F4F+ SME call: Impact of Encryption VPN on LTE/5G Radio & UE Resources (5G-OTTVPN)

George Kontopoulos

EIGHT BELLS

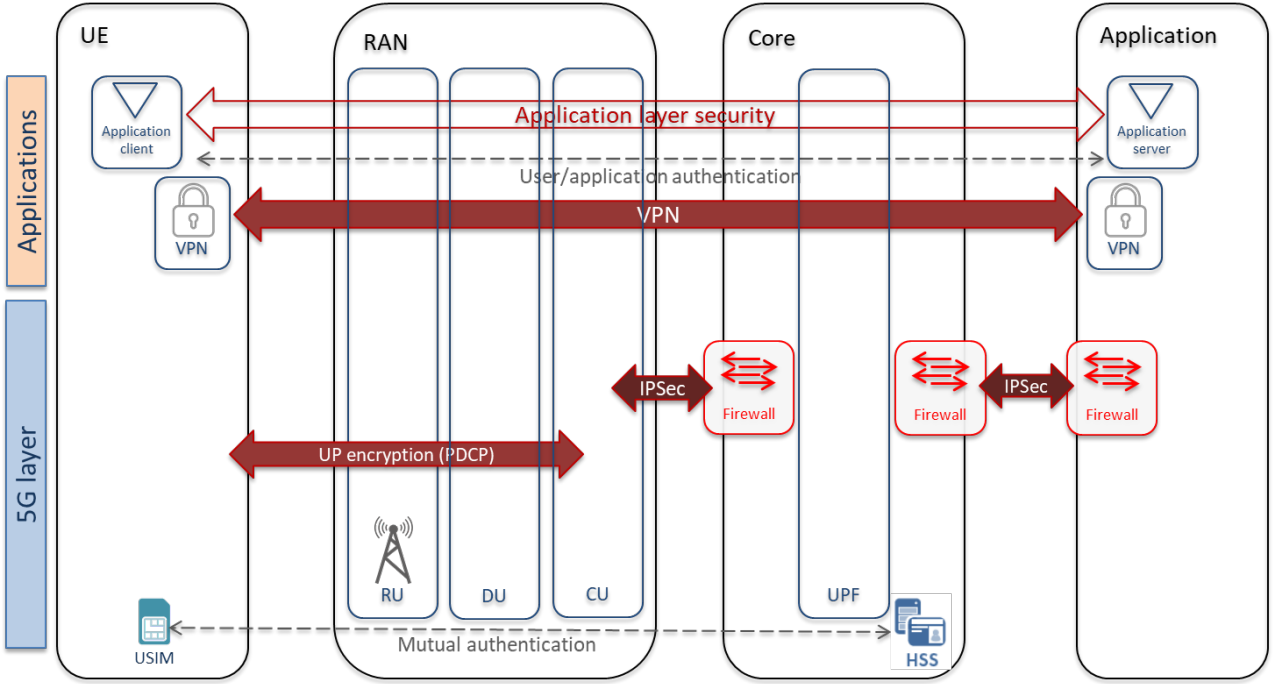
Open Call experiments Review FEC10

Online, 11/02/2022

Experiment Description

Concept & objectives

OVER-THE-TOP END-TO-END ENCRYPTION VPN



Background & motivation

VPN disadvantages:

- Throughput overhead
- Encryption latency
- CPU overhead
- Power consumption increase

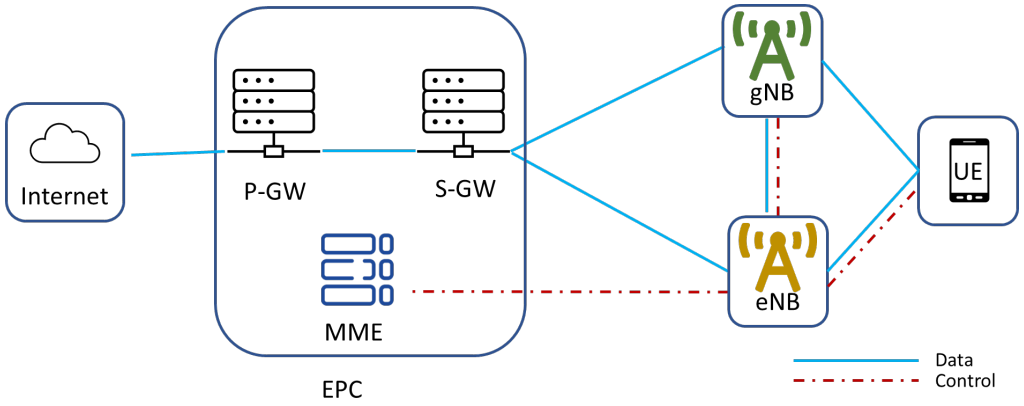
Lack of real-life data with measurements for VPN over 5G

Study the effect on: i) throughput (overhead due to encryption), ii) UE CPU utilization, iii) UE power consumption

Comparison of different encryption protocols

Experiment set-up

LTE & 5G NSA

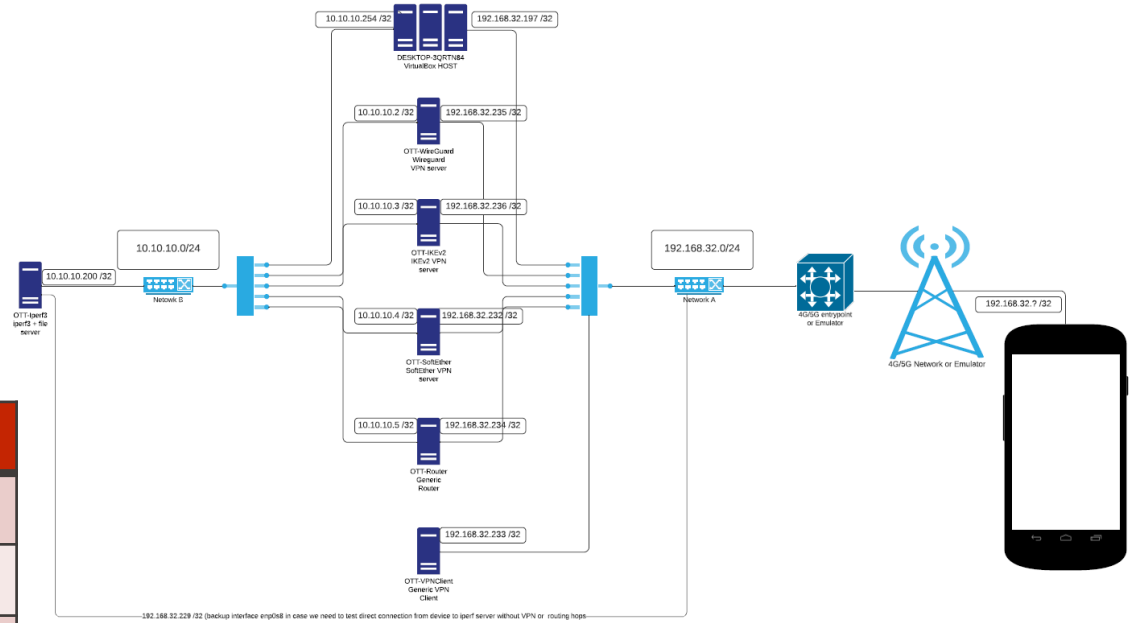


Band	n78	B7
Mode	TDD	FDD
Bandwidth	40 MHz	20 MHz
Carrier components	1 Carrier	1 Carrier
MIMO layer	2 layers	4 layers
DL MIMO mode	2x2 Closed Loop	4x5 Closed Loop
Modulation	256QAM	256 QAM
LTE to NR frame shift	3 ms	
Subcarrier spacing	30 kHz	
Uplink/Downlink slot ratio	2/8	
Scheduler configuration	Proactive scheduling	Proactive scheduling

Experiment set-up

IT INFRASTRUCTURE

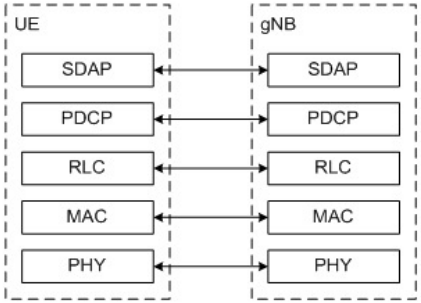
VPN Protocol	VPN Server	VPN Client (Android)
IPSEC/IKEv2	IKEv2 VPN server	StrongSwan Android application
WireGuard	WireGuard VPN server	Wireguard Android application
OpenVPN	SoftEther VPN server	OpenVPN Connect Android application
MS-SSTP	SoftEther VPN server	MS-SSTP Android application
IPSEC/L2TP (IKEv1)	SoftEther VPN server	Android built-in client



Project Results

LTE Measurements

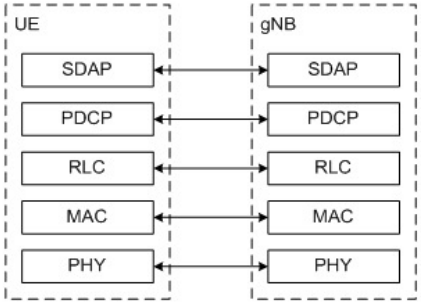
10 MBPS UL USER TRAFFIC



	Idle	no VPN	IPSEC-IKEv2	IPSEC-L2TP	WireGuard	OpenVPN	MS-STP
L2							
PDCP throughput (Mbps)		10,201	11,187	11,554	11,277	10,821	10,703
RLC throughput (Mbps)		10,209	11,208	11,570	11,298	10,844	10,725
MAC throughput (Mbps)		10,727	11,678	11,900	11,954	11,503	11,148
PHY							
PUSCH throughput (UL) (Mbps)		11,782	12,627	12,848	12,882	12,369	11,559
UE							
CPU Usage (%)	8,68	12,95	17,08	15,46	14,63	15,88	18,98
Device battery current (A)	-0,0646	0,0058	0,0992	0,0847	0,0626	0,0896	0,1632

5G Measurements

10 MBPS UL USER TRAFFIC



	Idle	no VPN	IPSEC-IKEv2	IPSEC-L2TP	WireGuard	OpenVPN	MS-STP
L2							
PDCP throughput (Mbps)		10,196	11,162	11,526	11,244	10,804	10,750
RLC throughput (Mbps)		10,263	11,288	11,654	11,377	10,932	10,826
MAC throughput (Mbps)		10,747	11,746	12,082	11,843	11,470	11,163
PHY							
PUSCH throughput (UL) (Mbps)		11,128	11,851	12,258	12,055	11,467	11,165
UE							
CPU Usage (%)	10,77	14,88	20,04	21,61	18,57	19,82	20,99
Device battery current (A)	0,2174	0,2831	0,4106	0,4280	0,3730	0,4686	0,5198

Lessons learned

ENCRYPTION PENALTY (CPU, POWER, THROUGHPUT) SEEMS MANAGEABLE

Throughput: there is a penalty to pay (additional throughput) introduced by the encryption. This additional throughput is in the range of 5% - 10% depending on the encryption protocol. Sshould be factored-in in the radio planning of the network.

CPU utilization: there is an increase when the encryption is in place. This increase is around 5% for the specific CPU capabilities of the terminal in use and the specific throughput (10Mbps).

LTE vs 5G: 5G is more demanding than LTE in terms of CPU & power consumption.

WireGuard protocol seems to impose less stress on both CPU and power consumption related to the other protocols.

Business Impact

Impact on 8BELLS business

KNOW-HOW

The knowledge acquired both regarding the impact of encryption and from setting-up the IT infrastructure (VPN servers & clients) is valuable to 8BELLS as it allows us to approach relevant projects with more confidence.

We are also focusing in designing an enterprise grade OTT VPN security solution, targeting market readiness within the next 12 months. The gained experience is also valuable towards this goal.

Impact on 8BELLS business

NEXT STEPS

We plan to continue studying the impact of OTT VPNs, especially from an implementation point of view for a commercial deployment. Therefore, we aim to compare different VPN protocols from the point of view of setup time, robustness (when the radio connection becomes unstable), reconnection mechanisms, statistics production, etc.

We would also like to study a double VPN solution (VPN within a VPN) for use cases requiring increased security.

Therefore, we would be interested to use the Fed4FIRE+ facilities again, especially after the 5G network becomes upgraded to 5G Stand Alone (SA).

Perceived value

The results produced by the experiment are valuable because they quantify the expected impact of encryption, and therefore allow us to better plan the network for relevant use cases.

In any discussion with end-users about use of encryption it is necessary to provide some benchmark of the network and user equipment impacts.

Feedback

Used resources & tools

PERFORMLTE (UMA) TESTBED

- LTE & 5G NSA network setup (Radio & Core)
- IT resources (server, UE)
- Measurement applications (Keysight Nemo Handy)
- Remote Mobile Device Management (VySor)
- Traffic generator (IPERF)

Used resources & tools

EXPERIMENT SETUP

The setup phase was significant and important.

We needed to install both VPN servers (in Virtual Machines – one for each VPN protocol), clients (in Android UE – one for each VPN protocol), and measurement tools (IPERF) in the physical server that has been provided by the testbed.

Then we needed to ensure that all connectivity issues have been solved before running the experiment and obtaining measurements.

Used resources & tools

POSSIBLE FUTURE UPGRADES (UMA)

- Upgrade the 5G network to SA
- Provide UE supporting 5G SA
- Capability to simulate different RF conditions (loss of coverage, internal/external interference, etc)

Added value of FED4FIRE

- Commercial grade network resources (vs network emulators/network-in-a-box solutions)
- Spectrum use
- Availability of commercial grade measurement tools (Keysight Nemo)
- Availability of budget
- Easy procedure without need to invest a lot of time to learn the use of special tools


Co-funded by the
European Union


Co-funded by the
Swiss Confederation

This project has received funding from the European Union's Horizon 2020 research and innovation programme, which is co-funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation, under grant agreement No 732638.

WWW.FED4FIRE.EU