A TWAMP Coordinated Data Compression System for 5G Backhaul

Yekta Türk[a] and Engin Zeydan[b]

[a]Ericsson Research, Istanbul, Turkey, 34396
[b]Centre Technologic de Telecomunicacions de Catalunya (CTTC), Castelldefels, Barcelona, Spain, 08860
[1]Emails: yekta.turk@ericsson.com, engin.zeydan@cttc.cat

***Abstract*—Latency and bandwidth limitations of mobile network operators (MNOs)' backhaul networks can have negative impacts on 5G service experience. Data compression methods, on the other hand, could allow data transmission using less bandwidth and buffer sizes that can provide solutions to backhaul latency problems of MNOs. Together with the combination of a quality measurement method in transmission network as well as softwarization components that allow data modification at both core network and base station (BS), an intelligent and dynamic solution can be created to improve the performance of 5G networks. In this demo work, we demonstrate how 5G BSs could be compatible with Internet Protocol (IP) payload compression using software components which do not require any changes to the existing backhaul network infrastructure. In our demonstration, a Two-Way Active Measurement Protocol (TWAMP) server continuously monitors transmission network performance and initiates compression/decompression operations on both core network and 5G BS when bandwidth and latency problems occur. After identifying that the problem has disappeared, the compression process ends. Furthermore, the amount of instant traffic inside the network and the gains achieved within the proposed system can also monitored via dashboards.**

***Index Terms*—5G, backhaul, TWAMP, data compression.**

I. Introduction

5G is finally becoming a reality and operators have already started to prepare their infrastructure to ensure highly available 5G services [1]. Transmission network of the Mobile Network Operators (MNOs) is one of the foresights that should be dimensioned for 5G which demands high bandwidth and requires little delay tolerance. 5G Base Stations (BSs) should not be fully dependent to this dimensioning and be capable of taking precautions against performance problems that may occur in backhaul to satisfy these stringent requirements. Moreover, resilience, reliability, and robustness of networks will be important in terms of adapting to dynamism of services and resources.

The Two-Way Active Measurement Protocol (TWAMP) [2] is often used by MNOs to measure the network transmission quality up to the BSs. Backhaul performance problems can be resolved by implementing Internet Protocol (IP) payload compression support to 5G New Radio (NR) (which is not supported by the existing equipment) and by using the results of TWAMP measurements in a proactive approach. A lossless data compression can be unnecessary when the transmission network has suitable conditions, but under poor performance of backhaul, usage of it will increase the 5G service quality. Next generation BSs and core network systems could provide a smart solution for the problems that can be experienced on the transmission side. Fig. 1 shows the high level architecture of the our demonstration. In addition to traditional next generation cellular network architecture, it includes TWAMP server and clients which are embedded into 5G NR and packet core as software components. This work aims to show handling backhaul capacity problems with autonomic methods that allows: (i) distinguishing the efficiency of 5G services from the performance of backhaul, (ii) finding solutions to the problems in transmission network for 5G NR, (ii) performing a TWAMP based coordination for network shortages with predefined script, (iv) applying a compression protocol that is compatible to existing network, (v) visualizing the reaction of the system to the network conditions and demonstrating the achieved gains.

978-1-5386-9376-6/19/$31.00 ©2019 IEEE

II. Demonstration

We used Graphical Network Simulator-3 (GNS3) [3] to simulate the fixed operator network, the cell site router and Security Gateway (SecGW). Open Shortest Path First (OSPF) [4] is activated as a routing protocol and Multi Protocol Label Switching (MPLS) [5] is running with Label Distribution Protocol (LDP) [6]. The leased line between the cell site router and the SecGW is provided with the MPLS Layer2 Virtual Private Network (L2VPN) [7] pseudowire in accordance with same configuration of the actual operating networks [8]. 5G NR, packet core and TWAMP server are demonstrated with Ubuntu Linux in running virtual machines which are connected to GNS3. Open-sourced Strongswan [9] software is used to setup an Internet Protocol Security (IPsec) tunnel between Linux virtual machine and SecGW. Data compression is done by using lossless Deflate algorithm [10].

A. System against Poor Backhaul Performance

The proposed system is a software that manages the performance data in near real-time by checking Round-trip time (RTT) values of the TWAMP tests. It is composed

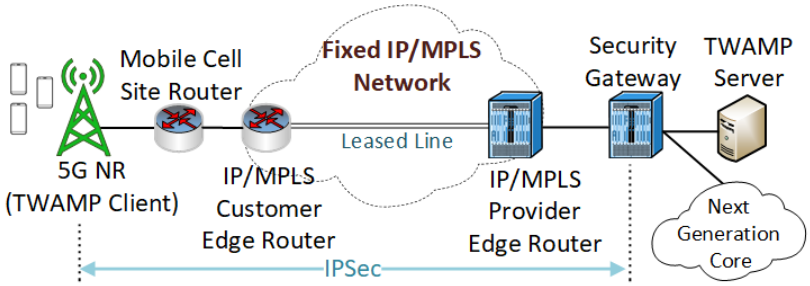

Fig. 1: High level architecture of the demonstration for TWAMP coordinated data compression system of 5G backhaul.

of three main modules as shown in Fig. 2: **(a) Testing and Action (b) Data Transform Activation/Deactivation (c) Analysis and Visualize**. TWAMP tests are running in a consecutive manner similar to MNO's implementation structure inside their network infrastructures. Fig. 2 illustrates the relations of the system with the rest of the network and workflows within our proposed solution.

In **Testing & Action** module, marked as steps-(1), (2), (3), (5) and (6) in Fig. 2, TWAMP testing runs continuously. If a predefined threshold value is exceeded in terms of traffic delay, *connect-and-compress method* initiates compression/decompression process by connecting to the virtual machines and running terminal commands via Secure Shell (SSH). Step-(2) shows the backhaul problem event (e.g. high latency, saturation in links) whereas step-(5) represents the removal of this problem. Both of them are triggered by the event manager scripts that are prepared for this demonstration. If the link returns to the normal operation, *connect-and-clear method* prompts both ends to stop compression/decompression processes.

In **Data Transform Activation/Deactivation** module marked as step-(4) and step-(7) in Fig. 2, the main responsibility is to compress the IP payload of the sent packets and to decompress the incoming packets at the kernel of the Linux machines by using policies in XFRM framework [11]. IP payload compression is activated in step-(4) and deactivated in step-(7) in the network interfaces of virtual machines by using policies.

Finally in **Analysis & Visualize** module marked as step-(8) in Fig. 2, network monitoring is present. Network graphing is prepared to show the amount of traffic on the links by using Cacti [12] which is collecting traffic data from the routers by using Simple Network Management Protocol (SNMP). We activated SNMP on all routers to observe the traffic in GNS3. In the dashboard screen, results of the TWAMP tests are also present. The traffic to 5G NR was generated using Iperf [13]. For this purpose, Iperf has been installed at Linux virtual machines on both ends. Wireshark [14] I/O graphs were used to visualize the status of the received packets, the decrease in traffic level after traffic congestion/saturation in the link, the activation of the compression and then the increase in bandwidth as a consequence of removal of traffic congestion.

B. Demonstration Workflow

We demonstrate working principle of the system in steps (1)–(8) as given in Fig. 2. The general workflow is as follows: First, a TWAMP server running in an Ubuntu server performs periodic TWAMP tests to the 5G NR which has a TWAMP client software as illustrated in step-(1). TWAMP server and client application use twampy [15] which is an open-source software implemented in Python. We integrate two connect-and-compress and connect-and-clear methods into the TWAMP server, which is responsible for controlling the compression/decompression operations. Later for a predefined duration, a script in event manager of the router in backhaul network creates a transmission problem by limiting the bandwidth in step-(2). By checking the RTT results, TWAMP server detects the latency problem when predefined threshold exceeds, then the connect-and-compress method runs and prompts the core network and 5G NR to perform IP payload compression for the

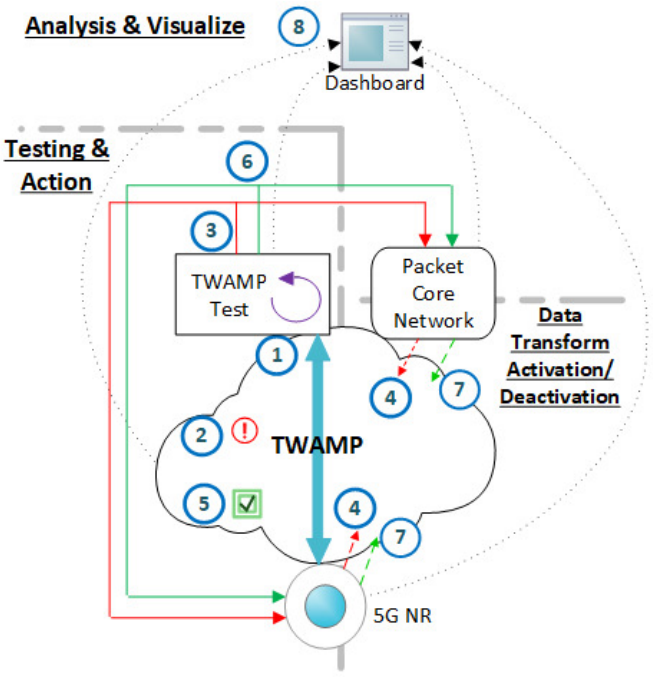

Fig. 2: Demonstration setup and workflow structure.

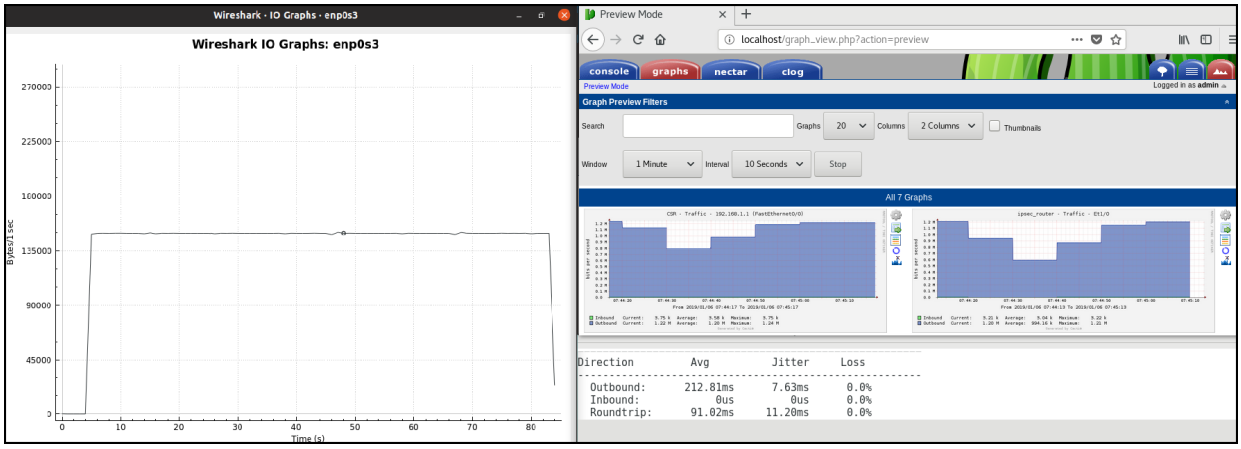

Fig. 3: Dashboard for visualizing the system operation.

downlink and uplink traffic in step-(3). In step-(4), both ends communicate with the compressed traffic to combat with the performance degradation in transport network. Another event manager script runs and eliminates this problem in step-(5). In step-(6), TWAMP server notices that the RTT results of TWAMP tests are under predefined threshold and connect-and-clear method informs both ends to stop compressed communication. This task is sent to the devices and network interfaces terminate the compression/decompression process in step-(7). In step-(8), the occurrence of the problem by the system is monitored via the dashboard via interaction with the mobile network during all the process and shows the introduced gains.

Dashboard in Fig. 3 displays the traffic level on the transmission links, results of the continuous TWAMP test and the level of the application traffic generated by end users. Measured traffic levels on the backhaul links are shown instantaneously on the Cacti graph which is on the right in Fig. 3. The status of the application traffic is shown in Wireshark graph that is on the left in Fig. 3. The results of the instantaneous TWAMP tests are shown on the bottom right. When traffic on the links is limited by the event manager to simulate the link failure, the drop in traffic level can be observed on the Cacti screens. The compression/decompression status of the both end systems can be interpreted by checking the traffic level on the links. Since the start of compression, no decrease in the end-to-end application is observed as also observed on the left side Wireshark graph. In this case, the proposed system takes action and no drawback at the service quality in end user application level is observed.

III. Acknowledgements

This work was partially funded by Spanish MINECO grant TEC2017-88373-R (5G-REFINE) and by Generalitat de Catalunya grant 2017 SGR 1195 and partially supported by The Scientific and Technological Research Council of Turkey in part under 1515 Frontier R&D Laboratories Support Program with project no: 5169902.

References

[1] D. Abecassis, C. Nickerson, and J. Stewart, "Global race to 5G - spectrum and infrastructure plans and priorities," in *Analysis Mason*, 2018.

[2] K. Hedayat, R. Krzanowski, A. Morton, K. Yum, and J. Babiarz, "A two-way active measurement protocol," in *IETF RFC 5357*, 2008.

[3] "GNS3 2.1.11." https://www.gns3.com/, 2018. [Online; accessed 2-Jan.-2019].

[4] J. Moy, "Ospf version 2," in *IETF RFC 2328*, 1998.

[5] E. M. Bocci, E. S. Bryant, E. D. Frost, L. Levrau, and L. Berger, "A framework for mpls in transport networks," in *IETF RFC 5921*, 2010.

[6] E. L. Andersson, E. I. Minei, and E. B. Thomas, "Ldp specification," in *IETF RFC 5036*, 2007.

[7] E. L. Andersson and E. E. Rosen, "Framework for layer 2 virtual private networks (l2vpns)," in *IETF RFC 4664*, 2006.

[8] "Cisco router: Configuration examples and technotes." https://goo.gl/ARVZGm, 2016. [Online; accessed 25-Feb.-2019].

[9] "Strongswan 5.7.2." https://www.strongswan.org/, 2018. [Online; accessed 1-Jan.-2019].

[10] P. Deutsch, "Deflate compressed data format specification version 1.3," in *IETF RFC 1951*, 1996.

[11] R. Rosen, "The XFRM framework," in *Linux Kernel Networking: Implementation and Theory*, pp. 280–305, Apress, 2014.

[12] "Cacti 1.2.0 beta 4." https://www.cacti.net/, 2018. [Online; accessed 4-Jan.-2019].

[13] "iperf 3.1.3." https://iperf.fr/, 2016. [Online; accessed 4-Jan.-2019].

[14] G. Combs, "Wireshark 2.6.5." https://www.wireshark.org/, 2018. [Online; accessed 4-Jan.-2019].

[15] "Twampy." https://github.com/nokia/twampy, 2018. [Online; accessed 10-Jan.-2019].