Exploring DSCP modification pathologies in mobile edge networks

Ana Custura André Venne Gorry Fairhurst
University of Aberdeen, UK

IEEE/IFIP Workshop on Mobile Network Measurement (MNM'17)

This work is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 644399

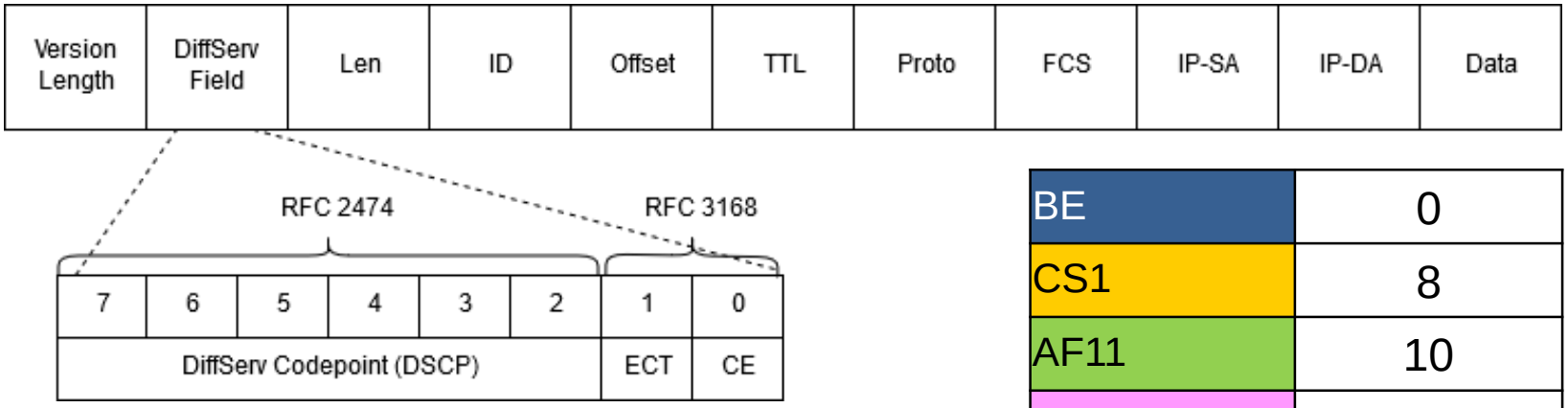
Introduction

- PREC Call 1 Project looks at IP-based robust communication in disaster situations
- Work examines path-level behaviour of DiffServ marked packets for Mobile BroadBand (MBB)

- Background:
  - Increased interest in DiffServ Interconnection
  - DiffServ well-suited to address some challenges for 5G
- However, DiffServ is currently perceived as unreliable beyond the local network – what actually happens?

Introduction to DiffServ

- **DiffServ allows applications to classify traffic and request a forwarding treatment**



BE	0
CS1	8
AF11	10
AF21	18
AF31	26
AF41	34
CS5	40
EF	46
Unassigned 3	3

- **Applications set a DiffServ codepoint (DSCP) to assign packets to a QoS class**
- **Remarking and policing can be done at boundary between DiffServ domains**

Measurement Campaign (Dec 2016-Jan 2017)

- Test packets sent from MBB edge sources
  - 86 randomly-chosen targets from Alexa top 1M list
  - Packets sent with high TCP and UDP ports
  - Measurements used the MONROE platform

- A tool was written for exploring DSCP remarking
  - Traffic generated with Scapy
  - Uses traceroute mechanism
  - Collected path-level data

  - On github: https://github.com/ana-cc/forger

Results- overview

- Data from over 107 vantage points
- 12 MBB providers
- 9202 unique source-destination pairs

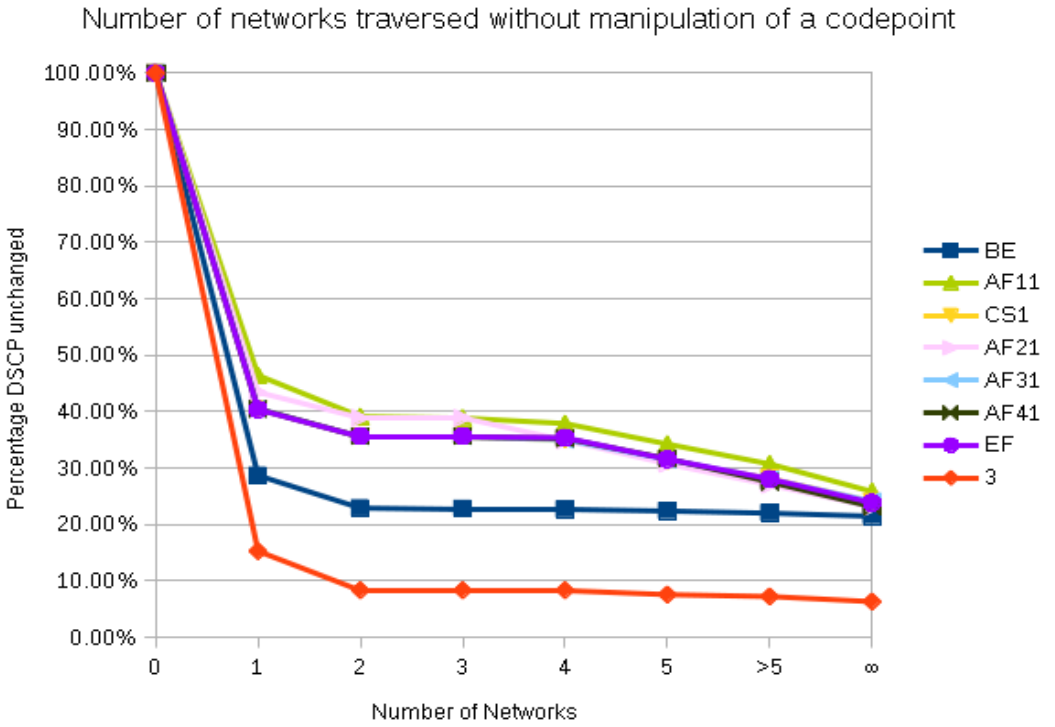
- Measurements using both TCP and UDP
- Tested diffserv codepoints: CS1, AF11, AF21, AF31, AF41, CS5, EF and codepoint 3

- Due to availability of nodes, data collected varies

Results – survivability of marks

- No transport-dependent remarking
- Almost two thirds of codepoints rewritten in operator network
- Aggressive remarking for codepoint 0, which was expected to remain unchanged

Codepoint 3 has most aggressive remarking (>90% remarked before exiting operator network)



Comparison with other networks

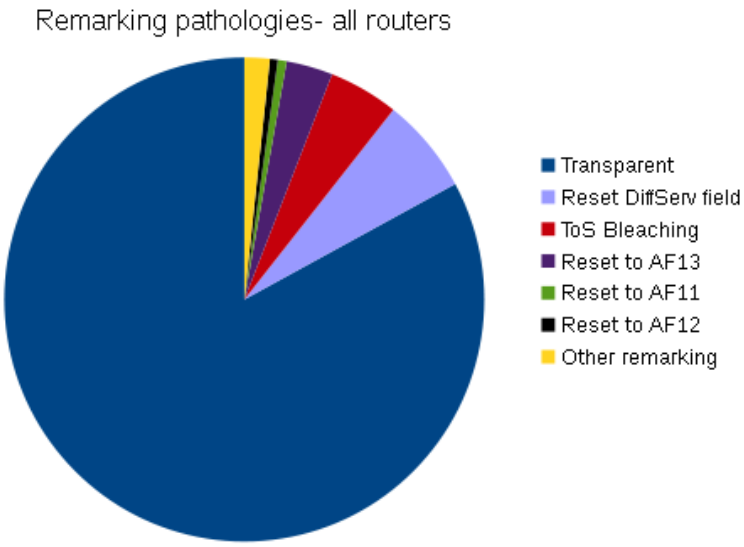
	Core	Wired edge	Mobile edge
Transport-Dependent remarking?	No	N/A	No
% of transparent routers	79.4%	N/A	5.1%
% of BE/DF packets remarked	10.3%	7%	78.9%
% of codepoint 3 remarked	17.7%	48%	91.7%

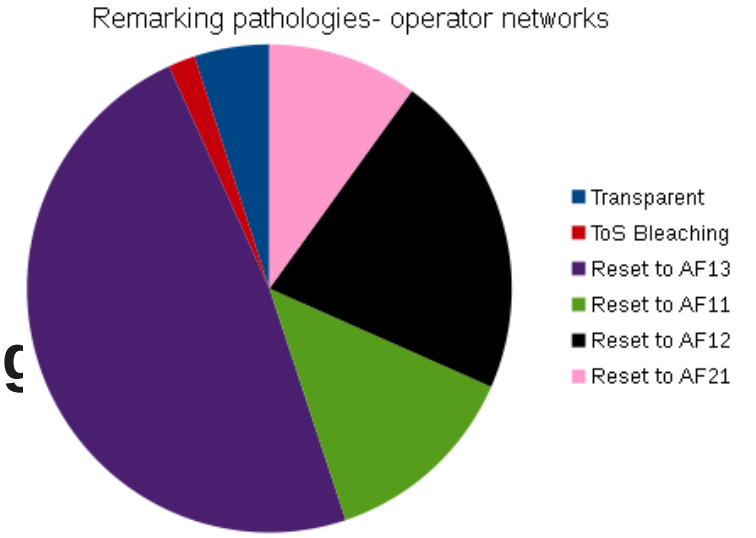
Core data- measurement campaign using the same tool from Digital Ocean data centres
Wired edge data- measured using edgetrace

- **Mobile edge appears to be less transparent to DSCP compared to both the core of the internet and wired access networks**

Remarking Pathologies

- Remarking pathologies of 705 routers over 63 AS:
  - 83% transparent to DSCP
  - 6.4% bleached DS field
  - 4.7% reset upper 3 bits (ToS bleach)
- However, in MBB networks…
  - Only 5% transparent to DSCP
  - 48.3 % remarking to AF13, 21.6% to AF12, followed by AF11 and AF21
  - Very little evidence of ToS remarking



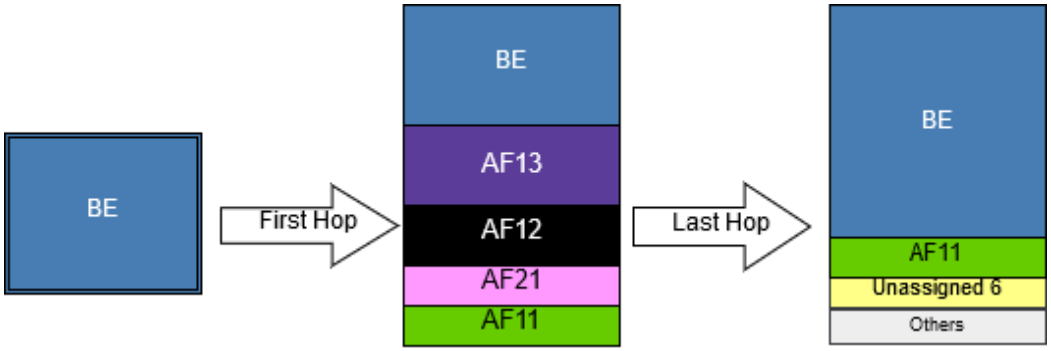


Results- Remarking within MBB networks

	Italy	Spain	Norway	Sweden
Remarkings	TIM: AF11 Vodafone: AF11 WIND: AF12	Orange: AF12 Vodafone: AF21 Yoigo: AF12	Telenor: AF13 Telia: AF13 ICE: AF13	Telenor: BE Telia: AF11 H3G: AF13
Transparent?	No	No	Partially	No

- **Packets remarked at first hop irrespective of initial value**
- **Second round of remarking as packet exits operator network, mostly bleaching**

BE- Remarking seen at first and last hops of operator networks



- **Remarking dependent on country and operator, not on codepoint sent!**

Impact of MBB remarking

- Remarking all traffic to a specific codepoint implies a non-BE default PHB
- Priority inversion in the case of a Spanish operator
- However, mobile networks are DiffServ aware and show no evidence of ToS bleaching
- GSMA guidelines are not followed

Impact of ToS based remarking

- 4.8% routers reset the upper 3 bits, implies equipment still operating using ToS semantics
  - ToS deprecated in December 1998!
- Can lead to unknown codepoint in the path; packets will likely not receive desired treatment
- If routers were configured to use DiffServ, rate of unknown codepoint at the end of path would reduce

ToS Field

7	6	5	4	3	2	1	0
IP Precedence			Type of Service				

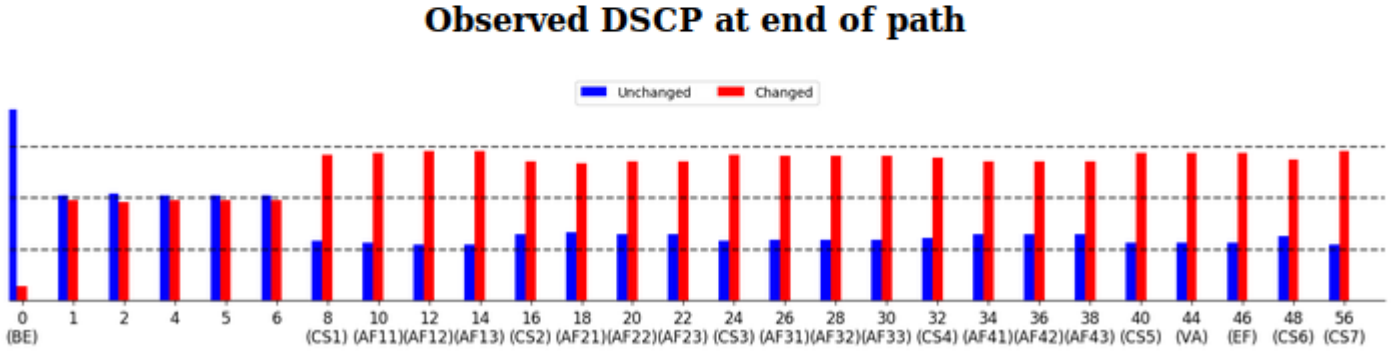
7	6	5	4	3	2	1	0
DiffServ Codepoint (DSCP)						ECT	CE

Recommendations

- Results show it is safe to enable DSCP marking for applications
- Applications can expect to sometimes exploit DiffServ locally
- Beyond local network ToS routers are the greatest hindrance; incorrectly configured or older equipment should be reconfigured
- None of the Intercon-recommended markings* were used by MBB operators; operators could implement GSMA guidelines

* RFC8100 on intercon for short-pipe MPLS

Questions?



New measurement tool, edgetrace:
https://trace.erg.abdn.ac.uk

Ana Custura
ana@erg.abdn.ac.uk