This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688421.

mami

Measurement and Architecture for a Middleboxed Internet

H2020-ICT-688421

Final Standardisation, Dissemination, and Exploitation Report

Author(s):	TID	Diego R. Lopez (ed.)
	ETH	Brian Trammell
	ULg	Benoit Donnet
	UNIABDN	Gorry Fairhurst, Ana Custura
	ZHAW	Stephan Neuhaus
	SRL	David Ros
	ALCATEL	Thomas Fossati
	U3CM	Pedro A. Aranda

Document Number:	D4.4
Internal Reviewer:	Mirja Kühlewind
Due Date of Delivery:	31 December 2018
Actual Date of Delivery:	21 December 2018
Dissemination Level:	Public

Disclaimer

The information, documentation and figures available in this deliverable are written by the MAMI consortium partners under EC co-financing (project H2020-ICT-688421) and does not necessarily reflect the view of the European Commission.

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user uses the information at its sole risk and liability.

Contents

Executive Summary

This deliverable covers the activities related to dissemination, exploitation, and standardisation of the project, describing the key aspects of these activities and their progress since last report made in D4.3 in June 2017. The three aspects mentioned before are detailed with respect to target stakeholder groups through the relevant channels identified.

Since this is the final report, a final analysis of the results of the MAMI project in these matters is provided as part of the conclusions of this document.

1 Introduction

The MAMI project has evolved from the original goal of developing a specific protocol to the definition of path-awaraness prinicples and their application to the nework and transport layers, based on the collection and analysis of large-scale middlebox impairment measurements in the Path Transparency Observatory (PTO) and experimentation in Internet testbeds, to support deployment of ubiquitous encryption while maintaining support of in-network functionality in a cooperative way between endpoints and middleboxes.

The MAMI goals could only be achieved by means of a high impact of the project results at the scientific, industrial, and societal levels, in Europe and beyond. This required a coordinated dissemination and outreach activity, with special emphasis on the standardisation matters, and therefore a dedicated workpackage (WP4: Standardisation, Dissemination and Exploitation) was devised to maximize the impact of the project results in all fields addressed in it.

This deliverable reports the activities related to the external communication and dissemination of project results, the identification of targets for further industrial exploitation, and the steps taken to contribute to the relevant standards organizations. Since this is the final report, a final analysis of the results of the MAMI project in these matters is provided as part of the conclusions of this document.

WP4 has worked towards creating the maximum awareness about the main goals for the project, related to the application of path-aware networking along the guidelines of measuring the real Internet, providing experimental evidence, and facilitate repeatability by means of virtualization. The previous periods have delivered significant results on scientific dissemination and standardization, and the consolidation of concepts such as explicit support for in-network measurements, trust-but-verify-based service differentiation, and automated management of short-lived trust links.

During this final period, the project has been able to address industrial impact as well, by means of a dedicated event with a good attendance of all possible industrial stakeholders (developers, integrators, service providers...), a whitepaper focused on the network service providers, and direct dissemination activities around industrial events on network technologies. This activity for creating industrial awareness has not interfered with the standardization and scientific publication activities, that have increased during this period (though papers and presentations as well as organization of a workshop, summer-school, and tutorial), consolidating the promising results mentioned in previous reports. Finally, the opportunities for close-to-real experimentation with some of the project results have open new ways for further exploitation.

2 Standardisation

The MAMI team has continued working in the contributions to the IETF QUIC WG and the related IETF activities focused on Internet stack evolution to incorporate the principles that inspired the original MCP proposal:

- Authoring and editing the QUIC applicability and manageability documents. The former discusses considerations for building and deploying applications (not limited to HTTP) over QUIC, and the latter is a "user's guide" to the QUIC wire image. These will be published as RFCs in 2019.
- Advocating for the incorporation of the latency spin bit in the QUIC standard for explicit measurability of end-to-end round-trip time of QUIC flows, despite the encryption of the QUIC header. This effort ended in success at IETF 103 in Bangkok in November 2018, as the WG reached consensus to include the spin bit in the protocol definition.

The MAMI team has driven forward work in the IETF Transport Services (TAPS) working group, contributing to the three core documents on the transport services architecture, an abstract interface to transport services, and implementations of this interface. TAPS has evolved from a transport agility mechanism – an Internet-standard version of the Flexible Transport Layer (FTL) envisioned by MAMI – into a full-fledged effort to define a new abstract interface to the transport layer that supports necessary features for future Internet transports: asynchronicity, stack agility, connection racing, peer-to-peer rendezvous, low-latency secure connection resumption, and so on. Work on this effort is shared with other European universities as well as telecom providers and platform companies, and should result in the publication of RFCs defining this new interface in late 2019.

These activities around the transport layer protocols and interfaces are complemented by contributions related to DSCP, MTU discovery, UDP options, and different proposals related to the use and effects of encryption at the transport layer, mainly in the IETF Transport Area working group (TSVWG). Especially a presentation in MAPRG in IETF 103 showed that the checksum that was specified in UDP options had poor support across middleboxed paths, and a replacement checksum was proposed by the MAMI project, the checksum compensation option, which TSVWG is now considering as an update to the UDP options specification.

The original contributions made to the IETF ACME WG to define mechanisms supporting key and certificate management able to control trust link delegation to unattended devices or processes through the STAR approach has been adopted by the WG and the main specification is on its way for final publication as an RFC. A companion mechanism enabling certificate delegation under complete control of the delegating entity has been adopted by the ACME working group during the recent Bangkok meeting.

Within the Internet Research Task Force (IRTF), the Path-Aware Networking Research Group (PANRG) founded by the project has transitioned from proposed to active IRTF RG, chartered to support research in bringing path awareness to transport and application layer protocols, very much in line with the goals of MAMI, as it addresses the communication and discovery of information about the properties of a path, the exploration of trust and risk models associated with this information, and algorithms for path selection at endpoints based on this information, including their interactions with the widely deployed routing protocols and network operations best practices. Likewise, the Measurement and Analysis for Protocols (MAP)RG, also founded

by MAMI, has continued its work on providing research evidence on Internet measurement to inform protocol engineering and practice, one of the key original goals of the MAMI project. And the results on the enhancements on experiment repeatability achieved by applying NFV descriptors were reported to the NFV RG.

MAMI authors contributed to an Internet Architecture Board stream document defining the "wire image" of a network protocol, as part of a wider effort to help frame discussions in the IETF about how network elements can and should interact with end-to-end protocols on the Internet. This document has been approved by the IAB in December 2018 for an early 2019 publication.

Besides the IETF, other standards organizations are considering the standardisation of mechanisms for the collaboration of network-hosted middleboxes and communication endpoints, especially from the point of view of providing security services. In particular, the work of ETSI TC CYBER on the features of what has been termed as a “Middlebox Cooperation Protocol”’ in their DTS/CYBER-0027 series of specifications. In particular, the project has supported and contributed to the definition of requirements, and to a profile applicable to the transport layer. In addition, the MAMI team has kept monitoring the evolution of the the IEEE Encrypted Traffic Inspection (ETI) WG, though this group has not gone beyond formulating a set of basic principles, to which we have contributed according to the results of the project and the coordination activities performed.

Finally, the project has continued the collaboration within the GSMA Internet WG in the realization of experiments to evaluate the impact of applying LoLa classification schemes to traffic management in mobile networks, leveraging the applicability of NFV descriptors to define and reproduce experiments. Originally run on the 5TONIC[1] testbed, the experiment descriptions are being made available as open-source to support additional evidence from independent experiments. The results from experimentation have successfully validated the LoLa hypothesis and the activity has now entered a further phase where the signalling and the APIs on top of that need to be standardised. As such, also work in the IETF TSVWG has been started to specify the needed DiffServ codepoints and the expected treatment by the mobile network.

Table 2 lists standardisation documents that have been published or revised with a contribution of the MAMI project in the last year since the last report. RFC8436 has been already published as output of the IETF’s standardisation effort in the RFC series, and all other documents are work in progress.

[1] http://http://www.5tonic.org/

Body/Group	Document name	partners	sub. date	exp. date
IETF QUIC	draft-ietf-quic-manageability-03	ETH	Oct 18	Apr 19
IETF QUIC	draft-ietf-quic-applicability-03	ETH	Oct 18	Apr 19
IETF QUIC	draft-ietf-quic-spin-exp-01	ETH	Oct 18	Apr 19
IETF QUIC	draft-trammell-why-measure-rtt-00	ETH	Aug 18	Feb 19
IETF TAPS	draft-ietf-taps-arch-02	ETH, UNIABDN	Oct 18	Apr 19
IETF TAPS	draft-ietf-taps-interface-02	ETH, UNIABDN	Oct 18	Apr 19
IETF TAPS	draft-ietf-taps-impl-02	UNIABDN	Oct 18	Apr 19
IETF TAPS	draft-kuehlewind-taps-crypto-sep-03	ETH	Jun 18	Jan 19
IETF TCPM	draft-ietf-tcpm-accurate-ecn-07	ETH	Jul 18	Jan 19
IETF ACME	draft-ietf-acme-star-04	Nokia, TID	Oct 18	Apr 19
IETF ACME	draft-ietf-acme-star-delegation-00	Nokia, TID	Dec 18	Jun 19
IETF TLS	draft-ietf-tls-dtls-connection-id-02	Nokia	Oct 18	Apr 19
IETF 6MAN	draft-hinden-6man-mtu-option-00	UNIABDN	Oct 18	Apr 19
IETF TSVWG	RFC 8436	UNIABDN	Aug 18	—
IETF TSVWG	draft-ietf-tsvwg-transport-encrypt-01	UNIABDN	Oct 18	Apr 19
IETF TSVWG	draft-ietf-tsvwg-datagram-plpmtud-06	UNIABDN	Nov 18	May 19
IETF TSVWG	draft-fairhurst-udp-options-cco-00	UNIABDN	Oct 18	Apr 19
IETF TSVWG	draft-trammell-tsvwg-spin-00	ETH	Jul 18	Apr 19
IETF TSVWG	draft-fossati-tsvwg-lola-00	Nokia, UNIABDN, ETH, UC3M	Dec 18	Jun 19
IETF IAB	draft-iab-wire-image-00	ETH	Nov 18	May 19
IRTF NFVRG	draft-aranda-nfvrg-recursive-vnf-06	TID, UC3M	Jul 18	Jan 19
ETSI CYBER	DTS/CYBER-0027-1 (ETSI)	TID	Oct 18	—
ETSI CYBER	DTS/CYBER-0027-2 (ETSI)	TID	Sep 18	—

Table 1: Standardisation documents: RFC8436 and work in progress.

3 Dissemination and Communication

Besides other dissemination and communication actions as listed below, the MAMI project continuously participates in EC clustering initiatives, such as the FIRE Dissemination Working Group (DWG). As a supplement of this dissemination efforts within the EU research landscape, the project has further developed cooperative relationships with related EC-funded projects during this last reporting period, reinforcing the connections with MONROE and NEAT, and starting a new one with 5GINFIRE, focused on the deployment of NFV-based versions of `Pathspider` and `Trafic` on the project NFV infrastructure as tools for monitoring and experimentation.

MAMI's communication actions have been focused on social media through a webpage blog and twitter, in-person dissemination at research and industry events, including the organization of research workshops a summer-school, and tutorials, as well as the publication of papers, both through the standard scientific peer-review process and by other means (e.g. white papers) when targeting a specific, industrial audience. These activities are further described below.

3.1 Communication Actions

The MAMI website `https://mami-project.eu/` has been continuously updated with information on publications, standardisation efforts, events, and a lively blog used to disseminate MAMI research results and activities. Currently there are 36 blog posts in total, with 12 new posts since the last report. The posts contain reports from standardisation events, workshops, project meeting as well as measurements reports and comments on on-going research or software development. Two additional blog post are planned beyond the end of the project in January 2019, on the PTO and a final conclusive note, before the webpage will be converted into a static page for long term archival.

Currently, a web front end to v3 of the MAMI PTO is online the subdomain (`https://v3.pto.mami-project.eu/`), however, will be moved to (`https://pto.mami-project.eu/`) by the end of the project for long term support. Further, MAMI provides own webpage for PATHspider (`https://pathspider.net/`), that will be maintained beyond the end of the project.

The MAMI twitter account (`@mamiproject`)has been actively maintained to announce MAMI work and publications as well as blog posts. As of 20 December 2018, the channel had 244 followers and a total of 3686 tweets since June 2016, that received 527 likes.

3.2 Workshops and Events

Just before IETF 101 in London in March, the MAMI project hosted an invitation-only MAMI Management and Measurement Summit (M3S `https://mami-project.eu/index.php/events/mami-management-and-measurement-summit-m3s/`), bringing together researchers, engineers, and vendors for a focused discussion on how to meet the challenges posed to network measurement and network management by the increasing deployment of strong encryption and the extension of encryption down the stack. The results of the summit where published in a whitepaper "Challenges in Network Management of Encrypted Traffic", discussing the prin-

ciples of allowing independent measurability of important metrics, the interaction of network management with the transport layer while not breaking application layer security, and the replacement of transparent middleboxes with middlebox transparency, where the middlebox and its functions are visible to the endpoints, and the endpoints have some control over how their traffic is treated by the network.

In June 2018, UNIABDN hosted the MAMI Summer School on Internet Path Transparency Measurements (`https://github.com/mami-project/roadshows/tree/master/mami-summer-school`). This consisted of a hands-on tutorial, with participation both on-site and remote via video conference, on different MAMI tools: Tracebox, PATHspider and the PTO.

The project organized a second edition of the joint workshop with the EU-H2020 MONROE project on Mobile Network Measurements (MNM18, `http://tma.ifip.org/2018/mnm-workshop/`), co-located with the Network Traffic Measurement and Analysis Conference (TMA 2018) which was held June in Vienna. The workshop included one invited and six regular talks focusing on WebRTC measurements, network QoS and mobile coverage, multipath and application performance, and concluded with an introduction to the use of the MONROE platform and mobile measurements using PATHspider.

At SIGCOMM 2018, held in Budapest in August, the MAMI project held a tutorial on Repeatability and Comparability in Measurement (RCM), again presenting PATHspider and the PTO as tools developed by the project in order to increase the user community.

Finally, a two-day PATHspider hackathon was organized with participants from MAMI and the Open Observatory of Network Interference (OONI) project[1] at the University of Aberdeen, and the collaboration of the Tor Project[2] on December 5-7, 2018. The goal of the hackathon was to share experiences in Internet measurement and an intregration of PATHspider into the OONI platform.

3.3 Industrial Dissemination

The concept of path-aware networking, how it has evolved during the MAMI project execution, and how it can be applied in current and next-generation network infrastructures was presented by TID at one of the best established industrial events on emerging network technologies in Europe, the MPLS+SDN+NFV World Congress (Paris, April 2018 `https://www.uppersideconferences.com/mpls-sdn-nfv/`)

In addition, the project has produced three white papers, addressed at the network industry. The first one (`http://arxiv.org/abs/1810.09272`), a direct output of the M3S workshop (see above), covering the discussions and distilling the recommendations that came out of the meeting. The second is a whitepaper on "Analysis and Consideration on Management of Encrypted Traffic" (`https://arxiv.org/abs/1812.04834`) specifically addressed to the telco ecosystem (network operators, providers, integrators, regulators...) with the goal of analysing the tussle between the pure end-to-end view and the application of middleboxes to enhance network services, considering the evolution and status of these approaches, and promoting the application of path-aware networking as a way for a more open and sustainable Internet environment. A third whitepaper, as the main outcome of T3.5, provide a analysis of "Security and Privacy Implications of Middlebox Cooperation Protocols" (`https://arxiv.org/abs/1812.05437`). The

[1] `https://ooni.torproject.org/`
[2] `https://www.torproject.org/`

project team has started the distribution in the wider telco industry of these papers.

3.4 Software

The MAMI project makes all software efforts openly available on GitHub (`https://github.com/mami-project/`). Table 2 lists all active repositories in the last year, as well as the MAMI partners that are currently working on the respective software or study. Repositories are ordered according to the most recent activity on them. After the end of the project, all partners will review these repositories in order to check documentation of completed software, guarantee appropriate access rights for future maintainance where needed, or remove obsoleted repositories.

Table 2: List of public MAMI software and documentation repositories in github

Repository	Description	Partner(s)
pathspider	Tool for A/B testing of path transparency to certain features in the Internet	ETHZ, UNI-ABDN
roadshows	Public slideware for the H2020-ICT-688421 MAMI project	All
vpp-mb	Modular MiddleBox (mmb) plugin for VPP (fd.io)	ETHZ
pto3-go	MAMI Path Transparency Observatory server (v3) and associated utilities	ETHZ, ZHAW
draft-pauly-transport-security	TAPS Survey of transport security protocols and their features and interfaces	ETHZ, extern
trafic	A traffic mix generator based on iperf3	Nokia, UC3M
gce-camp	Scripts for managing active measurement runs on Google Compute Engine	
nemo	Intent-based network description and NFVD generation	TID, UC3M
VPP-latency-middlebox	VPP-based passive latency measurement middlebox	ETHZ
three-bits-suffice	Supporting data and code for IMC 2018 submission "Three Bits Suffice"	ETHZ
monroe-puic-poll	puic-poll docker monroe	SRL, UNI-ABDN
pto3-web	Path Transparency Observatory (PTO) web frontend	ZHAW
pto3-ecn	ECN analyzers for Path Transparency Observatory (PAPI v3)	ETHZ

Table 2: List of public MAMI software and documentation repositories in github (continued)

Repository	Description	Partner(s)
sigcomm-rcm-tutorial	Slides and additional material for the SIGCOMM Tutorial on Repeatability and Comparability in Measurement (RCM)	ETHZ
tracebox	Tracebox over Scamper	ULg
bpqd	Basic Passive QUIC Diagnostics: figuring out what's going on with QUIC flows from PCAP	ETHZ
plus-probe	Probing PLUS	ETHZ
plus-lib	Library providing support for PLUS connections and packets	ETHZ
draft-kuehlewind-crypto-sep	Description of an architecture separating persistent cryptographic and ephemeral per-path transport state	ETHZ
pto3-trace	PTO analyzers for traceroute, tracebox, and other hop-sequence-like datasources	ETHZ, ZHAW
PyPLUSPacket	Python library to parse PLUS packets	ETHZ
plus-gopacket	Fork of google/gopacket with PLUS support plus	ETHZ
plus-quic-go	Fork of lucas-clemente/quic-go with PLUS support added	ETHZ
plus-pcap	Command line tool to inspect/capture PLUS packets	ETHZ
plus-debug	pdbg protocol	ETHZ
mcsVNF	VNFs providing support for demonstrating multi-context security	TID
hellfire	PATHspider Effects List Resolver	UNIABDN
pathspider-tutorial	Tutorial on PATHspider	UNIABDN
pathspider-evilbit	Demonstration plugin for MAMI Summer School on Internet Path Transparency Measurement	UNIABDN
pto3-access	Accessing the MAMI Path Transparency Observatory for analysis using Jupyter notebooks	ETHZ, ZHAW
lurk	ACME/STAR implementation	Nokia, TID
spinbit-testbed	Transport measurability tooling	ETHZ
postsocket	Go implementation of PostSockets over various transports	ETHZ
plusspector	Simple PLUS relay	ETHZ
plus-dissector	PLUS wireshark	ETHZ
plus-echo	plus echo server client	ETHZ
rtt-privacy-paper	Analysis of privacy implications of spin bit	ETHZ
pingme	Web service to perform measurements toward a client and respond with the results	
draft-trammell-plus-statefulness	Text for the draft	ETHZ

Table 2: List of public MAMI software and documentation repositories in github (continued)

Repository	Description	Partner(s)
draft-trammell-post-sockets	Post Sockets: An Abstract Programming Interface for the Transport Layer	ETHZ
ns3-aqm-l4s	ns-3 based implemenation of various AQM algorithms, uncoupled dualq, and coupled dualq (l4s)	
pto3	Deprecated Python PTO API v3 implementation	ETHZ, ZHAW
KeyServer	Key Server that implements the TLS Session Key Interface (SKI) defined in draft-cairns-tls-session-key-interface-00	Nokia
pathspider-monroe	Docker image for PATHspider on MONROE	UNIABDN
one-bit-experiment	Scripts for IETF hackathon and GSMA report	Nokia, TID

MAMI also attempts to distribute measurement tools developed during the project via packages in software distribution systems, for example the Debian Operating System[3] and the Python Package Index[4].

The PATHspider releases up to the current 2.0.1 are available for installation from PyPI[5]. PATHspider 1.0.1-1 has been included in the release of the latest stable version of the Debian operating system[6]. A full list of software release is provided below. Dates for Debian Operating System indicate the date that the software was published in the "unstable" suite.

Table 3: List of publication of software to collections

Software	Collection	Publication Date
canid	Debian Operating System	2018-01-25
canid	Debian Operating System	2018-06-13
canid	Debian Operating System	2018-07-08
hellfire	Debian Operating System	2018-01-25
hellfire	Debian Operating System	2018-07-08
PATHspider 0.9.0	Debian Operating System	2016-07-06
PATHspider 1.0.0	Python Package Index	2016-10-21
PATHspider 1.0.0	Debian Operating System	2016-10-31
PATHspider 1.0.1	Python Package Index	2016-11-04
PATHspider 1.0.1	Debian Operating System	2016-11-04
PATHspider 2.0.0	Python Package Index	2018-01-11
PATHspider 2.0.1	Python Package Index	2018-01-19
PATHspider 2.0.1	Debian Operating System	2018-01-23

[3] https://www.debian.org
[4] https://pypi.python.org/
[5] https://pypi.python.org/pypi/pathspider
[6] https://packages.debian.org/source/stable/pathspider

Additionally, as dependencies for PATHspider:

- python-libtrace was published to the Debian Operating System with MAMI acknowledgement on 2016-04-11, 2016-04-13, 2016-11-04, 2017-08-30, 2018-01-10 and 2018-06-09 (https://packages.qa.debian.org/p/python-libtrace.html)
- scapy3k was published to the Debian Operating System with MAMI acknowledgement on 2016-04-29, 2016-12-02, 2018-01-10 (https://packages.qa.debian.org/s/scapy3k.html)
- scapy was published to the Debian Operating System with MAMI acknowledgement on 2018-05-07 (https://packages.qa.debian.org/scapy.html)
- pycurl was published to the Debian Operating System with MAMI acknowledgement on 2018-01-22 and 2018-02-01 (https://packages.qa.debian.org/p/pycurl.html)

Each of these projects contains small contributions from MAMI, but the acknowledgements are intended to only cover the work to prepare the software for inclusion in Debian, or to update the existing packaging to include new upstream work.

Further, partners of the MAMI project regularly participate in IETF Hackathons to socialise ideas and code related to MAMI activities. During this last period, this participation has focused on ACME/STAR and the `Trafic` tool.

3.5 Publications and Talks

During this last period, the project has increased its activity in communicating project findings and results to the research community. The following table provides an overview of scientific talks and papers that are newly published or already accepted but not published yet since the last report in June 2017. The project webpage contains a full list usable for formal references.

Table 4: List of MAMI publications

Venue	Date	Title	Author(s)
ACM CoNEXT 2018 Workshop on the Evolution, Performance, and Interoperability of QUIC (EPIQ'18)	December 2018	**TAPS: an abstract application interface for QUIC**	Kühlewind, Mirja; Trammell, Brian; Brunstrom, Anna; Welzl, Michael; Fairhurst, Gorry
The TAPS Architecture for Transport Services provides a framework for the design of a protocol-independent asynchronous message-based transport API. While the traditional BSD socket API requires the user to make a choice about which protocol to use from the beginning, the TAPS API focuses on transport features and gives the transport stack itself the opportunity to select the most appropriate protocol. This exibility also supports deployment of new protocols, such as QUIC, because the application does not need to change in order to bene t from such new innovations. This poster de nes two API mappings for QUIC, either exposing multistreaming explicitly to the application or providing a way to utilize multistreaming without application input.			

Table 4: List of MAMI publications (continued)

Venue	Date	Title	Authors
Internet Measurement Conference (IMC) 2018	November 2018	**Three Bits Suffice: Explicit Support for Passive Measurement of Internet Latency in QUIC and TCP**	Vaere, Piet De; Bühler, Tobias; Kühlewind, Mirja; Trammell, Brian
This work introduces the latency spin signal as a lightweight, transport-independent and explicit replacement for TCP timestamps for passive latency measurement. This signal supports per-flow, single-point and single direction passive measurement of end-to-end RTT using just three bits in the transport protocol header, leveraging the existing dynamics of the vast majority of Internet-deployed transports. We show how the signal applies to measurement of both TCP and to QUIC through implementation of the signal in endpoint transport stacks. We also provide a high-performance measurement implementation for the signal using the Vector Packet Processing (VPP) framework. Evaluation on emulated networks and in an Internet testbed demonstrate the viability of the signal, and show that it is resistant to even large amounts of loss or reordering on the measured path.			
Mobicom 2018	October 2018	**Experience: Implications of Roaming in Europe**	Mandalari, Anna Maria; Lutu, Andra; Custura, Ana; Khatouni, Ali Safari; Alay, Özgü; Bagnulo, Marcelo; Bajpai, Vaibhav; Brunstrom, Anna; Ott, Jörg; Mellia, Marco; Fairhurst, Gorry
This paper provides an in-depth characterization of the implications of international data roaming within Europe. We build a unique roaming measurement platform using 16 different mobile networks deployed in six countries across Europe. Using this platform, we measure di erent aspects of international roaming in 3G and 4G networks, including mobile network con guration, performance characteristics, and content discrimination. We nd that operators adopt common approaches to implementing roaming, resulting in additional latency penalties of 60 ms or more, depending on geographical distance. Considering content accessibility, roaming poses additional constraints that leads to only minimal deviations when accessing content in the original country. However, geographical restrictions in the visited country make the picture more complicated and less intuitive.			
Network Traffic Measurement and Analysis Conference (TMA 2018)	June 2018	**Exploring usable Path MTU in the Internet**	Custura, Ana; Fairhurst, Gorry; Learmonth, Iain
To optimise their transmission, Internet endpoints need to know the largest size of packet they can send across a specific Internet path, the Path Maximum Transmission Unit (PMTU). This paper explores the PMTU size experienced across the Internet core, wired and mobile edge networks. Our results show that MSS Clamping has been widely deployed in edge networks, and some webservers artificially reduce their advertised MSS, both of which we expect help avoid PMTUD failure for TCP. The maximum packet size used by a TCP connection is also constrained by the acMSS. MSS Clamping was observed in over 20% of edge networks tested. We find a significant proportion of webservers that advertise a low MSS can still be reached with a 1500 byte packet. We also find more than half of IPv6 webservers do not attempt PMTUD and clamp the MSS to 1280 bytes. Furthermore, we see evidence of black-hole detection mechanisms implemented by over a quarter of IPv6 webservers and almost 15% of IPv4 webservers. We also consider the implications for UDP, which necessarily can not utilise MSS Clamping. The paper provides useful input to the design of a robust PMTUD method that can be appropriate for the growing volume of UDP-based applications, by determining ICMP quotations can be used as to verify sender authenticity.			

Table 4: List of MAMI publications (continued)

Venue	Date	Title	Authors
Network Traffic Measurement and Analysis Conference (TMA 2018)	June 2018	**Tracing Internet Path Transparency**	Kühlewind, Mirja; Walter, Michael; Learmonth, Iain R.; Trammell, Brian
Investigating Internet Path Transparency means measuring if a network path between two endhosts is impaired by in-network functions on the path. A path is considered transparent if it provides connectivity and the same performance independent of the protocol or protocol stack that is used for the transmission. Unfortunately this is not always the case. Simple firewalls that block e.g. UDP, are an example. Of course such in-network functions are often valuable, like firewalls. However, these middleboxes also, sometimes unintentionally, make assumptions about the traffic passing through them that restricts innovation in the Internet on the higher layers, e.g. the deployment of new UDP-based protocols such as QUIC, to stick with the previous example. PATHspider is an active measurement tool to test for Path Transparency. In this paper we present a new feature of PATHspider that integrates tracebox-based functionality and analysis to not only detect in-transparency but also further locate the origin of the impairment observed. As an example study we show updated and extended measurements on ECN support and connectivity. By using our enhanced ECN PATHspider plugin to test network support of the ECN IP codepoint and additional path tracing that is correlated with DSCP testing, we show that most in-network ECN IP codepoint zeroing is due to use of the deprecated definition of the IP ToS field for domain-internal service differentiation, while pure resetting of the ECN IP field is more likely an active inference in border networks.			
IEEE INFOCOM 2018	April 2018	**The Cloud that Runs the Mobile Internet: A Measurement Study of Mobile Cloud Services**	Michelinakis, F.; Doroud, H.; Razaghpanah, A.; Lutu, A.; Vallina-Rodriguez, N.; Gill, P.; Widmer, J.
Mobile applications outsource their cloud infrastructure deployment and content delivery to cloud computing services and content delivery networks. Studying how these services, which we collectively denote Cloud Service Providers (CSPs), perform over Mobile Network Operators (MNOs) is crucial to understanding some of the performance limitations of today's mobile apps. To that end, we perform the first empirical study of the complex dynamics between applications, MNOs and CSPs. First, we use real mobile app traffic traces that we gathered through a global crowdsourcing campaign to identify the most prevalent CSPs supporting today's mobile Internet. Then, we investigate how well these services interconnect with major European MNOs at a topological level, and measure their performance over European MNO networks through a monthlong measurement campaign on the MONROE mobile broadband testbed. We discover that the top 6 most prevalent CSPs are used by 85% of apps, and observe significant differences in their performance across different MNOs due to the nature of their services, peering relationships with MNOs, and deployment strategies. We also find that CSP performance in MNOs is affected by inflated path length, roaming, and presence of middleboxes, but not influenced by the choice of DNS resolver.			

Table 4: List of MAMI publications (continued)

Venue	Date	Title	Authors
15th USENIX Symposium on Networked Systems Design and Implementation (NSDI'18)	April 2018	**Stroboscope: Declarative Network Monitoring on a Budget**	Tilmans, Olivier; Bühler, Tobias; Poese, Ingmar; Vissicchino, Stefano; Vanbever, Laurent
We present Stroboscope, a system that enables fine-grained monitoring of any traffic flow by instructing routers to mirror millisecond-long traffic slices in a programmatic way. Stroboscope takes as input high-level monitoring queries together with a budget and automatically determines: (i) which flows to mirror; (ii) where to place mirroring rules, using fast and provably correct algorithms; and (iii) when to schedule these rules to maximize coverage while meeting the input budget. We implemented Stroboscope, and show that it scales well: it computes schedules for large networks and query sizes in few seconds, and produces a number of mirroring rules well within the limits of current routers. We also show that Stroboscope works on existing routers and is therefore immediately deployable.			
Passive and Active Measurement (PAM)	March 2018	**Revisiting the Privacy Implications of Two-Way Internet Latency Data**	Trammell, Brian; Kühlewind, Mirja
The Internet measurement community is increasingly sensitive to the privacy implications of both active and passive measurement. Research into the drawbacks of network data anonymization has led the community to investigate data sharing techniques, as well as to focus on active measurements and active measurement datasets. A key metric in these datasets is round-trip-time (RTT) as measured e.g. by ping or traceroute. This paper examines the assumption that the analysis of Internet RTT data is safe for open research by posing the question: what potentually-private inferences can be made about a remote target given periodic latency measurements from known vantage points under one's control? We explore the risks to end-user privacy both through a review of diverse literature touching on the subject as well as on the analysis of RTT data from fixed and mobile Internet measurement infrastruture. While we find that the common assumption of safety generally holds, we explore caveats and give recommendations for mitigation in those cases where it may not.			
IEEE Communications Magazine	February 2018	**Measuring ECN++: Good News for ++, Bad News for ECN over Mobile**	Mandalari, A. M.; Lutu, A.; Briscoe, B.; Bagnulo, M.; Alay, O.
After ECN (Explicit Congestion Notification) was first added to the Internet Protocol in 2001, it was hit by a succession of deployment problems. Studies in recent years have claimed that path traversal of ECN has become close to universal. In order to test whether a performance enhancement called ECN++ would face a similar deployment struggle, we measured its deployment over mobile as well as fixed networks. In the process, we discovered some bad news for the base ECN protocol—more than half the mobile carriers we tested wipe the ECN field at the first upstream hop. This throws into question whether previous studies used representative vantage points. This paper also reports the good news that, wherever ECN gets through, we found no deployment problems for the ECN++ enhancement. The paper includes the results of other more in-depth tests to check whether servers that claim to support ECN, actually respond correctly to explicit congestion feedback, including some surprising congestion behaviour unrelated to ECN. Given the results challenge accepted beliefs, this short paper has been produced to report the main findings accompanied by the measurement data. More detailed results and further testing continues.			

Table 4: List of MAMI publications (continued)

Venue	Date	Title	Authors
GSMA PACKET97	February 2018	**1-bit Content Classification**	Thomas Fossati
The wire image of an encrypted protocol is opaque by definition. It is important to expose the smallest amount of information to the path that is strictly necessary to implement a given function (e.g., measuring RTT/loss/reordering, optimising for a prevalent use case) Examples: QUIC “spin-bit”, LLT, mobile throughput guidance, QUIC PN, UDP options, QUIC & DTLS CID...			
International Conference on Network and Service Management (CNSM)	November 2107	**A Path Layer for the Internet: Enabling Network Operations on Encrypted Protocols**	Stepan Neuhaus, Mirja Kühlewind, Tobias Bühler, Brian Trammell, Roman Müntener, Gorry Fairhurst
The deployment of encrypted transport protocols imposes new challenges for network operations. Key in-network functions such as those implemented by firewalls and passive measurement devices currently rely on information exposed by the transport layer. Encryption, in addition to improving privacy, helps to address ossification of network protocols caused by middleboxes that assume certain information to be present in the clear. However, “encrypting it all” risks diminishing the utility of these middleboxes for the traffic management tasks for which they were designed. A middlebox cannot use what it cannot see. We propose an architectural solution to this issue, by introducing a new “path layer” for transport-independent, in-band signaling between Internet endpoints and network elements on the paths between them, and using this layer to reinforce the boundary between the hop-by-hop network layer and the end-to-end transport layer. We define a path layer header on top of UDP to provide a common wire image for new, encrypted transports. This path layer header provides information to a transport-independent on-path state machine that replaces stateful handling currently based on exposed header flags and fields in TCP; it enables explicit measurability of transport layer performance; and offers extensibility by sender-to-path and path-to-receiver communications for diagnostics and management. This provides not only a replacement for signals that are not available with encrypted traffic, but also allows integrity-protected, enhanced signaling under endpoint control. We present an implementation of this wire image integrated with the QUIC protocol, as well as a basic stateful middlebox built on Vector Packet Processing (VPP) provided by FD.io.			

Table 4: List of MAMI publications (continued)

Venue	Date	Title	Authors
NetDev 2.2 Conference	November 2017	**State of ECN and improving congestion feedback with AccECN in Linux**	Kühlewind, Mirja
Explicit Congestion Notification (ECN) is a TCP extension that allows networks to mark packets when congested instead of dropping them. While ECN provides a clear benefit by avoiding packet loss and subsequent retransmission delays, ECN was never widely deployed due to initial problems with network notes/home routers that would react incorrectly to ECN markings due to implementation errors. These initial problems were overcome and Apple announced in June 2016 that iOS and macOS devices would begin probabilistic attempts to negotiate ECN by default on the client side. While they actually detected some additional deployment problems, leading to reordering or limited throughput with a small number of operators during their beta testing, these operators fixed their networks and no further problems were reported from Apple since. In addition to the benefits provided by the ECN base extension, there is currently the More Accurate ECN (AccECN) extension under development in the IETF, providing more fine grained congestion feedback to the sender. AccECN introduces a new negotiation scheme that both endpoints have to support and changes the feedback format of the receiver to provide the exact number of markings observed to the sender, rather than just providing one indication of congestion per RTT. The sender can use this information as input for advanced and more scalable congestion control that reacts more gradually to the congestion level on the path. One example of such an congestion control, for data center environments, is Data Center TCP (DCTCP). One of the reasons that DCTCP can only be used in data centers is that there is no negotiation phase in DCTCP that ensures that both ends support the needed ECN feedback format. AccECN addresses this problem and can be easily integrated with DCTCP. Further, there are other current efforts in the IETF that target deployment of more scalable congestion control in the Internet and would also require the more accurate feedback information provided by AccECN. The AccECN development is basically completed in the IETF, facing the last processing steps before publication, and a proof-of-concept Linux implementation exists. This talk presents AccECN as a proposal for integration in the Linux kernel and aims to foster a discussion on activating ECN by default on the client side, similar as already deployed by Apple, enabling ECN for a proportion of all connections together with careful monitoring and potentially error detection/fallback.			
Internet Measurement Conference (IMC)	November 2017	**An Observatory for Internet Path Transparency**	Kühlewind, Mirja; Trammell, Brian
A poster introducing the Path Transparency Observatory (PTO) and use of PATHspider with the PTO.			
Internet Measurement Conference (IMC)	November 2017	**Enhancing encrypted transport protocols with passive measurement capabilities**	Bühler, Tobias; Kühlewind, Mirja; Trammell, Brian
A poster introducing the different approaches to support measurement in encrypted protocols: partially unencrypted wire images and tracking of encrypted traffic			

4 Exploitation of the project results

4.1 Industrial Exploitation

4.1.1 TID

TID has continued (and will continue after the project end) working to apply the MAMI results to future network infrastructure research projects, and network services provided by Telefonica Business Units along several directions: (a) utilizing and contributing to measurement data in the MAMI PTO; (b) leveraging the experience gained with NFV experimentation to facilitate repeatability of network scenarios; (c) applying path-awareness concepts in NFV and cloud-based services in the Telefonica portfolio, and (d) applying ACME and STAR for automating trust link management in network virtualization deployments.

The collaboration with industry associations like GSMA and the use of demonstration facilities like the 5TONIC 5G test lab are an important arguments for these activities, and TID keeps fostering cross-collaboration between the project and these industry associations, seeking for practical pre-commercial demonstrators, and leveraging dissemination activities at industrial events and social media to increase internal impact in Telefonica Business Units as well as external impact in cooperation with other industry partners.

MAMI PTO and measurement data

TID is continuously collaborating with different Telefonica Business Units on requests for trustworthy and independent data sources to evaluate the network impact of the currently on-going deployment of pervasive end-to-end encryption resulting in a potential need for changes in the currently applied network management techniques and the nature of the services offered by these business units. The MAMI PTO constitutes a referenve source of trustworthy measurement data that can influence the evolution of Telefonica's plans for its next-generation integrated telco cloud and the services hosted by it. In addition, TID fosters also their contribution to the PTO with its own measurement campaigns, as well as future consolidation of the measurement data beyond the project lifetime. The work in the http://isthewebhttp2yet.com site, and the growing awarenes about the results of the MONROE project are two examples of this exploitation path.

NFV-enabled experimentation

The MAMI experience with the development of VNF descriptors for the software developed by the project (such as `PathSpider` or the `Trafic` traffic generator) and their deployment oin NFV infrastructures has been essential to improve the tools currently in use at the TID network innovation labs, where we are applying it to improve the agility of experiments and demonstrator scenarios, as well as guarantee their repeatability. Beyond that, these VNF descriptors have allowed us to simplify the use of these tools for different purpose. In particular, `Trafic` is currently being used as an essential VNF to measure the capabilities of 5G technology choices.

Application of path-awareness principles

TID is further working on the application of path-awareness principles to ensure proof of transit (ensuring network functions in a given chain are applied) in UNICA deployments.

UNICA is an integrated cloud infrastructure committed to support a large variety of network elements and applications, including management tools and NFV-based services with the goal of enhancing software-based service provisioning, simplifying network management tasks, and taking advantage of NFV to address network service personalization. One of the main foreseen application of UNICA is Telefonica's Virtualized Home Environment (VHE), applying NFV principles to provide network services to residential and SME customers. Given all current home environments run several middleboxes (NATs, firewalls, parental control sytems), TID is working on developing further signaling mechanisms to support these functions in state management, allowing for cloud-native deployments.

Automated trust link management

One of the key challenges in the deployment of software-based network infrastructures is the dynamic managenment of trust links between the different components, that requires a high adapatability able to support short-lived connections. The development of ACME/STAR provides an ideal scenario to address these scenarios and to incorporate the logically centralized orchestration required in them. TID has developed a prototype implementation based on the ACME/STAR software developed within the project to demonstrate the proposal at the IETF, and demonstrated it to several operational units in the Telefonica Group, as well as providers and integrators working with them.

4.1.2 Nokia

Nokia plans to exploit the results of MAMI in many different sectors of its product portfolio including, but not limited to, mobile edge and core, SDN, analytics, IoT and IP video.

In particular, Nokia investigates to integrate MAMI results into the Velocix product line (CDN, mABR and Personalisation Platform) to provide enhanced cooperation with the mobile network to provide better QoE and expand the number of adaptation/personalisation functionality for OTT video delivery. To enable such services Nokia plans to change the way encrypted traffic negotiation is handled at edge locations of its CDN and mABR products, based on the use of the technology standardised in ACME STAR certificates. Moreover, design and experimentation conducted with the University of Aberdeen on use of a mobile throughput guidance signal by the TCP congestion controller on the edge cache has proven to be worth further investigation outside the simulation testbed.

Further, the results related to the connection identifier for and DTLS will be incorporated into the IMPACT IoT product line.

In GSMA, Nokia has driven to completion the first phase of activity related to the Loss-Latency (LoLa) tradeoffs ignalling with the publication of the "Content Classification" document describing the experiment goal, setup, and execution. A set of related experiments have been conducted in collaboration with TID and UC3M, which have validated the hypothesis and have made it possible to move the activity to a further phase in which we are coordinating standardisation of the signalling and API requirements from within GSMA across different SDOs.

Nokia analytics platform offers TCP releated measurments including RTT performance reporting, RTT based detection of RAN congestion, etc. The emergence of a spin bit in QUIC, as fostered by the MAMI project, allows similar use cases for UDP traffic which has increased to 20% of network traffic today and could grow to more. Nokia plans to introduce use of QUIC

RTT performance measurement based on signal provided by the spin bit.

4.2 Academic Exploitation

4.2.1 ETH Zurich

ETH Zurich has continuously involved master students in the research of the project, promoting their research skill and project work abilities. Since the last reporting period, additional four student project have been performed, which supported the development of PATHspider and the PTO as well as investigated passive measurability for QUIC. In total 9 student projects (four 6-months master and five 3-month semster projects) were performed during the project, contributing to all technical work packages. Further, the experimentation work of the MAMI project on passive network measurement contributed to the research performed for an on-going PhD thesis.

The architectural work of the project on flexible transport stack composition, a new transport API, as well as path aware networking consideration derived from middlebox cooperation research supported collaborations with other groups in ETH, as well as research groups and industry partners outside of the project. This enables exploitation of MAMI results in industry as well as future research projects as efforts in standardisation are on-going beyond the project life time.

The PTO that has been developed in close cooperation with ZHAW will be maintained by ZHAW after the end of the project and thereby provides a platform that makes MAMI measurements results available for researchers and network scientists outside of the project but also supports further measurement research for MAMI partners as well as other researchers by providing a repository system for comparable and reproducible measurements.

The PATHspider tool, which is based on ECNspider, a tool developed by ETH before the start of the project, and has been extended to a more generic framework for A/B testing in close cooperation with UoA during the project and is now maintained by Iain R. Learmonth, a former employ of UoA, who is now working at the Tor project. In his work he will be focusing on the use of PATHspider for Tor measurements as well as within the OONI project, a measurement platform for censorship detection.

4.2.2 ZHAW

ZHAW has involved one master student in the research project, resulting in a master thesis on how to fuzz shim-layer protocols in general, and PLUS in particular.[1]

ZHAW has also closely collaborated with ETH in the design and running of the PTO. As described in the previous section, ZHAW will operate the PTO after the end of the project. This is part of ZHAW's plans to continue researching data-heavy questions, where ZHAW will continue to gain valuable insights into questions of how to design and operate such repositories. ZHAW especially values the knowledge gained into how to operate repositories that are accessible to the public as well as to researchers.

[1] ZHAW, as a university of applied sciences, has a focus on education at the Bachelor level.

4.2.3 University of Aberdeen (UoA)

The results of the MAMI project have contributed to the University of Aberdeen's portfolio of research and standardisation activities. The quality of these activities are key to the securing national funding for the School of Engineering. Additional funding is being sought to ensure standards actions started in the project will continue to support their progress through to publication. (e.g., attendance at the next IETF meeting will be being supported by University funding). Along with other EU-funded activties the results of this project will form part of the Impact Case Studies UoA will submit to the UK REF2010 research funding exercise.

UoA will continue to explore important lines of research developed in MAMI, which will form the basis of new research proposals. A proposal will be submitted by the end of Janauary 2019 to develop the DPLPMTUD algorithm. This head-start is vital to ensure the active engagement of the industry partners and is essential to finally influence standardisation, and successful contribution to open source software.

MAMI-focused research and measurement methodology has been and will continue to be used to inform advanced undregraduate teaching in communications courses and to support the work of postgraduate students.

4.2.4 University of Liege (ULg)

ULg will use MAMI project results in follow-up research activities and for teaching purposes. In particular, the middlebox simulator (see MAMI Deliverable D2.2 for details) developed in WP2 will serve as basis for further researches. Among others:

- Comparing the simulator with state of the art middlebox implementation (e.g., FastClick and Metron)
- Using the simulator to push further researches and understanding the path impairment cause by middleboxes. In particular how those impairments lead to performance degradation.

The simulator (and in particular its capabilities to easily setup topologies) will be used in advanced courses in networking and computer security. This is already the case during this academic year. Indeed, the simulator is at the heart of the course "Network Engineering" for students learning routing, forwarding, and traffic engineering. Next year, it will be used for labs in Computer Security, in particular for setting up security-oriented middleboxes.

4.2.5 Simula Research Laboratory (SRL)

As an academic partner, SRL will build on the expertise and knowledge acquired through the MAMI project when developing future project proposals and for its graduate education activities. In particular, tools developed as part of MAMI (e.g., tools for the EU roaming study reported in section 3.1 of deliverable D1.3, or PATHspider) have been, or are being, fully integrated in MONROE and have contributed to expand the mobile-broadband measurement capabilities of the platform. The MONROE testbed will continue to be maintained, supported and extended via

the newly-established MONROE Alliance[2], and SRL is planning to leverage it in further funded projects, both national and European, as well as in future research work (e.g., a planned long-term, follow-up study of EU roaming), exploiting some of the tools developed in MAMI.

4.2.6 UC3M

UC3M will use MAMI project results in follow-up research activities and for academic purposes.

The `Trafic` generator framework has been promoted in different research projects of the H2020 framework where the University participates. One of the projects which has already started to get acquainted with the framework is 5GinFire[3]. Additionally, it has been transferred to the 5TONIC labs at IMDEA Research, where it is currently being used to test and characterise its local 5G network infrastructure. It will also be used in the context of 5G research projects where the institute is participating. The `NEMO` compiler for recursive VNFD definition is being evaluated by different follow-up initiatives in the context of the H2020 Framework programme as a means for agile definition of NFV-based experiments.

Further, the MAMI project has produced several results, that will be reflected in different Bachelor and Master theses. For example, the development of the `NEMO` compiler will be the base of a Bachelor thesis that is scheduled to be finalised around the summer of 2019.

[2] `https://www.monroe-project.eu/become-a-member/`
[3] `https://5ginfire.eu/`

5 Conclusion

This deliverable focuses on reporting the standardisation, dissemination, and exploitation activities carried out in MAMI during the last 18 months, including the project extension, clearly justified by the results both in terms of standardisation and further exploitation. For each area we include as well a brief analysis of the overall project results.

In what relates to standardisation, the project has managed to consolidate the goals of the strategy started during the previous reporting project. Once it became clear that a dedicated protocol (or substrate) for direct collaboration with middleboxes was not an acceptable approach for the IETF community, efforts focused on incorporating principles around path awareness and passive measurability in the evolution of the transport layer protocols embraced by the IETF, as well as in providing a general approach to them. This has been achieved by means of several adopted documents dealing with these general aspects, and the creation of two research groups within IRTF to continue exploring these principles and their realisation. Furthermore, other aspects related to trust and distributed key management has been actively pursued as well, with contributions in the related groups that are in the process to become published. The project has monitored and tried to bridge the gaps among the IETF (our main target) and other organizations interested in network stack evolution and especially in the aspects related to the generalized use of encryption at the transport layer. A total of 35 Internet Drafts were contributed during the project, of which two became published as RFCs (RFC 8095 and RFC 8436), and eleven have been adopted by the corresponding working groups. The project team has contributed to two ETSI TC-CYBER documents, which are considered final drafts close to publication.

MAMI's communication actions were focused on social media through websites (`https://mami-project.eu/`, `https://pathspider.net/`, and `https://v3.pto.mami-project.eu/`), a blog hosted at the website, and a twitter account (`@mamiproject`) as well as in-person dissemination at research and industry events.

The MAMI project makes all software efforts openly available on GitHub (`https://github.com/mami-project/`). The project has maintained 69 active repositories. MAMI also attempts to distribute measurement tools developed during the project via packages in software distribution systems, in particular the Debian Operating System, and the Python Package Index. Partners of the MAMI project has regularly participated in IETF Hackathons to socialise ideas and code related to MAMI activities. Further a PATHspider Hackathon has been organized together with OONI and the TOR Project, in-order to incorporate protocol-dependent connectivity failure test provided by PATHspider into a future release of the OONI measurement tool.

During the period considered in this deliverable, the project team has published 16 papers at different workshops and conferences as well as in journals, and given introductory talks on transport interfaces and the path-aware networking concept. During the whole project duration, 49 publications of different nature (peer-reviewed papers and conference contributions, invited talks, technical reports, presentations at industrial events...) on the project results have been made.

The MAMI Management and Measurement Summit (M3S, London March 2018) was a milestone in building awareness among the networking industry (operators, service providers, developers...) of the need for transparent middlebox cooperation schemes and independent measurement capabilities. Further a series of three whitepapers have been release for industry dissemination, where the first one summarizes the outcome of the M3S workshop and other

two focus on analysis and consideration of management of encrypted traffic as well as security and privacy implications of middlebox cooperation protocols.

Academic dissemination was driven by a new edition of the Mobile Network Measurement (MNM18), further to the previous one in Dublin was organized, the MAMI Summer School at the University of Aberdeen, as well as a SIGOMM tutorial on Repeatability and Comparability in Measurement (RCM). The MAMI project has further developed cooperative relationships with related EC-funded projects during the last year, especially with MONROE, NEAT and 5GINFIRE, running specific experiments with the first one, collaborating in transport abstractions with the second, and contributing the component-based traffic generator built by the project for enhancing experimentation and infrastructure monitoring with the third.

The industrial partners have refined the network services and products that can apply the results of the project. In particular, the application of measurement data in the MAMI PTO, and on applying automated certificate management in NFV cloud-based services, as well as in the applicability of NFV descriptors to facilitate experimentation and the incorporation of new services to operational networks. In what related to products, MAMI results have been considered for their application to mobile edge and core, Software Defined Networking (SDN), and IP video. The collaboration with industry associations like GSMA, as described above, is an important argument for the direct exploitation and further dissemination of these results. The academic partners have incorporated MAMI results in their research portfolios, used these results for advanced teaching, and involved students in the research work conducted in the project, through different activities dealing with the realization of theses.

As a general conclusion, we believe it is a fair statement to declare MAMI has fulfilled all its objectives related to WP4.