the coexistence of heterogeneous access technologies. This feature will ease the progressive introduction of new access technologies in the future.

The contributions of this thesis are as follows:

1. A complete analysis of current ERTMS from the communication and security point of view and identification of a set of shortcomings to be addressed to improve the train-to-ground signalling resilience.

2. Analysis of current redundant protocols as a cornerstone to achieve a more resilient communication system over IP. For the evaluation of the characteristics of each approach, a set of requirements composing a vector named Resilience Requirements for ERTMS (RRE) has been defined. Over this vector a semi-quantitative analysis is made which helps to select the most suitable approach.

3. A proposal of a new protocol stack for ERTMS is introduced which has as a basis the selected approach from the previous analysis. This protocol stack is designed not only for a scenario with completely multihomed equipment, but also for a transitional scenario where multihomed equipment with the support of the proposed protocol stack coexists and

interconnects with legacy ERTMS equipment in PS mode defined in the Subset-037.

4. Parametrisation of TCP and MPTCP protocols and their scheduler in accordance to the traffic to be carried (regular and HP). In total four different parametrisations are presented which correspond to the class services associated to the regular and HP traffic for full multihomed scenario and a transitional scenario.

5. Development of two evaluation systems to analyse the suitability of the proposal, one through a pure DES tests using the OPNET Modeler simulation tool, and another through a hybrid simulated scenario with real traffic.

In conclusion, the proposed protocol stack for the NGERTMS addresses the shortcomings detected in this chapter. The performance of this resilient protocol stack is evaluated under different harsh channel conditions with high packet loss and connection disruptions demonstrating the improved of the proposal comparing the legacy ERTMS communication protocol stack.

Part II

STATE OF THE ART

laburpena

Atal honetan komunikazioen erresilientzia dugu aztergai, beti ere erresilientzia hori kanal baten perturbazioaren aurrean zerbitzua automatikoki errekuperatzearen ahalmena bezala ulertuta. Horretarako, lehenengo eta behin erresilientzia lortzeko estrategia klasikoak aurkezten ditugu eta hauek burdinbideen testuingurura moldatzen ditugu. Gero, burdinbideen industriak gaur egun komunikazio erresilienteak lortzeko erabiltzen dituzten protokoloak aztertzen ditugu. Azterketa honetatik bi ondorio atera daitezke; batetik erredundantzia dela erresilientziaren giltzarri nagusia eta bestetik burdinbide industriak COTS ekipamendua erabili ahal izateko protokolo estandarrak erabiltzea behar beharrezkoa dela. Horrexegatik, protokolo erredundanteen artearen egoeraren azterketa sakona egiten da, OSI erreferentzia protokolo pilaren geruza ezberdinetan banatuz. Azkenik, azterketa horretatik, metodo sasi-kuantitatibo bat erabiliz, NGERTMSrentzako protokolorik aproposena MPTCP dela ondorioztatzen da, nahiz eta bere inklusioak tesi honetan egingo diren doiketa batzuk behar dituen.

resumen

En este apartado analizamos la resiliencia de las comunicaciones, entendidas como la habilidad para recuperarse automáticamente de disrupciones en el canal. Para ello, primero introducimos las estrategias clásicas para alcanzar la resiliencia y los adaptamos a las necesidades específicas del entorno ferroviario. Después hacemos un resumen de las estrategias y protocolos usados para alcanzar la resiliencia en otros sistemas del sector ferroviario. De este análisis se desprende que la redundancia es la piedra angular de la resiliencia y que la única forma de adoptar equipamiento COTS es el uso de protocolos estándar. Por ello, se realiza un profundo análisis del estado del arte de los protocolos de comunicaciones redundantes, dividido en las diferentes capas de la pila de referencia OSI. Por último, partiendo de ese análisis se evalúa mediante un método semi-cuantitativo el protocolo idóneo para su adopción por el NGERTM, que es MPTCP, a pesar de que su inclusión implica una serie de adaptaciones específicas que pretenden solventarse en esta tesis.

3 ANALYSIS OF NETWORK RESILIENT PROTOCOLS

> Science is organised knowledge. Wisdom is organised life.
>
> Immanuel Kant

3.1 INTRODUCTION

Railway signalling systems demand high reliability level as their performance affects directly to the passenger's life. In the previous chapter we have made a revision in depth of the European system ERTMS.

As we have seen, in this system there are two main types of messages: the regular and high priority messages. The normal operations of ERTMS make use of the first type of messages, whereas emergency commands, such as emergency break command, are delivered using high priority messages. Thus, the migration of ERTMS towards TCP/IP should take into account this message duality and propose mechanisms that could allow the application to deliver different messages with different associated policy.

From the point of view of heterogeneous wireless network coexistence, the NGERTMS should be able to exploit, if needed, this heterogeneity when multiple access networks are available.

On the one hand, this coexistence could help to become communications more robust against network disruptions. These disruptions could be unintentionally or intentionally created as part of a Denial of Service (DoS) attack. In any case, from the point of view of communication networks, both cases are originated by the eventual channel unavailability and have the same

potential solution, the use of an alternative channel. Therefore, the availability of heterogeneous networks could be exploited to overcome this problem.

On the other hand, the different pace of telecommunication and railway markets implies that the railway signalling systems cannot be attached to a single wireless technology. Moreover, along the life-cycle of the railway signalling equipment, new generation wireless technologies will become ubiquitous in the market. Therefore, new railway corridors or corridor sections will use these new technologies in order to adopt COTS equipments. From the communication network's point of view, effective vertical handovers between heterogeneous technologies vouch for the coexistence of these technologies.

In this chapter, we analyse the resilience of network communications, understood as the ability to recover from network disruptions, as it encompasses both challenges described above. This chapter is structured as follows. First we describe the general strategies to achieve resilience and we tailor them to the railway specific need in terms of safety and security, concluding that redundancy and path diversity are the cornerstones of resilience. Then, we provide an overview of resilience protocols in other railway contexts and similar industries. Afterwards, we define the key features to be fulfilled by a protocol responsible to provide end-to-end resilient communications in ERTMS. Based on these features, we provide an analysis of the state of the art present in the literature related to multihoming and multipath protocol capable to provide path redundancy. This analysis of the state of the art is divided in different OSI layers and for each technology a detailed description is provided followed by a critical analysis of the previously mentioned requirements. Finally, using a semi-quantitative analysis of previous requirements, we conclude this chapter identifying the most suitable proposal for including in the NGERTMS and we highlight the open points that should be addressed before its inclusion in the NGERTMS's protocol stack.

3.2 FROM GENERAL RESILIENCE DISCIPLINES TO RAILWAY SIGNALLING NEEDS

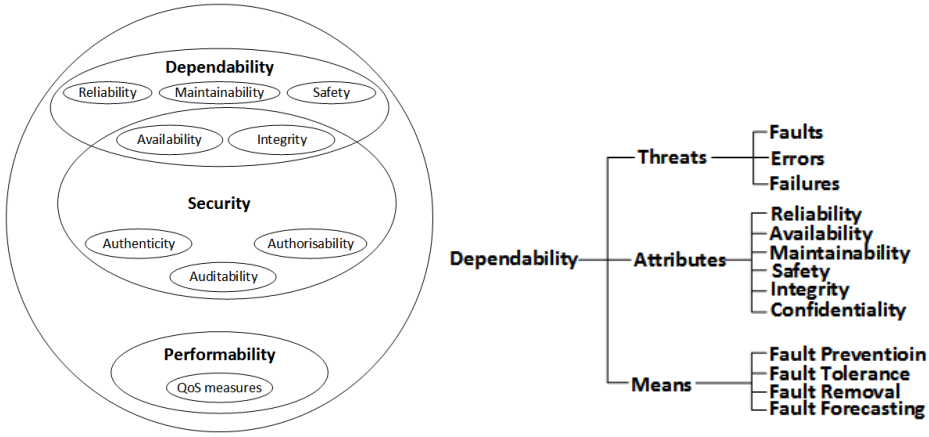
Before going into details of the existing network mechanisms for achieving communication resilience, there is a need to provide a set of basic definitions about what the resilience is, and which are the constrains defined by the railway industry.

Resilience has been traditionally defined as the combination of multiple disciplines that ensure that a given system can perform the task that it is defined for, without interruptions produced by errors. A resilient system is defined as a system that can ensure the trustworthiness in terms of dependability, security and performability (see Figure 3.8a) [2, 31]. The dependability quantifies the reliance of a service provided by a system and it is dependent on availability and reliability, which are described as the readiness for usage and the continuity of the service respectively [32]. The security protects from unauthorised access and modification to the system, as well as to the information delivered to/from it [33]. The performability [34] is the property of the system to perform according to the service requirements. This performance can be measured in communication networks for example with the channel delay, throughput, packet error rate or jitter.

In the railway domain, the dependability is measured using RAMS requirements [5, 7, 36]. These requirements can be represented as a dependability tree illustrated in Figure 3.8b. These requirements are generally extended including security requirements and performance requirements.

In the railway signalling case, the norm EN50126 [4] defines the reliability requirements to be fulfilled by a railway application, whereas the EN50159 [37] defines the security ones depending on the category of its system. This categorisation depends on the transmission system used, as well as on the type of application, i.e. if the application is safety-related or not.

The performance requirements for the concrete case of ERTMS are defined mainly in two documents; the EIRENE Functional Requirements Specification [38], which specifies the requirements for the underlying communication channel provided by GSM-R, and the ERTMS/ETCS SRS Subset 093 [39], which defines the requirements related to the transmission of ETCS messages. These



(a) Resilience requirements **(b)** Dependability tree RAMS [35]

Figure 3.8.: RAMS requirements for a railway resilient system

performance requirements are summarised in Table 3.5, as well as tentative requirements [1] presented by the Danish railway operator, Banedanmark, for the performance of ETCS over PS-based technologies and more concretely over GPRS.

In order to achieve the dependability, security and performability, there are seven detected enablers [2] that can provide the desired behaviour to the system. These enablers are:

- Connectivity and association - The end-to-end session should be maintained even if an underlying stable connection is not available, as far as the delay does not exceed the maximum specified by the performance requirements.
- Redundancy - The replication of entities or delivered data in space, time and information plays a key role for ensuring the resilience. In case of errors this redundancy prevents a service failure.
- Diversity - It is closely related to redundancy. It prevents correlated errors when redundant systems are used. Thus, diversity provides disjoint alternatives for redundancy.

	QoS Parameter	Value
	Min signal level (95% probability)	$-92\ dBm$
GSM-R Requirements	Connection establishment delay of mobile originated calls	<5 s (95%) <7.5 (99%)
	Connection establishment failure probability (per attempt)	$<10^{-2}$
	Bit error rate for 4.8 $Kbit/s$ channel	$<10^{-4}$
	End-to-end delay (of 30 octet frame)	<500 ms
	Data rates	2.4, 4.8 and 9.6 $Kbit/s$
	Probability of connection loss	$<10^{-2}$
	Maximum break during handover	500 ms
GPRS Requirements	Connection establishment delay: -GPRS attach -Packet Data Protocol context activation -Temporary Block Flow establishment	 <250 ms <250 ms <1 s
	Data Transfer Delay: - Mean delay for 128 byte packet - 95% of 128 byte packet delayed - Mean delay for 1024 byte packet - 95% of 1024 byte packets delayed	 <0.5 s <1.5 s <2 s <7 s

Table 3.5.: Performance requirements over GSM-R and GPRS

- Self-protection and security - It is implemented by numerous security mechanisms for ensuring entities' authentication and authorisation, as well as data confidentiality, integrity and non repudiation.
- Multilevel resilience - Resilience is needed in three dimensions; protocol layers where the resilience is provided, protocol planes (control, data and

management) and network architecture. The resilience mechanisms at different levels are represented in Table 3.6.

Level	Mechanism
Application	Adaptive applications
Transport	Eventual connectivity, erasure codes
Internetworking	Heterogeneity, realm diversity
Path	Multipath spreading, medium diversity
Topology	k-connected, geographic graph diversity
Links and nodes	Link error control, fault tolerance
Physical channel	Robust coding

Table 3.6.: Levels and selected resilience mechanisms [2].

- Context awareness - It is needed for resilient nodes to be aware of the network conditions and detect adverse events. The detection of these events would trigger mechanisms to overcome them.
- Translucency - It is needed to find a trade-off between the degree of abstraction and the visibility between levels.

Using the enablers mentioned above and summarised in Figure 3.9, it is expected to achieve an autonomic behaviour able to react automatically against system failures or malicious attacks. Moreover, the system should always ensure its adaptability to new situations and should be ready to work with new technologies coming from the inexorable evolution of the technology.

3.2.1 Communication redundancy approaches as a basis of resilience

A communication system that aims to be resilient should ensure, at different levels; communication redundancy and diversity - in order to prevent correlated failures - and, finally, automatic restoration capability. Namely, it must be able to react automatically for facing unpredictable disruptions.

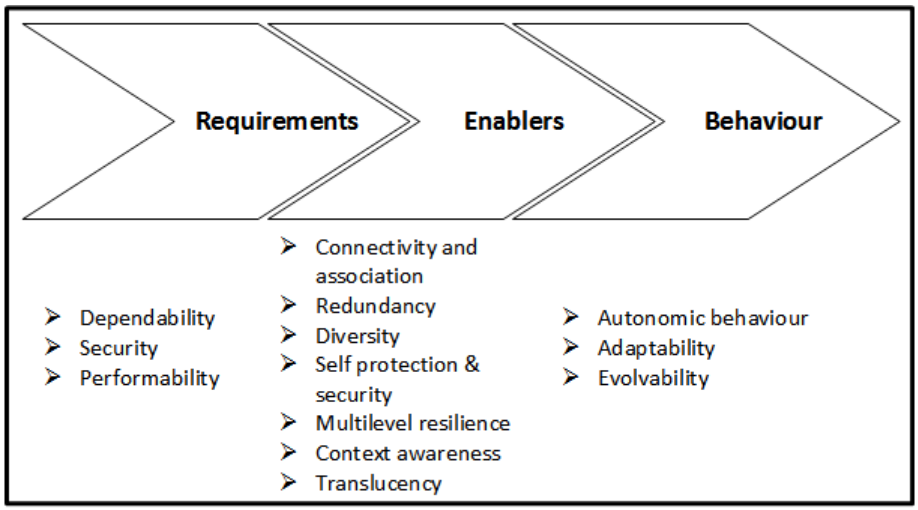


Figure 3.9.: Resilience principles

Network redundancy refers to the replication of network entities used in the communication in order to provide fault-tolerance. So far numerous solutions addressing redundancy have been presented in the literature.

These solutions can be mainly categorised in the following three main groups:

Spatial redundancy means the possibility to obtain information for a specific location from different sources.

Temporal redundancy refers to the act of delivering information more than once, skewed in time.

Information redundancy is defined as the use of redundant data in order to detect and allow the reconstruction of data by the receiver in case of failure.

Another categorisation that can be made is based on the OSI levels. Depending on the level where the redundancy is applied, the communication is differently protected. While implementations below the network layer protect a single link of the communication channel, the approaches deployed above this

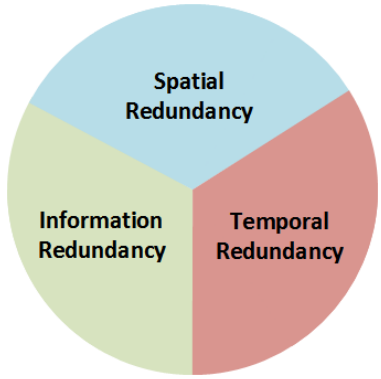


Figure 3.10.: Redundancy categorisation

layer intent to protect the complete communication channel from the source to destination. *In the case of proposed NGERTMS, the protocol able to exploit redundancy should be implemented in the OBU and RBC, being able to protect the end-to-end communication not only from the access network's failures, but also from core network's disruptions. Therefore, the protocol to be implemented should work above to the network layer.* Moreover, when the concurrent use of heterogeneous access technologies is envisaged, the network layer addressing must be also taken into account. In fact, each network interface acquires a new address when it is associated with a new network [40]. Thus, for the railway signalling purposes, end-to-end redundancy mechanisms should be implemented in upper layers (above the network layer).

3.3 SOLUTIONS APPLIED FOR SIMILAR RAILWAY CONTEXTS AND INDUSTRIES

Another signalling system used in railways for controlling the safe operation of vehicles using data communication is named Communication-Based Train Control (CBTC) [41]. CBTC, currently standardised in accordance with IEEE 1474 series, is mainly used in urban mass transit systems. In these contexts, the use of Wireless Local Area Network (WLAN) for establishing the bidirectional wireless

communication channel is the best choice due to the available commercial-off-the-shelf equipments [42]. Most existing WLAN-based CBTC networks are using traditional IEEE 802.11 technologies [43], such as 802.11a/b/g. However, Communication-based train control networks have stringent requirements for wireless communication availability and latency [44]. In order to increase operational security, reliability and availability, a redundant radio network is implemented. Nevertheless, only one network is active at a time, the other one remains in quiet back-up mode for ensuring operation continuity. In [45] and [46] authors propose two WLAN-based train-ground communication schemes with redundancy to improve the availability in CBTC systems. The availability is analysed using Continuous Time Markov Chain (CTMC) model. The introduced examples illustrate that the proposed schemes with redundancy can significantly improve the availability of WLAN-based train-ground communication in CBTC systems.

CBTC can be affected due to continuous movement of the vehicles along the rail which involves periodical handovers from one Access Point (AP) to another. In order to overcome this potential problem, in [47] authors propose a handoff management scheme based on Stream Control Transmission Protocol (SCTP) and IEEE 802.11p WLANs to provide high communication availability and low latency in CBTC networks. The multihoming feature enables the establishment of a SCTP session over multiple interfaces identified by multiple IP addresses.

Another recent proposal with the aim of improving the resilience in railway signalling is Rail Safe Transport Application (RaSTA) [48], which is used by the track field equipments. In correspondence with the requirements of EN50159 the RaSTA protocol ensures safe communications by introducing both, security and redundancy mechanisms [49] as it is illustrated in Figure 3.11.

For the communication between decentralised field elements in interlocking systems another architecture named Sinet [50] has been designed with the aim of offering real-time and high-availability communications. This system, as well as RaSTA, is a proprietary commercial product for railway market. This system implements redundancy mechanisms that prioritise operational data while providing the high system availability required. The redundant connections between controllers and interlocking are implemented by the standardised Parallel Redundancy Protocol (PRP) specified in IEC 62439-3 [51]. The protocol

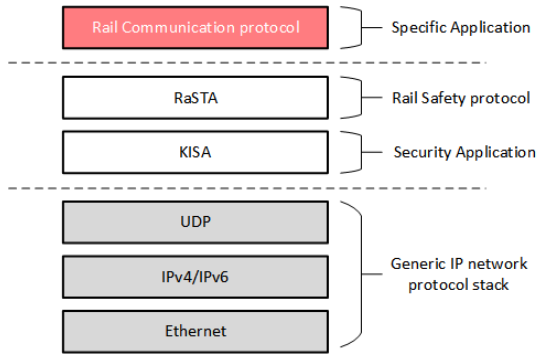


Figure 3.11.: Architecture of RaSTA

stack where the PRP is introduced is illustrated in Figure 3.12. Thanks to the use of redundancy, if a single fault in the communication infrastructure occurs, the services offered over this architecture remain available.

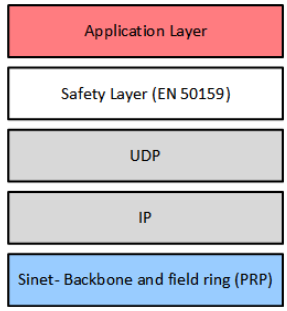


Figure 3.12.: Architecture of Sinet

Another industrial context where resilience is highly required is in the electric power systems, especially with the emergence of Smart Grids. For the communications within smart grids, HSR, IEC 62439-3 clause 5 [51], has been introduced as a protocol to provide resilience [52]. Although HSR has been criticised due to its unnecessary traffic created due to the duplicated copies of each sent frame, the standard IEC 61850-90-4 [53] recommends its use combined with Rapid Spanning Tree Protocol (RSTP) and PRP for communications in electric substations.

In electric power systems, the standard IEEE 802.11 has been identified as unsuitable [54] due to its non-determinism and interference liability which involve packet loss, exceeded and variable latency times due to retransmissions. In order to overcome these limitations of IEEE 802.11, in [54] authors propose the utilisation of PRP over this technology.

The automotive industry is another sector demanding high resilience in its communications. In [55], authors intend to overcome the relatively high average error rate of wireless communications by introducing a hybrid scheme of redundancy combining information and temporal redundancy. They introduce an incremental redundancy retransmission scheme in conjunction with concatenated coding and show that this further improves the Deadline Dependent Coding (DDC) scheme resented by the authors in [56] for improving the reliability of real-time communication over a wireless channel.

3.4 DEMANDED KEY FEATURES FOR COMMUNICATION RESILIENT PROTOCOL FOR NEXT GENERATION ERTMS

As previously mentioned in Section 3.3, the demanded enablers that a resilient strategy should support to achieve the needed requirements in terms of dependability, security and performability, are defined by the ResiliNets design principles [2]. This section provides a tailoring of these enablers to the railway context. At the same time, this tailoring is adapted to the special requirements detected for end-host communication protocol stack which is envisaged to be resilient. Thus, we enrich the general enablers classification proposed in [2] by specifying their significance in the ERTMS context and introducing additional requirements.

In order to ensure the **Connectivity & association (CA)** requirement in ERTMS the main issue is to guarantee that messages will arrive within their lifetime to destination. In current communication networks, when the connection is not disrupted, the delay does not exceed this lifetime because modern Internet solutions have low delay comparing to the maximum accepted end-to-end

delay defined in Table 3.5. Therefore, the requirements in this sense are based on the performance of the communication protocols used at the end-host (RBC or OBU).

1. *End-to-end approach*. The evaluated technology should be end-to-end. That is, only end-hosts should be changed and connection should not be middle-box dependent.

2. *Middle-box compatibility*. High percentage of equipments on the current Internet and packet-switched networks are middle-boxes, e.g. Network Address Translation (NAT) equipments, firewalls, etc. The protocol chosen should be fully compatible with these middle-boxes to guarantee correct performance of communications.

The introduction of **Redundancy (R)** requirements into NGERTMS protocol stack would allow achieving higher levels of service performance reliability, reducing the time that the system will be in degraded mode. Within this general requirement we identify two specific requirements that must be demanded to the protocol under analysis:

3. *Redundancy capabilities*. The protocol should be able to perform multipath transmissions as a basis of transmission redundancy. That is, the protocol should allow delivering datagrams through all available interfaces over the same session.

4. *Flexibility of different delivery policies*: The redundancy policy should be able to be adapted to the specific needs of the application. In the redundant protocol to be implemented in the NGERTMS we envisage to allow three policies: 1) the active-passive delivery policy (1:1), which makes use of secondary channels only when the primary one fails; 2) the active-active delivery policy (1+1), which allows the delivering through all available channels concurrently; and 3) the utilisation of a single channel.

Closely related to the redundancy, the **Diversity (Di)** requirement reduces the possible correlated errors in the communication. This diversity requirement is achieved in communication networks by providing mechanisms of path diversity provisioning in the network.

5. *Path diversity*. The path diversity mechanisms are usually provided by network entities that split the redundant traffic through disjoint paths along the network. The achievement of this capability needs for interaction with a network entity that controls the network traffic routing. Additionally, diversity can be achieved by the use of multiple networks with different service providers. However, it is worth noting that although the access networks are provided by different service providers, the traffic in the core network could eventually share routes to the destination.

The **Self protection & Security (SS)** requirements involve the protection of data integrity, authenticity and confidentiality, as well as the automatic reaction against attacks. In ERTMS, these security requirements are addressed by the Euroradio SFM which is independent to the communication protocol. However, the redundant communication protocol should not add any additional security risk. In order to achieve these general requirements, the following specific requirements must be fulfilled:

6. *Dynamical interfaces/addresses configuration*. For redundant mobile communications, the capacity of adding new interfaces/addresses is essential to adapt to the path availability of each moment.

7. *Security*. It is important to have a mechanism to guarantee that both sides are who say they are during the connection establishment. The lack of this security could allow flow hijacking by an attacker.

The **Multilevel resilience (M)** mechanisms are summarised in Table 3.6. As we have commented before, the ERTMS protocol stack should be unaware and independent to the underlying wireless technology. Moreover, the resilience mechanisms in the physical channel and the link layer are out of the scope of our research work, due to the fact that they do not address the resilience need of the end-to-end communication. Other mechanisms, if not directly provided by the resilient protocol, they should be at least promoted allowing the interaction with other network elements.

The end-node should be **Context Awareness (CA)** in order to detect eventual disruptions and trigger different measures to overcome them. For this general requirement two are the specific requirements that a multihoming proposal should fulfil:

8. *Path state notion*. During multipath delivery, it is important to control each path's state to know if it is available or not, to avoid waste of resources with unavailable paths. It is also useful to control the state of each path to detect events that can affect the path's characteristics such as interferences or handoffs.

9. *Loss detection and retransmission*. The wireless communications in railway domain have a high data loss probability, when compared to a fixed communication link. Thus, a mechanism to detect losses and a correct retransmission policy are essential for correct performance.

The degree of abstraction and visibility between layers is named **Translucency (T)**. On the one hand, this requirement is tailored to the ERTMS use case by defining it as the abstraction of the underlying technology that enables to become ERTMS agnostic to the wireless technology. On the other hand, for ensuring the compatibility with existing applications, the evaluated proposal must be wrapped, but keeping the capability to interact with the application layer.

10. *Wireless technology agnosticism*. The NGERTMS must be independent to the underlying communication technology. Moreover, the mobility from one wireless technology to another (handover) should be transparent to the ETCS application.

11. *Application compatibility*. The inclusion of a redundant protocol in the NGERTMS architecture must be transparent for existing applications. Moreover, ETCS should be able to work with the new architecture without any change or adaptation. However, the redundant protocol should allow the cross-layer interaction with the application for allowing the exploitation of redundant capabilities by future ETCS versions.

Besides the introduced requirements, some **Additional implementation requirements (A)** are detected in order to deploy a resilient protocol successfully in NGERTMS:

12. *Backward compatibility*. The introduction of redundant protocol should not prevent ERTMS node from operating with any legacy standardised

protocol. It is worth pointing out that when we talk about legacy protocol we already assume the migration towards TCP/IP protocol stack.

13. *Maturity*. The maturity of the potential redundant protocol is essential in the selection of the appropriate candidate. The railway industry is known for the adoption of well trust reliable technology. The maturity evaluation of state-of-the-art protocols could be ambiguous. Therefore, we have adopted the classification presented in [57], which specifies five levels of maturity: 1) protocol tested in simulation, 2) protocol theoretically analysed, 3) protocol experimentally analysed, 4) protocol implemented in real world, and 5) protocol standardised as RFC. Moreover, for the evaluation of the maturity, the temporal evolution of the proposal must be analysed since it was proposed for the first time, until it was definitely standardised.

The evaluation of the candidate proposals present in the literature will be made in the next section using this set of requirements that we have defined as RRE. This set of requirements is summarised as a vector of the requirements associated to each resilience enablers, $RRE : \{CA, R, Di, SS, M, CA, T, A\}$.

3.5 MULTIHOMING AND MULTIPATH SOLUTIONS FOR COMMUNICATION REDUNDANCY

As it is stated in Section 3.2, one of the key enablers to achieve resilience is the redundancy. Moreover, in Chapter 1 the new trend of equipping multiple communication transceivers for heterogeneous networks has been introduced. This trend can be exploited for enabling the redundancy of the train-to-ground communications in the NGERTMS.

Multipath delivery strategies have been widely used for providing resilience in communication networks, especially for backbone networks. These strategies are mainly based on multipath routing algorithms [58], such as the ones applied over MPLS [59, 60] to improve the QoS metrics (delay, throughput, jitter, etc).

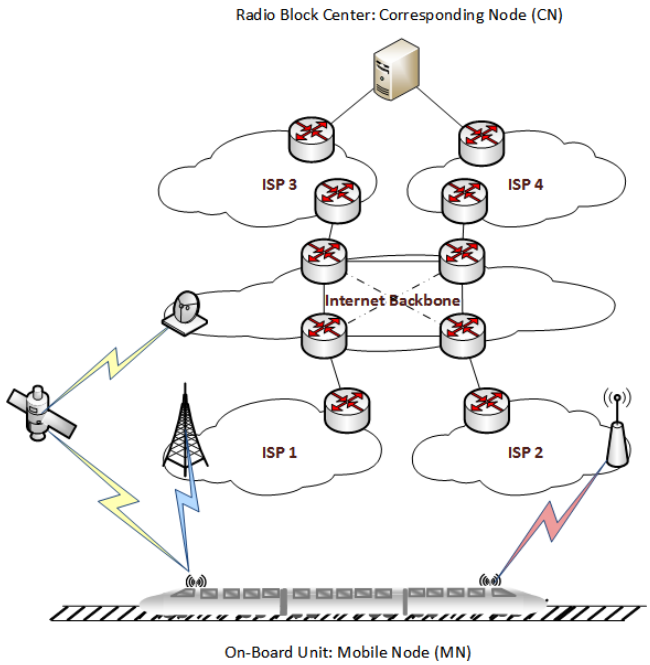


Figure 3.13.: Railway signalling Environment

In Figure 3.13 the future communication scenario of a train equipped with multiple transceivers is illustrated. This scenario will be used as a reference for the study made in this section. For this analysis, the terminology of network engineering has been adopted. Thus, the train's OBU has been referenced as Mobile Node (MN), whereas the RBC has been named as Corresponding Node (CN).

In this section we analyse the state of the art in multihoming and multipath proposals in order to evaluate the most suitable one for being used by the NGERTMS. This study of existing proposals is classified based on the OSI model layer where they operate as it is illustrated in Figure 3.14. As our goal is to increase the resilience of end-to-end connections, we analyse proposals that operate in the network layer or above. In the literature, other alternatives working bellow the network layer have been proposed [61] for the vehicular context. However, these alternatives do not have an end-to-end perspective of the communications. Each of evaluated proposals is set under analysis using the RRE requirement vector explained before.

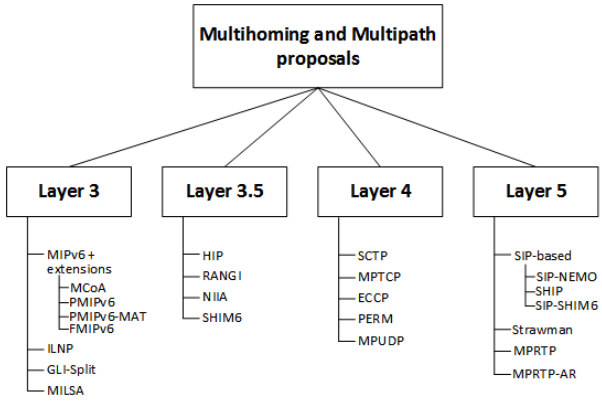


Figure 3.14.: Taxonomy of the proposals under analysis

3.5.1 Layer 3 proposals

Most multihoming proposals operating in layer 3 were originally designed to resolve the mobility problem of traditional IP networks. In IP architectures,

the network address is at the same time the identifier and the locator. Thus, when a host or a network changes its address, it changes both, the locator and identifier, breaking the ongoing sessions of transport layer. In order to address this problem, the Locator Identifier Split (LIS) concept has been widely use which is based on the decoupling of both functions in the network layer. As a result of this split the host or network is able to be identified with a single and static identifier, while multiple locators are added, allowing multihoming support.

In the following lines we analyse the most significant proposals which allow multihoming support in layer 3.

Solutions based on Mobile IPv6 (MIPv6)

Mobile IPv6 (MIPv6) [62] is not originally a multihoming protocol but a protocol to allow end-node mobility between different edge networks. However, some extensions of this protocol introduce multihoming. Therefore, it is interesting to analyse this protocol and its extensions within this evaluation of multihoming protocols.

MIPv6 was designed to provide mobility to Internet Protocol version 6 (IPv6) end-nodes following the same principle of existing Mobile IPv4 (MIPv4) protocol [63]. This principle consists on introducing a network element named Home Agent (HA) which links the address of the end-node in the foreign network, called Care-of Address (CoA), with its HA keeping the communication with a CN. This strategy has the side-effect known as "triangle routing" which is produced by the necessity to forward datagrams encapsulated from CN to MN via the HA. To reduce this routing inefficiency, MIPv6 introduces the route optimisation mechanisms that allow updating the CoA not only in the HA but also in the CN allowing the direct datagram exchange between MN and CN in both directions. However, MIPv6 does not support new addresses acting as the home address [64].

Multiple Care-of Address Registration (MCoA) [65] is an extension for MIPv6 that allows the MN to bind multiple CoAs with its HA. In order to distinguish uniquely each CoA Binding Identification (BID) is introduced. This extension make possible to use multiple network interfaces by the MN becoming it multihoming [66–69]. However, this multihoming support is limited to foreign

edge networks, as inside the home network all datagrams sent to the MN are routed through the same HA.

Proxy Mobile IPv6 (PMIPv6) [70, 71] introduces the mobility capability to regular IPv6 mobile with no mobility management protocol. This is made by introducing two network entities, Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG), which permit to delegate the mobility management to the network. The functionality of LMA is similar to the HA in MIPv6, whereas the MAG is the responsible to track the movement of the MN and update the routes to the MN in the LMA.

PMIPv6 enables the mobility, but it has limitations for supporting a host with multiple interfaces attaching to the PMIPv6 domain. In order to address this problem, Proxy Mobile IPv6 - MAG Address Translation (PMIPv6-MAT) has been proposed [72]. This proposal allows the continuous datagram delivery while handovers between heterogeneous access technologies are performed. In PMIPv6-MAT the LMA maintains binding entries for each interface and can sustain separate routes for each interface.

Fast Mobile IPv6 Handover (FMIPv6) [73] has been designed to overcome latencies of IP reconfiguration and to bind updates. The mobile source anticipates a handover, and receives its new CoA as part of a Fast Binding Acknowledgement (FBACK) prior to disconnecting. This make-before-break strategy enhances the handover process by allowing the registration of multiple CoA, becoming the node multihoming. However, during this process the tunnelling to a New Access Router (NAR) of one interface can incur performance degradation due to severe packet reordering when multiple interfaces are simultaneously used for load sharing. This is because the partial traffic flow coming from the interface involved in handover is suspended during this process and, later, tunnelled to a NAR, while the other partial traffic flow is continuously forwarded to the mobile node through other stable interfaces.

Identifier Locator Network Protocol (ILNP)

Identifier/Locator Network Protocol (ILNP) [74–77] addresses are split in two parts, the locator and the identifier. The locator is linked to the network topology and it can change when the end-node change from one network to another, whereas the identifier remains more static, at least while the transport

layer session is active. Although there are ILNP versions for IPv4 and IPv6, the last one offers further capabilities as it permits to keep the IPv6 header which enables the compatibility with non-ILNP architectures. By contrary, the IPv4 version needs for a new IPv4 Option to carry the Identifier values.

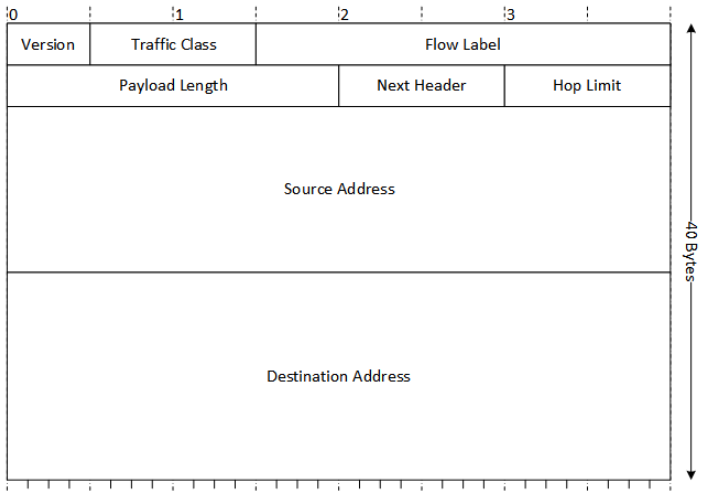
This new scheme assigns more than one valid locators to the multihomed end-nodes. When one stream connection fails, the node sends an Internet Control Message Protocol (ICMP) Locator Update message to each existing correspondent node to remove the unavailable Locator from the set of valid Locators. Thanks to this locator-identifier decoupling, ILNP permits to hide the multihoming to the transport protocol as it uses the identifier values for establishing its sessions. Moreover, ILNP enables multipath delivery without adapting the transport protocol. Thus, any transport protocol can use multiple paths concurrently, simply by using multiple (valid) locator values in that session's ILNP packets.

Global Locator, Local Locator, and Identifier Split (GLI-Split)

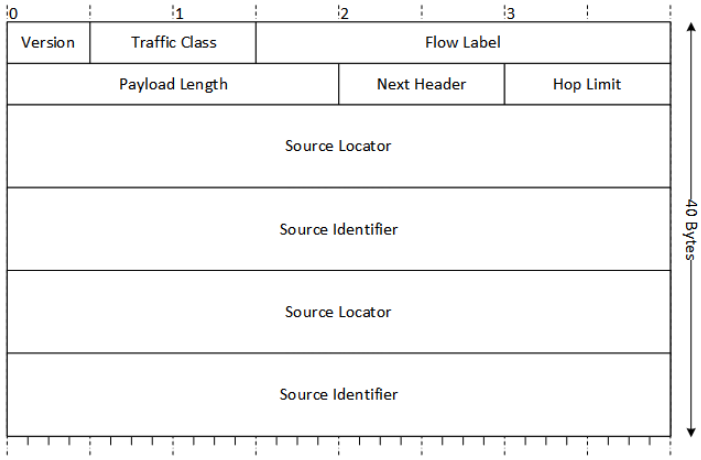
Global Locator, Local Locator, and Identifier Split (GLI-Split) [78], similar to ILNP, introduces the decoupling of locator and identifier functionalities of IP addresses. Nevertheless, GLI-Split splits the IP address into global locators, local locators, and identifiers with IDs that are independent of the current location. These IDs and locators are encoded in regular IPv6 addresses so that no new routing protocols are required. Thus, GLI-Split allows the backward compatibility with non-GLI-Split IPv6 nodes and network elements. Furthermore, the GLI-Split mechanism remains transparent for the transport layer which is only aware of the equivalent IPv6 address.

The splitting of the IPv6 address in three different GLI addresses is shown in the Figure 3.16. The 64 higher-order bits of each address are used for routing and special tasks, whereas the 64 lower-order bits contain an identifier. These addresses contain GLI-prefixes, used to differentiate them from other IPv6 addresses, and markers to determine whether the locator is local or global.

This protocol allows not only the network mobility, but also the multihoming, multipath-routing and traffic engineering. When source and destination networks are multihomed, multipath routing can be performed between the gateways of both networks. In order to do so, the GLI-node must request to the



(a) IPv6 header



(b) ILNP header

Figure 3.15.: IPv6 vs ILNP header

mapping system the global GLI-addresses of its domain and the one of the CN. Each combination of global source and destination GLI-addresses represents a different path. During the data delivery, the GLI-node selects the local GLI-

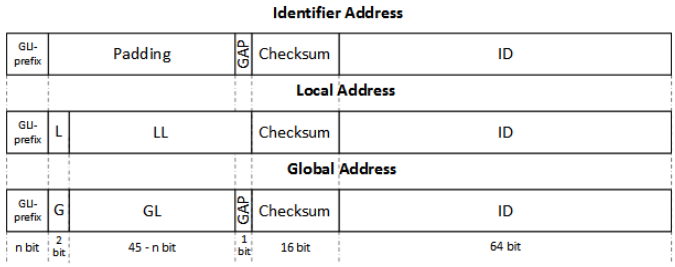


Figure 3.16.: GLI-Split addresses

gateway for its outgoing traffic and uses the appropriate global GLI-address for the destination node to select a specific GLI-gateway in the destination domain.

Mobility and Multihoming Supporting Identifier Locator Split Architecture (MILSA)

Mobility and Multihoming supporting Identifier Locator Split Architecture (MILSA) [79] similarly to GLI-Split and ILNP aims to provide mobility and multihoming support by decoupling the identifier and location functions of the network layer. This approach was firstly introduced based on the following main key designs [80]: a hierarchical identifiers system, a trust relationship based on the hierarchical structure, identifier-locator split and signalling and data plane separation. This original design permitted the use of applications, without any need to be modified, to benefit from this architecture. However, the proposed hierarchical identifiers were not compatible with legacy IP addressing.

From this proposal, the design of MILSA has been enhanced [81, 82] introducing a new MILSA identifier of 128 bits, compatible with IPv6 addressing.

In [79] the capability of MILSA for exploiting the path diversity through site multihoming is highlighted. Concretely, authors investigate the possibility of enabling multihoming networks to improve the performance of TCP connections coming from-to them by adding path diversity and enhancing the performance in case of path congestion/failure.

Requirements Analysis of Layer 3 proposals

As seen previously, MIPv6-based proposals have no end-to-end approach as they are all dependent of a HA or another middle-box such as a MAG or a NAR. However, as it keeps the structure of the IPv6 header, using the extensions headers for carrying the information related with mobility, they are fully compatible with network elements. From the redundancy capability point of view, MIPv6 has not a native redundancy support. However, the introduction of MCoA allows the multihoming support, associating different CoA to each network interface. In the case of FMIPv6 this multihoming support is exploited for performing fast handovers. As MIPv6-based proposals are designed for managing the node mobility, they are able to detect new interface configuration produced by the association of the node to a new network. This dynamic mechanism does not provide any security for preventing the session hijacking by an attacker. However, security mechanisms for authenticating the end-nodes can be deployed using Internet Protocol Security (IPsec) or another cryptographic algorithm at upper layers. These proposals do not implement any context awareness mechanisms as they are designed to manage mobility, delegating these functions to upper layers. MIPv6-based proposals fulfil all translucency requirements as they are all agnostic to the wireless technology and the application must not be adapted to exploit their functionalities. Moreover, they are all designed having in mind the backward compatibility, as soon as the legacy application is able to work with IPv6. Although presented proposals are stable RFC standards, the lack of any new proposal for exploiting their multihoming capability since 2009 illustrated in Figure 3.17 is considered a drawback. All in all, according this analysis, summarised in Table 3.7, the RRE vector defined in Section 3.4 has the following value (1):

$$RRE_{MIPv6} : \{1, 1, X, 1, X, 0, 2, 1\} \tag{1}$$

ILNP fulfils the connectivity and association requirements defined in Section 3.4 as it has an end-to-end communication approach and does not need from any intermediate network element. Additionally, as it introduces the identifier and locator respecting the IPv6 header structure, it is fully compatible with network middle-boxes. As mentioned above in Section 3.5.1, ILNP provides not only multihoming support, but also multipath delivery capability. However,

ILNP does not provide any flexibility for implementing different delivery policies. From the point of view of self protection and security, ILNP provides a mechanism for a dynamic interface configuration, but it does not implement any security mechanism delegating this function to upper layer protocols. Although ILNP is a layer 3 protocol, it makes a relative path state analysis as it detects the path failure and overcomes it sending ICMP Locator Update. However, it does not implement any loss detection and retransmission mechanism. Equally to MIPv6-based proposals, ILNP fulfils the translucency requirements, as well as the backward compatibility with no ILNP-capable nodes. The first reference to this proposal was in 2006 [77] and it was standardised in 2012, RFC6740. Recently, it has not been used as a referential multihoming/multipath protocol in any project. Taking all this into account the RRE vector for ILNP has the following value (2):

$$RRE_{ILNP} : \{2, 1, X, 1, X, 1, 2, 2\} \tag{2}$$

GLI-Split, as it follows a very similar approach to ILNP, has a very similar RRE vector. However, unlike ILNP, GLI-Split provides no path state awareness mechanism. Additionally, although GLI-Split was proposed more recently, in 2010 [83], there is no ongoing standardisation process. Actually, it has only been proposed in two papers [78, 83]. The RRE vector for GLI-Split has then the following value (3):

$$RRE_{GLI-Split} : \{2, 1, X, 1, X, 0, 2, 1\} \tag{3}$$

First MILSA proposal [80] introduced a disruptive hierarchical network architecture that was not fully compatible with IP nodes. However, this compatibility problem has been overcome in the last versions of the proposal [81, 82]. Nevertheless, the architecture makes use of intermediate network elements for the identifier/locator resolution. Thus, it has no end-to-end approach. MILSA fulfils almost the same requirements of ILNP with the exception of redundancy capability, which is not introduced, and the maturity, as since 2010 has not been used and has never been standardised. Comparing to other proposals, MILSA introduces a more sophisticate path state notion as it is able to detect failures and congestion situation of the TCP session and redirect the

traffic through other path, exploiting its multihoming capability. All in all, the RRE vector for MILSA has the following value (4):

$$RRE_{MILSA} : \{1, 0, X, 1, X, 1, 2, 1\} \tag{4}$$

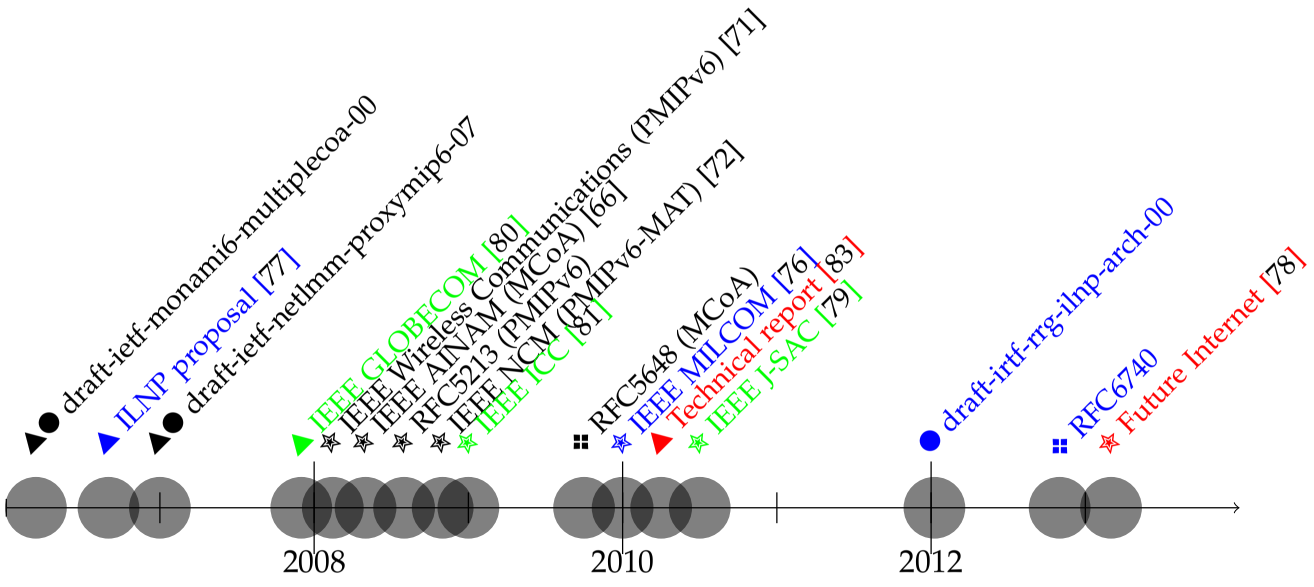


Figure 3.17.: Chronology graph of layer 3 proposals. ▲ refers to the First Publication. ● refers to the First Standardisation Draft. ❖ refers to the Standardisation (RFC). ✯ refers to the Last Publications. Technology by colour: MIPv6, ILNP, GLI-Split, MILSA.

Requirements		**Layer 3 proposals**			
		MIPv6 extensions	ILNP	GLI-Split	MILSA
General for resilience	**Specific for a redundant protocol**				
Connectivity & association (CA)	End-to-end approach	✗	✓	✓	✗
	Middle-box compatibility	✓	✓	✓	✓
Redundancy (R)	Redundancy capabilities	✓	✓	✓	✓
	Flexibility of different delivery policies	✗	✗	✗	✗
Diversity (Di)	Path diversity	-	-	-	-
Self protection & security (SS)	Dynamical interfaces/addresses configuration	✓	✓	✓	✓
	Security	✗	✗	✗	✗
Multilevel resilience (M)	Multilevel resilience (M)	-	-	-	-
Context awareness (CA)	Path state notion	✗	✓	✗	✓
	Loss detection and retransmission	✗	✗	✗	✗
Translucency (T)	Wireless technology agnosticism	✓	✓	✓	✓
	Application compatibility	✓	✓	✓	✓
Additional implementation requirements (A)	Backward compatibility	✓	✓	✓	✓
	Maturity	✓	✓	✗	✗

Table 3.7.: Requirement analysis of Layer 3 proposals

3.5.2 Layer 3.5 proposals

Several proposals in the literature are based on the introduction of an additional layer between the network and transport layers. These proposals were originally also designed mainly for providing mobility support. However, unlike the proposals working in the layer 3, the LIS concept is made by introducing an identifier in the layer 3.5, while the IP address is kept as network locator.

Host Identity Protocol

Host Identity Protocol (HIP) is defined in [84–87] and it has been proposed to solve limitations produced in the current Internet architecture by the dual role of IP. HIP is a protocol that works between the network and the transport level and identifies the host independently of the IP addressing. That is, a host can change the IP address or can have more than one assigned address with no effect to upper layer, because it is no longer identified by IP address. Instead, a Host Identity Tag (HIT) will be used, which is a generated combining a cryptographic hash of 100 bits, coming from host's public key, and a special prefix of 28 bits. This HIT, which has IPv6 format, is used by upper layers as a regular IP address, blinding the HIP functionalities to higher layers.

HIP has a native multihoming support and with a protocol extension proposed in [88], an end-user is also able to delivery concurrently through multiple available paths. As in this proposal IP addresses are used for routing and not as locators, the node that implements HIP has a native mobility support because the node can change the IP address, changing from one network to another, and it just must inform the other side with an address update message. Thus, the mobility, due to the physical movement of the user or due to connection disruptions in the preliminary network, is transparent for the transport layer protocol providing fault tolerance. The HIT-IP translation is made extending the functionalities of Domain Name System (DNS) [89]. However, DNS entries for locator resolution are not updated fast enough to face the host mobility, containing outdated entries. To solve this limitation, the RendezVous Server (RSV) extension was introduced [90], which stores the HIT and its associated IP addresses.

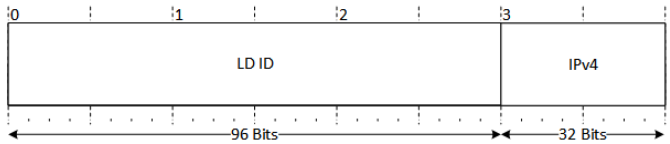


Figure 3.18.: RANGI's host locator structure

The biggest disadvantage of HIP is that both sides must have implemented the protocol to be able to communicate each other. Furthermore, network services, such as NATs and DNS name services, should be upgraded with HIP options in order to understand the protocol and do not drop its traffic, in the first case, and make the correct hostname-HIT translation in the second case.

Routing Architecture for the Next Generation Internet

Routing Architecture for the Next Generation Internet (RANGI) [91] presents an approach for LIS very similar to the one proposed by HIP. Like HIP, RANGI also introduces a host identifier layer between the network and the transport layers. However, unlike HIP, RANGI adopts a hierarchical and cryptographic host ID structure. This hierarchical structure is one of the main characteristics of RANGI. In fact, before being known as RANGI, this architecture proposal was named as Hierarchical Routing Architecture (HRA) [92]. RANGI uses IPv4-embeded IPv6 addresses as locator as illustrated in Figure 3.18.

For the host ID mapping, RANGI proposes a combination of two mapping system, one for Domain-Host ID and another for Host ID-Locator translation. For the first one, the use of DNS servers is proposed, whereas for the second mapping a distributed system can be used. When RANGI host moves from one network to another, it acquires a new locator that must be updated to the Host ID-Locator mapping server.

When a RANGI host is located in multihomed site, it can define the source locator that will be used for outgoing traffic. That is, traffic engineering to exploit multihoming can be made.

Node Identity Internetworking Architecture

Node Identity Internetworking Architecture (NIIA) was introduced [93–95] to allow routing along heterogeneous network domains. This proposal provides mobility and multihoming support based on the introduction of a new Node Identifier (NID) layer on top of the network layer. This way, a node with multiple interfaces can register in multiple locator domains at the same time. Unlike other approaches, NIIA needs for a changes in the current Internet routing architecture. The routing in this architecture is based on two approaches depending on the domain where it is applied. When routing is done within a local domain, the internal routing scheme is used wherever it is (e.g. IPv4, IPv6, MPLS, global and private address spaces, MAC addresses, etc). However, when traffic traverses different domains, the routing is only based on the NID of involved nodes.

The identifiers used in the NIIA proposal are based on cryptographic identifiers like in HIP in order to ensure end-to-end security.

Site Multihoming by IPv6 Intermediation

Site Multihoming by IPv6 Intermediation (Shim6) [96–98] is a multihoming protocol that, similarly to HIP introduces a new protocol layer between the network and transport layers. This new layer allows the application of LIS concept by introducing a new identifier name space known as Upper-Layer Identifiers (ULID). Therefore, the transport protocol session will remain working although the locator is changed in the network layer as the ULID is used for identifying the end-host, whereas the locator is used for the routing through each interface.

Shim6 provides loss detection and recovery functionalities by the Reachability Protocol (REAP) [99]. This detection can be performed in two ways; using keep-alive mechanisms that check the reachability of each destination locator, or using information of the transport layer. In any case, this functionality is independent to upper layer. Additionally, REAP also introduces recovery functionality through the detection of new locator pairs when failures occur. REAP protocol can be improved for faster detection of new locator during

node mobility [100]; however, some authors [98] have demonstrated that this detection is not fast enough for real-time applications.

Unlike HIP hosts, Shim6 hosts are able to communicate with non-Shim6 nodes due to its association process. It performs a 4-way handshake like in HIP, but the first two messages are used to check that both sides have Shim6 support and if not, conventional IPv6 is used. In affirmative case, the next two messages are used for exchanging locator sets.

The functionalities of Shim6 can be turned on/off from the application using an available API which allows the network interface management [101].

Requirements Analysis of Layer 3.5 proposals

Probably, the two most used protocols in the 3.5 layer which provide multihoming support are HIP and Shim6. All proposals working in the 3.5 level are designed with the philosophy of splitting the locator and identifier functions that currently fall to network layer. In order to do that, all of them introduce an additional identifier, whereas the IP addressing is kept. From the connectivity and association requirements point of view, HIP, RANGI, NIIA and Shim6 fulfil the end-to-end approach requirement, but not the middle-box compatibility. This is because the introduction of a new protocol between the network and transport layer is not always recognised by NATs and firewalls that are deployed to work with the standard TCP/IP protocol stack. Moreover, in the case of NIIA, a new internet routing architecture is introduced making more complex the interoperability with legacy networks. These protocols are designed mainly to provide secure mobility between different networks, so they all implement mechanisms for dynamical interface configurations and they are all agnostic to the wireless technology. By contrary, none of them implement loss detection and retransmission mechanisms, delegating these functions to upper layers. Additionally, all the presented proposals incorporate cryptographic end-to-end security mechanisms that prevent from session hijackings.

HIP protocol provides multihoming support, but by default it does not implement multipath delivery. However, the extension for implementing this capability, named Multipath Host Identity Protocol (mHIP), has been presented and deployed [102]. Thus, HIP can implement a failover multihoming

mechanism, as well as load-balancing using mHIP extension. However, neither HIP, nor mHIP, provides a flexible mechanism for setting up different delivery policies. HIP can maintain notion of the path state using heartbeat messages between HIP entities or analysing TCP traffic when this protocol is used at the transport layer. This protocol can be used by a legacy application able to work with IPv6, as the HIT used respects the IPv6 address format. However, one of the main inconvenient of HIP is that it is not backward compatible with non-HIP nodes, that is, both sides must understand HIP otherwise the communication will not occur. One of the positive aspects of HIP is its maturity, as it is not only standardised since 2008, but a new version of HIP is under standardisation process since 2015 as can be seen in the chronology graph of Figure 3.19. All in all, the RRE vector for HIP has the following value (5) according to Table 3.8:

$$RRE_{HIP} : \{1, 1, X, 2, X, 1, 2, 1\} \tag{5}$$

As commented previously in the description of RANGI, this proposal is very similar to HIP, but it differs with it in some point. Unlike HIP, RANGI does not have any extension for providing multipath capability. It only provides multihoming, but it is not able to deliver data concurrently through multiple interfaces. Another characteristic from HIP that it is not available in RANGI is the path state awareness. Like in HIP, backward compatibility is not fulfilled as both sides must understand RANGI protocol to communicate. However, the compatibility with legacy application is guaranteed as it uses IPv6 addressing as identifier/locator structure. Moreover, it uses IPv4-embeded IPv6 as locator address enabling its compatibility with IPv4 networks. From the maturity point of view, this proposal was published in 2008 and it started a standardisation process in 2009 without success. Since that moment, no new proposal has been made based on it. Thus, the RRE vector for RANGI has the following value (6):

$$RRE_{RANGI} : \{1, 0, X, 2, X, 0, 2, 0\} \tag{6}$$

NIIA proposal, like RANGI, supports multihoming but it does not implement multipath capability reducing the redundancy possibilities. It does not implement any path state awareness mechanism and it is not backwards compatible. However, like other proposals, it can be used with legacy applications as long as they are ready to work over IPv6. As it can be seen in the

chronology graph of Figure 3.19, this proposal was proposed for the first time in 2006 and its last mention was in 2010 with no standardisation process planned. Therefore it cannot be considered a mature technology, giving as result the following RRE value (7):

$$RRE_{NIIA} : \{1, 0, X, 2, X, 0, 2, 0\} \tag{7}$$

Last, but not least, the described Shim6 is one of the most prominent layer 3.5 multihoming protocol of the literature. It was standardised in 2009 and it is a mature technology used by many authors for enhancing the node mobility. It provides concurrent multipath capabilities, allowing using multiple interfaces for failover or load-sharing purposes. However, it is not possible to define new delivery policies to exploit this multipath capability. For the path state monitoring, it uses timestamps introduced in the transmitted packets and keep-alive messages, so it is able to detect path failure or a degradation of the channel conditions. Shim6 is designed to preserve the compatibility with legacy applications as well as with non-Shim6 equipment. However, for exploiting all multihoming capabilities, the use of a new API by the application layer is needed, and both sides must have Shim6 support. The RRE vector for Shim6 has the following value (8) according to Table 3.8:

$$RRE_{Shim6} : \{1, 1, X, 2, X, 1, 2, 2\} \tag{8}$$

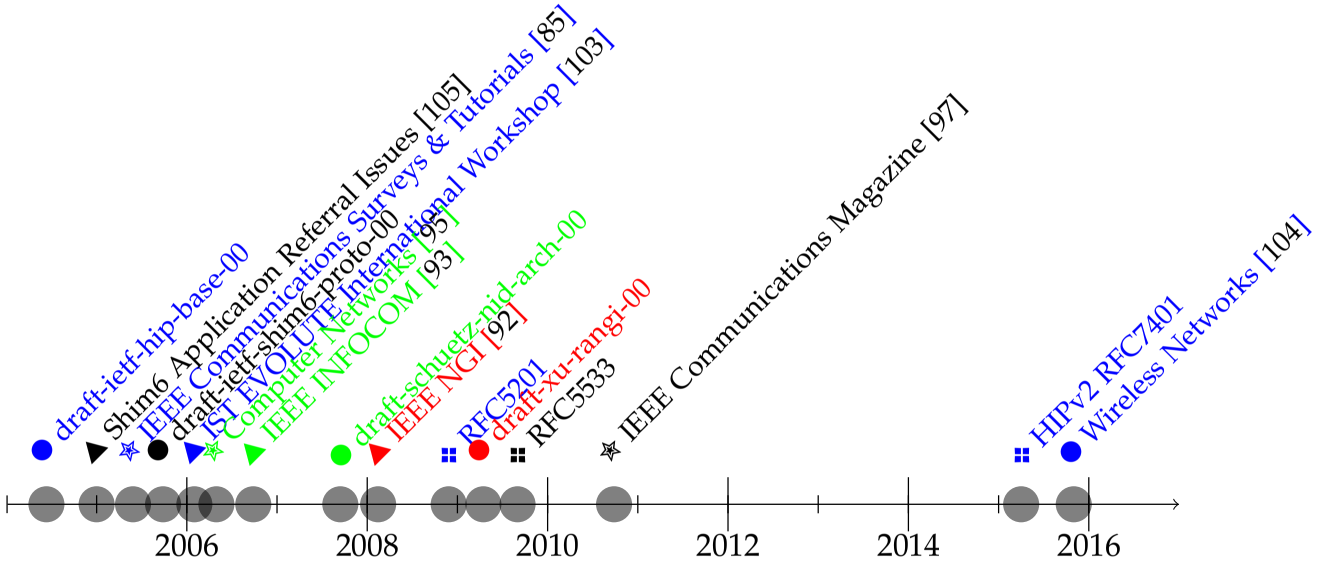


Figure 3.19.: Chronology graph of layer 3.5 proposals. ▲ refers to the First Publication. ● refers to the First Standardisation Draft. ❖ refers to the Standardisation (RFC). ✯ refers to the Last Publications. Technology by colour: SHIM6, HIP, RANGI, NIIA.

Requirements		Layer 3.5 proposals			
		HIP	RANGI	NIIA	Shim6
General for resilience	Specific for a redundant protocol				
Connectivity & association (CA)	End-to-end approach	✓	✓	✓	✓
	Middle-box compatibility	✗	✗	✗	✗
Redundancy (R)	Redundancy capabilities	✓	✓	✓	✓
	Flexibility of different delivery policies	✗	✗	✗	✗
Diversity (Di)	Path diversity	-	-	-	-
Self protection & security (SS)	Dynamical interfaces/addresses configuration	✓	✓	✓	✓
	Security	✓	✓	✓	✓
Multilevel resilience (M)	Multilevel resilience (M)	-	-	-	-
Context awareness (CA)	Path state notion	✓	✗	✗	✓
	Loss detection and retransmission	✗	✗	✗	✗
Translucency (T)	Wireless technology agnosticism	✓	✓	✓	✓
	Application compatibility	✓	✓	✓	✓
Additional implementation requirements (A)	Backward compatibility	✗	✗	✗	✓
	Maturity	✓	✗	✗	✓

Table 3.8.: Requirement analysis of Layer 3.5 proposals

3.5.3 Layer 4 proposals

Stream Control Transmission Protocol

SCTP [106–109] is a connection-oriented transport protocol as TCP, but its connection conception goes further than TCP's. SCTP creates a connection between SCTP endpoints which can include multiple IP addresses combined with SCTP ports where packets can be transmitted with assured reliability. That is, its native multihoming support is one of its basis for connection reliability. As multiple paths can be established within a single connection, the protocol defines control messages, heartbeats, to check the status of each path (active or inactive). Moreover, as SCTP uses Selective Acknowledgement (SACK) mechanism, it is able to measure accurately the RTT of each path. By default, only the primary path is used for data delivery, and only in case this path fails; alternative paths are used as a fault tolerance mechanism. This delivery change is done by SCTP automatically and in a transparent way for the application. However, the application must be adapted to work with SCTP as its socket definition is different to the ones for TCP and User Datagram Protocol (UDP). The failover mechanisms of SCTP are analysed in-depth in the PhD thesis [110], which proposes SCTP as transport layer multihoming protocol for providing end-to-end network fault tolerance and improved application performance. Taking the native multihoming support of SCTP as a reference, some extensions to the protocol have been proposed for adding multipath support [111, 112], as well as for handling the mobility [113–115]. This is the case of Concurrent Multipath Transfer (CMT) extension [116] and the Dynamic Address Reconfiguration extension [115] respectively. In [117] another concurrent multipath transfer scheme is proposed that makes uses also of address dynamic configuration to perform seamless vertical handovers. The first one makes use of different available path for delivering data concurrently through them. The second one permits the IP address reconfiguration allowing the change from one network to another transparently for the application. The biggest handicaps of SCTP are two. One is the lack of compatibility with the current middleboxes present in the current networks, such as NATs and firewalls, which don't understand SCTP and can drop SCTP messages. The second one is the lack of compatibility with legacy applications due to the

differentiated interfaces used by SCTP for communicating with applications with respect to ones used by TCP and UDP.

Multipath Transmission Control Protocol

MPTCP [118, 119] has been created as an extension to the well known reliable transport protocol TCP and it allows creating simultaneously multiple communication paths over the same logical connection between two end-hosts. As MPTCP is an extension, both sides have to inform each other if they are capable to understand MPTCP or if they only understand regular TCP protocol. This information is shared during the first TCP connection establishment, adding the information to the TCP header options. MPTCP works at the transport layer of the TCP/IP protocol stack and it obtains an abstraction of the eventual changes that can happen in the network layer such as the address change produced by network mobility. This abstraction hides to upper layers the possible faults occurred at underlying levels to the transport protocol. Thus, it is not required to change the application to benefit from MPTCP functions. However, for a full control of MPTCP functionalities from the application, a special API has been released [120].

MPTCP manages the reaction against failures redistributing the traffic through alternative paths providing fault tolerance to serve applications. Thanks to this capability MPTCP is able to keep the service working without any interruption. Additionally to the multihoming and multipath support, MPTCP specification lets open the delivery policy to use by the implementation. This way, this policy can be designed to fulfil resilient services adapting the subflow selection whereby the end-host will deliver the service data in accordance to different networks' state. Thus, MPTCP permits the pre-emption of some paths from another for achieving the best recovery policy after a network failure is detected. By default, MPTCP delivers data segments through the subflow with lowest SRTT and the congestion control across subflows is presented in [121].

Likewise MPTCP, other approaches before intended to provide multihoming support through the utilisation of multiple TCP flows. This is the case of Multiple TCP Fairness proposal [122] which allows the application to employ multiple TCP instances. The issue with this approach resides on the independence of each data path. For instance, it is hard to guarantee that

multiple TCP instances do not use more bandwidth than a single TCP instance over the path. Another variant of TCP with the same goal was presented in [123], which uses Fast TCP [124] as a base for introducing multihoming support, but which is sensitive to throughput problems, namely, on network congestion situations.

Taking MPTCP as a reference, multiple proposals have been made for improving network reliability in heterogeneous networks. One of most relevant approaches is the use of Network Coding (NC) in combination with MPTCP [125, 126]. This approach incorporates the previous knowledge of Network Coding in regular TCP [127, 128], consisting on delivering information of previous packets so that in case of message corruption or loss, the message can be recovered without triggering retransmissions. Special interest of this technology combination has been shown for mobile devices working over heterogeneous [129] and mesh networks [130]. However, the advantage of NC cannot be exploited in the specific case of ERTMS as the interval between consecutive ETCS messages is so long and the message size so small that the fact of sending this additional information does not provide any additional benefit with respect to the simply duplicate delivered packets. Moreover, it would produce higher computational cost, therefore higher delay.

End-to-end Connection Control Protocol

The End-to-end Connection Control Protocol (ECCP) [131] is a protocol that works under the transport layer and it allows hosts to communicate over multiple interfaces seamlessly to the transport protocol. Its conception is similar to HIP protocol because it creates a new local identifier for each flow that hides the different connections that are associated to the flow. This flow identifier is local, so each end-host has its own one for identifying the flow in its side. Thus, to keep coherence in the subflow, both sides must exchange their flow identifiers during a flow establishment process. Unlike layer 3.5 proposals, such as HIP, ECCP deals with the connection control instead of creating a new host identifier for satisfying LIS concept. Moreover, ECCP does not need any special host identifier; it only needs a destination host address to initiate the connection. During the establishment process a list of available interfaces of each end-host is

also exchanged, so that after the flow is established, different associated subflow can be created using these addresses.

Like HIP, ECCP does not define any reliability or congestion control mechanism by itself. Instead, it relies in the existing transport layer below to perform these functions. In ECCP, the IP addresses associated to a subflow and the addresses added to the available address list can be changed on-the-fly with no service disruption thanks to a resynchronise protocol used for updating peers when the end-host changes its addresses.

Practical End-host Multihoming

Practical End-host Multihoming (PERM) [132] is a proposal that permits the flow scheduling in multihomed hosts. The goal of this proposal is to allow end-users to share their Internet connections in residential networks, this way enhancing the connection performance. The particularity of PERM is that it analyses the end-users' networking behaviour and based on it, it exploits the recognised patterns for improving the connection performance by adopting different scheduling policies at the flow level. This proposal supports three general functionalities; the detection of new flows request and its binding to a link, the monitoring of link performances and the flow decision for scheduling traffic.

PERM's implementation is designed as an extension of Linux socket API which incorporates the following six components:

- *Connection Manager* - This element intercepts calls to the socket API and it triggers the flow scheduling.
- *Monitor* - It monitors the link state for detecting failures and for estimating its capacity and latency.
- *User Traffic Prediction* - It is used for determining the amount of traffic that will be introduced in the flow before the flow is scheduled.
- *Incentive Management* - This component monitors the Internet connection and interacts with other user's PERM's managers for exchanging the scheduling information.

- *Privacy and Security* - Its enforce privacy by preventing neighbours from gaining unintended access to important sites through the local connection.
- *Flow Scheduling* - Depending on the estimated flow volume, the load of a link and the respective associated RTT, PERM adapts between scheduling based on latency for light-volume flows and scheduling based on estimated transmission time for load balancing among heavy-volume flows.

Multipath UDP

An approach for multipath scheduling for UDP is introduced in [133]. This proposal, unlike others presented above, is not a protocol or new layer but an algorithm for addressing the delivery problem under UDP. In fact, this proposal can be considered as a cross-layer approach as it is the IP layer of the sender the responsible of splitting the traffic between available paths. However, as the end-to-end streaming mechanism for forwarding packets over different interfaces is based on transport protocol peculiarities, we have categorised it as a layer 4 proposal.

The main goal of this approach is to facilitate UDP to schedule transmission of packets over multiple paths in such a way that they are received at the destination in-order while imposing the minimum overall delay on the receiver's application. In order to do that, the packets are reordered in the sender based on the transmission delay of its path and they are consequently delivered for achieving the goal mentioned before. The main drawback of this proposal is that, in order to perform the reordering in the sender, data must be available before the transmission begins. Therefore, big buffers are needed in the sender, and more important, the approach affects directly to application with high delay constrains, such as the railway signalling.

Requirements Analysis of Layer 4 proposals

All described proposals share common characteristics for being protocols working in the layer 4, such as the end-to-end approach and their agnosticism with the underlying wireless technology. According to the chronology graph

illustrate din Figure 3.20, from introduced proposals the only two that can be considered mature are SCTP and MPTCP. ECCP has been formally verified, but since it was proposed in 2012, no other work has been presented based on it. Another point coincident between almost all proposals of this section is their compatibility with legacy middle-boxes, e.g. NATs and firewalls, with the exception of SCTP. The main problem of SCTP in this sense is its moderate deployment in current networks comparing to TCP and UDP. Consequently, many NATs and firewalls do not understand this protocol. By contrary, MPTCP, PERM and Multipath UDP (MPUDP) make use of regular TCP and UDP packets to their traffic, which both are compatible with these equipments. In the case of ECCP, although it introduces new headers, it is encapsulated over UDP packets to avoid compatibility problems. All of these proposals provide not only multihoming support, but also multipath feature. In some cases, such as SCTP and MPTCP, the delivery policy can be adapted being available different schedulers, i.e. round-robin, bandwidth aware, load-sharing, etc. In ECCP and MPUDP this feature is not introduced, whereas in PERM a new hybrid scheduling is incorporated which decides the path to be used depending on channel conditions and application needs.

MPTCP, SCTP and ECCP, unlike MPUDP and PERM, have mechanisms for the dynamic interface configuration. In fact, PERM has been designed for residential purposes where the change of address configuration as a consequence of mobility is not common. MPTCP, SCTP and ECCP make use of random keys, nonces, exchanged during the session establishment for preventing session hijacking. However, this mechanism only protects from off-path entities, i.e. entities that are not aware of these nonces. PERM incorporates a more sophisticated privacy enforcement mainly designed to hide user traffic pattern between neighbours sharing the same connection.

SCTP is a reliable transport protocol; therefore its multipath extensions have native loss detection and retransmission mechanisms. Additionally, for the detection of path state, SCTP uses heartbeat messages. The main backward of SCTP is the lack of compatibility with former applications. The use of an API designed for SCTP is mandatory, being necessary to adapt former applications to work with it. Additionally, the multipath extensions of SCTP do not introduce any backwards compatibility mechanism during the session establishment,

while they introduce a subflow level sequence numbering, making them incompatible with regular SCTP. The main advantage of SCTP is its maturity as it has been standardised and many works are present in the literature for its use as multipath protocol. All in al the RRE vector of SCTP has the following value (9):

$$RRE_{SCTP} : \{1, 2, X, 2, X, 2, 1, 1\} \tag{9}$$

MPTCP differs from SCTP in the implicit mechanism it uses for detecting the path state. MPTCP makes use of subflow SRTT for being aware of its state. MPTCP, likewise SCTP, has loss and retransmission mechanism as it is an extension of the reliable transport protocol TCP. Unlike SCTP, MPTCP is designed for being compatible with existing applications, and for keeping the backward compatibility with regular TCP. In order to guarantee these two compatibilities, MPTCP uses the default TCP/IP API and incorporates a negotiation during the session establishment where the MPTCP capability is advertised to the other side. When this capability does not exist in both sides the session is established as a regular TCP. MPTCP is standardised and it is being incorporated by the industry for mobile devices where vertical handovers are common; and data centres, where the load-balancing provides reliability and higher throughput. The RRE value for MPTCP has the following value (10):

$$RRE_{MPTP} : \{2, 2, X, 2, X, 2, 2, 2\} \tag{10}$$

ECCP does not provide any path state awareness mechanism, but it provides a loss detection and retransmission mechanisms based on timeouts. From the compatibility point of view, as ECCP is located below TCP, the used API by the applications remains. However, both sides must understand ECCP in order to communicate each other as the ECCP node introduces ECCP headers that would not be understandable for non-ECCP node. From the maturity point of view, although ECCP has been formally verified, it has never been standardised and, since 2012, no reference to ECCP has appeared in the literature. The RRE value for ECCP corresponds to the following value (11):

$$RRE_{ECCP} : \{2, 1, X, 2, X, 1, 2, 0\} \tag{11}$$

PERM provides a mechanism for detecting the path state, actually this measurement is the base for its hybrid flow scheduler. However, it delegates

the loss detection and retransmission to the transport protocol. PERM nodes are able to communicate with non-PERM nodes as this protocol only change the scheduling in the sender without altering the packet. Nevertheless, to use PERM in a node, new API is required, that is, PERM is not compatible with legacy applications. PERM has not been standardised and, since it was presented in 2006, it has not been used any more. Thus it cannot be considered a mature protocol. The corresponding RRE vector for PERM is (12):

$$RRE_{PERM} : \{2, 2, X, 1, X, 1, 2, 0\} \tag{12}$$

Last but not least, MPUDP incorporates a path awareness mechanism based on the measurement of the paths' RTT. However, it does not introduce any loss detection and retransmission mechanism, delegating these functions to upper layers. MPUDP guarantees the backward compatibility with both, legacy applications and non-MPUDP nodes. This proposal, although its last reference in the literature was in 2015, it has not been standardised, so it cannot be considered mature enough. The RRE vector for MPUDP has the following value (13) according to Table 3.9:

$$RRE_{MPUDP} : \{2, 1, X, 0, X, 1, 2, 1\} \tag{13}$$

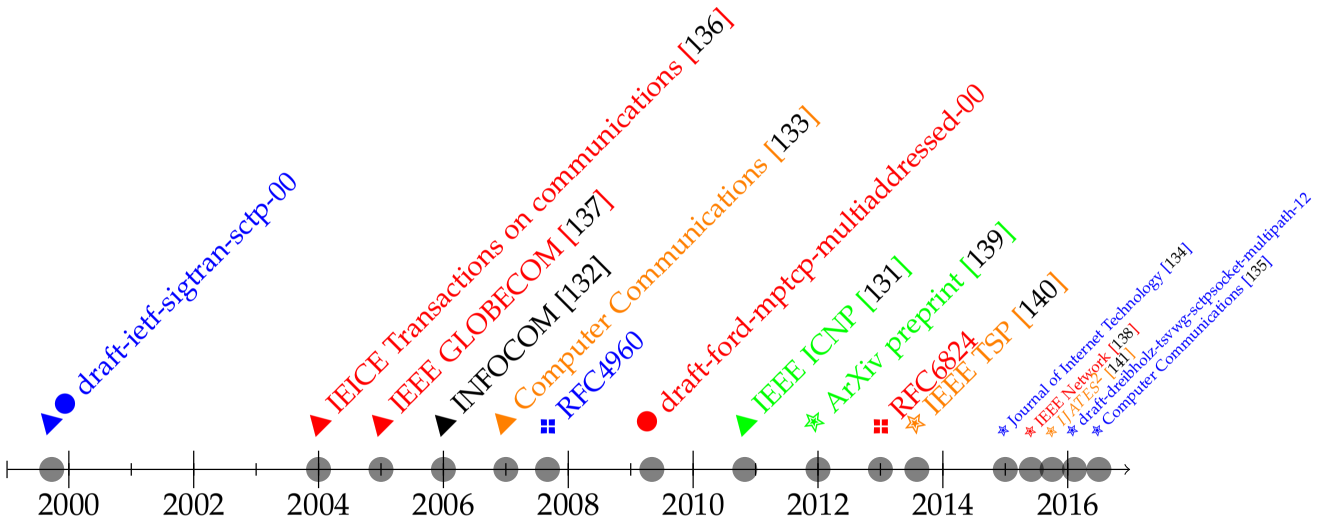


Figure 3.20.: Chronology graph of layer 4 proposals. ▲ refers to the First Publication. ● refers to the First Standardisation Draft. ❖ refers to the Standardisation (RFC). ✯ refers to the Last Publications. Technology by colour: PERM, SCTP, MPTCP, ECCP, MPUDP.

Requirements		**Layer 4 proposals**				
		SCTP	MPTCP	ECCP	PERM	MPUDP
General for resilience	**Specific for a redundant protocol**					
Connectivity & association (CA)	End-to-end approach	✓	✓	✓	✓	✓
	Middle-box compatibility	✗	✓	✓	✓	✓
Redundancy (R)	Redundancy capabilities	✓	✓	✓	✓	✓
	Flexibility of different delivery policies	✓	✓	✗	✓	✗
Diversity (Di)	Path diversity	-	-	-	-	-
Self protection & security (SS)	Dynamical interfaces/addresses configuration	✓	✓	✓	✗	✗
	Security	✓	✓	✓	✓	✗
Multilevel resilience (M)	Multilevel resilience	-	-	-	-	-
Context awareness (CA)	Path state notion	✓	✓	✗	✓	✓
	Loss detection and retransmission	✓	✓	✓	✗	✗
Translucency (T)	Wireless technology agnosticism	✓	✓	✓	✓	✓
	Application compatibility	✗	✓	✓	✗	✓
Additional implementation requirements (A)	Backward compatibility	✗	✓	✗	✓	✓
	Maturity	✓	✓	✗	✗	✗

Table 3.9.: Requirement analysis of Layer 4 proposals

3.5.4 Layer 5 proposals

SIP-based solutions

Session Initiation Protocol (SIP) works in the application layer and has been designed for establishing, modifying and closing end-to-end sessions for multimedia applications. SIP is not a multihoming protocol as it has not the capability for working simultaneously with multiple network instances. However, it decouples the node identifier and the network address using Uniform Resource Identifier (URI)s for its identification process. Due to this fact, SIP eases the dynamical change of network address enhancing the mobility performance [142].

Although SIP is not a multihoming protocol, it has been widely proposed as an enabler for enhancing other multihoming protocols' performances. This is the case of [143] which intends to enhance the Media Independent Handover (MIH)-based [144] network mobility by introducing SIP. This proposal works as follows, when SIP-Network Mobility (NEMO) is used, the mobile node establishes a session with the corresponding node and the SIP Network Mobility Server (SIP-NMS) - which can be seen as the multihomed gateway of the mobile network - registers this session in its session list. The status of each session of the list is controlled using the real-time signalling received from MIH. This way, when an event occurs, such as the progressive degradation of the used network, the SIP-NMS receives and checks if there is any existing session using the affected interface, if so, it can determine the most suitable alternative interface based on session information. After a new interface is selected, the SIP-NMS sends an INVITE request and re-registers itself with the URI of the selected interface.

Another proposal based on SIP was introduced in [145] and aims to combine SIP and HIP capabilities to provide a full mobility management for services between heterogeneous wireless IP networks. The proposed hybrid SIP-HIP scheme proposed works for all services and not only for applications that use SIP sessions. Moreover, according to the authors [145], Hybrid SIP and HIP (SHIP), comparing with SIP, has better performance in handover's signalling, whereas its signalling overhead is smaller.

In addition to the previous proposals, in [146] an approach for exploiting mobile multihomed terminals based on SIP and Shim6 is proposed. In order to do so, the authors of this paper [146] propose the combination of Shim6 multihoming protocol with the IP Multimedia Subsystem (IMS) [147] architecture. These two technologies provide seamless handovers and multimedia session with QoS respectively. Thus, this proposal enhances the Shim6 handover process by deploying a session renegotiation based on SIP which ensures the QoS of the service.

Strawman architecture

For the splitting of an application flow across several physical layers the Strawman architecture was proposed [148]. Unlike other multihoming proposals, the Strawman architecture works in the session layer. This way, the application flow can be (de)multiplexed in different transport instances using one or multiple interfaces. One of the main advantages of this proposal is that the multihoming support can be provided without any specific transport protocol. Another significant advantage is that the Strawman architecture could select the most suitable underlying transport protocol to work with, in order to achieve the service's requirements (reliability, throughput...) of the application layer.

Multipath Real-Time Transport Protocol

Multipath Real-time Transport Protocol (MPRTP) [149] is an extension of the Real-time Transport Protocol (RTP) [150] protocol that enables the use of multiple interfaces by creating concurrently different RTP flows through them, as it is illustrated in Figure 3.21. MPRTP, equally to RTP, is a protocol which works above the transport layer and used mainly by multimedia applications (see Figure 3.22). This protocol has been designed using many of the knowledge acquired in the deployment of MPTCP. It pays special attention in the backwards compatibility, for both, the legacy applications and existing network elements such as NATs and firewalls. In order to do so, MPRTP creates a well formed RTP flow through each interface. Thus, for the network middle-boxes, MPRTP traffic acts as a regular RTP one.

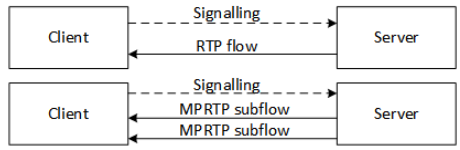


Figure 3.21.: Comparison between traditional RTP flow and Multipath RTP

Two valid ways for session signalling are available in MPRTP: in-band and out-of-band signalling. Within this signalling, MPRTP nodes exchange, among other data, the available interfaces of each node. In-band signalling refers to the use of RTP mechanisms for exchanging this information. In this case, the Real-time Control Protocol (RTCP) header must be extended. By contrary, out-of-band signalling refers to the use of a separate signalling connection (via SIP, RTSP, or HTTP) to exchange interface information.

For the data delivery, as MPRTP splits the traffic across multiple interfaces, RTP header is extended to allow subflow-specific sequence numbers to help calculating fractional losses, jitter, RTT, etc, in order to ease path selection, load balancing and fault tolerance decisions.

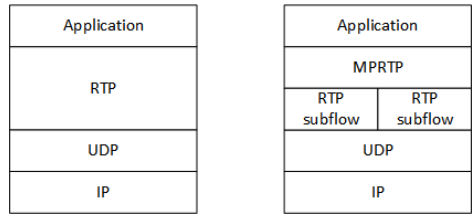


Figure 3.22.: Comparison between traditional RTP and Multipath RTP protocol stack

The MPRTP layer performs the following functions:

- Path Management - The layer is aware of alternate paths to the other host, enabling the end-host to transmit differently marked packets along separate paths. MPRTP also manages the port and IP address pair bindings for each subflow to send and receive data.

- Packet Scheduling - The layer splits a single RTP flow into multiple subflows. This load splitting can be done different scheduling approaches (load balancing, fault tolerance, etc).
- Subflow recombination - The layer creates the original stream by recombining the independent subflows. Thus, the multipath delivery is transparent for upper layers.

Multipath Real-Time Transport Protocol Based on Application-Level Relay (MPRTP-AR)

Another proposal to provide multipath support for multimedia applications is named MPRTP-AR [151]. This protocol is based on the framework of Multipath Transport System based on Application-level Relay (MPTS-AR) [152], which can provide multipath support for many application scenarios, including point-to-point, many-to-one and one-to-many communications.

MPRTP-AR protocol is located between the transport and application layers and it consists of two sublayers: the RTP sublayer and the Multipath Transport Control (MPTC) sublayer. As it is shown in Figure 3.23 the MPRTP-AR architecture is fully compatible with the existing RTP applications, as it makes use of the same API. Unlike MPRTP, MPRTP-AR makes use of intermediate entities, named RTP relay nodes (see Figure 3.24), for creating multiple relay paths between the sender and the receiver.

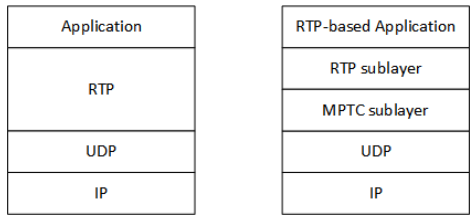


Figure 3.23.: Comparison between traditional RTP and MPRTP-AR protocol stack

The MPTC sublayer provides all functions related with multipath support, such as the path management, the flow splitting, subflow reporting, which is used to control the path state. This sublayer formats RTP packets into MPRTP-AR data packets adding a MPRTP-AR header. As this proposal introduces

the capability to delivery RTP packets through different paths, Subflow-Specific Sequence Number (SSSN) must be introduced. Additionally, a mechanism for controlling alive paths, based on keep-alive packets, is used.

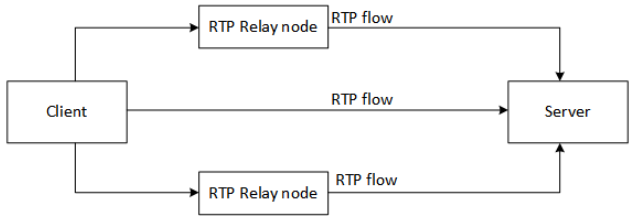


Figure 3.24.: A point-to-point MPRTP-AR session

When multiple subflows are used in MPRTP-AR, the flow partitioning can be performed based on payload coding scheme or path characteristics, adapting the scheduling to the requirements of the application layer.

Requirements Analysis of Layer 5 proposals

As it is depicted in Table 3.10, all described proposals share some characteristics as they all work in the layer 5 of the TCP/IP protocol stack. For example, they all are compatible with network middle-boxes, because these elements usually analyse the network traffic until the transport layer omitting any checking to upper layers' information. Moreover, for the MPRTP and MPRTP-AR cases, they transmit regular RTP flows along the network, so their functionalities are transparent for network elements. All these proposals have an end-to-end approach in their design, except MPRTP-AR, which delegates the multipath functionality to intermediate application relays. Strawman architecture, MPRTP and MPRTP-AR have been designed to provide multipath support. By contrary, SIP does not provide multipath nor multihoming support, but it eases the implementation of other underlying multihoming protocols, such as HIP or Shim6, by providing new method for updating locator-identifier association. All analysed proposals incorporate mechanisms to be aware of the path state. However, in terms of security, none of them provides any security mechanism to prevent session hijacking. It is worth noting that, in the case of MPRTP and MPRTP-AR, it is expected to analyse their security implication but at the time

of writing these lines this work was not made. From the translucency point of view, both the wireless technology agnosticism and the legacy application compatibility requirements are fulfilled by all proposals. These compatibilities are fulfilled thanks to the use of standard API, on the one hand, and for using standard TCP or UDP protocols in the transport layer, on the other.

Described SIP-based proposals do not introduce capabilities to define different delivery policies, but it facilitates the dynamical interface configuration to underlying protocols. These proposals do not provide loss detection and retransmission functionalities, as they rely on the transport layer for this goal, neither backwards compatibility. SIP is a mature standard widely used on the Internet, mainly for multimedia applications, but the proposals that integrate SIP with multihoming protocols are not standardised so they cannot be considered mature. In summary, the RRE value for SIP-based proposals is described with the following vector (14):

$$RRE_{SIP} : \{2, 1, X, 1, X, 1, 2, 0\} \tag{14}$$

The Strawman architecture, unlike SIP-based proposals, provides the possibility to decide the delivery policy depending on the requirements that are expected to be fulfilled e.g. throughput, reliability, etc. Similar to SIP-based proposals, the Strawman architecture is able to dynamically configure interfaces but it does not provide loss detection and retransmission mechanisms. This architecture must be implemented in both sides in order to be able to assemble the traffic, which has been split in different subflows. However, it does not deploy any negotiation to decide whether the architecture will be use or not. Thus, it is not backward compatible. This proposal was presented in 2006 and, as it illustrates the graph of Figure 3.25, since then, no other paper has been published. Therefore, it cannot be considered a mature proposal. All in all, the RRE for Strawman architecture can be summarised in the following vector (15):

$$RRE_{Strawman} : \{2, 2, X, 1, X, 1, 2, 0\} \tag{15}$$

MPRTP also incorporates a mechanism for the dynamic address configuration, different delivery policies and loss detection and retransmission mechanism inherited from regular RTP protocol. In the session establishment between two MPRTP nodes, they inform each other about their MPRTP capability and if

both sides do not have multipath support they perform a regular RTP session. MPRTP is a proposal with great potential but it is still within a definition stage. Therefore it is too early to be classified as a mature proposal. The RRE value of this proposal is expressed in the following vector (16):

$$RRE_{MPRTP} : \{2, 2, X, 1, X, 2, 2, 1\} \tag{16}$$

MPRTP-AR proposal is similar to MPRTP but it does not provide flexibility to implement different delivery policies, nor dynamic interface configuration. This proposal also provides loss detection and retransmission mechanism inherited from RTP and it is backward compatible with legacy RTP nodes. Like MPRTP, MPRTP-AR is still under definition at very early stage, so many points of its design are open. Therefore, the RRE analysis for this proposal can be summarised in the next vector (17):

$$RRE_{MPRTP-AR} : \{1, 1, X, 0, X, 2, 2, 1\} \tag{17}$$

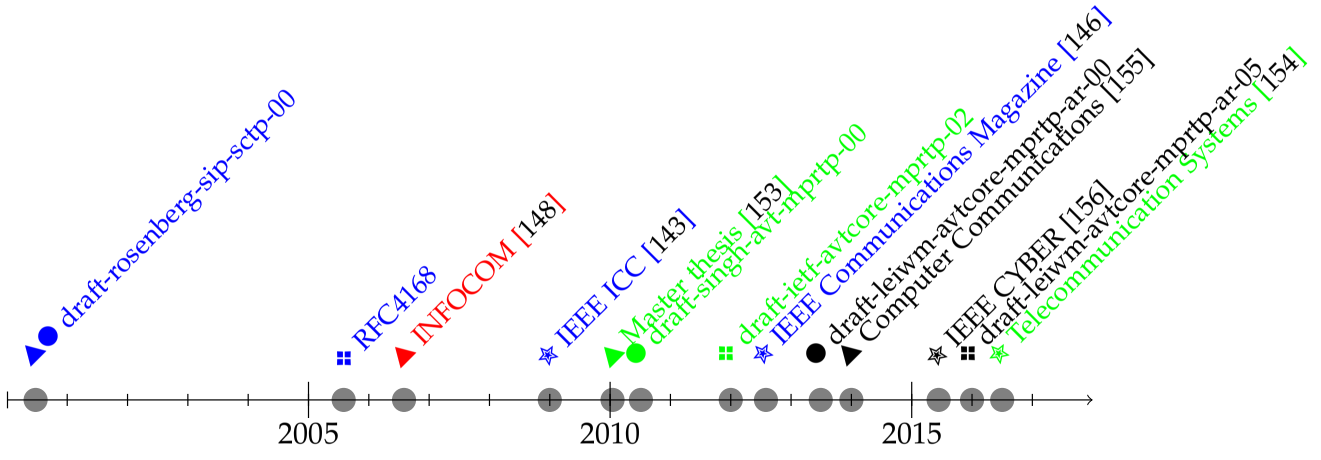


Figure 3.25.: Chronology graph of layer 5 proposals. ▲ refers to the First Publication. ● refers to the First Standardisation Draft. ❖ refers to the Standardisation (RFC). ✯ refers to the Last Publications. Technology by colour: MPRTP-AR, SIP-based, Strawman, MPRTP.

Requirements		**Layer 5 proposals**			
General for resilience	**Specific for a redundant protocol**	SIP-based solutions	Strawman architecture	MPRTP	MPRTP-AR
Connectivity & association (CA)	End-to-end approach	✓	✓	✓	✗
	Middle-box compatibility	✓	✓	✓	✓
Redundancy (R)	Redundancy capabilities	✓	✓	✓	✓
	Flexibility of different delivery policies	✗	✓	✓	✗
Diversity (Di)	Path diversity	-	-	-	-
Self protection & security (SS)	Dynamical interfaces/addresses configuration	✓	✓	✓	✗
	Security	✗	✗	✗	✗
Multilevel resilience (M)	Multilevel resilience	-	-	-	-
Context awareness (CA)	Path state notion	✓	✓	✓	✓
	Loss detection and retransmission	✗	✗	✓	✓
Translucency (T)	Wireless technology agnosticism	✓	✓	✓	✓
	Application compatibility	✓	✓	✓	✓
Additional implementation requirements (A)	Backward compatibility	✗	✗	✓	✓
	Maturity	✗	✗	✗	✗

Table 3.10.: Requirement analysis of Layer 5 proposals

3.6 SUMMARY AND CONCLUSION

In this chapter a comparison between different approaches and protocols to provide resilience to end-to-end communications has been done. Within this evaluation the RRE vector is defined in order to make a qualitative analysis. Each technology, designed to work at different OSI levels, has been evaluated under this vector. In order to turn this qualitative analysis into a measurable semi-quantitative analysis of all evaluated technologies (and taking into account that both, diversity and multilevel diversity, have been placed out of the scope of an end-to-end communication protocol) an equal value of $\frac{1}{12}$ has been assigned to each RRE vector field.

Based on this semi-quantitative evaluation, the comparison between all protocols is summarised in Figure 3.26.

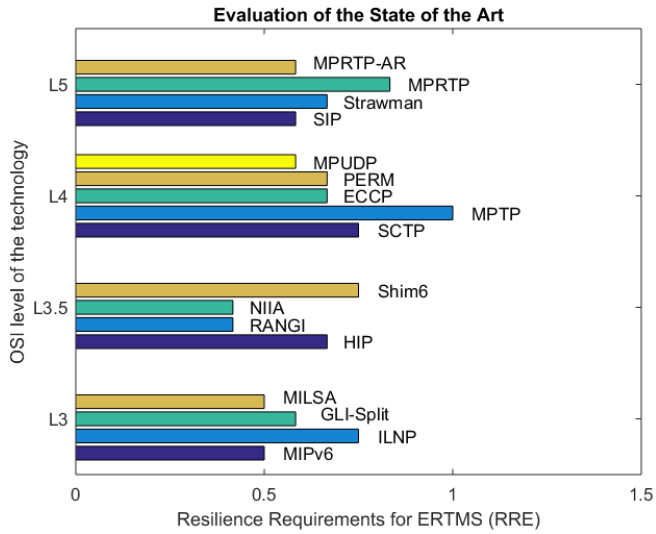


Figure 3.26.: Evaluation of the State of the Art

In conclusion, as a result of the analysis it can be concluded that the most interesting protocol for providing resilience for ERTMS train-to-ground communications is the protocol MPTCP, which operates in the transport layer. This protocol is a generic proposal which is not specifically designed for the

railway domain. On the one hand, this is a positive point because allows the industry to use a standard facility with a bigger market, this way decreasing the developing and deploying costs and using an open and potentially common interface for creating manufacturer interoperable equipments. On the other hand, MPTCP has not been designed taking into account the specific railway requirements in terms of maximum delay time and survivability against channel disruptions. However, this protocol provides an open architecture which facilitates the design and deployment of different schedulers and protocol configuration that can be adapted to these requirements.

Although in the literature several research efforts have been carried out for defining the most suitable communication protocol stack for IP-based ERTMS traffic, none of them had evaluated the potentiality of exploiting the multihoming and multipath approaches for improving the resilience of this traffic before we submitted our proposal in 2013, which was published in 2014 [14].

However, when talking about the adoption of MPTCP as carrier protocol for ERTMS traffic, some detected limitations must be overcome. One of these shortcomings is the fact that MPTCP only provides resilience when multiple used interfaces operate at different frequency channels or under different transmission mediums. However, in the short-term and mid-term, both, multihomed and single interface railway elements, will coexist. This means that the improvements in terms of resilience should not be reserved only for multihomed equipments. Another shortcoming is that each of ERTMS traffics described in Chapter 2, regular and HP messages should be treated differently, applying different schedulers which will increase the resilience depending on the robustness aimed for each of these two traffics.

This research work aims to make a step forward in this field providing a new backward compatible protocol stack for the NGERTMS based on MPTCP.

Part III

PROPOSAL FOR NEXT GENERATION ERTMS

laburpena

Atal honetan, lehenengo zatiak detektatutako mugak kontutan hartuz eta protokolo erredundanteen artearen egoera aztertu eta gero, MPTCP protokoloan oinarritutako komunikazio arkitektura berria proposatzen da, MP-CFM. Proposamen honek, muga horiek gainditzearen erronka betetzeaz gain, UNISIG orain dela gutxi plazaratutako arkitekturarekin atzerakako bateragarritasuna ere bermatzen du. Arkitektura honek lau zerbitzu klase mota inplementatzen ditu, bi zerbitzu mota lehentasun handiko mezuentzat eta beste bi lehentasun normaleko mezuentzat. Halaber, horietako bi OBUa eta RBCa interfaze aniztunak diren eszenatokietarako diseinatuak daude, eta beste biak RBCa interfaze aniztuna den, baina OBUa interfaze bakarrekoa den eszenatokietarako. Horrez gain, atal honetan MP-CFMren segurtasunaren ikuspuntutik ere azterketa bat egiten da. Azterketa honetan segurtasun arazo batzuk detektatzen dira eta horiek gainditzeko, ERTMSen aplikatzerakoan bete beharreko neurriak proposatzen dira. Azkenik, kontzeptu proba bat aurkezten da zeinak MP-CFMren eta sarearen arteko sinbiosia bilatzen duen. Horretarako sarean PCE bat kokatuko litzateke, MPTCPren azpi-fluxu bakoitzarentzat bide ezberdinak kalkulatuko lituzkeena eta informazio hori automatikoki MPLS sare batean banatuko lukeena.

resumen

En este apartado, considerando los desafíos previamente descritos en el segundo apartado y tras analizar el estado del arte en protocolos redundante, se propone una arquitectura de comunicaciones basada en el protocolo MPTCP, llamada MP-CFM, que permite superar dichos desafíos, a la par que mantener la retrocompatibilidad con el sistema de comunicaciones basado en conmutación de paquetes recientemente propuesto por UNISIG. Esta arquitectura implementa cuatro tipos de clase de servicio, los cuales son utilizados por los paquetes ordinarios y de alta prioridad para dos escenarios distintos; un escenario en el que ambos extremos, el OBU y el RBC, disponen de múltiples interfaces de red; y otro escenario transicional en el cual el RBC sí tiene múltiples interfaces de red pero el OBU solo dispone de una única interfaz. Además se hace un análisis del MP-CFM desde el punto de vista de seguridad, detectándose posibles problemas para los cuales se propone una solución que debería ser adoptada

junto con la inclusión de MP-CFM en la pila de protocolos de ERTMS. Asimismo, se presenta una prueba de concepto que permitiría establecer una simbiosis entre MP-CFM y la red de comunicaciones mediante un PCE situado en esta última que calcule caminos disjuntos para cada subflujo establecido y distribuya esta información automáticamente a lo largo de una red MPLS.

Part V

CONCLUSIONS AND DISSEMINATION RESULTS

laburpena

Tesiaren azkenengo atal honetan bertan aurkeztutako ikerketa lanen gainean errepaso bat egiten da. Azpimarratzekoa da, tesian bildutako proposamen eta emaitza gehienak inpaktu handiko aldizkarietan eta kongresuetan, nazioartekoak eta nazionalak, aurkeztuak izan direla. Horrez gain, kongresu eta eztabaida-leku industrialetan ere era aktiboan hartu da. Bestalde, hemen azaldutako zenbait proposamen, deialdi publikoko I+G proiektu ezberdinetan (nazioartekoak eta nazionalak) ekarpen moduan aurkeztuak izan dira.

resumen

En este apartado final de la tesis se hace un repaso de las contribuciones realizadas por los trabajos de investigación en ella presentadas. Se puede destacar que una gran parte de las propuestas y resultados de la tesis han sido presentados en numerosas revistas de alto impacto, congresos nacionales e internacionales y foros industriales ferroviarios. Además, algunas de las propuestas recogidas en esta tesis han servido como contribución en múltiples proyectos de I+D nacionales e internacionales financiados en convocatorias públicas.

10 CONCLUSIONS

> The goal of education is the advancement of knowledge and the dissemination of truth.
>
> John F. Kennedy

10.1 INTRODUCTION

In this chapter we summarise the contributions of this thesis. The work presented in the previous chapters is aligned with the European plan for creating a true Single European Railway Area (SERA) in order to improve the network performance and reliability of the sector as a whole. In this context, the migration of the communication systems towards TCP/IP technology is essential. This thesis document is the synthesis of a research work carried out along the last four years. During this timespan multiple contributions have been made which will be available for the plan mentioned above. The results of this research work have been presented in many academic and industrial journals and conferences. Moreover, since we proposed a MPTCP-based architecture in 2014 [14], this proposal has been taken as a basis for other researchers in Europe [208–210] and in Asia [211] to perform their works. In the following sections we summarise the main contributions of this research work, the dissemination results, the research projects where we have participated, as well as future potential research lines to complement our proposal.

10.2 CONTRIBUTIONS OF THIS RESEARCH

As we have demonstrated in previous chapters, the adoption of a MPTCP-based communication architecture, MP-CFM, is suitable for the NGERTMS. Moreover, its implementation would provide considerably higher resilience against channel errors to railway signalling applications.

In the following list, we point out the most significant contributions of this research work:

- *Analysis of the current ERTMS limitations*. The revision of the current ERTMS communication protocol stack made in this work has had as result the highlighting of its main limitations. This shortcoming evaluation defines the path that it should be followed in order to strengthen the railway signalling communications.

- *Survey of network redundancy protocols*. Within this work we have defined the redundancy as a cornerstone for achieving communication resilience. Based on this fact, we have defined ERTMS-specific requirements necessary to perform a deep analysis of the existing proposals and select the most suitable one based on a semi-quantitative analysis.

- *MPTCP-based communication architecture for NGERTMS*. In this research work, we propose a new communication architecture for NGERTMS, named **MP-CFm!** (**MP-CFm!**), which allows to send regular and HP messages providing to these last ones higher protection against network errors. Moreover, this architecture is backward compatible with the already defined PS-based communication system and it eases the migration to upcoming mobile technologies.

- *Parametrisation of the proposed architecture*. In this regard, four different parametrisations have been proposed and validated. Three of them are valid for the proposed architecture, whereas the parametrisation made for the tailoring of TCP can be also applied to the PS-based communication system of current ERTMS.

- *Development of a new simulation framework*. For the validation of the proposed architecture a new simulation framework which allows injecting

real ETCS-like traffic to simulated railway scenario has been developed. This framework permits to evaluate new signalling applications and network protocols in the railway domain reducing on-site testing.

10.3 DISSEMINATION OF THE RESULTS

Many of the results presented in this thesis work have been published in several international journals, in proceedings of international academic conferences, as well as in international industrial conferences related to the railway domain. Furthermore, the research work has been aligned with different national and international research projects related with the research topic. In this section we enumerate these contributions classifying them in different categories.

10.3.1 Publications in international journals

We have published three articles in two different international journals with impact factor according to the Journal Citation Report. These journals are in the Q1 of their scientific topics; telecommunications and transportation science and technologies.

- ***A Step Up in European Rail Traffic Management Systems: A Seamless Fail Recovery Scheme*** [207].

  Journal: IEEE Vehicular Technology Magazine (IF: 2.783 in 2016).

  Year: 2016.

- ***Cyber security analysis of the European train control system*** [13].

  Journal: IEEE Communications Magazine (IF: 5.125).

  Year: 2015.

- ***End-to-End Multipath Technology: Enhancing Availability and Reliability in Next-Generation Packet-Switched Train Signaling Systems***.

  Journal: IEEE Vehicular Technology Magazine (IF: 2.783).

  Year: 2014.

10.3.2 Publications in proceedings of international conferences

We have also published five papers to the proceedings of international conferences.

- ***Exploiting redundancy and path diversity for railway signalling resiliency*** [212].

  Conference: IEEE International Conference on Intelligent Rail Transportation (ICIRT).

  Year: 2016.

- ***A multi bearer adaptable communication demonstrator for train-to-ground IP communication to increase resilience*** [213].

  Conference: International Workshop on Communication Technologies for Vehicles.

  Year: 2016.

- ***SCADA Systems in the Railway Domain: Enhancing Reliability through Redundant MultipathTCP*** [214]

  Conference: IEEE 18th International Conference on Intelligent Transportation Systems (ITSC). Year: 2015.

- ***Towards a resilient railway communication network against electromagnetic attacks*** [173].

  Conference: Transport Research Arena (TRA).

  Year: 2014.

- ***Multipath technology to handle mobility and increase resilience in next generation ERTMS (Invited speaker)***.

  Conference: 5th International Workshop on Communication Technologies for Vehicles.

  Year: 2013.

10.3.3 Oral communications in industrial conferences

Due to the topic of the thesis and its involvement of the local railway industry we have made special effort to contribute with our results to different industrial international conferences.

- ***Cyber security study of the European Rail Traffic Management System***.

  Conference: UIC ERTMS Conference.

  Year: 2016.

- ***Defining challenges and opportunities for next-generation train signalling systems over IP communications (Invited speaker)***.

  Conference: Smart Rail 2014.

  Year: 2014.

10.3.4 Other publications related to this PhD thesis

During the last years we have also contribute with other three papers directly related with the research work presented in this thesis. These papers have been published in international journals and conferences.

- ***Eurobalise-Train communication modelling to assess interferences in railway control signalling systems*** [215].

  Journal: Network Protocols and Algorithms.

  Year: 2016.

- ***Modelling and Simulation of ERTMS for Current and Future Mobile Technologies*** [198].

  Journal: International Journal of Vehicular Technology.

  Year: 2015.

- ***Towards zero on-site testing: Advanced traffic management & control systems simulation framework including communication KPIs and response to failure events*** [196].

Conference: IEEE International Symposium on Wireless Vehicular Communications (WiVeC).

Year: 2014.

10.4 PARTICIPATION IN NATIONAL AND INTERNATIONAL PROJECTS

Along the last four years we have participated in different national and international research projects related with the research work presented in this thesis.

- **SAREMSIG**

  Funding entity: Spanish Ministry of Economy, Industry and Competitiveness

  Participants: UPV/EHU and CEIT

  Duration: 01/1/2014 - 31/12/2017

  Main researcher: Marina Aguado

  Number of participating researchers: 5

  Project budget: 72,300 €

- **SECRET (FP7-SEC-2011-1)**

  Funding entity: European Commission

  Participants: 11

  Duration: 01-08-2012 - 31-07-2015

  Main researcher: Eduardo Jacob

  Number of participating researchers: 4

  Project budget: 3,059,433.00 €

- **Cyber Security on Rails**

  Funding entity: CAF

Participants: 2

Duration: 01/11/2015 - 31/10/2016

Main researcher: Marina Aguado

Number of participating researchers: 6

Project budget: 39,870.59 €

- **TicTRAS**

  Funding entity: UPV/EHU

  Participants: 1

  Duration: 20/12/2013 - 25/12/2017

  Main researcher: Marina Aguado

  Number of participating researchers: 6

  Project budget: 73,636.53 €

- **CYRail (EU Project 730843)**

  Funding entity: European Commission

  Participants: 6

  Duration: 1/10/2016 - 30/9/2018

  Main researcher: Marina Aguado

  Number of participating researchers: 4

  Project budget: 1,500.000 €

10.5 FUTURE RESEARCH LINES

The presented thesis work has contributed to the state of the art of the railway communications. To move from an experimental proposal to an industrial implementation, two complementary points discussed in this thesis should be addressed; the protection of the proposed architecture against the security threats identified in Chapter 5 and the establishment of completely disjoint subflows introduced in Chapter 6. These two open points define the future research directions:

- The substitution of Euroradio Safety layer by the TLS algorithm and its integration with the proposed MPTCP-based architecture will help to protect all subflows of the connection against different security attacks.
- The effects of the adoption of more robust cryptographic algorithms, based on public or private key schemes will be evaluated, specially the impact of this algorithm in the ERTMS communications delay.
- The integration of the proposed MPTCP-based architecture with MPLS backbone networks used for railway signalling communications will be developed. In order to do so, we will continue with an ongoing research work aligned with the strategy presented in Chapter 6, which is based on the deployment of a smart ETCS application which will work together with a network PCE. This strategy will allow creating synergies between end-hosts and the network exploiting the MPLS TE capabilities to provide path diversity.

Part VI

APPENDIX

A APPENDIX: CYBER SECURITY THREATS: A TAXONOMY

A.1 INTRODUCTION

This appendix provides taxonomy of cyber security attacks in the general Information Technology (IT) domain. These cyber attacks can be classified according to their interaction with the target, their goal and the methodology used during the attack.

A.2 PASSIVE ATTACKS

These types of attacks do not require any interaction with the target or the network under attack. Usually, they are difficult to detect and their aim is to collect information for future, more complex, attacks.

- **Eavesdropping:** This is the most common type of passive attack and it is performed by capturing packets travelling along the network. This attack can be performed in both wireless networks and wired networks that are not correctly segmented.

A.3 ACTIVE ATTACKS

Unlike the passive attacks, these attacks interact directly with the target or with the network in order to cause intentional malfunctioning. These attacks are therefore more easily detected but also more dangerous.

- **DoS attacks:** As their name indicates, the goal of these attacks is to put the target out of service, usually by making the target work beyond its

capabilities. Depending on how the attack is performed, DoS attacks can be classified into different groups. They can be categorised into physical and logical attacks, but they can also be defined according to the origin of the attack, i.e. whether the attack has one or multiple sources:

  - **Physical attacks (jamming):** Jamming attacks do not require any logic or knowledge of the target andor its network. The attack occurs when physical conditions that are able to interrupt communication are introduced into the network. For example, high-power electromagnetic emissions can abruptly reduce the Signal to Noise Ratio (SNR) in the target's receptor.
  - **Logical attacks:** The execution of these attacks requires exhaustive knowledge of the target's system, or of the network topology where it is located. Usually, these attacks – also called replay attacks – are based on the attacker copying valid packets of the service provided by the target and inserting these extra copies into the network. This action causes a data overflow in the target.
  - **Distributed attacks:** When a DoS attack has more than a single source it is called Distributed Denial of Service (DDoS). DDoS attacks can be identical to the regular DoS attacks, but by carrying out the attack from different sources, the probability of success increases considerably. Moreover, as there are multiple sources, it is more difficult for the target to recover from the attack.

- **Identity theft or spoofing attacks:** These attacks permit the injection of packets into an unauthorised network by adopting the identity of an entity that is authorised by the network. When this identity theft is performed in both communication directions, it is called a "man-in-the-middle" attack; i.e. attacker C alters communication between entities A and B, by communicating with A as if they were B and at the same time communicating with B as if they were A.

- **Equipment infection:** The exploitation of known or unknown system vulnerabilities using viruses has become a common and effective means of cyber war. Cases such as StuxNet have demonstrated that incorrectly isolated industrial equipment can become a target. It is difficult to protect

industrial equipment against these attacks for two main reasons. Firstly, it is difficult to update such equipment in cases where the elements are geographically dispersed or where they are based on embedded systems. Secondly, protective software, such as antivirus software, has a negative effect on real-time performance.

BIBLIOGRAPHY

[1] D. Fisher, "Requirements on the gsm-r network for etcs support," *Banedanmark, Rep. FSI85-222-007*, 2008.

[2] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[3] G. Theeg, S. V. Vlasenko, and E. Anders, *Railway signalling & interlocking: international compendium*. Eurailpress, 2009.

[4] E. CENELEC, "50126 (1999): Railway applications–the specification and demonstration of reliability," *Availability, Maintainability and Safety (RAMS)*, 1999.

[5] *Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*, International Electrotechnical Commission Std., 2002.

[6] I. E. Commission *et al.*, "Functional safety of electrical/electronic/programmable electronic safety related systems," *IEC 61508*, 2000.

[7] *ERTMS/ETCS RAMS Requirements Specification*, EEIG ERTMS User Group Std., 1998.

[8] P. Winter, *Compendium on ERTMS: European rail traffic management system*. Eurail Press, 2009.

[9] V. Carpinelli, A. Missoumi, E. Brutin, and C. Filippini, *ATLAS of ERTMS implementations*, third edition ed. Railway Technical Publications, 2012.

[10] E. Brutin, "Ertms: Global dimensions, global challenges," *European Railway Review*, vol. 18(3), p. 36–38, 2012.

[11] S. Ruesche, J. Steuer, and K. Jobmann, "The european switch," *Vehicular Technology Magazine, IEEE*, vol. 3, no. 3, pp. 37–46, 2008.

[12] M. M. David Taylor, Nils Lofmark, "Survey on operational communications (study for the evolution of the railway communications system)," Final report for the European Railway Agency Ref: 37760-496 v04, Tech. Rep., 2015.

[13] I. Lopez and M. Aguado, "Cyber security analysis of the european train control system," *IEEE Communications Magazine*, vol. 53, no. 10, pp. 110–116, 2015.

[14] I. Lopez, M. Aguado, and E. Jacob, "End-to-end multipath technology: Enhancing availability and reliability in next-generation packet-switched train signaling systems," *ieee vehicular technology magazine*, vol. 9, no. 1, pp. 28–35, 2014.

[15] *Radio Transmission FFFIS for EuroRadio*, ERTMS/ETCS Std., 2015.

[16] G. Shafiullah, A. Gyasi-Agyei, and P. Wolfs, "Survey of wireless communications applications in the railway industry," in *Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on*. IEEE, 2007, pp. 65–65.

[17] V. Di Claudio, "Capacity enhancement for gsm-r networks," in *ERTMS Conference 2006*. UIC, 2006.

[18] A. Sniady and J. Soler, "An overview of gsm-r technology and its shortcomings," in *ITS Telecommunications (ITST), 2012 12th International Conference on*. IEEE, 2012, pp. 626–629.

[19] "Coexistence between gsm-r and 3g / 4g-systems in the 900 mhz frequency band - swedish view. trv 2013/13976," Trafikverket (Swedish Transport Administration), Tech. Rep., 2013.

[20] "Gsm-r and interferences: Managing the co-existence," European Union Agency For Railways, Tech. Rep., 2016.

[21] D. Briginshaw, "Get ready for the next signalling revolution," *International Railway Journal*, vol. 55, no. 10, 2015.

[22] K. Clive, "Finland opts for tetra," *Rail engineer*, 2015.

[23] M. Aguado, O. Onandi, P. Agustin, M. Higuero, and E. Taquet, "Wimax on rails," *IEEE Vehicular Technology Magazine*, vol. 3, no. 3, pp. 47–56, 2008.

[24] A. Sniady and J. Soler, "Lte for railways: impact on performance of etcs railway signaling," *Vehicular Technology Magazine, IEEE*, vol. 9, no. 2, pp. 69–77, 2014.

[25] A. Sniady and J. Soler, "Performance of lte in high speed railway scenarios," in *Communication Technologies for Vehicles*. Springer, 2013, pp. 211–222.

[26] S. Lugschitz and C. Pucher, "New applications through axle counter communications over open networks," *SIGNAL + DRAHT*, vol. 106, no. 10, 2014.

[27] B. S. Programme, "Online key management system concept," Banedanmark, Appendix 3.1 Att 11, SP-12-041120, Tech. Rep., 2011.

[28] E. Biham, "How to forge des-encrypted messages in 2ˆ 28 steps," *Technion Computer Science Department Technical Report CS0884*, 1996.

[29] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[30] C. Laurendeau and M. Barbeau, "Threats to security in dsrc/wave," in *Ad-Hoc, Mobile, and Wireless Networks*. Springer, 2006, pp. 266–279.

[31] J. P. Sterbenz, E. K. Cetinkaya, M. A. Hameed, A. Jabbar, S. Qian, and J. P. Rohrer, "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation," *Telecommunication systems*, vol. 52, no. 2, pp. 705–736, 2013.

[32] P. A. Lee and T. Anderson, *Fault tolerance: principles and practice*. Springer Science & Business Media, 2012, vol. 3.

[33] R. M. Savola, "Towards a taxonomy for information security metrics," in *Proceedings of the 2007 ACM workshop on Quality of protection*. ACM, 2007, pp. 28–30.

[34] J. F. Meyer, "Performability: a retrospective and some pointers to the future," *Performance evaluation*, vol. 14, no. 3, pp. 139–156, 1992.

[35] A. Avizienis, J.-C. Laprie, B. Randell *et al.*, *Fundamental concepts of dependability*. University of Newcastle upon Tyne, Computing Science, 2001.

[36] M. G. Park, "Rams management of railway systems," Ph.D. dissertation, University of Birmingham, 2014.

[37] B. STANDARD, "En50159—2001 railway applications: communication, signaling and processing systems," 2001.

[38] G.-R. F. Group, "Eirene functional requirements specification version 7.4.0," 2014.

[39] U. SUBSET, "Subset 093, gsm-r interfaces - class 1 requirements, version 2.3.0."

[40] W. M. Eddy, "At what layer does mobility belong?" *Communications Magazine, IEEE*, vol. 42, no. 10, pp. 155–159, 2004.

[41] R. Pascoe and T. Eichorn, "What is communication-based train control?" *IEEE Vehicular Technology Magazine*, vol. 4, no. 4, pp. 16–21, 2009.

[42] M. Aguado, E. Jacob, P. Saiz, J. J. Unzilla, M. Higuero, and J. Matias, "Railway signaling systems and new trends in wireless data communication," in *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, vol. 2. IEEE, 2005, pp. 1333–1336.

[43] M. Fitzmaurice, "Use of wireless local area networks in rail and urban transit environments," *Transportation Research Record: Journal of the Transportation Research Board*, no. 1916, pp. 42–46, 2005.

[44] F. WHITWOM, "Integration of wireless network technology with signaling in the rail transit industry," *Alcatel telecommunications review*, no. 1, pp. 43–48, 2003.

[45] L. Zhu, F. R. Yu, and B. Ning, "Availability improvement for wlan-based train-ground communication systems in communication-based train control (cbtc)," in *Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd*. IEEE, 2010, pp. 1–5.

[46] L. Zhu, F. R. Yu, and B. Ning, "A seamless handoff scheme for train-ground communication systems in cbtc," in *Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd*. IEEE, 2010, pp. 1–5.

[47] L. Zhu, F. R. Yu, B. Ning, and T. Tang, "Handoff management in communication-based train control networks using stream control transmission protocol and ieee 802.11 p wlans," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, pp. 1–16, 2012.

[48] H. Hungar, "Assuring standard conformance of partial interfaces," in *Tagungsband des Dagstuhl-Workshops*, p. 112.

[49] B. Elsweiler, *Beyond ETCS – Interoperable interfaces and more*, 2014.

[50] R. Wagner and P. Hefti, *SBB seeks cost savings with Sinet interlocking*, 2014.

[51] IEC 65C, *Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*, Geneva, Switzerland, July 2012, IEC 62439-3.

[52] S. A. Nsaif and J. M. Rhee, "Improvement of high-availability seamless redundancy (hsr) traffic performance for smart grid communications," *Communications and Networks, Journal of*, vol. 14, no. 6, pp. 653–661, 2012.

[53] IEC TC57, *Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines*, Geneva, Switzerland, August 2013, IEC/TR 61850-90-4.

[54] M. Rentschler and P. Laukemann, "Towards a reliable parallel redundant wlan black channel," in *Factory Communication Systems (WFCS), 2012 9th IEEE International Workshop on*. IEEE, 2012, pp. 255–264.

[55] E. Uhlemann and L. K. Rasmussen, "Incremental redundancy deadline dependent coding for efficient wireless real-time communications," in

10th IEEE Conference on Emerging Technologies and Factory Automation (ETFA), Catania, Italy, September 19-22, 2005. IEEE Press, 2005, pp. 417–424.

[56] H. Bengtsson, E. Uhlemann, and P.-A. Wiberg, "Protocol for wireless real-time systems," in *Real-Time Systems, 1999. Proceedings of the 11th Euromicro Conference on*. IEEE, 1999, pp. 168–174.

[57] J. Qadir, A. Ali, K.-L. A. Yau, A. Sathiaseelan, and J. Crowcroft, "Exploiting the power of multiplicity: a holistic survey of network-layer multipath," *Communications Surveys & Tutorials, IEEE*, vol. 17, no. 4, pp. 2176–2213, 2015.

[58] J. Tsai and T. Moors, "A review of multipath routing protocols: From wireless ad hoc to mesh networks," in *ACoRN early career researcher workshop on wireless multihop networking*, vol. 30. Citeseer, 2006.

[59] A. Autenrieth and A. Kirstädter, "Engineering end-to-end ip resilience using resilience-differentiated qos," *Communications Magazine, IEEE*, vol. 40, no. 1, pp. 50–57, 2002.

[60] M. Menth and R. Martin, "Network resilience through multi-topology routing," in *The 5th International Workshop on Design of Reliable Communication Networks*, 2005, pp. 271–277.

[61] J. Astorga, M. Aguado, N. Toledo, and M. Higuero, "A high performance link layer mobility management strategy for professional private broadband networks," *Journal of Network and Computer Applications*, vol. 36, no. 4, pp. 1152–1163, 2013.

[62] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775 (Proposed Standard), Internet Engineering Task Force, Jun. 2004, obsoleted by RFC 6275. [Online]. Available: http://www.ietf.org/rfc/rfc3775.txt

[63] C. Perkins, "IP Mobility Support for IPv4," RFC 3344 (Proposed Standard), Internet Engineering Task Force, Aug. 2002, obsoleted by RFC 5944, updated by RFC 4721. [Online]. Available: http://www.ietf.org/rfc/rfc3344.txt

[64] C. de Launois and M. Bagnulo, "The paths towards ipv6 multihoming," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2, 2006.

[65] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, "Multiple Care-of Addresses Registration," RFC 5648 (Proposed Standard), Internet Engineering Task Force, Oct. 2009, updated by RFC 6089. [Online]. Available: http://www.ietf.org/rfc/rfc5648.txt

[66] J.-Y. Pan, J.-L. Lin, and K.-F. Pan, "Multiple care-of addresses registration and capacity-aware preference on multi-rate wireless links," in *Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on*. IEEE, 2008, pp. 768–773.

[67] K. Mitsuya, R. Kuntz, S. Sugimoto, R. Wakikawa, and J. Murai, "A policy management framework for flow distribution on multihomed end nodes," in *Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture*. ACM, 2007, p. 10.

[68] B. Sousa, M. Silva, K. Pentikousis, and M. Curado, "A multiple care of addresses model," in *Computers and Communications (ISCC), 2011 IEEE Symposium on*. IEEE, 2011, pp. 485–490.

[69] U. Toseef, A. Udugama, C. Goerg, C. Fan, and F. Pittmann, "Realization of multiple access interface management and flow mobility in ipv6," in *Proceedings of the 1st international conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, p. 26.

[70] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC 5213 (Proposed Standard), Internet Engineering Task Force, Aug. 2008, updated by RFC 6543. [Online]. Available: http://www.ietf.org/rfc/rfc5213.txt

[71] K.-S. Kong, W. Lee, Y.-H. Han, M.-K. Shin, and H. You, "Mobility management for all-ip mobile networks: mobile ipv6 vs. proxy mobile ipv6," *Wireless Communications, IEEE*, vol. 15, no. 2, pp. 36–45, 2008.

[72] H.-J. Kim and S.-G. Choi, "A method to support multiple interfaces a mobile node in next generation wireless network," in *Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on*. IEEE, 2010, pp. 276–281.

[73] R. Koodli, "Mobile IPv6 Fast Handovers," RFC 5568 (Proposed Standard), Internet Engineering Task Force, Jul. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5568.txt

[74] R. Atkinson and S. Bhatti, "Identifier-locator network protocol (ilnp) architectural description," Tech. Rep., 2012.

[75] R. Atkinson, S. Bhatti, and S. Hailes, "Ilnp: mobility, multi-homing, localised addressing and security through naming," *Telecommunication Systems*, vol. 42, no. 3-4, pp. 273–291, 2009.

[76] R. Atkinson, S. Bhatti, and S. Hailes, "Evolving the internet architecture through naming," *Selected Areas in Communications, IEEE Journal on*, vol. 28, no. 8, pp. 1319–1325, 2010.

[77] R. Atkinson, M. Lad, S. Bhatti, and S. Hailes, "A proposal for coalition networking in dynamic operational environments," in *Military Communications Conference, 2006. MILCOM 2006. IEEE*. IEEE, 2006, pp. 1–8.

[78] M. Menth, M. Hartmann, and D. Klein, "Global locator, local locator, and identifier split (gli-split)," *Future Internet*, vol. 5, no. 1, pp. 67–94, 2013.

[79] J. Pan, R. Jain, S. Paul, and C. So-In, "Milsa: A new evolutionary architecture for scalability, mobility, and multihoming in the future internet," *Selected Areas in Communications, IEEE Journal on*, vol. 28, no. 8, pp. 1344–1362, 2010.

[80] J. Pan, S. Paul, R. Jain, and M. Bowman, "Milsa: a mobility and multihoming supporting identifier locator split architecture for naming in the next generation internet," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. IEEE, 2008, pp. 1–6.

[81] J. Pan, R. Jain, S. Paul, M. Bowman, X. Xu, and S. Chen, "Enhanced milsa architecture for naming, addressing, routing and security issues in the next generation internet," in *Communications, 2009. ICC'09. IEEE International Conference on*. IEEE, 2009, pp. 1–6.

[82] S. Paul, R. Jain, and J. Pan, "An identifier/locator split architecture for exploring path diversity through site multi-homing-a hybrid host-network cooperative approach," in *Communications (ICC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1–5.

[83] M. Menth, M. Hartmann, and D. Klein, "Global locator, local locator, and identifier split (gli-split)."

[84] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol," RFC 5201 (Experimental), Internet Engineering Task Force, Apr. 2008, updated by RFC 6253. [Online]. Available: http://www.ietf.org/rfc/rfc5201.txt

[85] P. Nikander, A. Gurtov, and T. R. Henderson, "Host identity protocol (hip): Connectivity, mobility, multi-homing, security, and privacy over ipv4 and ipv6 networks," *Communications Surveys & Tutorials, IEEE*, vol. 12, no. 2, pp. 186–204, 2010.

[86] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423 (Informational), Internet Engineering Task Force, May 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4423.txt

[87] P. Nikander, T. Henderson, C. Vogt, and J. Arkko, "End-Host Mobility and Multihoming with the Host Identity Protocol," RFC 5206 (Experimental), Internet Engineering Task Force, Apr. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5206.txt

[88] A. Gurtov and T. Polishchuk, "Secure multipath transport for legacy internet applications," in *Broadband Communications, Networks, and Systems, 2009. BROADNETS 2009. Sixth International Conference on*. IEEE, 2009, pp. 1–8.

[89] P. Nikander and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions," RFC 5205 (Experimental), Internet

Engineering Task Force, Apr. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5205.txt

[90] J. Laganier and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension," RFC 5204 (Experimental), Internet Engineering Task Force, Apr. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5204.txt

[91] X. Xu, "Routing architecture for the next generation internet (rangi), draft-xu-rangi-04. txt," 2011.

[92] X. Xu and D. Guo, "Hierarchical routing architecture (hra)," in *Next generation internet networks, 2008. NGI 2008*. IEEE, 2008, pp. 92–99.

[93] B. Ahlgren, J. Arkko, L. Eggert, and J. Rajahalme, "A node identity internetworking architecture," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*. IEEE, 2006, pp. 1–6.

[94] S. Schütz, R. Winter, L. Burness, P. Eardley, and B. Ahlgren, "Node identity internetworking architecture," 2007.

[95] S. Schütz, H. Abrahamsson, B. Ahlgren, and M. Brunner, "Design and implementation of the node identity internetworking architecture," *Computer Networks*, vol. 54, no. 7, pp. 1142–1154, 2010.

[96] E. Nordmark and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6," RFC 5533 (Proposed Standard), Internet Engineering Task Force, Jun. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5533.txt

[97] A. García-Martínez, M. Bagnulo, and I. Van Beijnum, "The shim6 architecture for ipv6 multihoming," *Communications Magazine, IEEE*, vol. 48, no. 9, pp. 152–157, 2010.

[98] A. Dhraief and N. Montavont, "Toward mobility and multihoming unification-the shim6 protocol: A case study," in *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*. IEEE, 2008, pp. 2840–2845.

[99] A. De la Oliva, I. Soto, A. García-Martínez, M. Bagnulo, and A. Azcorra, "Analytical characterization of failure recovery in reap," *Computer Communications*, vol. 33, no. 4, pp. 485–499, 2010.

[100] S. Barré, O. Bonaventure *et al.*, "Improved path exploration in shim6-based multihoming," in *Proc. ACM SIGCOM Workshop on IPv6 and the Future of the Internet*, 2007.

[101] G. Fekete, "Network interface management in mobile and multihomed nodes," 2010.

[102] T. Polishchuk and A. Gurtov, "mhip: Tcp-friendly secure multipath transport," in *Proc. of 5th International Conference on Access Networks (ACCESSNETS)*, 2010.

[103] P. Jokela, P. Nikander, J. Melen, J. Ylitalo, and J. Wall, "Host identity protocol: Achieving ipv4 œ ipv6 handovers without tunneling," 2003.

[104] Z. Faigl, "Performance analysis of signalling overhead in host identity protocol-based secure mobile networks: Ultra flat architecture or end-to-end signalling?" *Wireless Networks*, vol. 21, no. 2, pp. 531–555, 2015.

[105] E. Nordmark, "Shim6 application referral issues," *Work in Progress*, 2005.

[106] R. Ferrús, A. Brunstrom, K.-J. Grinnemo, R. Fracchia, G. Galante, F. Casadevall *et al.*, "Towards transport-layer mobility: Evolution of sctp multihoming," *Computer Communications*, vol. 31, no. 5, pp. 980–998, 2008.

[107] T. Dreibholz, E. P. Rathgeb, I. Rüngeler, R. Seggelmann, M. Tüxen, and R. R. Stewart, "Stream control transmission protocol: Past, current, and future standardization activities," *Communications Magazine, IEEE*, vol. 49, no. 4, pp. 82–88, 2011.

[108] R. Stewart, "Stream Control Transmission Protocol," RFC 4960 (Proposed Standard), Internet Engineering Task Force, Sep. 2007, updated by RFCs 6096, 6335. [Online]. Available: http://www.ietf.org/rfc/rfc4960.txt

[109] R. Stewart and C. Metz, "Sctp: new transport protocol for tcp/ip," *Internet Computing, IEEE*, vol. 5, no. 6, pp. 64–69, 2001.

[110] A. L. Caro Jr, "End-to-end fault tolerance using transport layer multihoming," DTIC Document, Tech. Rep., 2005.

[111] N. Ekiz, P. Natarajan, M. Becke, M. Tuexen, T. Dreibholz, P. Amer, R. Stewart *et al.*, "Load sharing for the stream control transmission protocol (sctp)," 2015.

[112] J. R. Iyengar, P. D. Amer, and R. Stewart, "Concurrent multipath transfer using sctp multihoming over independent end-to-end paths," *Networking, IEEE/ACM Transactions on*, vol. 14, no. 5, pp. 951–964, 2006.

[113] J. Fitzpatrick, S. Murphy, M. Atiquzzaman, and J. Murphy, "Using cross-layer metrics to improve the performance of end-to-end handover mechanisms," *Computer Communications*, vol. 32, no. 15, pp. 1600–1612, 2009.

[114] S. J. Koh, M. J. Chang, and M. Lee, "msctp for soft handover in transport layer," *IEEE communications letters*, vol. 8, no. 3, pp. 189–191, 2004.

[115] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama, and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration," RFC 5061 (Proposed Standard), Internet Engineering Task Force, Sep. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc5061.txt

[116] J. Iyengar, K. Shah, P. Amer, and R. Stewart, "Concurrent multipath transfer using sctp multihoming," *SPECTS 2004*, 2004.

[117] J. Liao, J. Wang, and X. Zhu, "cmpsctp: An extension of sctp to support concurrent multi-path transfer," in *Communications, 2008. ICC'08. IEEE International Conference on*. IEEE, 2008, pp. 5762–5766.

[118] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses," RFC 6824 (Experimental), Internet Engineering Task Force, Jan. 2013. [Online]. Available: http://www.ietf.org/rfc/rfc6824.txt

[119] A. Ford, C. Raiciu, M. Handley, S. Barre, and J. Iyengar, "Architectural Guidelines for Multipath TCP Development," RFC 6182 (Informational),

Internet Engineering Task Force, Mar. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6182.txt

[120] M. Scharf and A. Ford, "Multipath tcp (mptcp) application interface considerations," RFC 6897, March, Tech. Rep., 2013.

[121] C. Raiciu, M. Handley, and D. Wischik, "Coupled Congestion Control for Multipath Transport Protocols," RFC 6356 (Experimental), Internet Engineering Task Force, Oct. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6356.txt

[122] R. H. Tse, "Tcp fairness in multipath transport protocols," Ph.D. dissertation, Brown University, 2006.

[123] M. J. Arshad and M. S. Mian, "Issues of multihoming implementation using fast tcp: a simulation based analysis," *Proc IJCSNS*, vol. 8, no. 9, pp. 104–114, 2008.

[124] D. X. Wei, C. Jin, S. H. Low, and S. Hegde, "Fast tcp: motivation, architecture, algorithms, performance," *IEEE/ACM Transactions on Networking (ToN)*, vol. 14, no. 6, pp. 1246–1259, 2006.

[125] M. Li, A. Lukyanenko, and Y. Cui, "Network coding based multipath tcp," in *Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference on*. IEEE, 2012, pp. 25–30.

[126] F. du Pin Calmon, J. M. Cloud, M. Medard, and W. Zeng, "Multipath data transfer using network coding," Jan. 30 2013, uS Patent App. 13/754,398.

[127] J. K. Sundararajan, D. Shah, M. Médard, M. Mitzenmacher, and J. A. Barros, "Network coding meets tcp," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 280–288.

[128] J. K. Sundararajan, D. Shah, M. Médard, S. Jakubczak, M. Mitzenmacher, and J. O. Barros, "Network coding meets tcp: Theory and implementation," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 490–512, 2011.

[129] J. Cloud, F. du Pin Calmon, W. Zeng, G. Pau, L. M. Zeger, and M. Medard, "Multi-path tcp with network coding for mobile devices in heterogeneous networks," in *Vehicular Technology Conference (VTC Fall), 2013 IEEE 78th*. IEEE, 2013, pp. 1–5.

[130] Z.-q. Xia, Z.-g. Chen, Z. Ming, and J.-q. Liu, "A multipath tcp based on network coding in wireless mesh networks," in *Information Science and Engineering (ICISE), 2009 1st International Conference on*. IEEE, 2009, pp. 3946–3950.

[131] M. Arye, E. Nordstrom, R. Kiefer, J. Rexford, and M. J. Freedman, "A formally-verified migration protocol for mobile, multi-homed hosts," in *Network Protocols (ICNP), 2012 20th IEEE International Conference on*. IEEE, 2012, pp. 1–12.

[132] N. Thompson, G. He, and H. Luo, "Flow scheduling for end-host multihoming." in *INFOCOM*. Citeseer, 2006.

[133] M. Yabandeh, S. Zarifzadeh, and N. Yazdani, "Improving performance of transport protocols in multipath transferring schemes," *Computer Communications*, vol. 30, no. 17, pp. 3270–3284, 2007.

[134] J. Gan, N. N. Xiong, H. Wen, and Q. Zhu, "Analysis of sctp concurrent multipath transfer in vehicular network communication," *JOURNAL OF INTERNET TECHNOLOGY*, vol. 16, no. 3, pp. 495–504, 2015.

[135] A. J. F. Torres, E. P. Ribeiro, and C. M. Pedroso, "Predictive delay-centric handover for video streaming over sctp," *Computer Communications*, 2016.

[136] K. Rojviboonchai and A. Hitoshi, "An evaluation of multi-path transmission control protocol (m/tcp) with robust acknowledgement schemes," *IEICE transactions on communications*, vol. 87, no. 9, pp. 2699–2707, 2004.

[137] Y. Hasegawa, I. Yamaguchi, T. Hama, H. Shimonishi, and T. Murase, "Improved data distribution for multipath tcp communication," in *Global Telecommunications Conference, 2005. GLOBECOM'05. IEEE*, vol. 1. IEEE, 2005, pp. 5–pp.

[138] D. Zhou, W. Song, P. Wang, and W. Zhuang, "Multipath tcp for user cooperation in lte networks," *Network, IEEE*, vol. 29, no. 1, pp. 18–24, 2015.

[139] M. Arye, E. Nordstrom, R. Kiefer, J. Rexford, and M. J. Freedman, "A provably-correct protocol for seamless communication with mobile, multi-homed hosts," *arXiv preprint arXiv:1203.4042*, 2012.

[140] B. Almasi and S. Szilagyi, "Throughput performance analysis of the multipath communication library mpt," in *Telecommunications and Signal Processing (TSP), 2013 36th International Conference on*. IEEE, 2013, pp. 86–90.

[141] B. Almási and S. Szilágyi, "Investigating the performance of the mpt multipath communication library in ipv4 and ipv6," *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, vol. 5, no. 1, pp. 53–60, 2016.

[142] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "Session Initiation Protocol (SIP) Session Mobility," RFC 5631 (Informational), Internet Engineering Task Force, Oct. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5631.txt

[143] C.-M. Huang, C.-H. Lee, and P.-H. Tseng, "Multihomed sip-based network mobility using ieee 802.21 media independent handover," in *Communications, 2009. ICC'09. IEEE International Conference on*. IEEE, 2009, pp. 1–5.

[144] K. Taniuchi, Y. Ohba, V. Fajardo, S. Das, M. Tauil, Y.-H. Cheng, A. Dutta, D. Baker, M. Yajnik, and D. Famolari, "Ieee 802.21: Media independent handover: Features, applicability, and realization," *Communications Magazine, IEEE*, vol. 47, no. 1, pp. 112–120, 2009.

[145] J. Y. So, J. Wang, and D. Jones, "Ship mobility management hybrid sip-hip scheme," in *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-Assembling Wireless Networks. SNPD/SAWN 2005. Sixth International Conference on*. IEEE, 2005, pp. 226–230.

[146] A. Achour, K. Haddadou, B. Kervella, and G. Pujolle, "A sip-shim6-based solution providing interdomain service continuity in ims-based networks," *Communications Magazine, IEEE*, vol. 50, no. 7, pp. 109–119, 2012.

[147] G. Camarillo and M.-A. Garcia-Martin, *The 3G IP multimedia subsystem (IMS): merging the Internet and the cellular worlds*. John Wiley & Sons, 2007.

[148] A. Habib, N. Christin, and J. Chuang, "Taking advantage of multihoming with session layer striping," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*. IEEE, 2006, pp. 1–6.

[149] S. Ahsan and L. Eggert, "Multipath rtp (mprtp) draft-ietf-avtcore-mprtp-02," 2016.

[150] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," RFC 3550 (INTERNET STANDARD), Internet Engineering Task Force, Jul. 2003, updated by RFCs 5506, 5761, 6051, 6222. [Online]. Available: http://www.ietf.org/rfc/rfc3550.txt

[151] W. Lei, W. Zhang, and S. Liu, "Multipath real-time transport protocol based on application-level relay (mprtp-ar)," *draft-leiwm-avtcore-mprtp-ar-05*, 2014.

[152] W. Lei, W. Zhang, and S. Liu, "A framework of multipath transport system based on application-level relay (mpts-ar)," *draft-leiwm-tsvwg-mpts-ar-05*, 2014.

[153] S. Ahsan, "Multipath rtp: Applying multipath communication to real-time applications," 2011.

[154] R. Herrero, "Integrating hec with circuit breakers and multipath rtp to improve rtc media quality," *Telecommunication Systems*, pp. 1–11, 2016.

[155] W. Zhang, W. Lei, S. Liu, and G. Li, "A general framework of multipath transport system based on application-level relay," *Computer Communications*, vol. 51, pp. 70–80, 2014.

[156] G. Li, W. Lei, S. Liu, and W. Zhang, "A multipath relay transport control method for real-time video service," in *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2015 IEEE International Conference on*. IEEE, 2015, pp. 756–760.

[157] N. Cardwell, S. Savage, and T. Anderson, "Modeling tcp latency," in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3. IEEE, 2000, pp. 1742–1751.

[158] S. D. Strowes, "Passively measuring tcp round-trip times," *Communications of the ACM*, vol. 56, no. 10, pp. 57–64, 2013.

[159] M. Allman and V. Paxson, "On estimating end-to-end network path properties," in *ACM SIGCOMM Computer Communication Review*, vol. 29, no. 4. ACM, 1999, pp. 263–274.

[160] W.-T. Tan and A. Zakhor, "Real-time internet video using error resilient scalable compression and tcp-friendly transport protocol," *Multimedia, IEEE Transactions on*, vol. 1, no. 2, pp. 172–186, 1999.

[161] V. Jacobson, R. Braden, and D. Borman, "TCP Extensions for High Performance," RFC 1323 (Proposed Standard), Internet Engineering Task Force, May 1992. [Online]. Available: http://www.ietf.org/rfc/rfc1323.txt

[162] M. Allman, V. Paxson, and E. Blanton, "TCP Congestion Control," RFC 5681 (Draft Standard), Internet Engineering Task Force, Sep. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5681.txt

[163] M. Allman, K. Avrachenkov, U. Ayesta, J. Blanton, and P. Hurtig, "Early Retransmit for TCP and Stream Control Transmission Protocol (SCTP)," RFC 5827 (Experimental), Internet Engineering Task Force, May 2010. [Online]. Available: http://www.ietf.org/rfc/rfc5827.txt

[164] M. Allman, H. Balakrishnan, and S. Floyd, "Enhancing TCP's Loss Recovery Using Limited Transmit," RFC 3042 (Proposed Standard), Internet Engineering Task Force, Jan. 2001. [Online]. Available: http://www.ietf.org/rfc/rfc3042.txt

[165] M. Mellia, M. Meo, and C. Casetti, "Tcp smart framing: a segmentation algorithm to reduce tcp latency," *Networking, IEEE/ACM Transactions on*, vol. 13, no. 2, pp. 316–329, 2005.

[166] R. Ludwig and M. Meyer, "The Eifel Detection Algorithm for TCP," RFC 3522 (Experimental), Internet Engineering Task Force, Apr. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3522.txt

[167] E. Blanton and M. Allman, "Using TCP Duplicate Selective Acknowledgement (DSACKs) and Stream Control Transmission Protocol (SCTP) Duplicate Transmission Sequence Numbers (TSNs) to Detect Spurious Retransmissions," RFC 3708 (Experimental), Internet Engineering Task Force, Feb. 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3708.txt

[168] P. Sarolahti, M. Kojo, K. Yamamoto, and M. Hata, "Forward RTO-Recovery (F-RTO): An Algorithm for Detecting Spurious Retransmission Timeouts with TCP," RFC 5682 (Proposed Standard), Internet Engineering Task Force, Sep. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5682.txt

[169] R. Ludwig and A. Gurtov, "The Eifel Response Algorithm for TCP," RFC 4015 (Proposed Standard), Internet Engineering Task Force, Feb. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4015.txt

[170] J. Nagle, "Congestion Control in IP/TCP Internetworks," RFC 896, Internet Engineering Task Force, Jan. 1984. [Online]. Available: http://www.ietf.org/rfc/rfc896.txt

[171] R. Braden, "Requirements for Internet Hosts - Communication Layers," RFC 1122 (INTERNET STANDARD), Internet Engineering Task Force, Oct. 1989, updated by RFCs 1349, 4379, 5884, 6093, 6298, 6633. [Online]. Available: http://www.ietf.org/rfc/rfc1122.txt

[172] K. Ramakrishnan, S. Floyd, and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP," RFC 3168 (Proposed Standard), Internet Engineering Task Force, Sep. 2001, updated by RFCs 4301, 6040. [Online]. Available: http://www.ietf.org/rfc/rfc3168.txt

[173] M. Heddebaut, S. Mili, D. Sodoyer, E. Jacob, M. Aguado, C. P. Zamalloa, I. Lopez, and V. Deniau, "Towards a resilient railway communication network against electromagnetic attacks," in *TRA-Transport Research Arena*, 2014.

[174] M. Bagnulo, "Threat Analysis for TCP Extensions for Multipath Operation with Multiple Addresses," RFC 6181 (Informational), Internet Engineering Task Force, Mar. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6181.txt

[175] M. Bagnulo, C. Paasch, F. Gont, O. Bonaventure, and C. Raiciu, "Analysis of Residual Threats and Possible Fixes for Multipath TCP (MPTCP)," RFC 7430, Jul. 2015. [Online]. Available: https://rfc-editor.org/rfc/rfc7430.txt

[176] C. Paasch and A. Ford, "Application Layer Authentication for MPTCP," Internet Engineering Task Force, Internet-Draft draft-paasch-mptcp-application-authentication-00, May 2016, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-paasch-mptcp-application-authentication-00

[177] "SEC 2: Recommended Elliptic Curve Domain Parameters," Certicom Research, Standards for efficient cryptography, 2000. [Online]. Available: http://www.secg.org/SEC2-Ver-1.0.pdf

[178] C. Paasch and O. Bonaventure, "Securing the MultiPath TCP handshake with external keys," Internet Engineering Task Force, Internet-Draft draft-paasch-mptcp-ssl-00, Oct. 2012, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-paasch-mptcp-ssl-00

[179] E. B. Barker and A. L. Roginsky, "Sp 800-131a. transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths," Gaithersburg, MD, United States, Tech. Rep., 2011.

[180] "The algorithms, key size and parameters report," Tech. Rep., 2014.

[181] F. Sheet, "Suite b cryptography," *National Security Agency (NSA)*, 2014.

[182] M. Hartong, R. Goel, and D. Wijesekera, "Key management requirements for ptc operations," *Vehicular Technology Magazine, IEEE*, vol. 2, no. 2, pp. 4–11, 2007.

[183] U. SUBSET, "Rbc-rbc safe communication interfaces, version 3.0.0."

[184] G. Iannaccone, C.-N. Chuah, S. Bhattacharyya, and C. Diot, "Feasibility of ip restoration in a tier 1 backbone," *Ieee Network*, vol. 18, no. 2, pp. 13–19, 2004.

[185] A. Kvalbein, A. F. Hansen, T. Cicic, S. Gjessing, and O. Lysne, "Fast recovery from link failures using resilient routing layers," in *Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE Symposium on*. IEEE, 2005, pp. 554–560.

[186] T. Čičić, A. F. Hansen, S. Gjessing, and O. Lysne, "Applicability of resilient routing layers for k-fault network recovery," in *International Conference on Networking*. Springer, 2005, pp. 173–183.

[187] J. P. Rohrer, A. Jabbar, and J. P. Sterbenz, "Path diversification: A multipath resilience mechanism," in *Design of Reliable Communication Networks, 2009. DRCN 2009. 7th International Workshop on*. IEEE, 2009, pp. 343–351.

[188] J. P. Rohrer and J. P. Sterbenz, "Predicting topology survivability using path diversity," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on*. IEEE, 2011, pp. 1–7.

[189] X. Yang and D. Wetherall, "Source selectable path diversity via routing deflections," in *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 4. ACM, 2006, pp. 159–170.

[190] A. Farrel, J.-P. Vasseur, and J. Ash, "A Path Computation Element (PCE)-Based Architecture," RFC 4655 (Informational), Internet Engineering Task Force, Aug. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4655.txt

[191] S. Zannettou, M. Sirivianos, and F. Papadopoulos, "Exploiting path diversity in datacenters using mptcp-aware sdn," in *Computers and Communication (ISCC), 2016 IEEE Symposium on*. IEEE, 2016, pp. 539–546.

[192] U.-R. S. Department, "Ip introduction to railways—version 2.0-guideline for the fixed telecommunication network," 2013.

[193] J. P. Rohrer, R. Naidu, and J. P. Sterbenz, "Multipath at the transport layer: An end-to-end resilience mechanism," in *Ultra Modern Telecommunications & Workshops, 2009. ICUMT'09. International Conference on*. IEEE, 2009, pp. 1–7.

[194] A. Mendiola, J. Astorga, E. Jacob, M. Higuero, A. Urtasun, and V. Fuentes, "Dynpac: A path computation framework for sdn," in *Software Defined Networks (EWSDN), 2015 Fourth European Workshop on*. IEEE, 2015, pp. 119–120.

[195] B. Hesmans, G. Detal, S. Barre, R. Bauduin, and O. Bonaventure, "Smapp: Towards smart multipath tcp-enabled applications," in *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies*. ACM, 2015, p. 28.

[196] M. Aguado, C. Pinedo, I. Lopez, I. Ugalde, C. De Las Munecas, L. Rodriguez, and E. Jacob, "Towards zero on-site testing: Advanced traffic management & control systems simulation framework including communication kpis and response to failure events," in *Wireless Vehicular Communications (WiVeC), 2014 IEEE 6th International Symposium on*. IEEE, 2014, pp. 1–2.

[197] "Riverbed Modeler, howpublished = https://www.riverbed.com/es/products/steelcentral/steelcentral-riverbed-modeler.html, note = Accessed: 2016-09-16."

[198] C. Pinedo, M. Aguado, I. Lopez, and J. Astorga, "Modelling and simulation of ertms for current and future mobile technologies," *International Journal of Vehicular Technology*, vol. 2015, 2015.

[199] C. Pinedo, I. Lopez, M. Aguado, and E. Jacob. (2015, Jun.) Redundant mptcp repository. [Online]. Available: https://github.com/i2t/rmptcp

[200] "Multi-Generator (MGEN), howpublished = http://www.nrl.navy.mil/itd/ncs/products/mgen, note = Accessed: 2016-09-16."

[201] V. Paxson, M. Allman, J. Chu, and M. Sargent, "Computing TCP's Retransmission Timer," RFC 6298 (Proposed Standard), Internet Engineering Task Force, Jun. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6298.txt

[202] M. Rajiullah, P. Hurtig, A. Brunstrom, A. Petlund, and M. Welzl, "An evaluation of tail loss recovery mechanisms for tcp," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 1, pp. 5–11, 2015.

[203] P. Hurtig, A. Brunstrom, A. Petlund, and M. Welzl, "Tcp and stream control transmission protocol (sctp) rto restart," Tech. Rep., 2016.

[204] V. Jacobson, "Congestion avoidance and control," in *ACM SIGCOMM Computer Communication Review*, vol. 18, no. 4. ACM, 1988, pp. 314–329.

[205] Y. C. N. Dukkipati, N. Cardwell and M. Mathis, "Tail Loss Probe (TLP): An Algorithm for Fast Recovery of Tail Losses," Internet Engineering Task Force, Apr. 2013. [Online]. Available: https://tools.ietf.org/html/draft-dukkipati-tcpm-tcp-loss-probe-01.txt

[206] "ITU-R Rec. M.1457-8", Detailed Specifications of the Radio Interfaces of International Mobile Telecommunications-2000 (IMT-2000)," International Telecommunication Union, 2008. [Online]. Available: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2134-2008-PDF-E.pdf

[207] I. Lopez, M. Aguado, and C. Pinedo, "A step up in european rail traffic management systems: A seamless fail recovery scheme," *IEEE Vehicular Technology Magazine*, vol. 11, no. 2, pp. 52–59, 2016.

[208] Y. Liu, A. Neri, and A. Ruggeri, "Integration of plmn and satellite networks for train control and traffic management via mptcp," in *ITS Telecommunications (ITST), 2015 14th International Conference on*. IEEE, 2015, pp. 75–79.

[209] Y. Liu, A. Neri, A. Ruggeri, and A. M. Vegni, "A mptcp-based network architecture for intelligent train control and traffic management operations," *IEEE Transactions on Intelligent Transportation Systems*, 2016.

[210] F. Mazzenga, R. Giuliano, A. Neri, and F. Rispoli, "Integrated public mobile radio networks/satellite for future railway communications," *IEEE Wireless Communications*, 2016.

[211] H. Zhang, W. Quan, J. Song, Z. Jiang, and S. Yu, "Link state prediction-based reliable transmission for high-speed railway networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9617–9629, 2016.

[212] I. Lopez, M. Aguado, D. Ugarte, A. Mendiola, and M. Higuero, "Exploiting redundancy and path diversity for railway signalling resiliency," in *Intelligent Rail Transportation (ICIRT), 2016 IEEE International Conference on*. IEEE, 2016, pp. 432–439.

[213] C. Pinedo, M. Aguado, I. Lopez, M. Higuero, and E. Jacob, "A multi bearer adaptable communication demonstrator for train-to-ground ip communication to increase resilience," in *International Workshop on Communication Technologies for Vehicles*. Springer International Publishing, 2016, pp. 98–100.

[214] I. Lopez, M. Aguado, C. Pinedo, and E. Jacob, "Scada systems in the railway domain: enhancing reliability through redundant multipathtcp," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*. IEEE, 2015, pp. 2305–2310.

[215] L. Rodriguez, C. Pinedo, I. Lopez, M. Aguado, J. Astorga, M. Higuero, I. Adin, G. Bistué, and J. Mendizabal, "Eurobalise-train communication modelling to assess interferences in railway control signalling systems," *Network Protocols and Algorithms*, vol. 8, no. 1, pp. 58–72, 2016.