



College of Engineering, Design and Physical Sciences
Electronic and Computer Engineering

Contextually and Identity Aware 5G Services

A Thesis Submitted in Partial Fulfilment of the Requirements
for the Degree of DOCTOR OF PHILOSOPHY

Year of Submission: 2021

Kareem Ali
Student Number: 1430231

Professor John Cosmas
Principal Supervisor

Dr Hongying Meng
Second Supervisor

Abstract:

The fifth generation (5G) mobile networks aim to be ten times faster than the existing 4G connection, whilst providing low latency, and flexibility. Hence, various alterations are planned to the existing network infrastructure to be able to reach the 5G expected performance levels. The main technologies that were used, to ensure high performance, flexible network, and efficient resource allocation, are Software Defined Network and Network Function Virtualization. As these technologies are replacing the device-based architecture with, a service-based architecture.

This thesis provides a design of location database interactive web interface and interactive mobile application. The implementation of real time video streaming location server, the streaming system's performance parameters demonstrated a high level of QoS (0.07ms jitter and 9.53ms delay). In regard to experimental examination, it measured the localisation coverage, accuracy measurements and a highly scalable security solution. The localisation coverage and accuracy measurements were achieved through the mmWave and VLC link transmitters. The proposed simulated annealing algorithm aimed at data optimisation for location measurements accuracy showed results of the average location error of x and y which showed significant improvement from $x=22.5$ and $y=21.6$ to $x=11.09$ and $y=11.63$.

The proposed indoor location security solution showed significant results, as it provides a high scalability solution using the VNF. The solution showed that it was not 100% effective, as some of the fake discover packets still reached the DHCP server. This was due to the high load of traffic passing through the network. Nonetheless, 90% of the fake DHCP discover packets never reached the DHCP server because the scripts began blocking all fake discover packets after realising it was an attack. This conveys that the proposed system was able to run successfully without crashing or overloading the controller.

Overall, the main challenges facing 5G have been addressed with their proposed solutions, which showed promising results. Conclusively showing that there is a lot more space for technological advancements to support the future of mobile networks.

Acknowledgments:

I would like to express my gratitude to my primary supervisor, Professor John Cosmas, who not only guided me throughout my thesis, but also motivated me to work hard and finish my thesis. It has been an honour to work under his supervision.

I would like to thank my second supervisor, Dr. Hongying Meng, for his assistance and support to finish my thesis.

Additionally, I would like to express my sincere gratitude to European Union's Horizon 2020 research program for its financial support to the Internet of Radio-Light (IoRL) project H2020-ICT 761992, which allowed me to complete my PhD.

I would like to thank and acknowledge the academic and technical assistance provided by Brunel University. Also, sincere gratitude to all the supportive staff in the Post-Graduate Research Office, Library, Student Centre and Admissions.

Dedication:

I dedicate this work to my mother and sister for all their sacrifices and their endless support to help me get the best education;

I would like to thank my friends for their support and encouragement;

It wouldn't have been possible without you all.

Table of Contents

Abstract:	ii
Acknowledgments:	iii
Dedication:	iv
Table of Contents	v
List of figures	ix
List of tables	xi
List of abbreviation	xi
List of Publications	xiii
A. Journals	xiii
B. Conferences.....	xiii
C. Co-Author	xiv
Chapter 1 : Introduction	16
1.1 Introduction	16
1.2 Motivation	16
1.3 Technical Challenges	16
1.4 Aims and Objectives	17
1.5 Contributions	18
1.6 Thesis Outline	18
Chapter 2: Literature review	20
2.1 Chapter Outline	20
2.2 Introduction	20
2.3 Mobile network	21
2.3.1 The fifth generation (5G)	22
2.3.2 5G Enabling technologies and capabilities	23
2.3.2.1 Wireless networks	24
2.3.2.2 Small cells	25
2.3.2.3 Software defined network.....	26
2.3.2.4 Network Function Virtualisation (NFV)	27
2.3.2.5 Key requirements.....	29
2.4 System Application (Software)	30
2.4.1 OpenStack	30
2.4.1.1 OpenStack components	30
2.4.1.1.1 Nova.....	31
2.4.1.1.2 Neutron	31
2.4.1.1.3 Swift.....	31
2.4.1.1.4 Cinder	31
2.4.1.1.5 Keystone	32
2.4.1.1.6 Glance	32
2.5 5G Indoor Location Based Services	32
2.5.1 Overview	32
2.5.2 Challenges and potential solutions of indoor LBS.....	33
2.5.2.1 Beacon-based positioning systems	33
2.5.2.2 Dead-Reckoning (DR).....	36
2.5.2.3 Device Free.....	37

2.6	VLC and mmWave.....	37
2.7	The Theory and Practice of Simulated Annealing	39
2.7.1	Introduction.....	39
2.7.2	Process Optimisation.....	40
2.7.3	Simulated Annealing Algorithm	41
2.7.3.1	SA algorithm procedure	42
2.7.3.2	Advantages and Shortcomings of SA.....	44
2.8	Real Live Streaming.....	45
2.8.1	Internet of Things (IoT)	45
2.8.2	5G Real live streaming.....	46
2.9	Denial of Service Attacks	46
2.9.1	DHCP Attacks.....	47
2.9.2	Spoofing.....	50
2.10	5G Security Location Monitoring.....	51
2.11	Summary.....	53
Chapter 3: 5G Indoor Location Database and Interactive Services		55
3.1	Chapter Outline.....	55
3.2	Introduction	55
3.3	Methodology	56
3.4	5G System Architecture Diagram.....	56
3.4.1	Video Streaming and Network Resources Usage	58
3.5	Location Based Data and Video Transmission and Reception for a Museum Scenario	59
3.5.1	Museum Scenario.....	59
3.5.1.1	The Use Case.....	60
3.5.2	Location Based Data Transmitting and Receiving Scenario Description	61
3.5.2.1	Location Based Data Transmitting.....	61
3.5.2.2	Location Based Data Receiving	61
3.6	Location database System Design on the VNF for access from User Equipment .61	
3.6.1	Database System Architecture	61
3.6.2	System Development	63
3.6.2.1	Front-end development.....	63
3.6.2.2	Back-end development.....	63
3.6.2.3	Both the front-end and back-end system	63
3.6.2.4	System flowchart.....	64
3.7	Design implementation of transmit and receive interactive services	64
3.7.1	Interactive web interface.....	64
3.7.2	End User Application.....	67
3.7.2.1	Functionality.....	67
3.8	Development and testing.....	67
3.8.1	Indoor location-based data access.....	68
3.8.2	Location-Based Image Retrieval.....	69
3.8.2.1	Accessing the Location Database.....	70
3.8.2.2	Data receiving.....	70
3.8.2.2.1	TDOA data upload.....	70
3.8.2.2.2	VLC data upload.....	71
3.8.3	4K Real-Time Video Streaming Location Server.....	71
3.8.3.1	Streaming VNF.....	71
3.8.3.2	Experimental Set up	73
3.8.3.2.1	VideoLAN Client media player (VLC player)	73
3.8.3.2.1.1	VideoLAN Streaming Solution	74

3.8.3.2.1.2	VLC setup.....	74
3.8.3.2.2	Testing Scenario	75
3.8.3.3	Results and analysis.....	75
3.8.3.3.1	Jitter	78
3.8.3.3.2	Delay.....	80
3.9	Summary	82
Chapter 4: 5G Localisation Coverage and Accuracy		84
4.1	Chapter Outline.....	84
4.2	Propagation Distance and Coverage Measuring Experimental Setup.....	84
4.3	Coverage Measuring Experimental Procedure	87
4.3.1	VLC coverage	87
4.3.2	mmWave coverage.....	88
4.4	VLC Coverage Results.....	88
4.5	mmWave Downlink Coverage Results	89
4.5.1	mmWave Transmit Antenna Pointing Vertically Down	89
4.5.2	mmWave Transmit Antenna Point 30° from Vertical about antenna y-axis.....	90
4.5.3	mmWave Transmit Antenna Point 40° from Vertical about antenna y-axis.....	92
4.6	Challenges (VLC and mmWave)	92
4.7	Location Accuracy Measuring Procedure	93
4.7.1	System Architecture Diagram	93
4.7.2	Experimental Setup	94
4.7.2.1	Recording of distance from VLC RSS measurements from the Radio-Light Heads.....	95
4.7.2.2	mmWave location data.....	95
4.7.2.3	Data process script.....	96
4.8	Data Optimisation for Location Measurements Accuracy.....	97
4.8.1	Positioning algorithm	97
4.8.2	SA results and analysis.....	99
4.9	Challenges	104
4.10	Summary	104
Chapter 5: 5G Contextual Aware Indoor Location Security.....		106
5.1	Chapter Outline.....	106
5.2	Introduction	106
5.3	Related work.....	107
5.3.1	Dynamic Host Configuration Protocol (DHCP)	108
5.2.1.1	Current DHCP Mitigation Solutions	108
5.2.1.1.1	Port Security.....	108
5.2.1.1.1.1	Specifying trusted MAC-addresses.....	109
5.2.1.1.1.2	Limiting number of MAC addresses per port (Port security):	109
5.2.1.1.1.3	Sticky MAC address:	109
5.2.1.1.1.4	Port Security and specifying trusted MAC addresses:	109
5.2.1.1.1.5	Detecting DHCP message rate:.....	109
5.4	Indoor Location Security Application.....	110
5.4.1	Security architecture.....	110
5.5	Implementation.....	111
5.5.1	Main Script.....	112
5.5.2	Attack Detection Script.....	113
5.5.3	Check Trusted Script.....	115
5.5.4	Discover Rogue Script	116

5.6	Performance evaluation	118
5.6.1	Testbed description	118
5.6.1.1	Testing plan	118
5.6.1.2	Developing the Network.....	118
5.5.1.3	DHCP configuration	119
5.6.2	Testing the attack	120
5.6.3	Testing the scripts	122
5.7	Results and analysis	124
5.8	Summary	128
<i>Chapter 6: Conclusion and future works</i>		<i>129</i>
6.1	Conclusion	129
6.2	Future works	130
<i>Bibliography</i>		<i>131</i>
<i>Appendix 1</i>		<i>139</i>

List of figures

Figure 2-5: Speed test between 3G and 4G	22
Figure 2-6: Latency vs time	22
Figure 2-7: Wireless Network Types	25
Figure 2-8: Small cells types and their capabilities	25
Figure 2-9: SDN Architecture.....	26
Figure 2-10: NFV Vision	27
Figure 2-11: NFV decoupling	28
Figure 2-12: NFV Structure	28
Figure 2-13: Conceptual diagram of DDoS attack	47
Figure 2-14 - DHCP Discover flood	48
Figure 2-15 - DNS spoofing	49
Figure 2-16: IP spoofing	50
Figure 3-1: IoRL System Architecture	57
Figure 3-2: Museum use case scenario	60
Figure 3-3: Django architecture	62
Figure 3-4: Database Museum Exhibits.....	65
Figure 3-5: Database Museum Test Content	65
Figure 3-6: Creating new content	65
Figure 3-7: Create treasure hunt game.....	66
Figure 3-8: Creating new questions	66
Figure 3-9: App first page.....	67
Figure 3-10:Application Login page.....	67
Figure 3-11: Empty exhibits page.....	68
Figure 3-12: Exhibits uploaded.....	68
Figure 3-13: Backend database uploading information to the app	68
Figure 3-14:Treasure hunt.....	69
Figure 3-15: Access permission.....	69
Figure 3-16: Upload page	69
Figure 3-17: Uploaded image	69
Figure 3-18: The location of the uploaded image	69
Figure 3-19: Image Matching Script.....	70
Figure 3-20: Streaming System Diagram	72
Figure 3-21: Video Streaming through VLC to UE.....	73
Figure 3-22: Dell R730xd server	73
Figure 3-23: VideoLAN Streaming solution	74
Figure 3-24: Streaming Scenario	75
Figure 3-25: Overall number of packets vs jitter	76
Figure 3-26: Overall number of packets vs delay	77
Figure 3-27: Resolutions vs Average Jitter.....	78
Figure 3-28: traditional vs proposed streaming 360p	79
Figure 3-29: traditional vs proposed streaming 1080p	79
Figure 3-30: traditional vs proposed streaming 4K	80
Figure 3-31: Resolutions vs Average Delay	80
Figure 3-32: traditional vs proposed streaming delay 360p.....	81
Figure 3-33: traditional vs proposed streaming delay 1080p.....	81
Figure 3-34: traditional vs proposed streaming delay 4K.....	82
Figure 4-1: VLC Link	85
Figure 4-2: mmWave Link.....	85
Figure 4-3: 10MHz Reference Distribution	86

Figure 4-4: Experimental setup.....	87
Figure 4-5: Four VLC TX LEDs pointing vertically down and Rx PD Non-Angled (pointing vertically up), EVM Test results at ground level	88
Figure 4-6: 4 Four VLC TX LEDs pointing vertically down and Rx PD Angled towards Tx, EVM Test results at ground level	89
Figure 4-7: One mmWave TXs, receiver at 0.7m above ground EVM Test	89
Figure 4-8: One mmWave TXs, receiver at 0m ground level EVM Test.....	90
Figure 4-9: One mmWave TXs angled at 30o, receiver at 0m above ground EVM Test	91
Figure 4-10: One mmWave TXs angled at 30, receiver at 0m above ground EVM Test	91
Figure 4-11: One mmWave TXs angled at 30°, receiver at 0.7m above ground EVM Test ...	91
Figure 4-12: One mmWave TXs angled at 40o, receiver at 0m above ground EVM Test	92
Figure 4-13: 5G positioning system architecture	93
Figure 4-14: MobaXterm	94
Figure 4-15: 14 OFDM symbols, the geographic data	94
Figure 4-16: VLC floor measurement points	95
Figure 4-17: mmWave floor measurement points	95
Figure 4-18: Script Output .txt file	96
Figure 4-19: Data processing Script	96
Figure 4-20: Positioning algorithm diagram.....	98
Figure 4-21: Error against x and y for LEDs A, B, C, D with m=1 and OFDM = 4	99
Figure 4-22: Error against angle from Communication LED for LEDs A, B, C, D with m=1 and OFDM = 4.....	100
Figure 4-23: Error against x and y for LEDs A, B, C, D with simulated annealing optimised m and OFDM numbers	101
Figure 4-24: Error against angle from Communication LED for LEDs A, B, C, D simulated annealing optimised m and OFDM.....	101
Figure 4-25:Error against x and y of 80 iterations for LEDs A, B, C, D with simulated annealing optimised m and OFDM numbers	103
Figure 4-26:Error against angle from Communication LED for LEDs A, B, C, D simulated annealing optimised m and OFDM numbers	103
Figure 5-1: DHCP 4 Stages.....	108
Figure 5-2: Security Architecture	110
Figure 5-3: UML diagram.....	111
Figure 5-4: sniffing	112
Figure 5-5 - Main Script HandlePacket	112
Figure 5-6 - Stop filter	113
Figure 5-7: Libraries	113
Figure 5-8: Attack Detection (detectAttack) Script	114
Figure 5-9: Check Trusted Script.....	115
Figure 5-10: Generate random MAC address	116
Figure 5-11: create DHCP Discover	116
Figure 5-12: Send Packet	117
Figure 5-13: Network Model	118
Figure 5-14 - DHCP Configuration	119
Figure 5-15: Device check	120
Figure 5-16: Check for IP address	120
Figure 5-17: DHCP Binding	121
Figure 5-18: DHCP packets	121
Figure 5-19: Console for PCI.....	121
Figure 5-20: Wireshark with security	122

Figure 5-21: DHCP leased IP addresses	122
Figure 5-22: Detected malicious packets	123
Figure 5-23: PC1 acquires IP from the DHCP Server	123
Figure 5-24: Discover Script.....	124
Figure 5-25: Discover Script output	124
Figure 5-26: CPU usage of the DHCP server during an attack	125
Figure 5-27: CPU usage of the DHCP server during an attack while running scripts.....	126
Figure 5-28:DHCP Discover mitigation	127

List of tables

Table 2-1: Comparison between 3G and 4G networks	22
Table 2-2:Latency and speed test of 3G vs 4G	22
Table 3-1 : Typical Bandwidth Requirements for Video Codecs	58
Table 3-2: Programming languages used for front-end system	63
Table 3-3: Average Jitter	78
Table 3-4: Average Delay	80
Table 4-1: Transmitted Signal Parameters.....	86
Table 4-2: Average Distance Error based on change in Iterations	102
Table 5-1: CPU usage before running the scripts	125
Table 5-2: CPU usage after running the scripts	125
Table 5-3: DHCP Attack without the running security scripts	126
Table 5-4: DHCP Attack while running the security scripts	127

List of abbreviation

ABC	Artificial Bee Colony
ACO	Ant Colony Optimisation
AI	Artificial Intelligence
ARPAN	Advanced Research Projects Agency Network
ARP	Autoradiopuhelin
AMPS	Advanced Mobile Phone System
AMTS	Advanced Mobile Telephone System
BLE	Bluetooth Low Energy
CDMA	Code Division Multiple Access
CHDC	Cloud Home Data Centre
C-RAN	Cloud Radio Access Network
DDoS	Distributed DoS
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DR	Dead-Reckoning
DVB-T	Digital Video Broadcasting — Terrestrial
EVM	Error Vector Magnitude
GA	Genetic Algorithms
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service

GPS	Global Positioning System
GSM	Group Special Mobile
HSCSD	High-Speed Circuit Switched Data
HSGNSS	High-Sensitivity GNSS
ICN	Information Centric Networking
IHIPGW	Intelligent Home IP Gateway
ILBDA	Indoor Location-Based Data Access
ILM	Indoor Location Monitoring
IMU	Inertial Measurement Unit
IoRL	Internet of Radio Light
IoT	Internet of Things
LAN	Local-Area Network
LBS	Location Based Service
LD	Location Database
LOS	Line Of Sight
LS	Location Server
LTE	Long-Term Evolution
MANO	NFV Management and Orchestration
MCC	Mobile Cloud Computing
MEC	Multi-Access Edge Computing
MEMS	Microelectro Mechanical System
MMS	Multimedia Messaging Service
MPEG DASH	Dynamic Adaptive Streaming over HTTP
MTS	Mobile Telephone System
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NFG	Network Flow Guard
NLOS	Non-LOS
ODL	Open Daylight
OFDM	Orthogonal Frequency-Division Multiplexing
OpEx	Operational Expenses
OVS	Open Virtual Stack
PDR	Pedestrian Dead Reckoning
pINS	plain Inertial Navigation Systems
PL	PseudoLites
PSO	Particle Swarm Optimisation
PTT	Push To Talk
QoE	Quality of Experience
QoPS	Quality of Positioning Services
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RF	Radio Frequency
RFID	Radio-frequency Identification
RRH	Remote Radio Heads
RRHL	Remote Radio Head Light
RSS	Received Signal Strength
SA	Simulated Annealing

SAL	Simulated Annealing-based Localisation
SDN	Software Defined Network
SHS	Step and Head Systems
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
TDMA	Time Division Multiple Access
ToA	Time of Arrival
UE	User Equipment
UWB	Ultra-WideBand
VLC	Visual Light Communication
VM	virtual machine
VNF	Virtual Network Function
WLAN	Wireless Local Area Networks

List of Publications

A. Journals

- **Kareem Ali, “Measurement Campaign on 5G Indoor millimeter Wave and Visible Light Communications Multi Component Carrier System”** IEEE Transactions on Broadcasting Print ISSN: 0018-9316 Online ISSN: 1557-9611 Digital Object Identifier: 10.1109/TBC.2021.3120918
- Yue Zhang, Hequn Zhang, John Cosmas, Nawar Jawad, **Kareem Ali**, Ben Meunier, Adam Kapovits, Li-Ke Huang, Wei Li, Lina Shi, Xun Zhang, Jintao Wang, Israel Koffman, Muller Robert, and Charilaos C. Zarakovitis “**Internet of Radio and Light: 5G Building Network Radio and Edge Architecture**” **ITU Journal of Intelligent and Converged Networks**, Volume 1, 01 March 2020, DOI:10.26599/ICN.2020.9070002, Online: 2020-04-24
- Lina Shi, Benjamin Meunier, Hequn Zhang, Xun Zhang, Andrei Vladimirescu, Wei Li, Yue Zhang, John Cosmas, **Kareem Ali**, Nawar Jawad, Rudolf Zetik, Eric Legale, Matteo Satta, Jintao Wang, Jian Song “**Indoor 5G Location-based geographic data broadcasting system in museums**” IEEE Transactions on Broadcasting, Special Issue on the Convergence of Broadcast and Broadband in the 5G Era, vol. 66, no. 2, Part II, June 2020. Print ISSN: 0018-9316, Online ISSN: 1557-9611, DOI: 10.1109/TBC.2020.2977552
- Nawar Jawad, Mukhald Salih, **Kareem Ali**, Benjamin Meunier, Yue Zhang, Xun Zhang, Rudolf Zetik, Charilaos Zarakovitis, Harilaos Koumaras, Michail-Alexandros Kourtis, Lina Shi, Wojciech Mazureczyk and John Cosmas “**Smart Television Services using NFV/SDN Network Management**” IEEE Transactions on Broadcasting (Volume: 65 , Issue: 2 , June 2019) Page(s): 404 – 413, ISSN Information: DOI: 10.1109/TBC.2019.2898159

B. Conferences

- **Kareem Ali**, J. Cosmas, X. Zhang, L. Shi and B. Meunier, "Simulated Annealing Optimisation for Optimising 5G Visible Light Communications Location Measurements," 2021 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), 2021, pp. 1-6, doi: 10.1109/BMSB53066.2021.9547187.



- **Kareem Ali**, Nawar Jawad, Benjamin Meunier, John Cosmas “**IoRL Real-Time Video Lan Client Player Streaming through SDN Network** ” IEEE Broadband Multimedia and Broadcasting Conference, Paris, 26nd to 29nd October 2020
- **Kareem Ali**, Akram Alkhatar, Nawar Jawad, John Cosmas, “**IoRL Indoor Location Based Data Access, Indoor Location Monitoring & Guiding and Interaction Applications**” IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, June 5th – 8th 2018, Valencia, Spain DOI: 978-1-5386-4729-5/18/\$31.00 ©2018 IEEE

C. Co-Author

- Ben Meunier, John Cosmas, Nawar Jawad, **Kareem Ali** “**Realising a new generation of 5G VR systems through Internet of Radio Light**” IEEE Broadband Multimedia and Broadcasting Conference, Paris, 26nd to 29nd October 2020
- John Cosmas, Nawar Jawad, **Kareem Ali**, Ben Meunier, Yue Zhang, Wei Li, Marcin Gregorczyk, Wojciech Mazurczyk, Krzysztof Cabaj, Mathias Lacaud, Daniel Negru, Sara Cuerva Navas, Ignacio Losas Davila, Charilaos C Zarakovitis, Harilaos Koumaras, Michail-Alexandros Kourtis “**Network and Application Layer Services for High Performance Communications in Buildings**” IEEE Broadband Multimedia and Broadcasting Conference, Paris, 26nd to 29nd October 2020
- J. Cosmas, B. Meunier, **K. Ali**, N. Jawad, M. Salih, Y. Zhang, Z. Hadad, B. Globen, H. Gokmen, S. Malkos, M. Cakan, H. Koumaras, A. Kourtis, C. Sakkas, D. Negru, M. Lacaud, Moshe Ran, Einat Ran, J. Garcia, W. Li, L-K Huang, R. Zetik, K. Cabaj, W. Mazurczyk, Xun Zhang, A. Kapovits “**A 5G Radio-Light SDN Architecture for Wireless and Mobile Network Access in Buildings**” IEEE 5G World Forum, Santa Clara, California, USA, 9-11 July 2018.
- J. Cosmas, B. Meunier, **K. Ali**, N. Jawad, M. Salih, H. Meng, M. Ganley, J. Gbadamosi, A. Savov, Z. Hadad, B. Globen, H. Gokmen, S. Malkos, M. E. Cakan, H. Koumaras, M. Kourtis, C. Sakkas, E. Salomon, Y. Avinoam, D. Negru, M. Lacaud, Y. Zhang, L-K. Huang, R. Zetik, K. Cabaj, W. Mazurczyk, A. Kapovits “**A Scalable and License Free 5G Internet of Radio Light Architecture for Services in Homes and Businesses**” IEEE International Symposium on Broadband Multimedia Systems and

Broadcasting, June 5th – 8th 2018, Valencia, Spain DOI: 978-1-5386-4729-5/18/\$31.00 ©2018 IEEE

- J. Cosmas, B. Meunier, **K. Ali**, N. Jawad, M. Salih, H. Meng, J. Royo, P. Fernandez, D. Sánchez, Z. Hadad, B. Globen, H. Gokmen, S. Malkos, M. E. Cakan, M. Kourtis, H. Koumaras, C. Sakkas, E. Salomon, Y. Avinoam, D. Negru, M. Lacaud, Y. Zhang, L-K. Huang, R. Zetik, K. Cabaj, W. Mazurczyk, A. Kapovits “**A Scalable and License Free 5G Internet of Radio Light Architecture for Services in Train Stations**”, EU Wireless Conference, 2-4 May 2018, Catania, Italy.
- J. Cosmas, B. Meunier, **K. Ali**, N. Jawad, H. Meng, F. Goutagneux, E. Legale, M. Satta, P. Jay, X. Zhang, C. Huang, J. Garcia, M. Negru, Y. Zhang, A. Kourtis, C. Koumaras, C. Sakkas, L-K. Huang, R. Zetik, K. Cabaj, W. Mazurczyk, A. Kapovits “**5G Internet of Radio Light Services for Musée de la Carte à Jouer**” Global LIFI Congress, Paris, France, 8th / 9th of February, 2018 (Invited paper) DOI: 10.23919/GLC.2018.8319095
- J. Cosmas, B. Meunier, **K. Ali**, N. Jawad, M. Salih, H. Meng, J. Song, J. Wang, M. Tong, X. Cao, X. Li, X. Zhang, C. Huang, Y. Zhang, M. Ran, E. Ran, E. Salomon, Y. Avinoam, Z. Hadad, B. Globen, D. Negru, M. Lacaud, M. Kourtis, H. Koumaras, C. Sakkas, L-K. Huang, R. Zetik, K. Cabaj, W. Mazurczyk, A. Kapovits “**5G Internet of Radio Light Services for Supermarkets**” 14th China International Forum on Solid State Lighting (SSLCHINA 2017), November 1-3, 2017 (Invited paper) ISBN 978-3-8007-4426-8
- Nawar Jawad, Mukhald Salih, **Kareem Ali**, Benjamin Meunier and John Cosmas “**Indoor Unicasting/Multicasting service based on 5G Internet of Radio Light network paradigm**” BMSB2019 Jiju Island Korea June 20

Chapter 1: Introduction

1.1 Introduction

This chapter reveals the motivation behind the research, followed by a review of the technical challenges facing mobile networks that limits the new performance deployment services and demands. It highlights the aims and objectives and describes the main contributions of the research. Finally, it outlines all the chapters of the thesis with a brief description.

1.2 Motivation

The motivation of this research is to develop a safer, more secure, customisable and intelligent building network. This network intends to deliver a reliable increased throughput greater than 10 Gbps from access points, and be able to locate a user with an accuracy of less than 10 cm. This has been emerged by the Internet of Radio Light's (IoRL) innovative solution to improve the network performance indoors using new access technologies like mmWave and VLC.

The IoRL's Intelligent Home IP Gateway (IHIPGW) was designed to be cost efficient, flexible, and resourceful using Software Defined Networking (SDN) and Network Function Virtualisation (NFV) technologies. As both bring huge benefits, for example, easier management and enhanced resource utilisation.

1.3 Technical Challenges

The demand for mobile networks has been witnessing a rapid increase in data traffic, as it is influenced by the increasing number of users. Around 77 Exabytes per month of broadcasting data traffic is expected by 2020, with 70% to 90% of that traffic taking place indoors, according to data obtained from Cisco [12].

This section will summarise the challenges of the existing networks that limit the new performance demands and expectations.

The communication networks are heavily relying on proprietary solutions and devices. This limits the network from advancing as it lacks efficiency, flexibility, and resources. Thus, it becomes very expensive to upgrade the network and extremely difficult to add new services. Virtual and augmented reality games, as well as live streaming services, are examples of broadcasting services. These services are becoming increasingly reliant on the accuracy of the indoor environment position. Due to the rise in broadcasting data traffic indoors, the difficulty is to get high position accuracy for indoor locations. Furthermore, radio interference makes it more difficult to deliver precise location information. One of the most significant issues facing

the Location Based Service (LBS) is providing a high Quality of Positioning Services (QoPS). The existing Beacon positioning technologies suffer from various challenges like expensive costs to install indoors. Moreover, one of the most significant issues is the small number of emitters. The receiver must also recognise and match the incoming signal to a certain emitter. This raises the question of how precise and dependable this can be done, thereby increasing the danger of position estimate errors. Finally, the drift of position and the difficulty of stabilising the positional information of the double integration of acceleration data are two challenges that inertial dead reckoning encounters.

IP-based communication enables the internet security vulnerabilities and wireless issues to be migrated in the 3G wireless network generation. IP-based communication is becoming more important, 4G mobile networks have enabled multimedia traffic, the spread of smart gadgets, and new services in the mobile realm. As a result of this change, the threat landscape has become more complex and dynamic.

SDN/NFV based solutions for the new mobile networks generation has been a trending topic by both industry and academic researchers. As they allow flexibility and pools of resources that makes the system more efficient. This thesis presents work that addresses the challenges and subsequent proposed solutions. Finally, all the proposed services have been evaluated and provided with a numerical quantification to support their legitimacy and performance improvement.

1.4 Aims and Objectives

The aims of this thesis are as follows:

- To provide an efficient, easier management and enhanced resource utilisation.
- To provide an accurate and dependable indoor positioning system.
- To protect the network from DHCP starvation attack.
- To ensure the network is always accessible to users.

The objectives of this thesis are as follows:

- Design and build a multiaccess edge cloud computing (indoor Location Database and Server VNF that allows the integration of Location data from VLC RSSI and mmWave TOA on network edge for multiple applications to use it e.g., merging of location data and use with applications such as enhancing security and location accuracy and service intelligence).
- Improve real live streaming system's performance parameters.
- To evaluate a novel 5G architecture using mmWave and VLC.

- Perform a world first experiment to measure the coverage for both technologies.
- Perform a world first experiment to measure the location accuracy of VLC.
- Test if the location accuracy data can be enhanced using Simulated Annealing algorithm.
- To Protect the network from malicious attacks (DHCP starvation attack) using VNF on the multiaccess edge cloud that provides a scalable solution to ensure user connectivity.

1.5 Contributions

- Build and implement a Multi Edge Cloud Computing VNF Location Database, that incorporates the IoRL's architecture.
 - Exploiting the Openstack functionalities to provide a dynamic system with resource utilisation.
 - Implement a proposed streaming service to provide an improved performance of QoE for users.
- Present the location coverage and accuracy data optimisation from a 5G indoor mmWave and VLC multi component carrier system. It includes the following field tests:
 - VLC received signal quality measured as Error Vector Magnitude (EVM) against coverage.
 - mmWave received signal quality measured as EVM against coverage.
 - VLC location accuracy against a prescribed grid using received signal strength.

Additionally, Simulated Annealing-based Localisation (SAL) algorithm is proposed to assess the estimated optimised solution of the data.

- Presents a new 5G indoor location security architecture that runs on top of the SDN controller, which aims to protect the system from DHCP starvation attack.
 - Improved network security.
 - Ensured connectivity for all the legitimate users at all times.

1.6 Thesis Outline

The thesis consists of five chapters, starting with an introductory chapter that outlines the motivation of the research and the challenges that exist around the topic. The thesis is organised as follows:

- **Chapter 2:** Presents the relevant literature insight concerning 5G. It discusses what can 5G offer and its benefits. Also, it describes one of the biggest challenges that 5G can

assist in providing location-based services with a QoPS. Real live streaming using 5G is explained. Finally, it defines indoor location security.

- **Chapter 3:** Presents the indoor location proposed solution interactive applications. It presents the system architecture, implementation of the indoor location database, interactive application for the users, and real-time video streaming location services.
- **Chapter 4:** This chapter presents the location positioning procedure (location coverage and location accuracy). Whilst, introducing a data optimisation solution, which assess the estimated optimised solution of the data.
- **Chapter 5:** Presents the proposed security architecture for 5G indoor location security. It focuses on the DHCP starvation attack and presents a solution to protect the 5G system from DHCP attacks.
- **Chapter 6:** This chapter presents a summarisation of all the contributions. It examines what has been implemented and developed throughout the thesis. Also, it discusses how this work can be extended for future work and advancements.

Chapter 2: Literature review

2.1 Chapter Outline

This chapter presents the research topics that relate to the main contributions of the thesis. This chapter is organised as follows: Section 2.2 introduces internet of things. Section 2.3 presents the 5G technology and its enabling services. Section 2.4 presents the platform that was used for the deployment of the location database. Section 2.5 analyses indoor location based challenges being faced by the 5G. Section 2.6 presents VLC and mmWave technologies. Section 2.7 considers and reviews the simulated annealing algorithm. Section 2.8 discusses the experiments and complexities facing the streaming industry due to the rapid increase in the demand. Section 2.9 presents the different security attacks. Section 2.10 conveys the 5G security location vulnerabilities. Finally, Section 2.11 provides a summary.

2.2 Introduction

The Long-term evolution (LTE) is a standard high speed wireless communication that could see data speeds occurring up to 10 times faster than the current existing one. The 4G LTE connection is worldwide, however the prospect is 5G. This is the next generation of wireless technology, which could be ten times faster than the existing 4G connection that will give a superb speedy and steady internet access.

The transfer of enormous amounts of data to and from connected devices and objects will alter the world of technology. Visible light communication (VLC) is a data communications technology for wireless transmitting and receiving information using visible light. Additionally, the process goes from infrared through visible light into ultra-violet visible light spectrum of about 400 THz to 800 THz instead of using radio waves.

Internet of Things (IoT) is a technology that is promising, and which intends to transform and connect the world by seamlessly connecting heterogeneous smart devices. Recent cellular standards such as Long-Term Evolution (LTE) for mobile devices have been introduced, but these are not well suited for low power and low data rate like IoT devices [1]. Particularly, the fifth mobile (5G) generation network aims to address the constraints of previous cellular standards and to be a potential key enabler to the future of IoT [1].

Recently, the prevailing trend in networking has been wireless technology [2]. Wireless service demands are increasing rapidly and create both challenges and opportunities in mobile networks by introducing the 5G wireless system [3] [4]. Distinct service requirements and features vary in 5G [5] [6]. A flexible and open network to ensure a better efficiency of resource allocation on the network is required for coordination and management of various applications, user requests and networks. The virtualisation of mobile network [7] , which coordinates

network resources and integrates various wireless networks can address these demands [2]. There have been numerous efforts to improve the 5G networking and to develop better technologies to respond to user requirements. 5G focuses its design objectives on versatility, scalability and efficiency in order to satisfy device capacity and connectivity improvement [2].

5G offers various technological advancements, which have a huge transformation and impact if merged with broadcasting services [8]– [11]. The demand from broadband networks for mobile data location broadcasting services has been rapidly increasing. It is predicted that broadcasting data traffic will reach approximately 77 Exabytes per month by 2020, while 70% to 90% of the overall traffic will be in indoor environments, according to the data obtained from Cisco [12]. With all the services, that require high data speeds and high-definition videos, there is still a lot of demand for location-based services (LBS) [13]. According to Basiri’s paper, there are 52.63% positioning capabilities in the common day to day used devices, like mobile devices, tablets and many other electronics. The facilitated positioning capabilities by 5G, will allow the advancements of LBS [14].

2.3 Mobile network

What is a cellular network (mobile network)? It is the native connectivity approach, which is deployed on dial-up devices and smartphones. It is a mobile-based network that is utilised with a radio antenna [15]. The evolution of cellular networks made it a “high-speed, high-capacity voice and data communication networks with enhanced multimedia and seamless roaming capabilities for supporting cellular devices”[16].

A standard for high speed mobile communications is the long-term evolution. 4G LTE communication is currently the main method or standard used in the world, however 5G is the evolution from 4G. The fifth generation of mobile communications can be ten times faster than the existing 4G communication method, which will give a more reliable internet access and a high-speed access.

A comparison was conducted in 2015, by Hendrik Ferreira, between 3G and 4G networks. The main objectives of the study were to compare some features like scalability, latency, and data transmission rate [17]. The study also compared the uplink and downlink speed. As shown in Table 0-1, Ferreira compares the architecture, speed, frequency bandwidth, switching techniques and internet protocols [17].

	3G	4G
Major requirement driving architecture	Predominantly voice driven data was always add on	Converged data and voice over IP
Network architecture	Wide area cell based	Hybrid-integration of WLAN

Speed	384Mbps – 2Mbps	2Mbps – 200Mbps
Frequency bandwidth	1800MHz – 2400MHz	2GHz – 8GHz
Switching technique	Circuit and packet switching	Packet switching
Internet Protocol	A number of air link protocol including IP5.0	All IP based (IPv6)

Table 0-1: Comparison between 3G and 4G networks

4G system applications was able to facilitate sending data like video, picture and audio during a phone call [18]. A latency and speed test have been conducted on a network, based on MTN South Africa network, as shown in Table 0-2.

Network Features	3G	4G
Latency Time	91ms	44ms
Uplink rate	2.11 Mbps	7.74 Mbps
Downlink rate	17.68 Mbps	23.92 Mbps

Table 0-2: Latency and speed test of 3G vs 4G

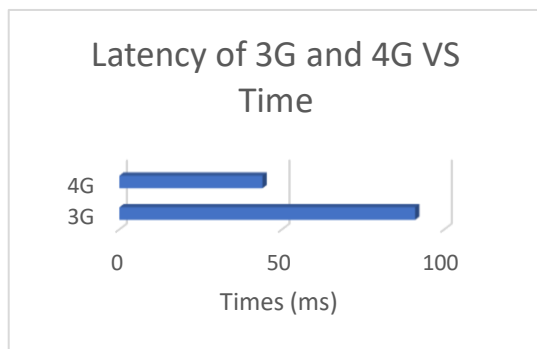


Figure 0-2: Latency vs time

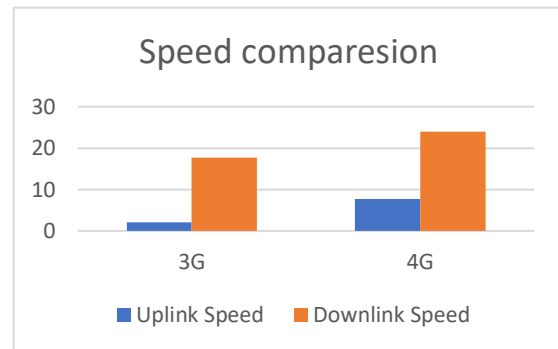


Figure 0-1: Speed test between 3G and 4G

To be able to illustrate Table 0-2, the results were represented in a chart, as shown in Figure 2-5. The data shows that the 4G's uplink is better than 3G by a variation of 5.63 Mbps, with a downlink speed difference of 6.24 Mbps. This clearly shows the superiority of 4G over 3G considering the delay measured between the two generations in Figure 2-6. Latency is the time taken for a packet transmitted from the server to the end user and back to the server [17]. Evaluating the latency of 4G being 44 ms to the 3G being 91 ms in delay time. This means that the delay time has decreased by 55 ms for the packet sent. Hence, 4G could support features like games and teleconferencing applications like skype as it has less latency [17].

2.3.1 The fifth generation (5G)

The increasing demands have a major impact on the future of mobile network architectures. To understand the necessity for a radical change to the network, first, the

challenges must be identified. There are four major challenges: high traffic volume, indoor and small cell/hotspot traffic, high number of subscribers, and energy consumption [19].

- **High traffic volume:** From 2012-2016, the compound growth rate of mobile data traffic was 78% reaching up to 3.7 Exabytes per month [12]. By 2022, the compound annual growth rate will be 46 % reaching up to 77.5 Exabytes per month [20]. Increases in the demand of several magnitudes to be able to support a massive capacity is a requirement [19].
- **Indoor and small cell/hotspot traffic:** Most mobile traffic volume will be made up of indoor and hotspot traffic. In 2017, an estimated of 60% voice traffic and 70% data traffic was happening indoors [19]. It was anticipated to be over 90% in 2020 [19], however, reported in June 2019 by Ericsson that indoor data traffic has been 82% [21].
- **Vast number of subscribers:** In 2018, the number of subscribers worldwide was 7.9 billion [22]. In 2019, it had reached 8.3 billion mobile subscriptions [22]. The number are growing day by day and the next mobile network needs to accommodate all the users.
- **Energy consumption:** With the increase of subscribers and the higher traffic volume, 5G mobile network must reduce the power consumption.

The fifth generation of mobile communications can be ten times faster than the existing 4G communication method, which will give a more reliable internet access and a high-speed access. 5G enables a new form of network that is designed to virtually connect everything and everyone together [23]. 5G is destined to deliver high data speeds, low latency, massive network capacity, and increased availability [23].

All the other generations discussed prior led to 5G providing more connectivity than it was available before. “5G is a unified, more capable air interface. It has been designed with an extended capacity to enable next-generation user experiences, empower new deployment models, and deliver new services” [23]. 5G will have a huge impact on every industry by providing negligible latency, where remote healthcare can be achieved [23].

2.3.2 5G Enabling technologies and capabilities

The future generation of communication networks are anticipated to be applied and executed on virtualised infrastructures. So instead of deploying network functions on the current proprietary equipment, it would be deployed on virtual machines [24]. “Moving away from an architecture that is based on a multitude of black boxes that are equipped with

specialised network hardware and pre-loaded with specialised software to a new architecture consisting of a “white box” running a multitude of specialised network software appears to be the dominant choice and the direction in current and future communication and computing infrastructures”[24].

Managing networks has been very difficult as it requires a lot of resources, however, Software Defined Network (SDN) and Network Function Virtualization (NFV) have proven to be the promising future of managing networks. Both bring enormous benefits, such as easier management, enhanced resource utilisation and reduced operational costs. In the era of network management there were two key objectives: operational costs and resource utilisation. SDN and NFV are decreasing the costs and increasing the network resources [24]. Also, NFV allows additional flexibility by allowing the dedicated hardware network functions to be migrated to virtual machines that runs on commodity hardware. A key for technological innovation and changes in networking has been SDN as it has allowed new factors to converge. Some of the factors are convergence of infrastructures like computing, storage, and network. Subsequently, another factor would be the growth of cloud applications [24].

2.3.2.1 Wireless networks

In 1885, Heinrich Hertz used the discoveries of Maxwell by demonstrating and proving that electromagnetic waves travel at the speed of light [25] [26]. In addition, he proved that electricity can be carried on the electromagnetic waves [26]. In 1990, wireless networks started to infiltrate the market.

The main question is still how the above relate to wireless networks? And what is wireless networks? Data was propagated through wires in the form of electrical signals, which was the standard Local-Area Network (LAN) [26]. Hertz’s discovery allowed the same data to travel as electrical signals but without the need of wires [26]. Therefore, wired networks evolved from the existing wired network connections (Ethernet) to wireless networks that operate without wired connection between network nodes. Wireless network is also referred to as Wi-Fi or 802.11 networking [27]. Moreover, wireless network relies on using radio waves similar to mobile phones.

Nowadays wireless networks are universally used as interconnectivity mediums, due to their fast connection. The standards have been evolving throughout the years as shown in Figure 2-7. The performance and speed (data rate) kept on progressing with the new technological advancements.

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Figure 0-3: Wireless Network Types

However, there are issues that are encountering the wireless networks now. These issues are very challenging and overcoming them will be revolutionary. The issues are interference, heavy congestion, restricted propagation, and poor indoor location services. To increase the mobile network coverage and capacity in localised areas, the deployment of small cells is needed.

2.3.2.2 Small cells

What are small cells? It is a term for low powered mobile base stations that are operator controlled. “It encompasses those that operate in licensed and unlicensed spectrum, including cellular technologies, Wi-Fi and emerging standards such as WiGig” [28]. There are four types of small cells, which are distinguished by the radius and number of users [28].

Cell Type	Output Power (W)	Cell Radius (km)	Users	Locations
Femtocell	0.001 to 0.25	0.010 to 0.1	1 to 30	Indoor
Pico Cell	0.25 to 1	0.1 to 0.2	30 to 100	Indoor/Outdoor
Micro Cell	1 to 10	0.2 to 2.0	100 to 2000	Indoor/Outdoor
Macro Cell	10 to >50	8 to 30	>2000	Outdoor

Figure 0-4: Small cells types and their capabilities

As shown in Figure 2-8, the four types are Femto, Pico, Micro and Macro cells. Femtocell has the smallest radius, which allows it to only cover a small area like in homes. Picocell range is slightly more than femtocell, which allows it to cover wider area like a hotel. Microcell covers areas like companies and shopping centres. Finally, Macrocells is the largest in radius coverage, which covers areas like public venues [28].

Small cells are used to expand the coverage of mobile networks for indoor locations, due to the lack of outdoor signals as they cannot penetrate properly. The capabilities provided by small cells allow them to be a crucial part of 5G networks [28]. As small cells have the capability to improve and expand the network capacity, density, and coverage primarily indoors. In addition, they are cost effective as they have low cost of deployment and low power

devices. Moreover, the banding together of different sized cells is called a HetNet. It provides an ultra-dense coverage in specific geographic areas, which is an extremely vital necessity for the 5G networks [28].

In the 5G networks, small cells will offer ultra-dense networks and coverage [28]. Also, it will allow usage of higher frequency spectrum bands and when there is a low usage, it will automatically be switched off to save power [28]. Small cells will allow the deployment of new services like indoor proximity for the user's location. For example, a user going into a shopping centre, the network would automatically be alerted of the user's location to allow services like indoor guiding and provide the user with information.

2.3.2.3 Software defined network

Software defined network is a network architecture, which allows the network to be controlled and modified using software applications. It extracts the logical part of computer networks to a centralised controller. One of the most characterising properties of the SDN is that it separates the control plane from the data plane [29]. The control plane decides how and where will the traffic by sent. On the other hand, the data plane, which “forward data flows and provides programmable interfaces to control network traffic”[29]. Due to the separation, the necessity for admins to state hardware parameters in low level was available because the decoupling made the network configuration and management simpler. Another important feature of the SDN was programmability as it is easier to implement and maintain the complex control logic by the aid of software programs [29].

Figure 2-9, shows how the SDN is divided into three layers: application layer, control layer and infrastructure layer. the layers interact with each other through APIs. The northbound permits the communication between the application layers and the control layer. The southbound permits the communication between the infrastructure layer and the control layer.

The application layer contains the network applications like security management, firewall, load balancing and other network utilisation services. The control

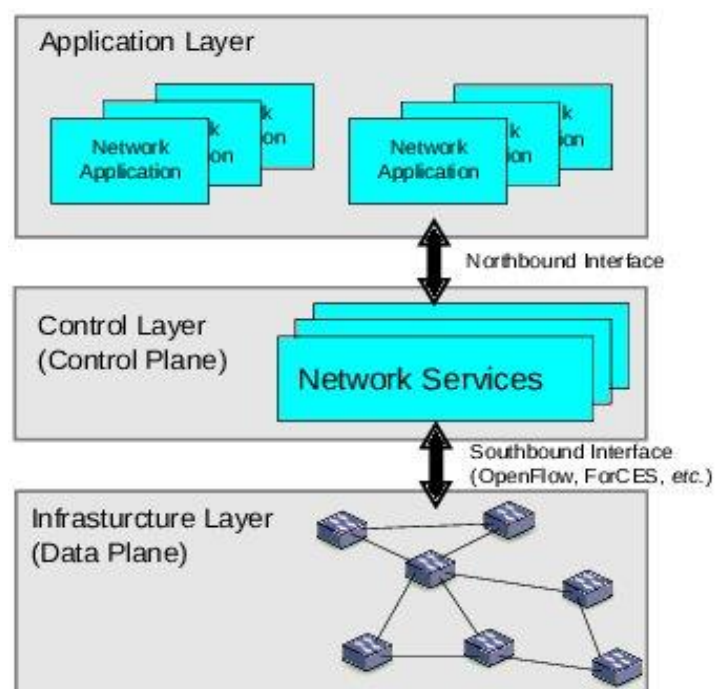


Figure 0-5: SDN Architecture

layer (control plane) is the logical brain of networks [29], which has a global view of the network and controls all the network devices. This indicates that network devices are not required to implement and understand a lot of the different network protocol standards anymore. They only accept instructions from the SDN controller, which saves a lot of resources and time. In addition, this makes it easier for the network to be controlled and managed by programming applications [30]. There are different types of controllers such as NOX and Floodlight [29]. Also, the network controller uses programs written in high level abstract languages to implement different policies [31]. The infrastructure layer (data plane) contains all the network devices such as switches. One of the highly common SDN programmable interfaces is OpenFlow, which is used for controlling packet forwarding [29]. SDN and NFV are highly complementary as both are beneficial but not dependent on each other. The NFV provide us with new and robust ways to design and build networks.

2.3.2.4 Network Function Virtualisation (NFV)

As network operators perceived that there will be a huge deficiency in the future of network capabilities. Network function virtualisation has been considered due to its functionality, capacity, and services [32]. NFV concentrates on the virtualisation of network functions such as load balancers, gateways, proxies, and firewalls. In addition, NFV focuses on any network function that is running on a hardware to virtualise and migrate it to software-

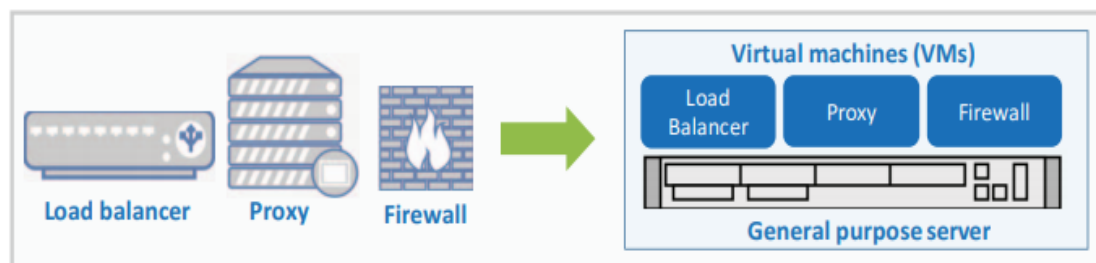


Figure 0-6: NFV Vision

based running on Virtual Machines (VMs) [33]. These VMs can run on all hardware resources like networking devices, servers, and storage devices. They are managed as a shared resource pool, as they can be instantiated and moved in different locations on the network without the requiring any new installations. Figure 2-10, demonstrates a clear illustration of the NFV vision [33].

NFV splits the functionality from the capacity. This decoupling encourages heterogeneity and increases the network elasticity. An example to illustrate a better picture is shown in Figure 2-11, as it separates the network services from the hardware that deliver them [33]. NFV's network services are based on a set of Virtual Network Functions (VNFs). These VNFs must be assigned on top of the physical network infrastructure [33].

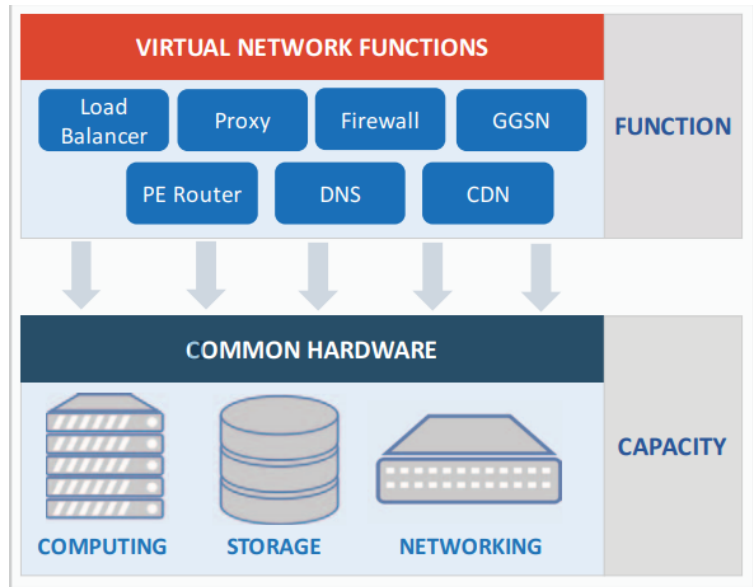


Figure 0-7: NFV decoupling

Maximising the usage of hardware resources is vital for the future of network operators. A hypervisor layer is used to manage all the hardware resources due to the VNFs being able to run on VMs. “The virtualization technology along with cloud computing principles provide to NFV technology a dynamic operation and on-demand deployment of services” [33].

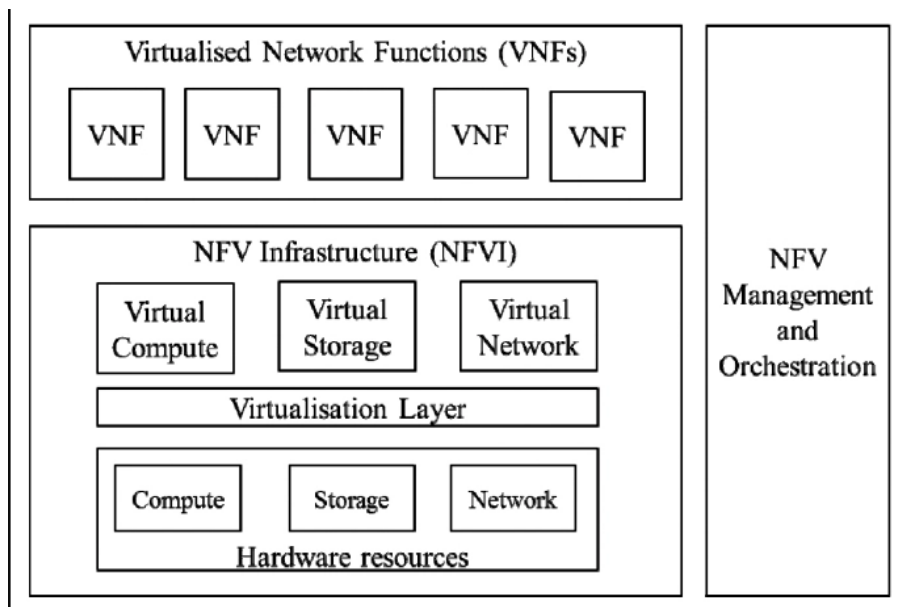


Figure 0-8: NFV Structure

Figure 2-12, describes the NFV framework at a high-level implementation. The network functions implementation is on both the physical and virtual infrastructure [34]. It is based on three main domains of NFV:

- **Virtualized Network Function (VNF):** It is a software deployment of a network function, where it creates a virtualised network away from the hardware. It has the capability of running on top of the NFVI [34].
- **NFV Infrastructure (NFVI):** NFVI is a set of both physical and virtual resources that are used to connect and host VNFs, like networking or storage [34].
- **NFV Management and Orchestration (MANO):** It organises the networks and recourses needed for services and applications. Also, it is vital for supervising VNFs [34].

The benefits of NFV are better optimisation, flexibility, and resources efficiency. The suggestion here is that better optimisation means a reduced power consumption. The flexibility offered by the easy software implementation of network functions. It uses the resources efficiently as it runs as many VMs on one machine [35].

Both SDN and NFV technologies makes the entire network agile and modular. As both can deliver reliable, consistent, and high-quality to the users. OpenStack integrates the SDN technology through the neutron module, while it is always used in conjunction with the NFV.

2.3.2.5 Key requirements

Requirements	SDN	NFV
Control	Standardization of the control interfaces. Protection of commercial business operating schemes. Measures to avoid performance degradation. Maintenance of information of the controlling	Seamless control and provisioning. Real-time and dynamic provisioning. Creation of network granularity policies.
Reliability	Seamless connectivity and fast connection recovery. Security and reliability of the transport and data network. Security requirements in EPC and RAN. Equilibrium among performance, security and flexibility	The high complexity of 5G (technologies, devices, IoT). Seamless and high-quality connectivity. Virtualization of terminal points. Security concerns (same physical medium).
Scalability	Support of technology and device heterogeneity. Controller messages with performance and survivability	Carrier-grade scalability and robustness. Acceleration of implementation.

	(low packet loss levels) Optimization of flow rules-better network slicing.	Openness and interoperability, global reach and cross administration
Cost efficiency	Reduce CAPEX & OPEX	Reduce equipment costs (CAPEX) and operational costs (OPEX)
Energy efficiency	Reduce power consumption.	On demand allocation of resources, and efficient utilization of network resources
Security	Firewall, access control, DOS attack detection/ mitigation, traffic anomaly detection.	Micro-segmentation is a security technique that enables fine-grained security policies to be assigned to data centre applications, down to the workload level. Many data centre virtualization technology vendors, including Cisco, Nuage, and VMware have been touting the benefits of micro-segmentation as an advantage of network virtualization.
Reason of being	Separation of control and data, centralization of control and programmability of network.	Relocation of network functions from dedicated appliances to generic servers

2.4 System Application (Software)

2.4.1 OpenStack

OpenStack is an open source platform which builds and manages private and public clouds using pooled virtual resources. The tools, called Projects, which include the OpenStack platform, handle the core computer, network, storage, images and identity. There are also over a dozen optional projects that can be grouped together to create unique, usable clouds [36].

OpenStack allows users to deploy virtual machines and instances to manage a cloud environment with different tasks. It simplifies horizontal scales, so that simultaneously functioning tasks can easily serve users by simply spinning more instances [37].

Most importantly, the OpenStack software is open source, which means that anyone who decides to access the source code can make the modifications that may be needed and share the changes freely with the community. OpenStack has the advantages of thousands of developers worldwide who work together to develop the most robust, strongest, and safest product possible [37].

2.4.1.1 OpenStack components

OpenStack has nine components, core services that handle computing, networking, storage, identification, and images, while more than a dozen options vary in maturity. The six

core services are the structure for managing dashboarding, bare-metal provisioning, orchestration, containers, messaging and management in all other projects [36].

2.4.1.1.1 Nova

Nova is an OpenStack computer resources management and access tool [36]. It is used to deploy and manage many virtual machines and other instances in order to handle computing tasks [37]. Nova's architecture allows the design of the cloud without the need to develop proprietary software or hardware, and also enables the integration of legacy systems and third-party products [38].

2.4.1.1.2 Neutron

Neutron offers networking capability for OpenStack, such as network management and IP addresses. It ensures that the network does not limit a cloud deployment factor and provides users with the ability to self-serve through network settings. Networking OpenStack enables users to create own networks and connect servers and devices to one or several networks. SDN technology can be used by developers to support large-scale multi-tenancy [38].

In addition, it offers a framework for the development of other network services, like the VPN network, firewalls, load balancing and intrusion detection system. It also offers an extension frame (IDS) [38].

2.4.1.1.3 Swift

OpenStack Swift provides scalable, redundant data store that stores accessible data petabytes. You can leverage, recall and update the stored data. The architecture is distributed and offers greater redundancy, scalability and performance without a central control point [38].

In other words, the developer can refer to a unique identifier that refers to the file or piece of information by the location of files on a disc, and allow OpenStack to decide on where this information should be stored. This simplifies scaling because developers have no concern about the abilities of a single software system. The system can also worry more about how best to ensure that the data are backed up if a machine or network connection fails [37].

Swift is a fully available shared object store which is eventually consistent. It supports organisations in safer, cheap, and efficient storage of vast amounts of data. Swift ensures the replication and distribution of data over different devices, making this ideal for economical scale-out storage [38].

2.4.1.1.4 Cinder

OpenStack Cinder provides certain block-level storage devices for OpenStack compute instance applications. By integrating block storage volumes with Nova and Dashboard, a cloud user can manage their storage needs [38]. It is similar to the traditional idea that a computer

can access certain locations on the drive. In scenarios with data access speed, this traditional way of accessing files is the most important [37] .

Cinder could use many different storage platforms such as Linux server, CloudByte, IBM, etc. Also, it is suitable for extendable database storage and file systems [38].

2.4.1.1.5 Keystone

Keystone offers list of all the users mapped against all OpenStack services. It integrates with existing backend services like LDAP while acting as a common cloud authentication system. Keystone also supports different forms of authentication such as standard username and password credentials, AWS-style logs and token-based systems (Amazon Web Services). Furthermore, a list of services deployed in an OpenStack cloud will be provided in the catalogue [38].

2.4.1.1.6 Glance

OpenStack Image Service provides virtual machine image discovery, registration, and restoration. With the client-server architecture, Glance offers a REST API to allow the query of the image metadata and the recovery of the actual image on the virtual machine. Glance uses the stored images as templates when deploying new virtual machine instances. Also, OpenStack Glance supports Virtual Machine Images (Qemu/KVM) as well as VMWare (VMDK, OVF), Hyper-V (VHD) [38].

OpenStack enables users to manage a cloud environment by deploying virtual machines and instances. This will allow location based services to be deployed as the openstack will be able to provide it with a lot of resources and flexibility.

2.5 5G Indoor Location Based Services

2.5.1 Overview

Location Based Services are being used widely by many people around the world as it assists in finding and tracking [39]- [40]. According to Pew Research 2013, active users of LBS are about 74% of smartphone owners. Thus, when LBS is used indoors, it becomes very difficult to provide the same location accuracy with the same reliability level as outdoors [41]. There are numerous life-saving services, such as security and emergencies, that would benefit from indoor LBS.

Based on a web survey that was conducted in May 2015 over a period of three months, had 245 participants aged between 18 and 73 years. The results showed 26.32% use location enabled devices once a day and 21.05% 2 to 5 times a day. The frequency of use of the application by users of LBS showed that 44.4% use it 2 to 5 times a day [42]. These results

verify how important is indoor LBS. One of the most important challenges that faces the LBS is being able to provide a Quality of Positioning Services (QoPS).

2.5.2 Challenges and potential solutions of indoor LBS

Location based application services are in demand by many and it is required to be reliable, accurate and work simultaneously with the outdoor positioning [14]. The three main Localisation technology groups will be introduced in review of their QOS to give an understanding of the huge challenge that they are currently facing. The three technologies are: Beacon Positioning Technologies, Dead-Reckoning (DR), and Device Free. These technologies can be merged, and this can be the fourth technology, which is called Multisensory Positioning [43].

2.5.2.1 Beacon-based positioning systems

The most used outdoor positioning technology is Global Navigation Satellite System (GNSS), which demands on using Radio Frequency (RF) signals. Thus, the signals can be easily reflected or blocking by the surroundings such as walls, ceilings, and buildings [49]. There have been different approaches to attempt using GNSS indoors using ground-based PseudoLites (PL), which repeating and mirroring satellite signals or using High-Sensitivity GNSS (HSGNSS) receivers [50]. Despite the theoretical possibility, it was not able to become a universal feasible solution for indoors due to expensive costs.

Many station installations are required for PL, and must be planned well, to not interfere with GNSS. The benefits of HSGNSS come at an expensive price (up to hundred euros), and it all depends on the features of module offers [51]. Additionally, it is very difficult to acquire a position due to weak signals. The achieved position accuracy is not accurate as it is greater than 50m [52]– [55]. The advantage of cellular signals and television broadcast over GNSS is that they penetrate buildings better [56].

In addition to these technologies, there are some other methods that can be applied for GNSS-based positioning in partially denied areas, which include shadow matching [57]. Digital Video Broadcasting — Terrestrial (DVB-T) relies on Orthogonal Frequency-Division Multiplexing (OFDM), which can provide fine information regarding the channel state. Besides that, the emitters' locations are usually known, which also offers a great advantage over the other technologies. However, one of the main challenges is the low number of emitters. In addition, the receiver has to identify and match the incoming signal to a specific emitter. This poses a question on how accurate and reliable this can be done, increasing the risk of errors in the position estimation [58].

Wireless Local Area Networks (WLAN) technologies are definitely one of the most popular RF-based technology for positioning, that were not originally developed. IEEE 802.11 is one of the most commonly used WLAN standards. Almost every electronic device now supports this protocol. Since, OFDM signals are used in most recent IEEE 802.11 protocols, they present a new opportunity for positioning. It can be used for indoor positioning with acceptable availability due to its widespread availability in urban environments, both residential and industrial. These networks have mainly been used for positioning under fingerprinting solutions, providing a reasonable performance of 5 to 10 metres in densely covered areas [44] [45].

These signals report on the channel state that can be used to obtain range measurements in a positioning context. This measurement is more reliable than the RSSI, but requires accurate environmental models too. Nevertheless, these models are hard to build as most channel effects are hard to model or to understand how to model them properly. A training phase might therefore also be required [46].

Many Wi-Fi Access Points are available today. The required attributes are signal strength and flight time. 802.11v includes the placement protocol as well. The 802.11v standard for Time of Arrival (ToA) is assessed [47]. The interference and coverage of the different protocols in the 802.11 Families is also compared [14]. Wi-Fi signal strengths for fingerprinting have been obtained in [14]. The signal strength was embodied through Wi-Fi. Wi-Fi with the GNSS Receiver and the IMU was used by Hejc et al. [48]. It is a challenge to move from indoor to outdoor, because the GNSS takes time to make the first fix. These transition area characteristics between the technologies used therefore need to be identified. The next generation amendment for 802.11az is also being developed for new positioning systems designed to run on wireless networks[49].

Ultra-WideBand (UWB) offers distinct advantages in the handling of multipath propagation. Its short pulses, in particular, make detecting the multi-path components easier. The ultra-wideband approach has a strong advantage of repeatability. The position result therefore remains consistent over a period of time [50]. UWB tags were placed on the helmet and shoe in [51]. Due to Non-Line-Of-Sight conditions, the tag measures on the shoe had much more outliers. While the high-time resolution of UWB signals allows the distinction between original and multipath signals to be made easier, the visual non-line conditions are still a challenge.

Another increasingly popular short-range wireless data exchange protocol is Bluetooth, which was introduced after Bluetooth 4.0 was unveiled [14]. The use of Bluetooth Low Energy

(BLE) allows many applications to stay active for a few months at a time. BLE can be applied in several locations to improve location indoors, due to its low cost and power efficiency [14]. Proximity-based positioning means improved performance with respect to estimated position error. Experiments show that over 20 metres, RSS becomes very low, causing positioning to be impossible [52].

Radio-Frequency Identification (RFID) is made up of RFID readers and tags or transceivers. There are two different approaches; Active approach and passive approach. The user carries the reader and scans the tags in the environment during the active approach. However, during the passive approach, the user carries the Tag passively and readers are positioned in the environment. There is a very short (2 m) passive RFID detection range, and a standalone passive system is costly to install. In particular, privacy is important in passive RFID tag systems, where cryptographical data protection is not supported by the calculation capacity of the tag. RFID is generally used as a nearness positioning system [53] [54] [55] [56].

Moreover, camera can be used in several ways for positioning. The user can carry the camera and the images can match with the geo-referenced pictures available [56]. Basiri [14], have used codes/markers placed at buildings and a smartphone camera was used to track and identify the unique marks, then look up the corresponding position in the database. However, Golay and microbolometer cells infrared cameras are very costly and cannot be used in several indoor LBS applications. In addition, thermopiles and pyroelectric sensors are very affordable but less accurate [14]. These can be effective when the conventional picture processing becomes impossible in low lighting conditions [14].

Ultrasonic signals and sound travel through a medium such as air and the received strength or time of travel can assist by calculating the position of the receivers. Common methods used to derive the position or the location are form recognition, travel time and signal strength. The signal amplitude envelope detection approach was, used by Hoflinger 2014, on received chirp-form signals. In order to calculate the position, Rishabh 2012, used the Time of Arrival (ToA). The timing was based on the detection of certain sound signals by comparing them with the base station reference signals. Cross-correlation was used to correlate the recorded signal with the reference signals. The sound source can be transmitted by the user or several sound sources can be located as base stations in the environment. The sound-based localisation system design would be really challenging, if there are echoes, ambient noise and multipath within the environment [14].

2.5.2.2 Dead-Reckoning (DR)

Dead reckoning positioning systems could be classified into two groups; Head Systems (SHS) and plain Inertial Navigation Systems (pINS). The new system that allowed a wide use was Microelectro Mechanical System (MEMS) INS. Smartphones that have inertial sensors (gyroscopes and accelerometers), allow them to be used as input devices for Pedestrian Dead Reckoning (PDR). MEMS sensors have gained a lot of interest due to its low cost and their small sizes [14]. The MEMS inertial provide the user position by comprising the accelerometers “by double integrating the specific force along its sensitive axis” [57].

Racko’s paper used smartphone sensors, together with low cost Inertial Measurement Unit (IMU), for a PDR and compared it with expensive Xsens IMU and more precision [57]. In the past years, there was an increase in the accuracy of inertial sensors. However, they alone cannot provide a proper accurate position due to the various negative effects, like heading drift caused due to the gyroscope bias [58]. Additionally, inertial navigation has been aided by using the map matching techniques [58], as it brought the low-cost MEMS INS accuracy close to what is required for indoor LBS.

Generally dead reckoning systems are not considered as a stand-alone positioning system because they rely on external positioning technologies for calibration such as Wi-Fi and GNSS due to their drift. A challenge that it faces inertial dead reckoning is the drift of position and that it is hard to stabilize the positional information of the double integration of acceleration data. There is another challenge, which is initializing the IMU parameters [59] .

Harle [14] published a comprehensive review on the inertial positioning systems. The evaluations used by Step and Heading Systems (SHS) is the estimates of step length and heading. Some of the approaches that can be used to detect steps are template matching, peak-detection, spectral frequency and zero crossing [60].

The three step detection algorithms were compared by Isaac Skog [60]: acceleration moving variance detector, acceleration magnitude detector, angular energy rate detection. There is a lot of challenges to be able to estimate the next step position like shuffling, slippery ground and the use of lifts. These make it hard to detect the zero angular velocity or the zero velocity thresholds [61]. Moreover, there is another approach but it is much more complex to get the inertial navigation solution, which is using learning methods like artificial neural networks and statistical model comparisons [14]. To conclude, the DR systems are not satisfactorily for indoor positioning by themselves [14].

2.5.2.3 Device Free

The presence of a user at a certain position can be recognised by tactile sensors such as piezoelectric, capacitive touch surfaces, buttons and levers [14]. The tactile localization is based on the use of sensors or samples, which are in direct physical contact with a surface or blockage. It is relatively simple and precise to locate using tactile localization sensors [14]. However, in public environments identifying the correct location for the targeted user may require additional information, such as a camera picture. Odometry identity is easier to use but it requires the users to have the sensor on them [62].

Another device that can be used for positioning is cameras, such as CCTVs. The user can be detected by the camera network that is covering the environment [14]. The location can be traced via visual odometry by comparing sequential image patterns via the image flow. For a more precise estimate of camera motion or three-dimensional positioning, a stereovision setup can also be applied [63].

For measurement of air pressure, in particular indoors, barometers are relatively simple to use and are thus possible to use for detection of altitude or height changes, which [14] distinguished the floor level successfully. With weather conditions changing, it is difficult to calculate the correct height in a real time application, which affects measured pressure, reference pressure and the temperature [64].

The IoRI proposed using two promising technologies for future 5G indoor communications, mmWave and VLC, allowing for gigabit-per-second data transmission while meeting ever-increasing capacity demands.

2.6 VLC and mmWave

In 2006, Afghani and Haas were the first ones to use OFDM for visible light communication [65]. A DC-OFDM scheme was used to achieve a data rate of 500 Mbps. VLC is now defined by the IEEE 802.15.7 standard, and its task group is primarily responsible for designing the physical and MAC layers for VLC [66].

The most common type of light source is a white LED, which can be constructed from red, green, and blue (RGB) or yellow and blue (YBB) components. LEDs exhibit a non linear effect at high frequencies, which is highly undesirable. This can be verified by employing the proper DC bias and OFDM scheme. The non linearity, in turn, restricts the operating range of a given LED. Another way to use LED is to modulate different colours with different data, resulting in an extremely efficient transmission system. Optical OFDM systems have the high crest factor of the time domain signal, which is a big disadvantage of traditional OFDM systems but an advantage in Optical OFDM systems, which makes

OFDM an even more appealing choice for VLC. Additionally, OFDM has the advantage of having a simple equaliser structure and being able to avoid low frequency distortion. OFDM with quadrature-amplitude modulation (QAM) can reach 513 Mbps with VLC, according to [67]. In addition, [68] shows a 1Gbps broadband white LED application using OFDM. According to [69], the system can achieve data rates of up to 1Gbps by employing MIMO-OFDM.

Traditional OFDM is bipolar in nature, containing both real and complex values. The signals used in intensity modulation and direct detection (IM/DD) systems must be real and unipolar to work. The Hermitian symmetry of the signals being fed into OFDM structures is used to ensure that the output is real. DC optical OFDM and asymmetrically clipped optical OFDM are two methods for making a signal unipolar. In ACO-OFDM, the negative parts of the signal are directly clipped, while in DC optical OFDM, a strong DC bias is applied to make the signal positive (DCO-OFDM).

Spatial Multiplexing MIMO (or Massive MIMO or Multi User MIMO) is when different VLC signals from multiple different luminaires in spatially distinct locations arrive at a single PD or an image PD array sensor receiver, which increases the throughput [70]. The transmission rate was reported to be increased to around 600 M bits/second using Space-Time Block Coding (STBC) with Pulse Position Modulation using three transmit LEDs and two circularly arranged sets of four PD receivers [71]. A four-channel spatial multiplexing MIMO link using white LED sources and a 3x3 imaging PD optics receiver was reported to increase the transmission rate to 1.1 Gb/s [69]. Using spatial multiplexing M-QAM OFDM, RGB LED with coverage of 1m² @ 2.88 m [72], 14 Gbit/s was achieved, with the potential to increase to 100 Gbit/s with more LEDs. Multifunctional MIMOs can combine the advantages of multiple MIMO schemes.

IoRL proposes to investigate a novel multifunction MIMO system for VLC in which spatial diversity MIMO, which will be used to maintain LOS between transmitters and receivers, is combined with spatial multiplexing MIMO, which will be used to increase data rates that are limited by the limited modulation bandwidth of LED devices. In the case of virtualization, this will simplify and lower the prices of terminals, APs, and networks. The VLC is just another Frequency. OFDMA and NR 5G will allow us to communicate over much longer distances.

Terrestrial wireless systems have largely limited their operation to the relatively narrow range of microwave frequencies that extends from several hundred megahertz to a few gigahertz and corresponds to wavelengths in the range of a few centimetres to

approximately one metre. This spectral band, often referred to as "beachfront spectrum," is now nearly fully occupied, especially during peak hours and in peak markets. Fortunately, in the millimetre wave (mmWave) range of 30–300 GHz, where wavelengths are 1–10 mm, vast amounts of relatively idle spectrum exist. In the 20–30 GHz range, there are several GHz of plausible spectrum. Several tens of gigahertz could potentially become available for 5G, providing a significant increase over what is currently available. To make these bands available for mobile networks, work must be done on spectrum policy [70].

The main reason for the mmWave spectrum's idleness is that it was previously deemed unsuitable for mobile communications due to rather hostile propagation characteristics, such as strong path loss, atmospheric and rain absorption, low diffraction around obstacles and penetration through objects, as well as strong phase noise and exorbitant equipment costs.

IoRL proposes to investigate a multi-user mmWave in-house communication system architecture using distributed mmWave antennas/RRLHs in a room for coverage and capacity enhancements, and a tool to plan the number and optimal locations/orientations of RRLHs in a room for coverage and capacity enhancements. Modification of co-working with the VLC will bring the MmWave into the 5G NR range. The results for coverage and accuracy for both technologies are to be using by an AI algorithm to find the best optimal solution.

2.7 The Theory and Practice of Simulated Annealing

2.7.1 Introduction

The optimisation of manufacturing processes is a critical topic in today's industrial sector, as it refers to determining the optimal values of process parameters that correspond to the desired response characteristics observed at the process output. As manufacturing processes become more complex, with a growing number of process control parameters, possible noise sources, and a growing number of process responses, advanced methods are required to address the optimisation problem[73].

The complexity of such problems increases as the number of responses increases, particularly due to the interdependence of the responses. Multi-response goals frequently conflict with one another in the scenario of a process with multiple responses. This is frequently resolved through the engineers' judgement, prior experiences, or a variety of approximations. Approaches as such cannot support the company efficiently in achieving a stable position in a highly competitive industrial market. Also, it cannot assure the anticipated outputs in a market where the most emphasised topic is consumer driven quality. Thus, advanced optimisation

techniques are required to translate consumer expectations for product quality characteristics into the design of manufacturing process parameters capable of producing the desired quality. This is particularly true for newly developed manufacturing processes whose behaviour has not been extensively studied and for which analytical models of input-output relationships have not yet been established [73].

The appropriate process parameter design is critical for manufacturing effectiveness and quality in terms of producing parts with the desired quality characteristics. Additionally, tuning manufacturing process parameters has a significant impact on other manufacturing system parameters, such as, overall equipment effectiveness, lead time, cost, productivity and time to market.

Due to complex mathematical models for conventional manufacturing processes and obscurity or uncertainty of process models for emerging processes, techniques for process-modelling and optimisation were increasingly used for Artificial Intelligence (AI). Numerous studies have demonstrated the importance of utilising evolutionary techniques such as Particle Swarm Optimisation (PSO), Genetic Algorithms (GA), and Simulated Annealing (SA) for the design of process parameters in order to deal with highly multidimensional, nonlinear, and ill-behaved complex optimisation problems [73].

2.7.2 Process Optimisation

Optimisation in engineering refers to the process of selecting a controllable input factor setting from a set of alternatives in order to achieve the desired outputs while adhering to certain constraints. Process optimisation is the process of determining the controllable process parameters that best meet the specifications for the product's quality characteristics, i.e., desired process responses and reduced variation. Modern manufacturing processes are usually controlled by multiple control factors, namely process parameters (x_1, x_2, \dots, x_k), are typically influenced by uncontrollable factors, namely noise factors (N_1, N_2, \dots, N_q), and exhibit multiple quality characteristics, namely process responses (y_1, y_2, \dots, y_p), at the output [73].

To assess the effect of process control factors on responses in a structured and systematic manner, designed experiments are conducted to collect an adequate set of input-output data from which a relationship between process parameters and process responses can be established. Orthogonal arrays, which are frequently used in Taguchi's robust parameter design methodology, and response surface methodology are the most frequently used methods for experimental design and analysis (RSM). Alternatively, if

conducting an actual experiment is prohibitively expensive or impossible, process historical data can be used to optimise the process in some cases [73].

Since most manufacturing processes provide multiple responses, process parameters must now be set, which produce simultaneously the desired results for all answers but also minimise dispersions of response, i.e. reducing variations in processes. Those variations are typical causes of noise factors, so that optimal process parameters can be defined to minimise the noise effect. This is effectively addressed by Taguchi robust parameter design, but only for a single response, trade-offs are required for multiple responses. Other conventional optimisation techniques are ineffective at resolving this issue. Typically, when analysing experimental data, each response is modelled separately as a function of the process parameters. However, as process responses are almost always correlated, optimising one response will degrade other responses. Optimising the process solely for one response will result in non-optimum solutions for the remaining responses. Thus, the objective of multi-response process optimisation is to determine the process parameter settings that result in the best compromise of the response variables, such that each response is as close to its ideal value as possible with the least amount of dispersion [73].

2.7.3 Simulated Annealing Algorithm

Simulated annealing is a type of metaheuristic search technique used in the field of artificial intelligence (AI). The metaheuristic algorithm is an iterative process that directs and modifies the operation of subordinate heuristics in order to generate high-quality solutions efficiently. For every iteration, the algorithm uses a single solution complete or incomplete or a set of solutions for every iteration [74]. Most of the metaheuristic techniques are based on animal or nature behaviour, such as a Particle Swarm Optimisation (PSO), Ant Colony Optimisation (ACO), Artificial Bee Colony (ABC), and Genetic Algorithm (GA) [73]. It has been demonstrated that heuristic-based search algorithms are extremely beneficial in situations where conventional, statistical optimisation techniques are ineffective, such as problems with a large search space and numerous local optima. SA algorithms, for example, have been widely used to solve multi-objective optimisation problems in a wide variety of engineering problems [73].

The SA algorithm is a simplification of the solids annealing process. It begins by selecting an initial random point at an initial temperature (high) and proceeds to a randomly selected new point according to the specified function. The difference between the function values of these two points ΔE is calculated. Therefore, if the objective function of the new point is superior to the current one, then the new point is accepted [73]. However, depending on the specified

probability function, enhanced solutions are always accepted, a fraction of (inferior) non-improving alternatives in the hope of escaping local optima in search of global optima. Acceptance of non-improving solutions is dependent on a temperature parameter, which is typically non-increasing with each algorithm iteration [75].

After accepting a new point, the temperature is decreased in accordance with the cooling rate or annealing schedule. As the temperature decreases, the probability of moving to an inferior point decreases as well, thereby reducing the randomness in a search that mimics the slow cooling process used in metal annealing to achieve a perfect crystalline state. To simulate this equilibrium, a number of points (iterations) are typically tested at a given temperature before the temperature is reduced. When the temperature is nearly zero at the end of a search, the probability of accepting inferior points is extremely low, so the algorithm converges to an optimal solution [76].

2.7.3.1 SA algorithm procedure

The simulated annealing algorithm's most frequently used procedure as [73] outlined is as follows:

1. Start: set the algorithm specific parameters like the initial point and the termination measure (the total number of algorithm iterations, the change in objective function, and the final temperature).
2. Initial point: Calculate the objective function $f(x)$ of the initial point.
3. New point: Calculate a new neighbourhood point using a probability distribution proportional to the current temperature, i.e. the annealing function; calculate the new point's objective function $f(x)$.
4. ΔE : Calculate the change in the objective functions between the current and the new point ΔE , which is $\Delta f(x)$.
5. Replacement: If $\Delta E < 0$, accept the new point and move to the next step. However, if $\Delta E \geq 0$, create a random number r in the range $(0, 1)$, then check whether $r \leq \exp(-\frac{\Delta E}{T})$. If yes, accept the point. If not, begin with a new point and go back to step 3.
6. Iterations at a particular temperature: If the number of iterations performed is less than the specified number of iterations (n) at a specified temperature, move to the next step, but if not perform iterations.
7. Temperature decrease: Reduce the temperature on a periodic basis in accordance with the temperature update function specified. If the current temperature exceeds the final, proceed to step 3. If not, go to step 9.

8. Reannealing: To avoid local optima, increase the temperature in each dimension, i.e., perform reannealing after a specified number of points.
9. Termination: Terminate the procedure if the termination criterion is satisfied (e.g., if the current temperature is less than or equal to the specified final temperature, and/or the specified number of algorithm iterations is reached, and/or the change in the objective function is less than the specified value).

The following points should be considered when determining the values for these algorithm specific parameters [77]:

- The initial temperature must be sufficiently high to permit movement to any neighbourhood state. It determines the probability of accepting an inferior solution, preventing the algorithm from becoming stuck in a local optima and compelling it to conduct a broader search. However, if the initial temperature is too high, the search can be redirected to any neighbour, resulting in a random search.
- The final temperature is typically set to zero, this can cause the algorithm to run indefinitely. Thus, the algorithm is terminated in practise when a sufficiently low temperature is obtained, a minimal change in the objective function value is obtained, or the algorithm reaches a specified number of iterations.
- The temperature update function adjusts the annealing schedule in accordance with a temperature decrease. While the slower decrement rate is beneficial for convergence to the global optimum, it adds to the algorithm's run time.
- At each temperature, the number of iterations should be sufficient to ensure that the system stabilises at that temperature. Since this number is exponential to the problem size, only one iteration at each temperature is sometimes recommended and the temperature slowly decreases. Alternatively, the number of iterations could be dynamically varied, with a greater number of iterations being performed at lower temperatures to fully explore the local optimum.
- The annealing function specifies how a new point is generated in the next iteration. The algorithm determines the distance between the new random point and the current one using a probability distribution whose scale is proportional to the current temperature, which is controlled by the annealing function.
- The reannealing interval indicates the number of acceptable points beyond which the temperature begins to rise. Reannealing reduces the annealing parameters to values less

than the iteration count, thereby increasing the temperature in each dimension and avoiding a local optima. This parameter must be weighed against the initial temperature. In general, reannealing too soon may be detrimental to identifying an optimum, which is why a relatively long interval is recommended.

As described previously, appropriately tuning the algorithm parameters significantly reduces the likelihood of being trapped in a local optima. With infinitely slow cooling, it has been demonstrated that the algorithm is almost certain to find the global optimum. SA typically produces very good results in practise by combining exploration features such as random search and exploitation features such as hill climbing [73].

2.7.3.2 Advantages and Shortcomings of SA

The SA algorithm's primary advantages can be summarised as follows [76], [100]– [102]:

- It is capable of dealing with arbitrary systems and objective functions, as well as models that are highly nonlinear and multimodal, chaotic and noisy data, and a large number of constraints.
- It ensures that an optimal solution is found after a sufficient number of iterations.
- It is capable of efficiently locating the global optimum when the objective function is constrained by its surroundings.
- It is a generalised optimisation technique, as it does not rely on any restrictive properties of the model and does not require a gradient calculation to determine the direction of the search.
- It is relatively straightforward to implement, and is thought to be less sensitive to the magnitude of a problem.
- Provides reasonably good solutions to most optimisation issues.

The SA algorithm's primary shortcoming can be summarised as follows [98], [100]– [102]:

- Due to the fact that this is not a population-based algorithm, it may not develop a comprehensive view of the search space.
- Convergence of the algorithm can be significantly influenced by algorithm specific parameters, and there are no universally acceptable parameter values for various types of optimisation problems.
- According to the cooling schedule, it could be slow, in particular, if the objective function is complicated.

- Repetition with the same initial conditions is not guaranteed for the ideal solution obtained by SA algorithm.

2.8 Real Live Streaming

2.8.1 Internet of Things (IoT)

The Internet of Things (IoT) is a trending topic of research in the direction of the Future Internet. It modifies the current model of host-to-host communication by introducing the concept of a network object. Every object, in its view, can be connected to the Internet, which means that every object will have networking capabilities. On the other hand, these objects have limited CPU power, memory, energy, and networking performance [81].

IoT's goal is to provide more effective solutions and improve services by providing information streams from various sources. These objects may include various types of built-in sensors and actuators [82]. IoT device, services and networks are designed and deployed outside the sphere of traditional computer environments. The computing elements have become more integrated, ubiquitous, and pervasive. Due to the integrated nature of IoT devices, they can be used for a variety of purposes, ranging from real-time monitoring to smart-infrastructure, smart-home, cyber-security applications to health management applications [82].

This led the research community to design new protocols that would expose those smart objects and overcome these limitations, such as typical hosts, to the network [81]. Upon definition of the underlying protocols, smart objects must expose their features to other services, objects, hosts, and thus increase usefulness or utility. A large percentage of current networks require high-quality video streaming. It has special features and therefore network needs. It is very sensitive to network and protocol conditions. That means that video streaming is dynamic and the dynamics and limits of the underlying network architectures must be considered [81].

Video encoding and processing are still a computationally intense and complex process, in spite of the vast array of video applications [83]. This is a challenge for video inclusion in IoT applications [84][85][81][86]. This means that powerful processing elements are needed to encode and process video streams. The computing capacity and power resources of wireless and mobile devices are significantly less than normal platforming. Whereas, these devices are the mostly used for video applications [83].

2.8.2 5G Real live streaming

5G has a lot of benefits and features, which makes it significant towards broadcastings services, such as virtual and augmented reality games, and follow me TV service. These services rely progressively on the indoor environment position accuracy. The challenge is to obtain a high position accuracy for indoor locations, due to the broadcasting data traffic increase indoors. Also, radio interference makes it more difficult to provide accurate position. To be able to provide a high-quality indoor broadcasting service, a flexible and adequate communication system and radiation free are required.

Nevertheless, precise location data broadcasting is not only based on the characteristics of the uplink and downlink signals, but also on network configurations and new technologies. For example, Global Positioning System (GPS), Satellite Navigation, Bluetooth, Beacon Systems, and sensors. [9]. Although these non-3GPP technologies are widely used due to their low-cost, they do not promise to provide suitable positioning resolution for 5G network in particularly indoor areas, as it lacks of poor accuracy and bad service coverage.

In the past everyone used the traditional television broadcasting, which then advanced to the IPTV systems. It was able to completely deliver the multimedia services over an IP based network [87]. The performance of streaming applications is based on the implementation choices made at the infrastructure level. For example, the configuration of resources allocated and its amount [88]. There are different methods of streaming deployment models. One of the commonly used methods would be MPEG Dash (Dynamic Adaptive Streaming over HTTP). It is one of the video streaming technologies, which is able to deliver real-time streaming over the internet [88]. In addition, its main objective is to provide the best quality content with low buffer time and minimal dropouts [89].

Real-time video streaming applications are rapidly increasing, and the demand is highly growing. The technological advancements are supporting the growth of streaming, as it requires high-level performance and low latency. Streaming applications are everywhere nowadays, such as, e-learning applications, video conferencing, and video streaming, [90]. The aim to provide a better Quality of Service (QoS) for streaming applications as it is using the next generation of communications technology.

2.9 Denial of Service Attacks

Denial of Service (DoS) is an attack on a computer network in which a user is destitute of the services provided on the server. This kind of attack focus on the server, as it disrupts the traffic by flooding the server with requests or false messages. The goal of this attack is to shut

down the server. As shown in Figure 2-13Figure 2-13: Conceptual diagram of DDoS attack, the attacker machine uses compromised machines (slaves) to flood the targeted server with false requests to shut it down.

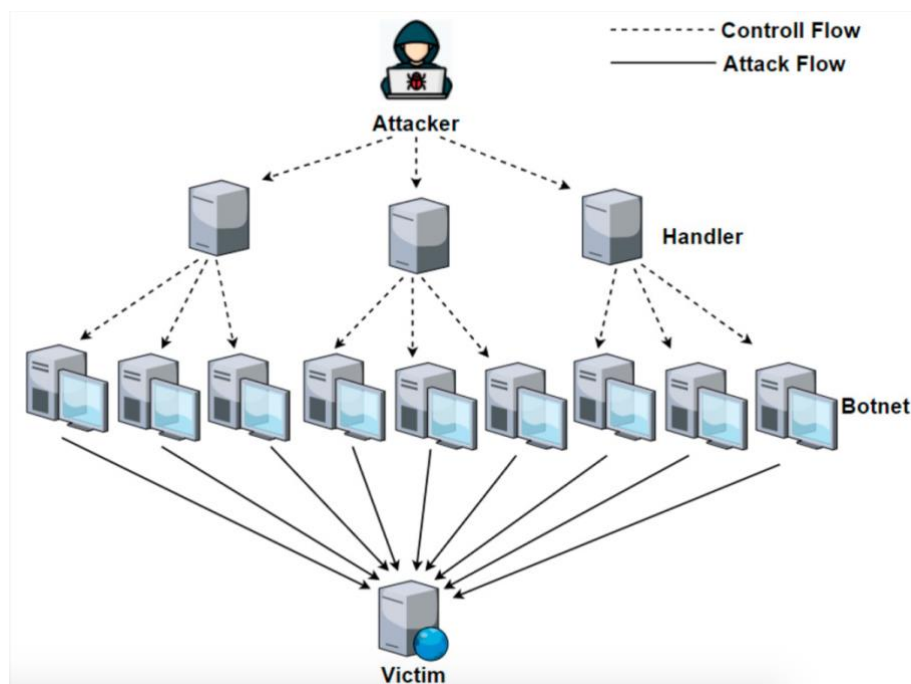


Figure 0-9: Conceptual diagram of DDoS attack

There is different nature of attacks, where may be a part of a larger attack and they can be implemented by any of the following methods:

- Attempt to disrupt service to a specific person or a system.
- Attempt to disrupt connections between two machines, preventing access to a service.
- Attempt to prevent a specific user from accessing the service.
- Attempt to flood the network, thereby preventing legitimate network traffic.

Types of Denial of Service Attacks

- Flooding / Bandwidth Attack
- Buffer Overflow/Ping of Death Attack
- Email Flooding Attack
- SYN Flooding Attack
- Teardrop Attack
- Smurfing / Smurf Attack
- Distributed DoS (DDoS)/ Botnet attacks.

2.9.1 DHCP Attacks

The DHCP is a simple protocol used to assign IP addresses for any client joining the network. But due to the lack of security in it, many attackers were able to compromise its vulnerabilities. There are two main DHCP attacks which are the DHCP starvation attack and the DHCP server impersonation [91]. Both attacks have different impacts on the network as one of them denies access to any client trying to connect to the network (active attack), and the other one can lead to the malicious user having unauthorized access to some data in the network (passive attack).

Each DHCP server has an IP address pool which consists of 254 IP addresses available to give to any client trying to connect to the network. One approach that attackers use to attack the DHCP protocol is by sending DHCP Discover messages using forged MAC addresses in each message [91]. Any device that has a network card must have a Media Access Control (MAC) address. This is a physical address for the hardware that cannot be changed. However, attackers were able to develop a software that is able to generate fake MAC addresses and include them in a DHCP Discover message which is sent to the DHCP server. In order to perform this attack successfully, there are 3 steps that needs to be done [92]:

1. Send Discover message with forged MAC address.
2. Save each Discover message sent and wait for the OFFER message from the DHCP server
3. Reply to the server by sending a REQUEST message to each OFFER message received.

By completing these 3 steps, the attacker will successfully be able to obtain all the IP addresses available in the DHCP pool. Therefore, if any legitimate client tries to connect, the DHCP server will refuse due to the unavailability of IP addresses.

Another approach that an attacker could take is to send a large amount of DHCP Discover messages with fake MAC addresses, this is referred to as DHCP Discover flood [92]

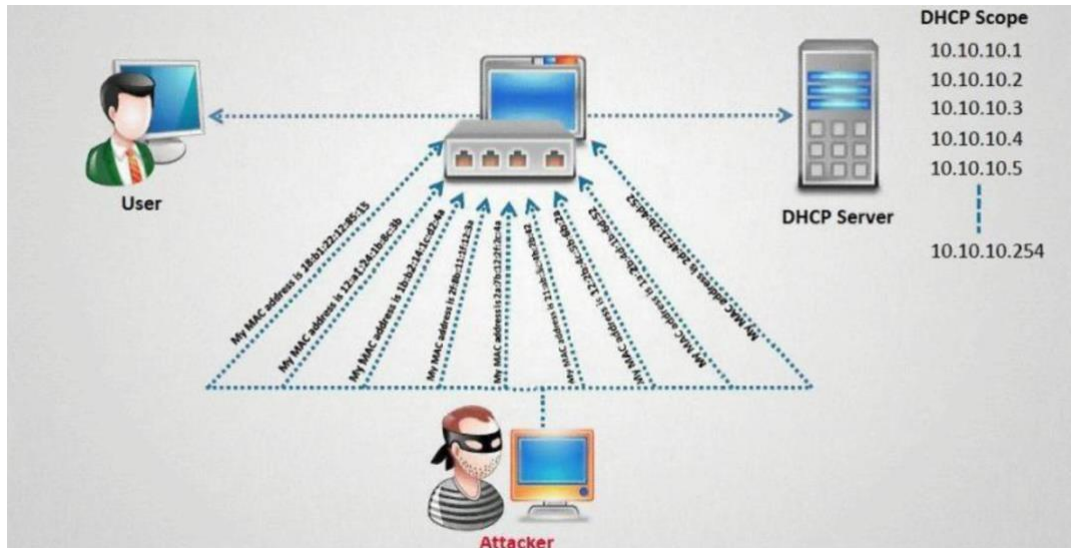


Figure 0-10 - DHCP Discover flood

As shown in

Figure 0-10 above, the malicious user will generate fake MAC addresses and will keep sending Discover messages to the server. In return, the server will send OFFER messages, however, the malicious machine will not reply to it and the whole process will terminate. The issue here is that during the attack is taking place, the DHCP server will not be able to handle the amount of Discover messages received and it will alter its performance [92]. Hence, during the attack is active, no client will be able to communicate with the DHCP server and will be denied access to the network. However, as soon as the attack terminates, the functionality of the server will go back to normal as no IP addresses have been leased.

Both attacks explained above have one target which is to deny the service of the DHCP server. If the attacker was successfully able to take down the DHCP server, then he/she could introduce their own rogue DHCP server to the network. This is the other type of attack mentioned above which is called DHCP server impersonation. If the malicious user was able

to introduce his own DHCP server to the network, then he/she could configure it in any way they want. By doing that, they can send false information to all clients connected to the network such as replacing the IP address of the legit gateway with their own machine's IP address. Therefore, all the traffic that will be sent from any machine will be redirected to his machine and he could potentially be able to monitor all the traffic leading to gaining unauthorized access to sensitive data.

The attacker would also be able to change the IP address of the DNS server in the network with another IP address for a DNS server that he/she configured. DNS server stands for Domain Name System, and it provides a service of converting any domain name such as www.google.com to its corresponding IP address [93].

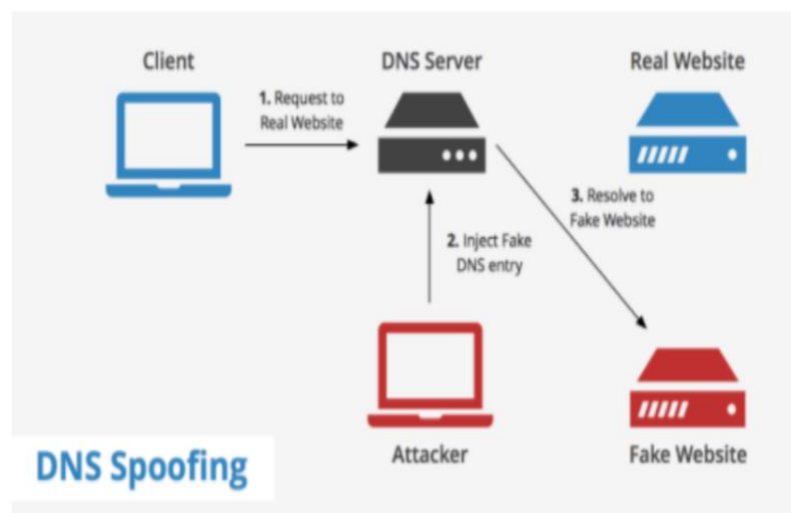


Figure 0-11 - DNS spoofing

Consequently, if the attacker were able to introduce his own DNS server, he/she could redirect traffic to any IP address they want. Figure 0-11 above shows a demonstration of how DNS spoofing is done by redirecting the legitimate traffic to another website of the attacker's creation. This attack also leads to many other attacks that could be done.

2.9.2 Spoofing

The term spoof means to "fool", this happens on the internet from people and programs that fool others through the process of impersonating and cheating others, as they get authorised in order to gain access to software and personal information. Spoofing is when a person or program masks his identity to represent as another (victim) by falsifying information to gain an illegitimate advantage on the behalf of the victim's name.

There are two different types of spoofing: IP Spoofing and Email Spoofing

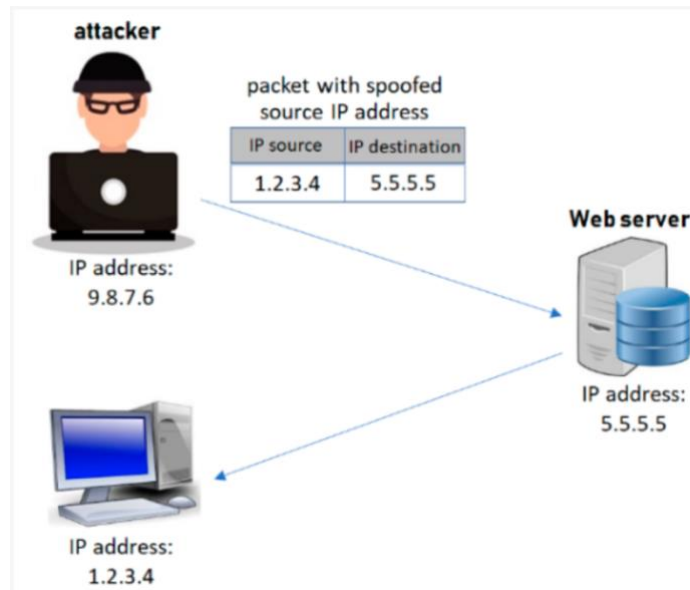


Figure 0-12: IP spoofing

There are four main way of spoofing IP addresses

Non-Blind Spoofing: This type of attack is done when both the victim and the attacker share the same subnet, which helps to gain easy access of the other IP addresses.

Blind Spoofing: This type of attack is done when both the victim and the attacker share the different subnet, which is a lot harder than a non-blind attack because the IP address is unreachable, however access can be still gained by sending packets to the victim's computer.

Man in the middle: This type of attack (spoofing) happens between two legitimate parties communicating. The attacker would intercept their communication allowing himself a control, where the attacker can delete, change, coax personal information from one of the parties without both of them knowing.

Denial of Service Attacks: This is where the attacker's main objective is to flood the victim with as much spoof data and traffic as possible to consume resources like bandwidth or memory buffers. The attacker would need to keep the attack going as long as possible to be able to use the resources.

Spoofing can occur at higher level protocol as in Simple Mail Transfer Protocol (SMTP). For example, email spoofing is the forgery of an email header or email addresses where the attacker uses someone else's email address in order to send their email so it cannot be traced back to the attacker. Attackers may also use email spoofing so they can impersonate another person or a company to gain access to personal information such as a bank account.

Usually, wireless communications are protected from eavesdropping, unauthorized access, and modification of messages. There are three security mechanisms that can be used to protect visual light communication: cryptographic protection, stenographic protection, and proximity- based protection [94].

Cryptography addresses confidentiality, integrity, and authentication. This method can be applied in different layers. Confidentiality and integrity services are provided services for the VLC at the MAC layer. The modern cryptographic protection relies on secret keys. However, key management is one of the most difficult problems in cryptography. A method to bypass this problem is to utilise the properties of wireless channels to create secure keys to subsequently secure wireless links [95], [96].

Furthermore, channel reciprocity can be used where two neighbouring receivers experience the same signal envelope without any interference [97]. However, interferences are always present, therefore an effective technique can be used that is explained in the paper by Sadjadi [95]. The advantage of this technique is that it does not require signal envelopes for the terminals that are communicating as they are only matching deep fades. Subsequently, this results to interference immunity to a satisfactory base level.

“It is possible to exploit channel reciprocity, whereby two closely located receivers experience the same signal envelope in the absence of interference” [97]. As a result, practical channels not being immune to interference. Sadjadi presented a technique that does not entail matching signal envelopes but however, entails deep fades. Deep fades are immune to a satisfactory level of interference [95].

2.10 5G Security Location Monitoring

The 5G wireless network vision is to provide extremely high data rates and coverage through dense base station deployment with increased capacity, extremely low latency, and significantly improved Quality of Service (QoS) [98]. To deliver the required services, 5G will require novel networking, storage, service deployment, and processing technologies. Cloud computing enables operators to efficiently manage data, services, and applications without having to own the underlying infrastructure. Thus, mobile clouds based on the same concepts will consolidate technologically disparate systems into a single domain on which multiple services can be deployed to achieve a higher degree of flexibility and availability while incurring fewer capital and Operational Expenses (OpEx) [99].

Softwarising network functions enables networking systems and services to be more portable and flexible. By separating the network control and data forwarding planes, Software Defined Networking (SDN) enables the softwarisation of network functions. SDN, on the other

hand, innovates networking through abstraction and simplifies network management on the other. Network Function Virtualization (NFV) enables the placement of various network functions in different network perimeters based on their requirements, obviating the need for function or service-specific hardware. SDN and NFV, when used in conjunction, increase network elasticity, simplify network management and control, and eliminate the barrier associated with vendor specific proprietary solutions. As a result, they are viewed as critical for future networks. Nonetheless, even with these novel technologies and concepts, user privacy and network security continue to be a significant challenge for future networks [99].

The security vulnerabilities of wireless communication were prone from the outset. Wireless networks, mobile phones, and wireless channels of the first generation (1G) were targeted for illegal masquerading and cloning. Message spamming became prevalent in the second generation (2G) of wireless networks, not only for pervasive attacks, but also for broadcasting unwanted marketing information or injecting false information. In the third (3G) wireless network generation, IP-based communication enabled vulnerabilities and wireless challenges of the internet to be migrated. Due to the growing importance of IP-based communication, fourth-generation (4G) mobile networks enabled the multimedia traffic, proliferation of smart devices and new services in the mobile domain. This evolution has resulted in a more complex and dynamic threat landscape. With the advent of fifth-generation (5G) wireless networks, security threat vectors will be larger than ever before, and there will be an increased emphasis on privacy [99].

Due to the fact that cloud computing systems comprise a variety of resources that are shared among users, it is possible for a user to spread malicious traffic in order to degrade the system's performance, consume additional resources, or stealthily access the resources of other users. Likewise, interactions can result in network configuration conflicts in multi-tenant cloud networks where tenants run their own control logic. Mobile Cloud Computing (MCC) extends cloud computing concepts into 5G eco-systems. This results in a number of security vulnerabilities, the majority of which are related to the architectural and infrastructural changes associated with 5G. As a result of the open architecture of MCC and the versatility of mobile terminals, adversaries can launch threats and compromise privacy in mobile clouds [100].

The Radio Access Technologies (RATs), that interface mobile to the cloud, are targeted at network-based mobile security threats. This could be standard Wi-Fi, 4G, Long-Term Evolution (LTE), or other novel Radio Access Technologies (RATs) that will accompany 5G.

This category of attacks includes session hijacking, address impersonation, Denial of Service (DoS) attack and Wi-Fi sniffing [101][102]. Another critical area of interest in analysing the security challenges associated with 5G mobile clouds is the Cloud Radio Access Network (C-RAN). C-RAN has the potential to address the industry's capacity expansion requirements for 5G mobile communication systems' increased mobility [103]. C-RAN, on the other hand, is vulnerable to the inherent security risks associated with virtual systems and cloud computing technology; for example, the centralised architecture of C-RAN creates the risk of a single point of failure. Other threats, such as intrusion attacks, in which adversaries breach the virtual environment in order to monitor, modify, or execute software routines on the platform undetected, also pose significant risks to the system [103].

5G uses mobile clouds, SDN and NFV to meet the challenges of massive connectivity, flexibility, and costs. With all the benefits, these technologies also have inherent security challenges.

2.11 Summary

The Internet of Things (IoT) is a promising technology that has the potential to revolutionise and link the world by connecting disparate smart gadgets in a seamless manner. The fifth generation of mobile communications might be 10 times quicker than the current 4G technology, providing more consistent internet access and higher speeds. 5G allows for a new type of network that aims to link everything and everyone [29]. High data rates, low latency, vast network capacity, and enhanced availability are all expected to come with 5G. Virtualised infrastructures are expected to be used to develop and execute the next generation of communication networks. As a result, virtual computers would be used to implement network operations rather than the present proprietary equipment [30].

Additionally, due to the inability of outside signals to penetrate sufficiently, small cells are employed to enhance the coverage of mobile networks for inside sites. Small cells can be an important feature of 5G networks because of their capabilities [34]

The importance of OpenStack is also highlighted, as it allows users to deploy virtual machines and instances to administer a cloud environment with various responsibilities. It simplifies horizontal scaling such that jobs that are running at the same time can easily serve more or fewer people by spinning more instances [43]. Most crucially, the OpenStack software is open source, which means that anybody with access to the source code may make whatever changes they want and share them with the rest of the community.

Furthermore, many individuals all around the globe utilise location-based services since they help them discover and track [45]- [46] information. Many people want location-based application services, and they need to be dependable, precise, and function with outside positioning concurrently [14]. The three primary Localisation technology groups will be introduced, together with a review of their QOS, in order to offer an understanding of the enormous problem they are now facing. Beacon Location Technologies, Dead-Reckoning (DR), and Device-Free are the three technologies in question.

5G offers several advantages and features, making it important for broadcasting services such as virtual and augmented reality games, as well as the follow me TV service. The precision of the interior environment location is becoming increasingly important for these services. Due to the rise in transmitting data traffic indoors, the difficulty is to achieve a high level of position accuracy. Furthermore, radio interference makes providing a precise position more challenging. A flexible and sufficient communication system that is radiation free is necessary in order to deliver a high-quality indoor broadcasting service.

Lastly Security is also important since it safeguards the network's infrastructure. It ensures that data is transferred and communicated in a secure network environment. With the introduction of fifth-generation (5G) wireless networks, security threat vectors will be greater than ever before, and privacy will be prioritised [89]. As a result, 5G makes use of mobile clouds, SDN, and NFV to address the issues of huge connectivity, flexibility, and affordability. These technologies have significant security issues, despite their numerous advantages.

Chapter 3: 5G Indoor Location Database and Interactive Services

3.1 Chapter Outline

The objective of this chapter is to design and build an indoor Location Database and Server VNF that allows the integration of Location data from VLC RSSI and mmWave TOA on network edge for multiple applications to use it. This chapter discusses the different applications that will be able to provide the 5G services using the merging of the location data. This chapter is outlined as follows: Section 3.2 provides an introduction, by discussing the different services and their capabilities. Section 3.3 presents the methodology. Section 3.4 provides an overview of the architecture. Section 3.5 presents the museum scenario. Section

3.6 provides the location database framework. Section 3.7 provides the design implementation of applications (Web interface and mobile application). Section 3.8 explains the development and the testing. Section 3.9 provides a summary.

3.2 Introduction

The application layer services capabilities are constrained by the wireless network on which they operate. Wireless networks in buildings suffer from interference, congestion, poor indoor location accuracy and restricted propagation [104]. The restricted bandwidth denies fast access to the database. Additionally, the use of indoor location monitoring, guiding and data access applications are restricted due to poor indoor location accuracy.

This chapter presents the 5G applications that can be provided for the museum scenario by using the location context developed in Chapter 3. This chapter proposes that various networking interfaces should be manipulated using video streaming as one of the vital services towards delivering the best experience for the user equipment side. There are several complexities and challenges facing the deployment of streaming servers (Virtual streaming servers).

The service requirements for widely diverse indoor environments such as train stations, homes, and supermarkets would appear to be significantly different. In fact, when closely analysing there are various similarities between these services in indoor environments. For instance, they all require to know the user's location and which RRHL to send the information from. With the new network capabilities, new applications can be developed and grouped into a set of applications, which would be common to all three environments [104]. These applications are Indoor Location Monitoring (ILM) and Interaction Applications. This chapter illustrates how these applications are common. This chapter shows how the applications have been developed to have a universal functionality [105].

Indoor 5G positioning system is primarily proposed for museums. The system uses unlicensed visible light spectrum to offer the visitors at the museum with interactive services, 4K real time multimedia streaming, and position monitoring. The location data transmitting and receiving are explained in detail in chapter 4.

3.3 Methodology

The increasing demands have a major impact on the future of mobile network architectures. Mobile operators face vast amounts of limitations due to the lack of flexibility in certain interfaces, long latency, inefficient routing mechanisms and user plane congestion. Subsequently, they are considering a new network plan with new technologies to be able to accommodate the increase of users, while improving the user experience.

The proposed services and solutions are designed to work specifically with the IoRL architecture. Thus, the foremost goal is to test the services and the proposed solutions on the actual IoRL system. During the project development stages, there were constant developments taking place for the wireless access links, which did not fully make it feasible to test all the contributions on the system. However, the tests were simulated to provide a proof of concept. The obtained results were analysed and evaluated accordingly.

3.4 5G System Architecture Diagram

The Internet of Radio Light (IoRL) system concept is to integrate Remote Radio Heads (RRH) and Visible Light Communication (VLC) into light roses installed on the ceilings of indoor environments, thereby improving connectivity, and assisting in the achievement of critical 5G targets. A critical component of our strategy is the use of 5G modulation and coding over VLC.

The IoRL system is a 5G indoor location solution, which will provide a more secure, safer and customisable building network. Most importantly it focuses on enhancing the user's quality of service. IoRL system consists of Intelligent Home IP Gateway (IHIPGW), UE, and Radio Access Network (RAN). The architecture was structured in three layers: application layer, NFV/SDN layer, and access layer as shown in Figure 0-1.

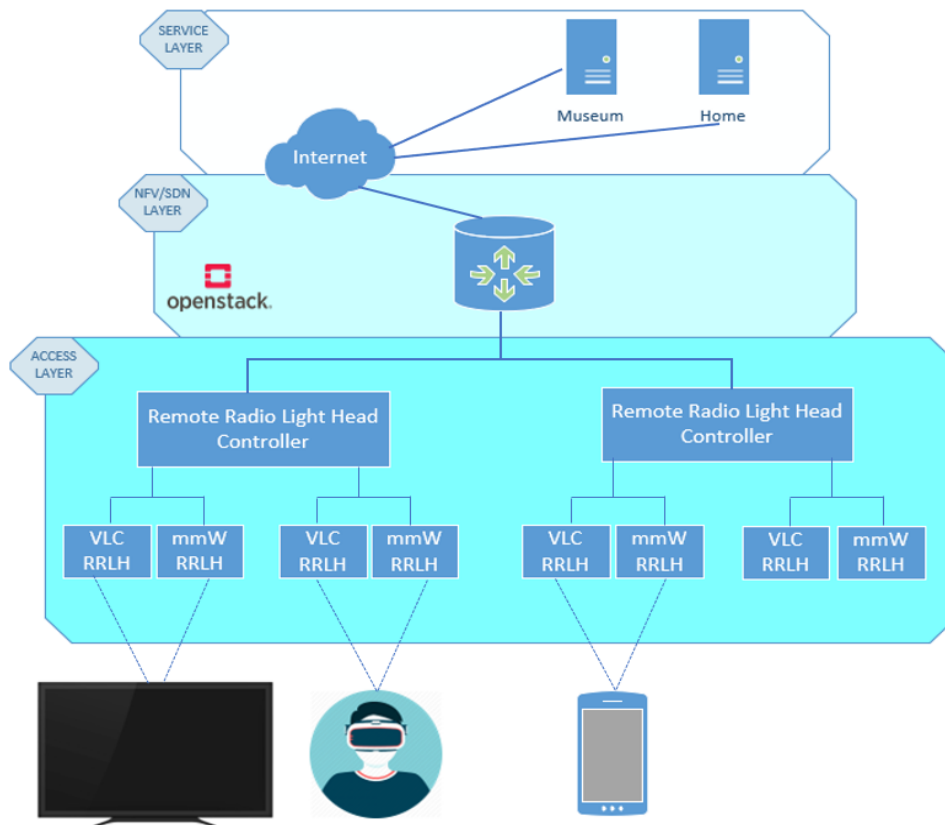


Figure 0-1: IoRL System Architecture

The IoRL system's Software Defined Network (SDN) Architecture, shown in Figure 0-1, not only enables network service developers to create applications for Security Monitoring, Network Slicing, Location Sensing, Lights Configuration, Energy Saving, Video and Network Transport Configuration, and Network Security, but also enables network operations and management functions to be located between the Intelligent Home IP Gateway (IHIPGW) and the Cloud Home Data Centre (CHDC) server in a configurable way to be able to deal with the different OPEX and CAPEX of the different MNOs [106].

Due to the extremely constrained space available in Light Rose housings, the concept of Network Function Virtualisation (NFV) is applied to the VLC and mmWave RANs in order to offload the complexity of the electronic systems required within the RRLH onto the CHDC or Intelligent HIPG. The design of strategies for configuring video streams to be transported in various percentage proportions over the various available home networks and paths (WLAN, HeNB, VLC, mmWave, etc.) is critical for ensuring service connectivity continuity by providing numerous radio transmission paths. The SDN will be attained through the enhancement of two network elements with OpenFlow capabilities: The Intelligent Home IP Gateway and the Remote Radio-Light Head [106].

The SDN offers network function virtualisation (NFV), which enables and allows the deployment of services such as streaming over wireless links, rather than optical fibre. In the past, before the development of NFV, the deployment of network functions was dependent on a physical infrastructure, rather than a virtual. However, it improves the network with several new capabilities such as network, storage and computation resources by executing it on the existing hardware using a virtual layer. Also, it enables a set of orchestration and management functions as an addition to the existing model of operation [1].

The network layer (SDN/NFV) is deployed on the OpenStack platform, which is an open-source platform for cloud computing. It assists the proposed system with a lot of resources like creating and managing as many instances of network computation and storage. The SDN controller runs using Open Daylight (ODL), which is an open platform for automating and customising networks of any scale and size [48]. It controls the Open Virtual Stack (OVS) to forward the traffic to the required destination based on the flow matches on IPV4 headers or Ethernet headers [45]. The aim of using these services is to improve the user's QoE by the enormous flexibility available by the SDN and NFV.

3.4.1 Video Streaming and Network Resources Usage

The existing real-time video streaming has a huge challenge, which is that it consumes a lot of the network bandwidth as shown in Table 3-1. The resolution is the height and width

of a video in pixels. Codecs are compression technologies with two mechanisms: an encoder and a decoder. The encoder compresses the file and the decoder decodes the file when played [105]. The frame rate is the number of frames displayed per second. Network bandwidth is the connection speed to the internet [107]. This emphasises the fact that the higher the resolution the more bandwidth required.

Resolution	Compression	Frame Rate(fps)	Network Bandwidth(Mb/s)
UHD 8k (8192x4320)	H.265/HEVC	120	280
UHD 4K(3840 x 2160)	H.265 HEVC	60	26.8
UHD 4K(3840 x 2160)	H.265 HEVC	50	22.3
UHD 4K(3840 x 2160)	H.264	60	36.2
UHD 4K(3840 x 2160)	H.264	50	30.1
Full HD(1920 x 1080)	H.265 HEVC	60	6.7
Full HD(1920 x 1080)	H.264	60	9

Table 0-1 : Typical Bandwidth Requirements for Video Codecs

Over the years, information technology (also known as communication technology) evolution had a big issue that was never solved. The issue was that there was a lack of bandwidth for applications like streaming, as it demanded more. Therefore, with limited bandwidth available, providing a higher quality video streaming is impractical. Nevertheless, in the event that 5G can offer 10 Gbps, which provides a high performance with a low latency that means a better QoS can be achieved.

Dynamic resource allocation is critical for distributed multimedia systems with application-level control. One of the difficulties associated with resource reallocation is the global coordination of feedback data from multiple streams [108].

Due to the scarcity of bandwidth resources on today's Internet, it is critical to manage available bandwidth resources efficiently, and send only the most relevant contents to the receiver based on the available bandwidth. If the essential contents are available in an acceptable state of quality, the final quality may be higher than if all the contents are available in an unacceptable state of quality [108].

Different applications, such as file transfer, audio/video streaming, and web browsing, have varying tolerances for rate mismatches between sending and receiving rates. For instance, file transfer is not time-sensitive. On the other hand, audio/video streaming is time-constrained. The difference in sensitivities to human aura and visual systems indicates that audio and video should be treated differently under adverse conditions, affecting media stream playback. It is well established that the auditory sense is more susceptible to disturbances than the visual

sense. As a result, giving audio precedence over video makes sense. If data must be discarded due to network congestion, it is preferable to discard video data first. In some applications, it may also be possible to use receiver information to improve the subjective quality of video data, for example, by deleting backgrounds or transmitting high-priority objects when there is insufficient bandwidth available. When bandwidth is limited in some other applications, we may only transmit the critical layers such as the base layer and lower enhancement layers. Thus, protecting scene content selectively based on its importance and application is extremely beneficial and critical for the final subjective impact [108] .

3.5 Location Based Data and Video Transmission and Reception for a Museum Scenario

3.5.1 Museum Scenario

The scenario is based on a real museum in France called Musée de la Carte à Jouer (Playing card Museum). In order to communicate with visitors, the museum uses Li-Fi devices as access points. There are no networked devices in the museum's current Li-Fi system. The museum provides a wide range of activities for the benefit of the many school groups who visit. Hence, there is a need for an interactive service to make their visits more entertaining.

- Create a system that will allow the managers to update, add, edit and delete exhibits through a user-friendly interface.
- A database to hold and store all the information uploaded by the managers.
- Creating a “smart” interactive application that provides the users with clues (example: find the picture of a lady on the horse entering the city gates on an artefact) within the museum.
- Once the artefact is found, the users would upload an image on the interactive application, which then gets compared to the reference image on the database and return the results to the users.

3.5.1.1 The Use Case

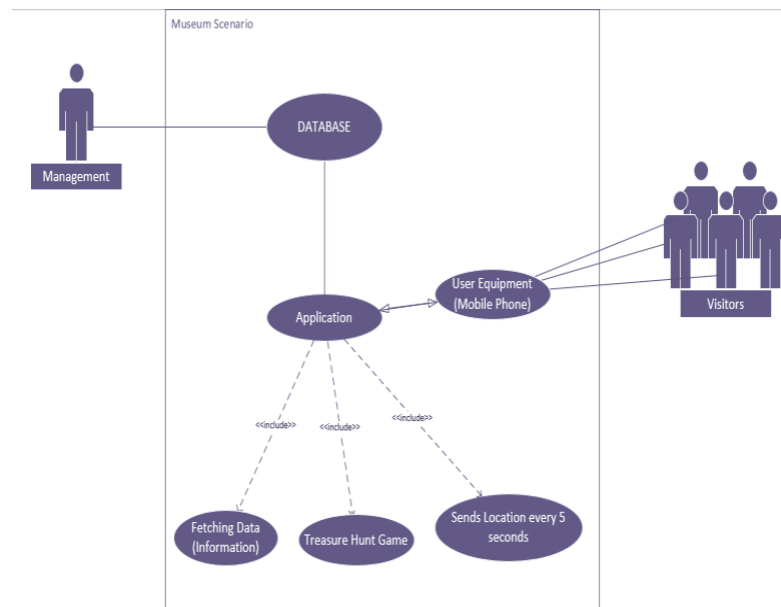


Figure 0-2: Museum use case scenario

The use case scenario defines or shows the overall view of the application and what it has to offer. The managers have access to the application through its database, which will be discussed in Section 3.6 and its interactive interface to make it more user friendly was discussed in Section 3.7. The museum visitors can use the application through their mobile phones or tablets. It offers information regarding the exhibits based on the estimate user location. The user's location gets sent to the location server every 5 seconds. Finally, it allows the users to use the interactive application, where they upload their answers (image) to the application, which uploads it to the database. Additionally, the database compares it to a reference image and sends back the result.

3.5.2 Location Based Data Transmitting and Receiving Scenario Description

3.5.2.1 Location Based Data Transmitting

There are two main requirements needed, a database that holds information about current exhibits, and an interactive application for the users that uses location information of the user to determine if the image that has been taken is closest to the exhibit that they have photographed.

The interactive application requires the users to sign up and login to use the service. The users would have to follow the clues and hints given in the game to find the card and then take a picture through the app, which will be sent back to the database to cross correlate it with the reference image.

Additionally, the application does not only allow the users to upload images, but also helps the visitors by providing information of the different collection of cards using the lights. Finally, it allows users to fetch data from the database.

3.5.2.2 Location Based Data Receiving

The limitations that currently exist in the museum scenario is that there is no recording of the temporary collection that changes every 2 to 3 months. Furthermore, the data transmitted from the VLC transmitter needs to be manually changed. The issue with existing Li-Fi devices is that they are not networked and rely on USB sticks to store location-based data for each specific light. However, a museum, may have 1000's of Li-Fi access points. As a result, if the curator wishes to update data on the Li-Fi system, a step ladder will be required to extract the USB stick from the Li-Fi access point. Additionally, the curator will need to connect the USB stick to a PC and manually update the data. Finally, the curator should return and reconnect the USB to the Li-Fi transmission system. Clearly, this is not feasible for a museum with thousands of lights [107].

The interactive application sends the users location every 5 seconds to the database using the different the radio light heads installed. This gives the system information about the user location so it sends the right information to where the user is in the museum.

3.6 Location database System Design on the VNF for access from User Equipment

3.6.1 Database System Architecture

There were two different architectures to use for developing the database, namely: the Django framework and the JavaScript's Node.JS framework. The Django framework was chosen even though Node.JS provides high performance and is very efficient, because Node.JS is still a new framework and does not have as many resources as Django, thus Django was chosen.

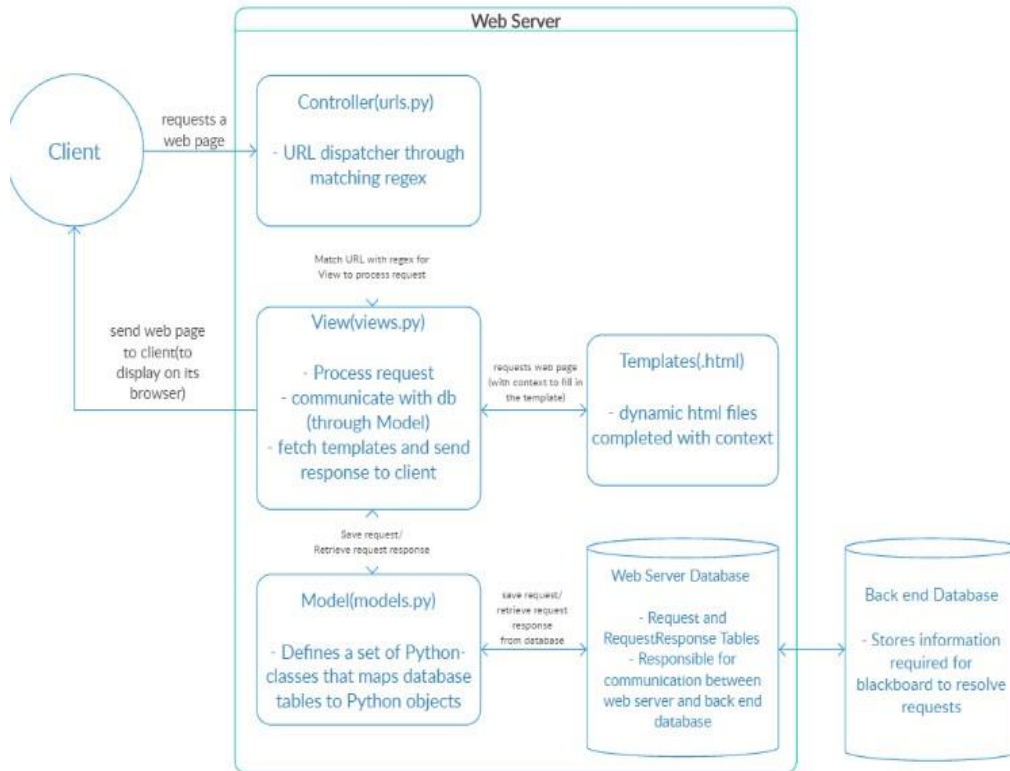


Figure 0-3: Django architecture

The Django architecture works using different python modules as shown in Figure 3-3 on a web server. The different modules within the framework allows data access from the database on the VNF and the server provides the data to the front-end dynamic web page on the UE.

To clearly demonstrate the process that happen inside the Django architecture in Figure 3-3. A client requests a webpage from the web server. The web server receives the request and sends it to the controller (urls.py module), which has a list of all the links that can be requested. The controller looks at which URL is requested and matches it with a REGEX, once matched with one of the URL patterns. Subsequently, it requests the link from the views.py, where it process the request. Then the templates module sends the back the information to the views. The templates hold information from the database. The views module checks models (model.py) for the requested objects from the template. Models create objects and fill it up with the information given by the database and sends it back to the views. Views send the web page to the client, where it will be displayed on their web browser

3.6.2 System Development

3.6.2.1 Front-end development

Without the right software, it will not be possible to transmit data based on the location of the connected devices (smart phones). In order to receive information from the backend VNF and display it on the user equipment a front-end interface is needed. The front-end of such system should look like what users are used to such as a website, but with the main important features. The features are; ease of usage, functionality, and appealing.

3.6.2.2 Back-end development

The back-end on the VNF can be easily defined as the support to the front-end. It is the development of the background resources and processes that serves all the information that has been gathered by the server from the front-end. Therefore, it manages the processing of information from the database and deploying them on templates serving the HTTP requests. It also serves the data to and from the database.

3.6.2.3 Both the front-end and back-end system

The Front-end of the system consists of the following components as there is not one programming language that can cover all the functionalities needed for the front-end. The five components are HTML5, CCS3, JavaScript, Bootstrap, and jQuery as shown in Table 0-2 below.

HTML5	It is served to web browsers, which makes it universal to all different platforms and still being easy to use.
CCS3	It controls the size, colour and how will the elements appear on the web page.
jQuery	This framework, which is based on JavaScript, is used to provide interactivity on the web pages.
JavaScript	It simply makes the element interactive without having to reload the webpage
Bootstrap	This framework provided flexibility for the website. It resizes the elements based on the size of the device used or the user's screen size.

Table 0-2: Programming languages used for front-end system

The back-end of the system primarily consisted of two main components, Django and MySQL. Django runs its modules, which controls the whole system and interlinks the different platforms used. Django uses python programming language for its modules. Also, python allows for the creation of scripts to access the database through PHP and MySQL.

Django interlinks the front-end and back-end together. Once a request is made, Django makes use of the various modules to fulfil it. Obtaining all information and incorporating it into a front-end response is a part of the request. The dynamic modules load the response of the request with the information from the database and sends it back to the user. Database-

driven applications are designed to have dynamic content that can be effortlessly changed as needed.

3.6.2.4 System flowchart

The system flowchart shown in Appendix 2

Appendix 2

Appendix 2

Appendix , begins at the start, which is accessing the museum domain name (as this was made for development and testing reasons, the access to the system is “127.0.0.1:8000”). The system must be notified that the manager is logged in, because if the manager is not logged in, the system will loop back to the login page until it is logged in. As soon as the manager is logged in, the system takes managers to the homepage. There is a navigation menu, where it allows the manager to navigate to any other page on the system, for example to view all content and all exhibits on the web pages. Also, the manager can view specific information, for example, a specific content or exhibit. Additionally, other web pages allow managers to create new content, exhibits and add information to the database.

3.7 Design implementation of transmit and receive interactive services

The development of the required applications relays on the system architecture network defined in chapter 3. Also, the same database was reused to allow the implementation of the following requirements of this chapter.

3.7.1 Interactive web interface

A website was created to allow the managers to update, edit, delete and add information. This website is user friendly and interactive. The website was created as a front-end user interface that retrieve information from the backend and the server onto the webpage for museums as an example but can be dynamically change for other scenarios such as supermarkets and train stations. This was achieved by using the Django framework and python. Finally, the website was created using HTML, JavaScript, CSS3 and bootstrap.

These components were critical in developing a system that was dynamic, interactive, and responsive. Each component was critical to the front-end's outcome. Front-end systems are critical because they make content updating easy for the managers to edit, delete, add, and update content. The front-end interactive web interface for the managers is shown in Figure 0-4 and Figure 0-5.

Musée Français de la Carte à Jouer & Galerie d'Histoire de la Ville

Exhibit	Exhibit ID	Added By	Added on
Test-content		akram	Dec. 5, 2017, 9:44 a.m.
Cards		akram	Dec. 4, 2017, 1:25 p.m.

Figure 0-4: Database Museum Exhibits

Musée Français de la Carte à Jouer & Galerie d'Histoire de la Ville

Exhibit	Added By	Added on
Cards	akram	Dec. 4, 2017, 1:25 p.m.

Test-content

Logo

Test-content

Figure 0-5: Database Museum Test Content

Musée Français de la Carte à Jouer & Galerie d'Histoire de la Ville

Create new content

Title

Type

Content Upload No file chosen

Caption

Year

Time

Figure 0-6: Creating new content

Figure 3-6, presents the interactive web interface that allow managers add new exhibits to the database.

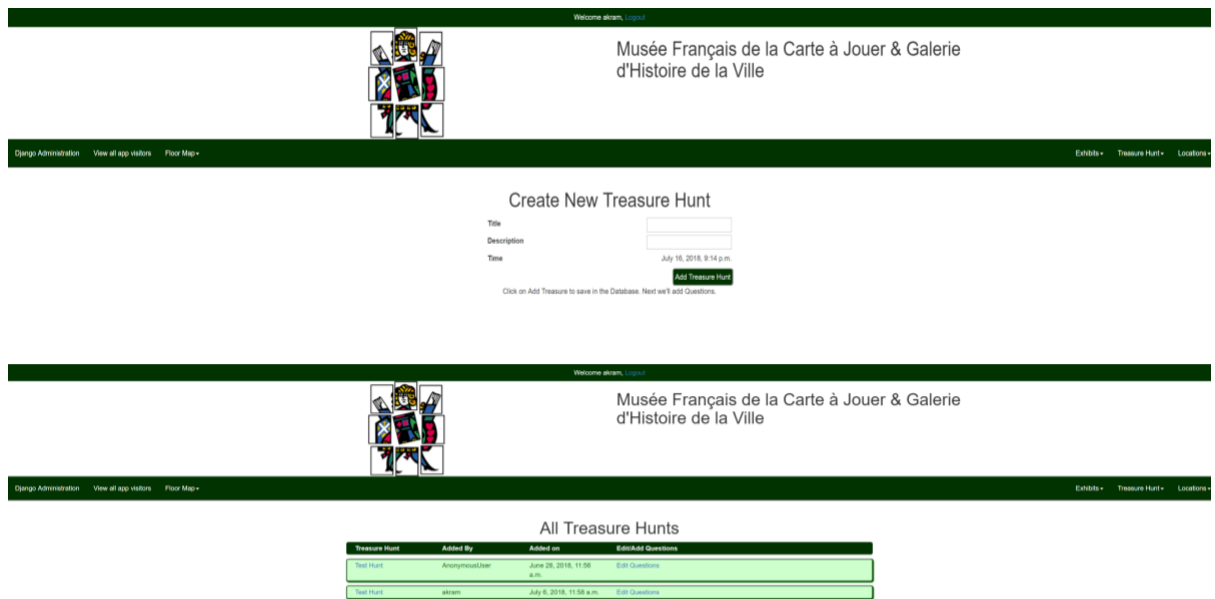


Figure 0-7: Create treasure hunt game

Figure 0-7, does not only show how can managers create the interactive application but also it allows them to create more than one game. Also, the managers can view all the games that has been created and based on that they can add, edit or delete any.

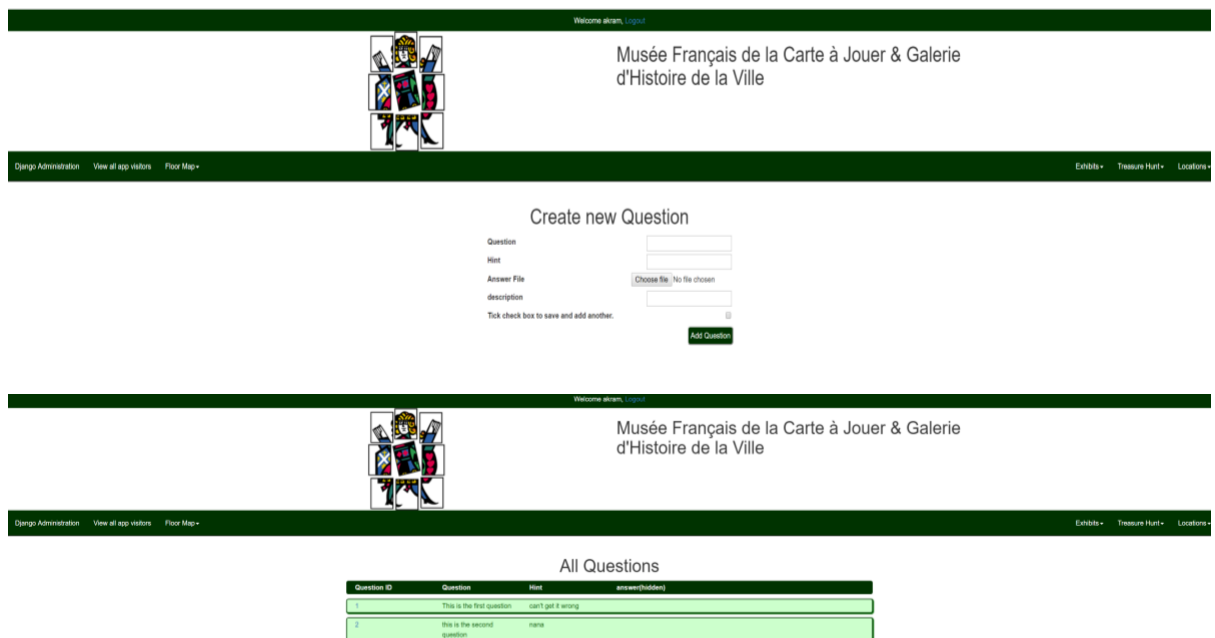


Figure 0-8: Creating new questions

Figure 0-8, shows how the manager can create questions for the interactive application and how the manager can add new questions and view all the saved questions.

3.7.2 End User Application

3.7.2.1 Functionality

The android application was created to provide three main functionalities. Firstly, it allows museum visitors to access and fetch data (information, videos and audio) through the database. Secondly, the app allows the users to use the interactive application, where they play and upload their answers through the database. Finally, the application sends the user's location every 5 seconds to the server. It runs while the application is running on the background

3.8 Development and testing

The concept was to incorporate the different functionalities in one application. The application has been developed through Android Studio as it is more common and has a lot of open sources.

- Indoor location-based data access
- Interaction application
- Indoor location monitoring



Figure 0-9: App first page

A signup system has been developed for the users to register their information in the database. Figure 0-10 shows, the login page of the application, where it allows the user to register and login in. Also, the backend where it saves the users information.

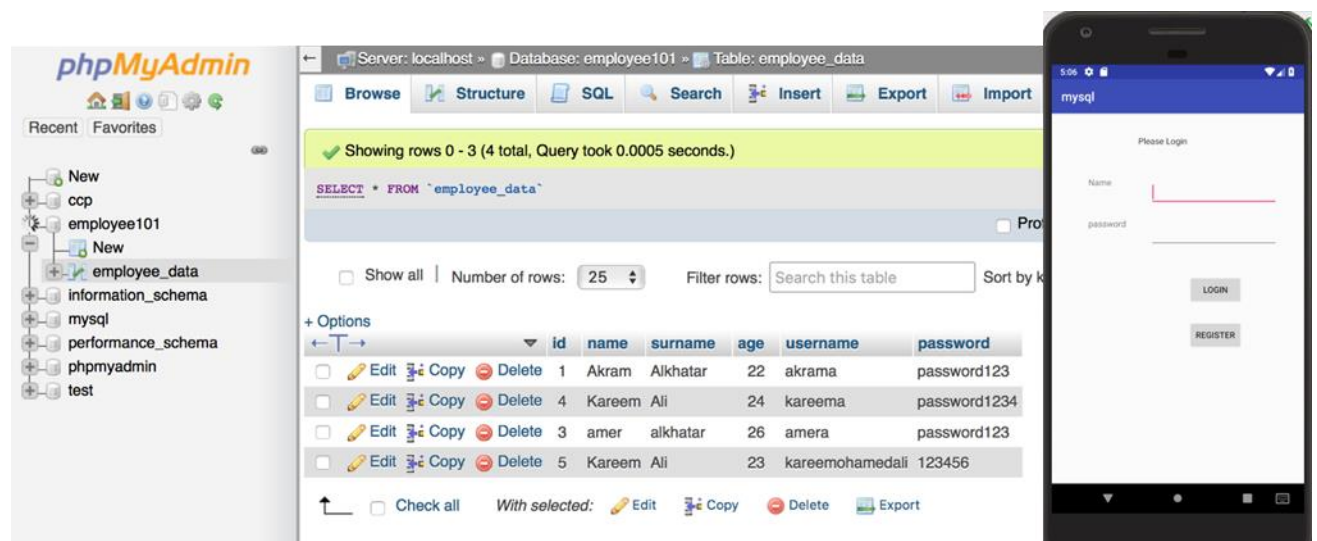


Figure 0-10: Application Login page

3.8.1 Indoor location-based data access

As previously stated, indoor location-based data access should be available to all managers for the purpose of adding, editing, updating, or deleting exhibits or information. A test has been conducted to determine the application's capability and its interconnection with the database. The test resulted in the following evidence that it works.



Figure 0-11: Empty exhibits page

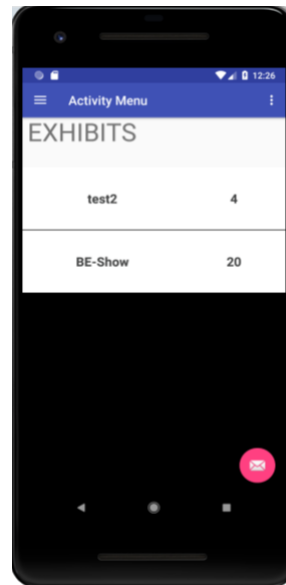


Figure 0-12: Exhibits uploaded

The process of testing involved adding exhibits content on the database and then check if the user can see it on the application. Figure 3-11, shows the empty exhibits page before adding any exhibits to it. Figure 3-12, shows the exhibits page after adding the different exhibits through the backend of the database as shown in Figure 3-13. This shows that the functionality is operating.

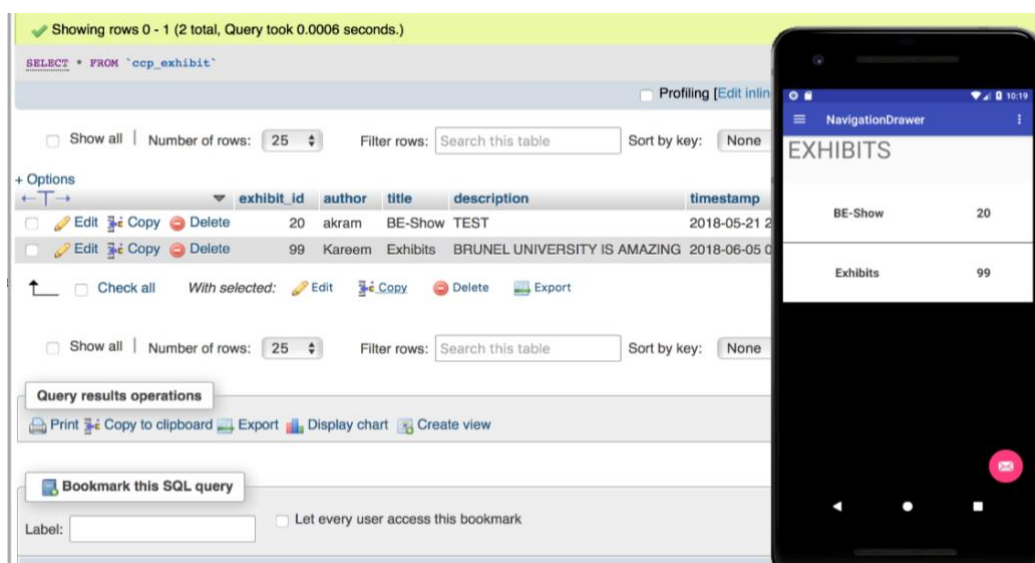


Figure 0-13: Backend database uploading information to the app

3.8.2 Location-Based Image Retrieval

The interactive application was made for the users to allow them to practice problem-solving in a fun way. The application gives the visitors different clues about a specific artefact in the museum and they need to figure out, which one it is. Also, it allows them to upload their answers in terms of images and check with the reference image and then give them the results.



Figure 0-14: Treasure hunt

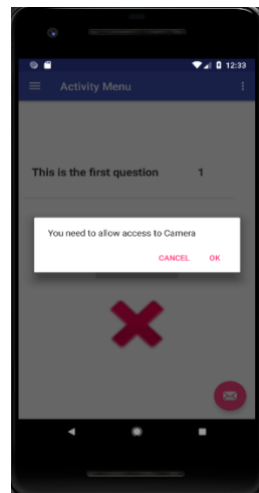


Figure 0-15: Access permission

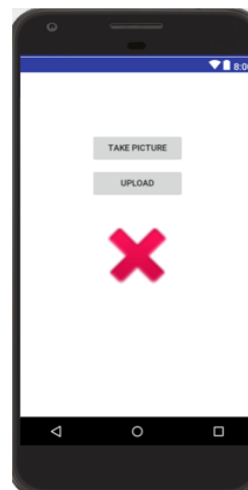


Figure 0-16: Upload page

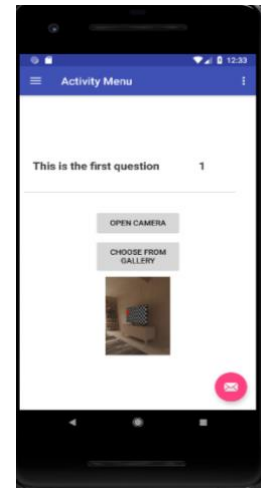


Figure 0-17: Uploaded image

Figure 3-14, shows the interactive application and by pressing on it to take the users to the second page, where it asks for permission to access the camera as shown in Figure 3-15. Figure 3-16, shows the page, in which the users have the option of taking a picture or uploading an image they already have saved in the gallery. The visitors afterwards can see whichever image the uploaded to the system as shown in Figure 3-17.

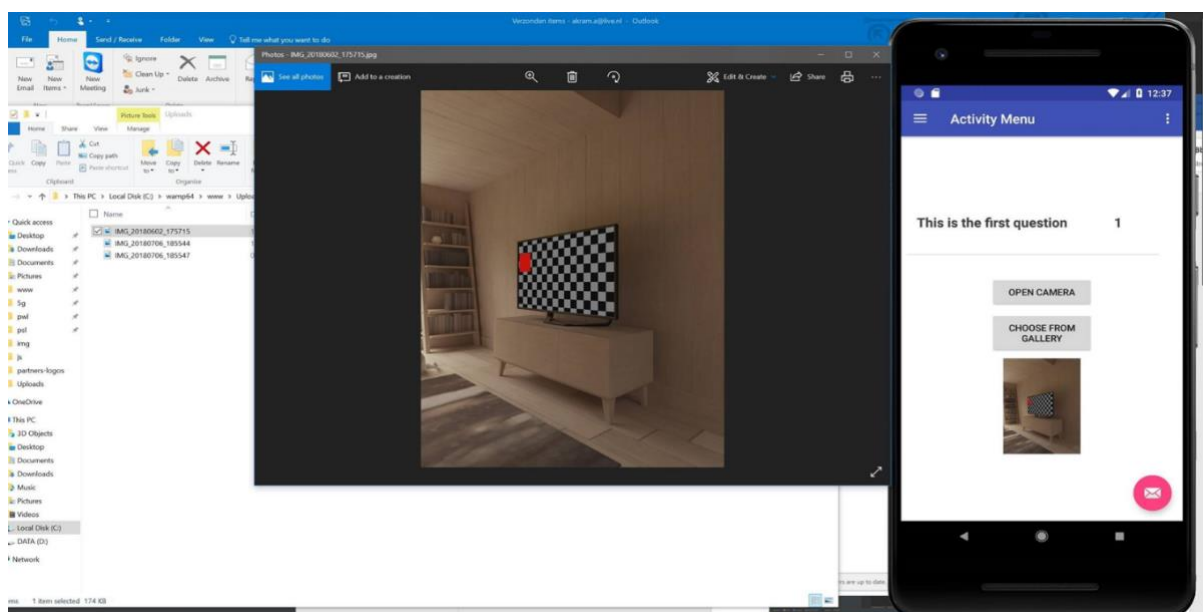


Figure 0-18: The location of the uploaded image

Figure 3-18, shows the location of the uploaded image. It gets sent to the database, where it then saves it on the physical server then a python script runs as shown in Figure 3-19 , whenever a new picture gets added to the file, where it compares it to the reference image of that specific game and then sends back the result to the database, where it sends it back to the user who uploaded it.

```
img > matchingface.py > ...
1 import face_recognition
2 from PIL import Image
3
4 # Setting this as the default image
5 default_image = face_recognition.load_image_file('./img/default/Barack Obama.jpg') # <-- Alter this image for testing
6 # Converting this image to code format & perform analysis
7 default_image_encoder = face_recognition.face_encodings(default_image)[0]
8
9 # Inserting a secondary image to compare with the default image
10 secondary_image = face_recognition.load_image_file('./img/secondary/Former President.jpg') # <-- Alter this image for testing
11 # Converting this image to code format & perform analysis
12 secondary_image_encoder = face_recognition.face_encodings(secondary_image)[0]
13
14 # Comparing faces/facial features -- determines whether match or unmatched
15 output = face_recognition.compare_faces([default_image_encoder], secondary_image_encoder)
16
17 # The output message corresponds to the type of match
18 if output[0]:
19     print('This is a match!')
20 else:
21     print('This is NOT a match!')
22
```

Figure 0-19: Image Matching Script

3.8.2.1 Accessing the Location Database

As mentioned before, the LD is provided by the OpenStack as one of its VNF services. Firstly, the VNF virtual machine needs to be accessed. Secondly, open Firefox and type the following; '127.0.0.1/phpMyAdmin/' into the web search bar. Finally, to login in to the phpMyAdmin page credentials are required, which are

- Username: databasubuntu
- Password: root@1234

On the left-hand side is a toolbar, which should be used to access the 'database_location' LD. It contains all the relevant tables. TDOA_Data, which stores all TDOA data, UE_Pos, where it stores all the position estimates of the users, and the VLC_Data, which stores all the RSS data

3.8.2.2 Data receiving

PyMySQL library was very critical to be able to upload data to the database. The connect () function is simply to connect and gain access to the database. Also, there is the upload position function, which requires modification depending on which data are being uploaded.

3.8.2.2.1 TDOA data upload

Please input:

```
update_table = ''' INSERT INTO `TDOA_Data` (`ID`, `UE_ID`, `RRLHC_ID`, `TDOA1`, `TDOA2`, `TDOA3`, `TDOA4`, `TDOA5`, `TDOA6`, `TDOA7`, `VLC1`, `VLC2`, `VLC3`, `VLC4`, `VLC5`, `VLC6`, `VLC7`, `VLC8`, `TimeStamp`) VALUES (NULL,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s, '0', '0', '0', '0', '0', '0', '0', '0', '0',%s);'''
```

```

pos_data = (ue_id, RRLH_ID, data1, data2, data3, data4, data5, data6, data7, Timestamp)
cursor.execute(update_table, pos_data)
conn.commit()
except:
    print ("Table not updated")
else:
    print ("Table updated")

```

The pos_data line is where the data (in blue) are inserted to be updated.

3.8.2.2.2 VLC data upload

```

INSERT INTO `VLC_Data` (`ID`, `UE_ID`, `RRLHC_ID`, `VLC1`, `VLC2`, `VLC3`,
`VLC4`, `VLC5`, `VLC6`, `VLC7`, `VLC8`, `TimeStamp`) VALUES (NULL, '1', '1', '2', '3',
'4', '5', '6', '7', '7', '7', CURRENT_TIMESTAMP);

```

try:

```

update_table = " INSERT INTO `VLC_Data` (`ID`, `UE_ID`, `RRLHC_ID`, `VLC1`,
`VLC2`, `VLC3`, `VLC4`, `VLC5`, `VLC6`, `VLC7`, `VLC8`, `TimeStamp`) VALUES
(NULL,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s);"

```

```

pos_data = (ue_id, RRLH_ID, data1, data2, data3, data4, data5, data6, data7, data8,
Timestamp)

```

```

cursor.execute(update_table, pos_data)

```

```

conn.commit()

```

```

except:

```

```

    print("nope")

```

```

else:

```

```

    print("table updated")

```

The pos_data line is where the data (in blue) are inserted to be updated.

3.8.3 4K Real-Time Video Streaming Location Server

3.8.3.1 Streaming VNF

The suggested method is providing a more efficient and scalable approach with the use of its dynamic network environment. This method is a complementary to the previously discussed method, which would allow the deployment of the system in various settings. Figure 3-20 ,is striving to provide a real-time streaming through UDP with a more reliable approach and low buffer time.

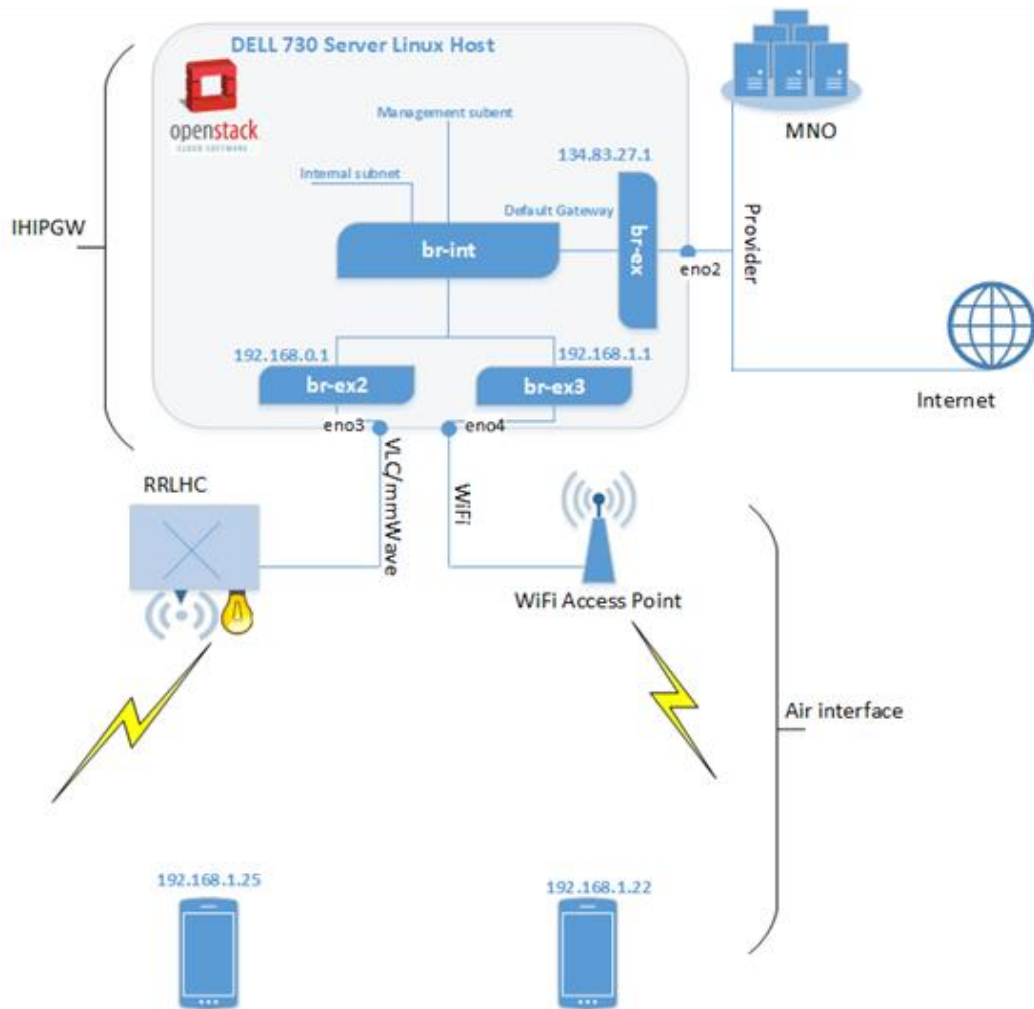


Figure 0-20: Streaming System Diagram

The proposed streaming system is shown in Figure 3-20. The system is built on OpenStack, with a deployed software defined network (SDN). The SDN is implemented in the Intelligent Home IP Gateway (IHIPGW). It shows the management subnet (br-int) divided into three different subnets. Subnet (br-ex) is a provider to the internet and mobile network operators (MNO). The other two subnets are essential as they provide access to users. The first subnet (br-ex2) is serving access through two modules, Visual Light Communication (VLC) and mmWave. These modules allow communication between the IHIPGW and the User Equipment (UE). The mmWave module is used for up-link-down-link connection and VLC is used for down-link. “These modules are installed inside a Remote Radio Light Head Controller (RRLH), which sends and receives the data back to the IHIPG after going through layer 1 and 2 processes” [107]. To illustrate Figure 3-21, shows an example of a user requesting a video and the server provides the requested content to the lamb driver to send to it to the user.

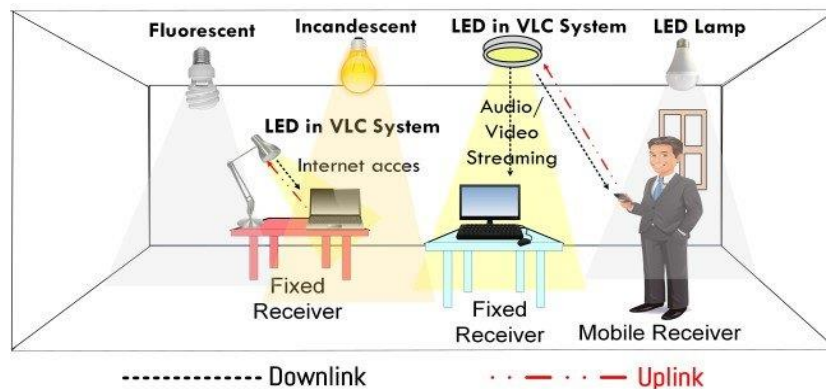


Figure 0-21: Video Streaming through VLC to UE

The second subnet (br-ex3) is serving access through Wi-Fi. By providing the different pools of resources, the streaming application can have more utilised resources and efficient system to achieve better quality of service. A higher quality of videos would also be streamed with low latency.

3.8.3.2 Experimental Set up

To show a proof of concept of the proposed service, a streaming server was deployed as a VNF within the OpenStack platform. The host machine has the VNF streaming server, which is connected to a logical network with a subnet given by the OpenStack. The physical server that was used was Dell R730xd server. The server runs Ubuntu Linux 16.04LTS. The specifications of the servers were as follow:

- CPU: 2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz
- Memory (RAM): 192 GB
- 2x Drives: 240GB SSD and 1TB
- Network Interface: 2x 10GbE and 1x GbE



Figure 0-22: Dell R730xd server

3.8.3.2.1 VideoLAN Client media player (VLC player)

VLC player is a multi-media player and framework, free and open source, that plays multimedia files and has different streaming protocols [109]. VLC can be used to transmit and receive network streams as a server and client.

3.8.3.2.1.1 VideoLAN Streaming Solution

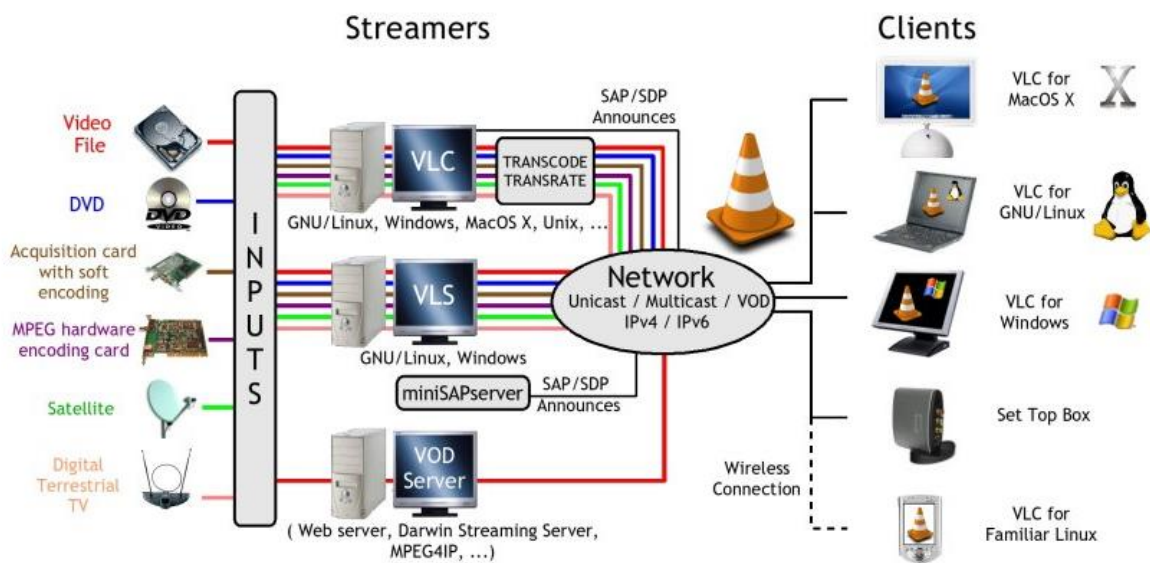


Figure 0-23: VideoLAN Streaming solution

Figure 0-23, presents VLC organisation's streaming solution. The network for setting up the VideoLAN solution can be as small as a 10/100 Mb Ethernet switch or hub and as large as the internet as a whole [110]. The file that needed to be transmitted gets added to the VLC player and then its multicast the file using the network protocol chosen, which is UDP and then it transmits.

3.8.3.2.1.2 VLC setup

VLC player was installed on the streaming virtual machine, which is deployed on the OpenStack. Then a video was streamed from the VLC player to a 4K TV using UDP protocol.

The following are the steps used to set up a successful stream:

- 1- Open terminal and type VLC
- 2- Inside VLC press on Media, stream, then press on add file (Add the video, you want to stream). Then press stream then Next
- 3- There is a box on the bottom left that to be ticked at, which says display locally. Tick this box ON to view the video being streamed.
- 4- In the New Destination box, pick UDP then press ADD
- 5- Insert the IP address of the other machine (In this case the TV's IP address) and leave the port number as it is 1234. Then press Next.
- 6- Keep pressing next without changing any of the other configurations until you stream.
- 7- Go on the TV and open the TV app and add the IP of the virtual machine and the port number set, which was 1234 and play

3.8.3.2.2 Testing Scenario

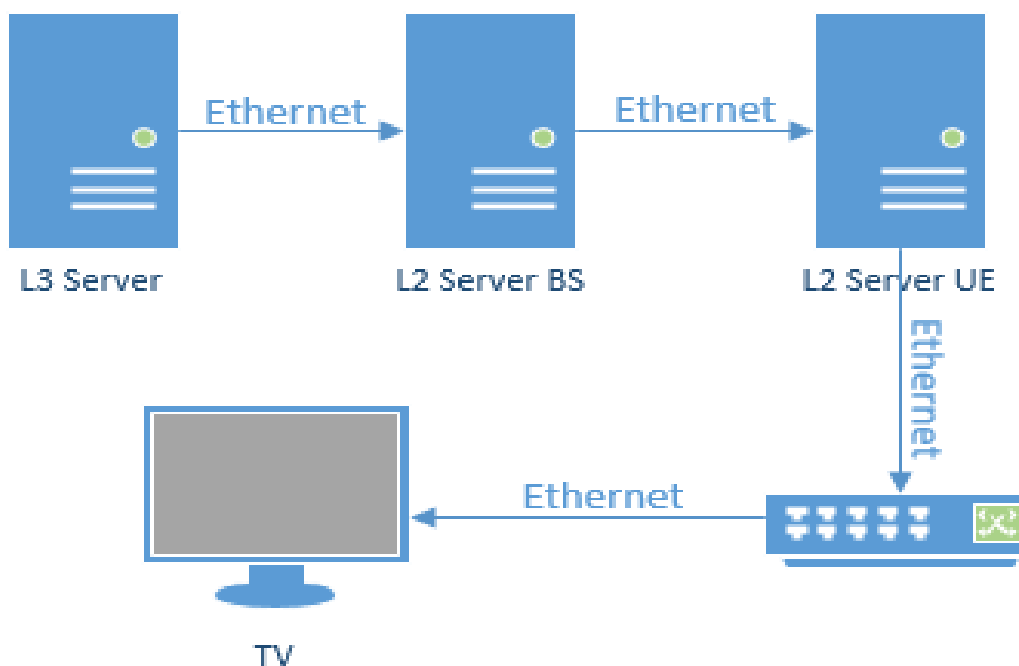


Figure 0-24: Streaming Scenario

The following scenario was designed to examine the proposed streaming method to improve the QoS and QoE for all the users. As discussed previously, broadcasting services are rapidly growing, and it is essential to look for new solutions to be able to accommodate the increasing number of users. Figure 3-24, presents the stream from the VNF on layer 3 server through the system's base station server to the user equipment to a switch to the 4K TV.

3.8.3.3 Results and analysis

This section will be demonstrating the three streaming resolutions used to conduct the tests on the streaming scenario. Figure 0-25 and Figure 0-26 below, presents the overall number of packets verses jitter and delay for all the resolutions. By examining Figure 0-25 ,it is not very clear but however it shows that the proposed streaming method didn't surpass 0.05 s. Figure 0-26, shows that the delay has been reduced and that was no spikes during the stream. The following sections, **Error! Reference source not found.** and 3.8.3.3.2 , shows the jitter and delay for each resolution examined separately. Also, it shows the traditional streaming vs the proposed streaming method.

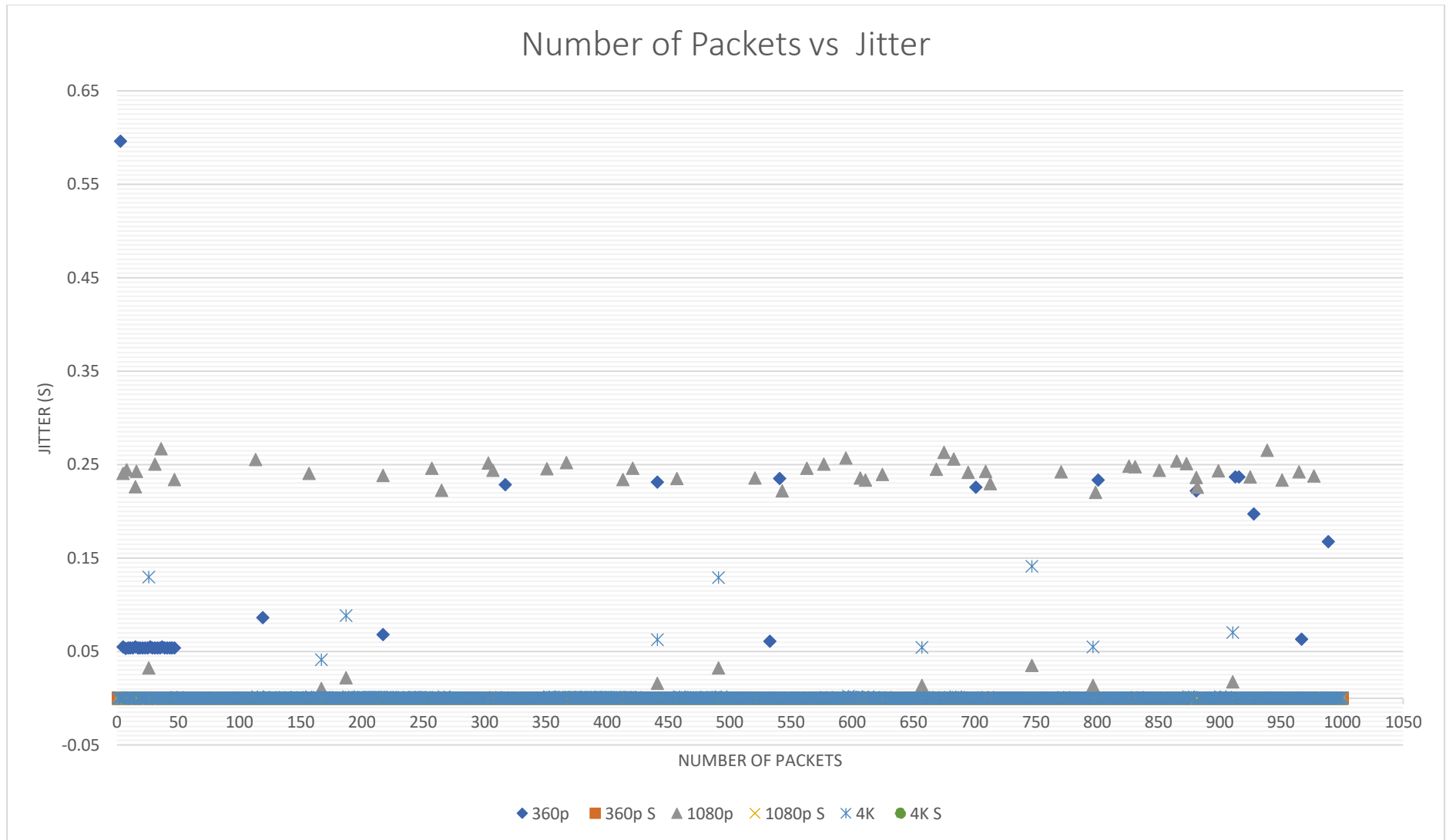


Figure 0-25: Overall number of packets vs jitter

Note: S stands for the proposed Solution

Number of Packets vs Delay

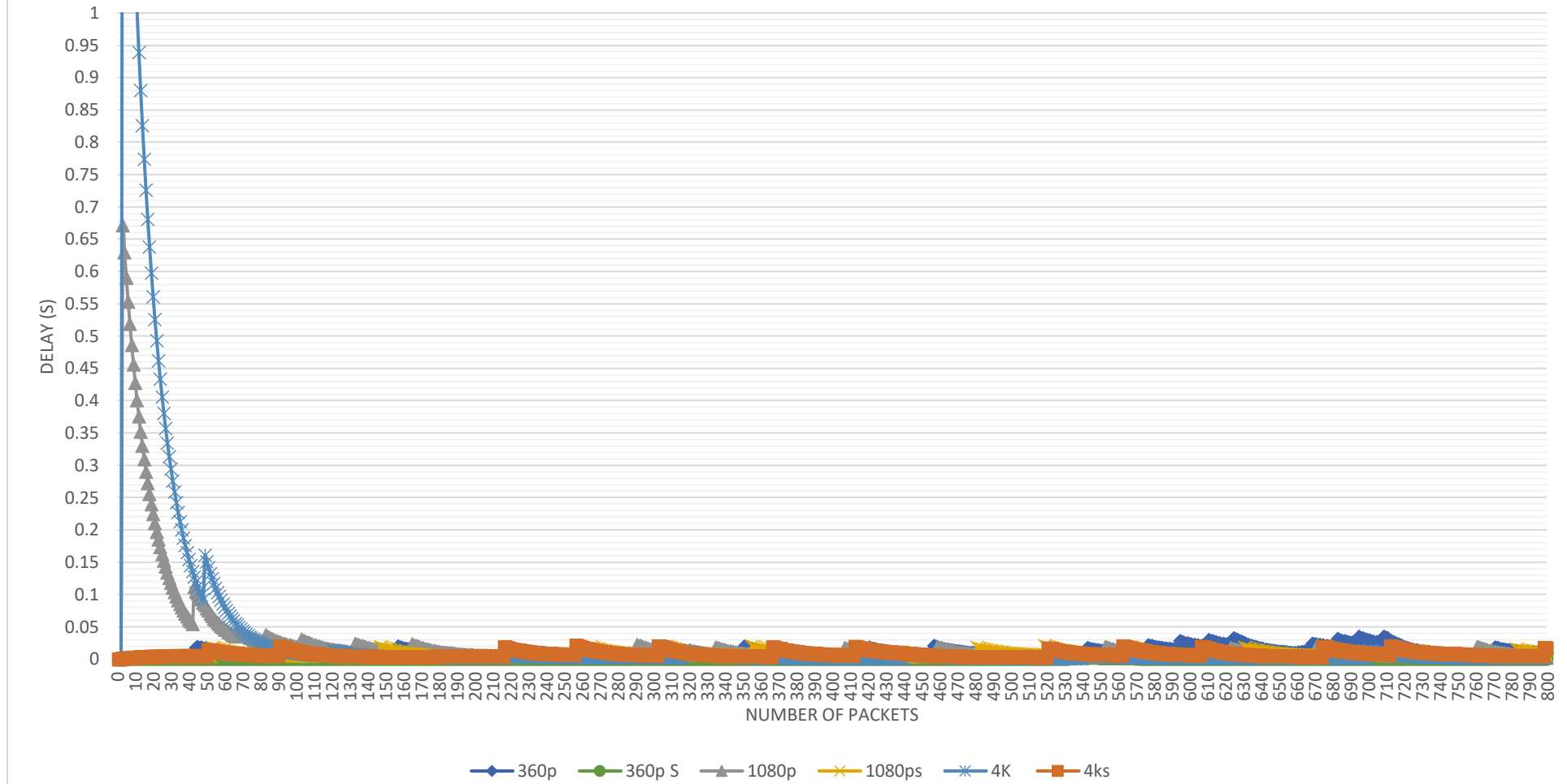


Figure 0-26: Overall number of packets vs delay

Note: S stands for the proposed Solution

3.8.3.3.1 Jitter

Table 0-3: Average Jitter

Resolution	Average Jitters (s)
360p	0.00431875
360p S	0.00002084
1080p	0.01190814
1080p S	0.00004957
4K	0.04763375
4K S	0.00006800

Note: S= Proposed System

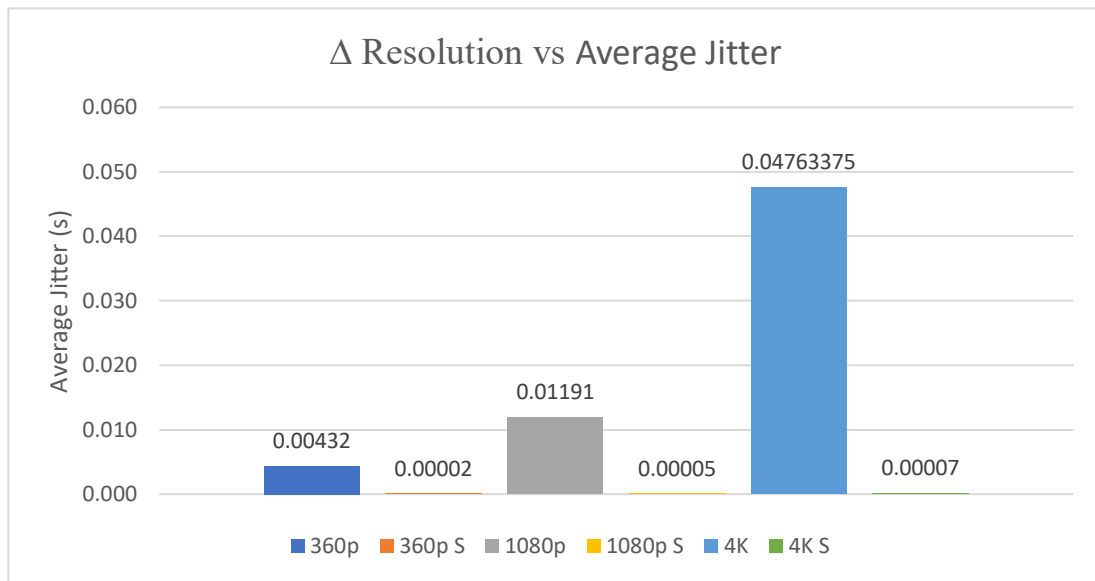


Figure 0-27: Resolutions vs Average Jitter

Figure 3-27, presents the results from Table 0-3. As shown, comparing each of the resolutions, there is a clear sign of improvement in all the resolutions. Whilst looking at the average jitter for all the proposed resolution method. The proposed 360p stream was able to obtain 0.02 ms of jitter, while 1080p S was 0.05 ms jitter and finally 4K was 0.07 ms jitter.

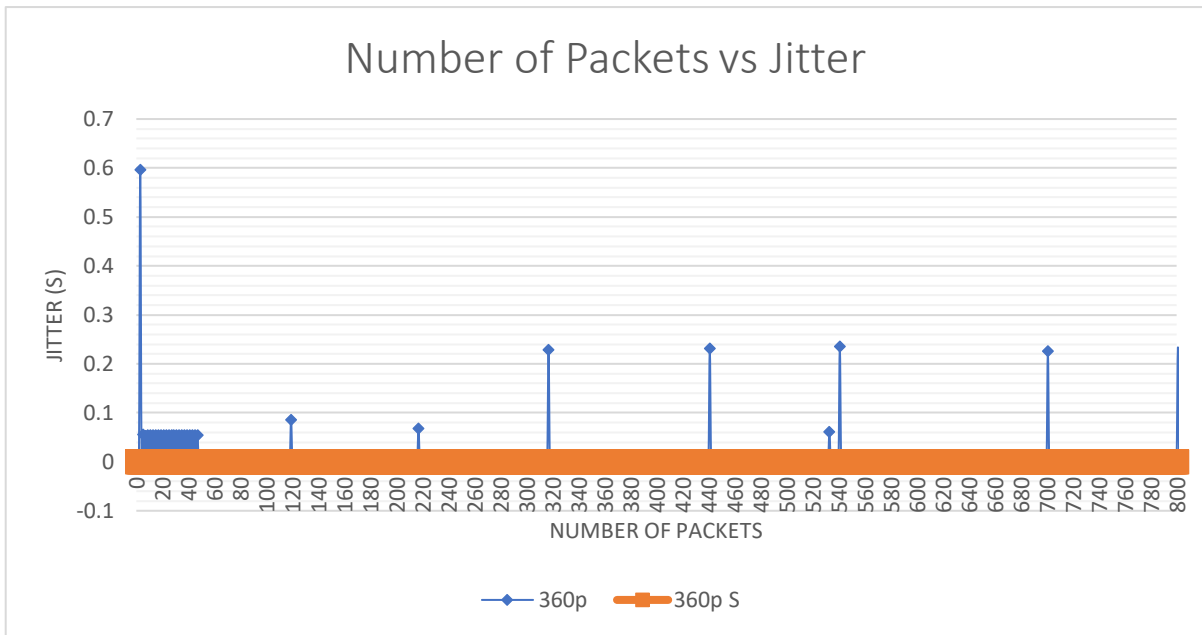


Figure 0-28: traditional vs proposed streaming 360p

As shown in Figure 3-28, on a closer look the traditional method is unstable at the beginning and the jitter gradually decreased and it was constant until 50 packets. But then there were some spikes. On the other hand, the proposed method was stable throughout without any spikes and major jitters and averaged at 0.02 ms of jitter.

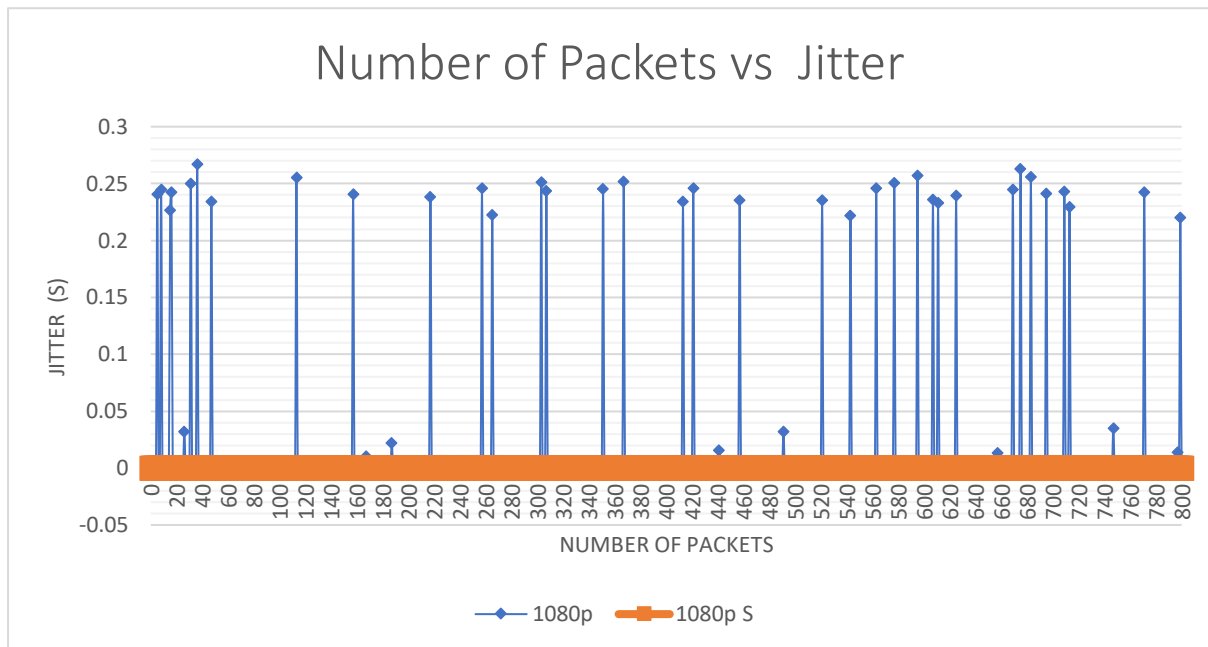


Figure 0-29: traditional vs proposed streaming 1080p

As shown in Figure 3-29, the traditional method had spikes throughout the whole stream, which was averaged at 11.9 ms, while the proposed method was constant, and the average jitter was kept at 0.05 ms.

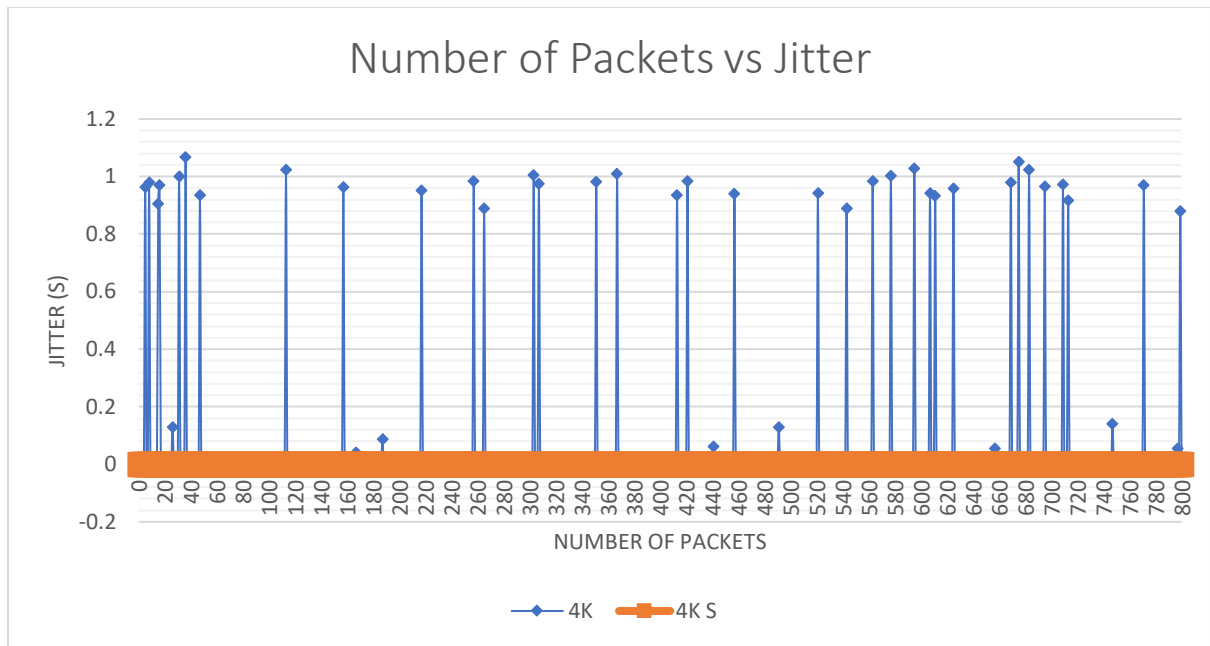


Figure 0-30: traditional vs proposed streaming 4K

Figure 0-30, demonstrates that the traditional method showed massive spikes reaching 1s. However, the proposed method stayed persistent throughout with very low jitters (0.07 ms).

3.8.3.3.2 Delay

Table 0-4: Average Delay

Resolution	Average Delay (s)
360p	0.01002270
360p S	0.00073600
1080p	0.02009161
1080p S	0.00754544
4K	0.03014092
4K S	0.00953448

Note: S= Proposed System

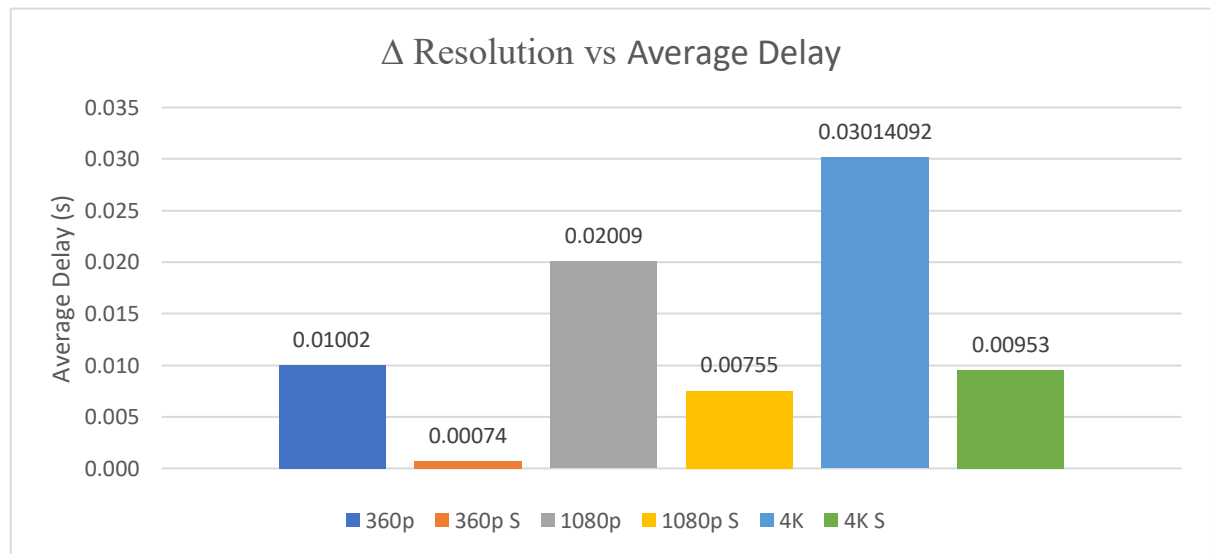


Figure 0-31: Resolutions vs Average Delay

Figure 3-31, presents the results from Table 0-3. As shown, comparing each of the resolutions, there is a clear sign of improvement in all the resolutions. The proposed 360p stream was able to obtain 0.74 ms of delay, while 1080p S was 7.55 ms and finally 4K was 9.53 ms delay. The results are acceptable and show a huge improvement from the traditional method. Additionally, the slot interval of the 5G subcarrier used for the proposed method, sends packets every 0.50 ms.

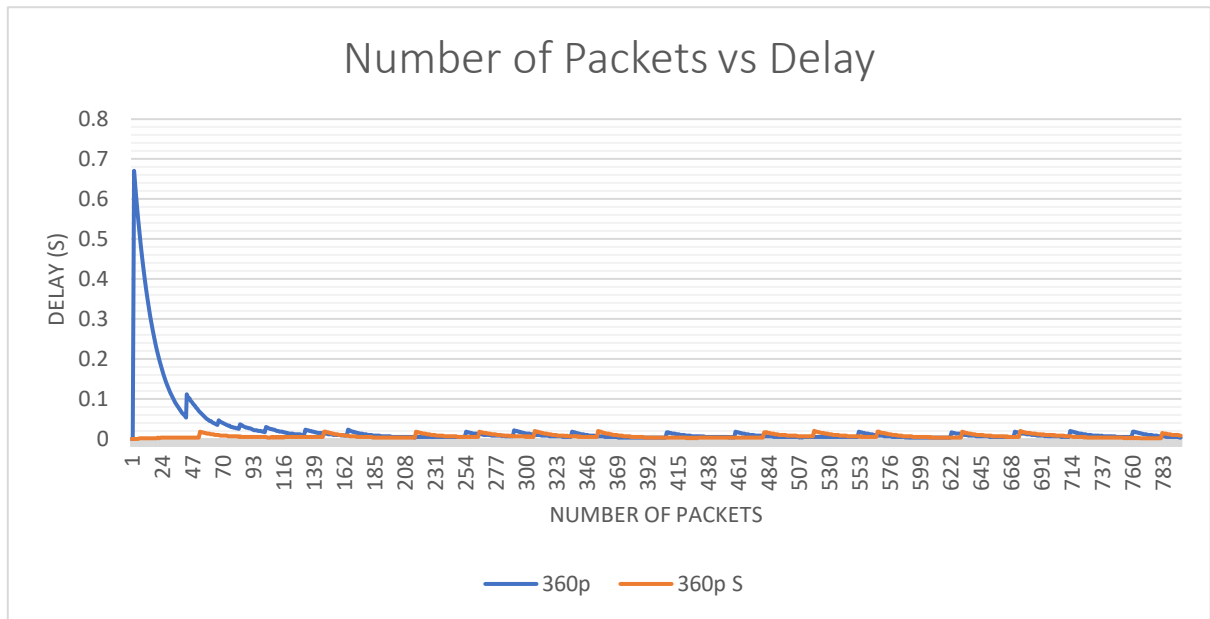


Figure 0-32: traditional vs proposed streaming delay 360p

Figure 3-32, shows that the traditional method has suffered many fluctuations, beginning with a high peak oscillation that was followed by several small identical continuous oscillations. This showcases that the traditional method is unstable. Subsequently, the proposed method has shown a stabilised set of results, where the delay has been kept at a minimal.

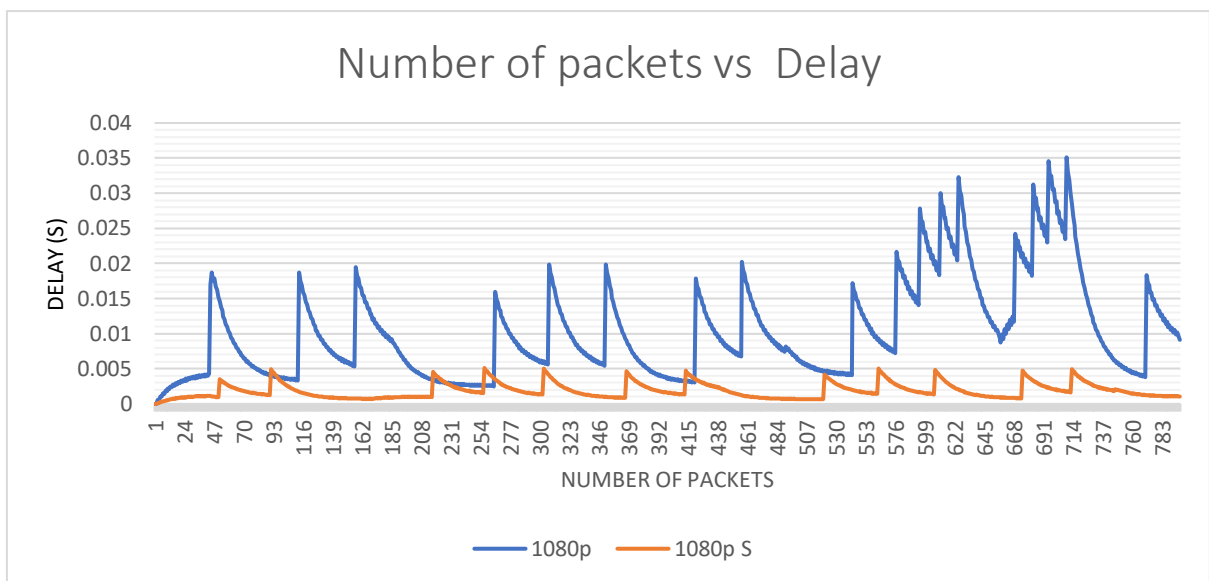


Figure 0-33: traditional vs proposed streaming delay 1080p

Figure 3-33, illustrates that the traditional method resulted in inconsistent fluctuations, with no clear chronological pattern. Post analysing this issue, the proposed method was able to stay stable even though the resolution of the video was higher than the previous streaming test. However, the proposed method had minor fluctuations that did not exceed 0.005 s and an overall average of 0.00755 s.

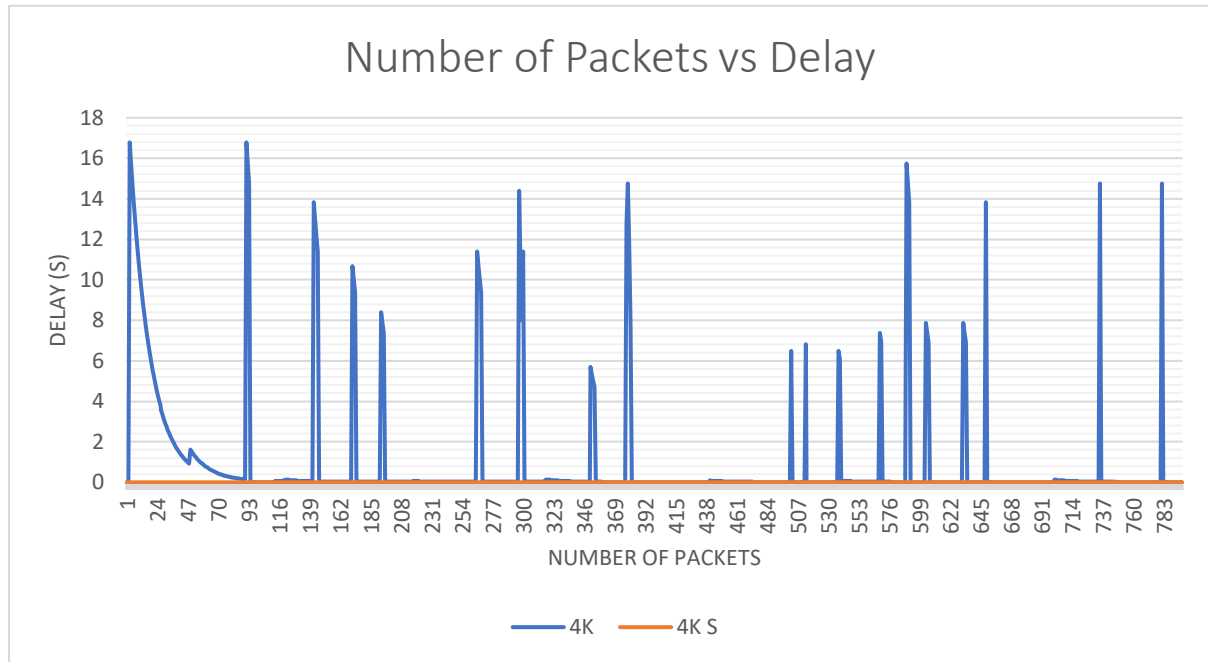


Figure 0-34: traditional vs proposed streaming delay 4K

Figure 3-34 presents that the traditional method had numerous fluctuations, which started with one high oscillation, which then was followed by a decrease, then back up with continuous fluctuations. This showcases that the traditional method is unstable. When using the proposed method; a stabilised set of results were displayed with very minimal delay, which is acceptable.

3.9 Summary

Location based services are difficult to provide indoors because of the limitations of indoor location-based data access (ILBDA) systems. Instead of VLC and mmWave, other technologies like Wi-Fi, BLE, UWB, and RFID can be used. However, due to limitations (such as range, accuracy, and tracking indoors), current technologies cannot be used indoors. Many applications have been developed for the same purpose on the market, but none of them have the accuracy needed to make it practical for users to use.

This chapter focused on the museum scenario, however, the same applications can be modified to different scenarios like supermarket, where users will need the same LD, with all the different products. Likewise, it can be modified to provide information in the train station

environment. A database-based user interface was developed to allow a full control of all the information on the database that the Remote Radio Head Lights (RRHL) sends to the users.

Furthermore, Real-Time video streaming is a new service that has been proposed to improve the quality of experience through utilising an SDN concept of reactive traffic routing, and NFV technology. This was done to enable flexible service deployment, as well as leveraging the IoRL system's massive bandwidth and location estimation accuracy. It demonstrates the IoRL system's ability to accommodate multiple services, whilst maintaining a higher quality of experience for its clients due to its flexible and intelligent design. The system's performance parameters demonstrated a high level of QoS (Zero packet loss due to route switching, very high throughput, 0.07 ms jitter and 9.53 ms delay). The current service performance tests were conducted by simulating the RAN network, which is still in development, and the video contents are already present on the local cache server. Wireshark was used to capture all the UDP packets during the streaming to examine the data.

Finally, the new types of services, that were introduced as promising technologies, are only providable with the localisation system proposed. The improved results obtained using the proposed system, resulted in an improved jitter and delay using the 5G streaming network.

Chapter 4: 5G Localisation Coverage and Accuracy

4.1 Chapter Outline

The objective of this chapter is to measure the localisation coverage and accuracy of mmWave and VLC. This chapter examines the localisation measurement procedure for the location accuracy and coverage. This chapter is organised as follows: Section 4.2 presents the coverage experimental setup. Section 4.3 provides the experimental setup. Section 4.4 provides the results of the VLC tests. Section 4.5 provides the results of the mmWave tests. Section 4.6 reviews the coverage challenges faced. Section 4.7 describes the location accuracy procedure. Section 4.8 details the optimisation data for the location accuracy with analysis and results. Section 4.9 discusses the accuracy challenges faced. Section 4.10 provides a summary.

4.2 Propagation Distance and Coverage Measuring Experimental Setup

Both, VLC and mmWave, use the 5G multicomponent carrier indoor system, which has six core components [111]. Firstly, DRAN (Distributed Radio Access Network) and RRLH Control Units are part of a 5G base station. FEC decoding, beam management, data distribution to RRLHs over 10 Gbps Ethernet rings, and the interface with the MAC and higher layers are all handled by DRAN, which is responsible for carrying out the duties of L1 upper layer. Most of the PHY layer processing is handled by RRLH Control Units. The main processing tasks are data modulation/demodulation, air interface resource mapping, antenna/LED management, precoding, and IFFT. The 10 Gbps Ethernet rings and the VLC and mmWave modules are connected via a switch and/or splitter/combiner to the D/A and A/D sides of these units. Secondly, A signal analysis software and a USRP are hosted by user equipment that includes a 5G NR baseband processing server. 5G NR Baseband software can demodulate the USRP's transmitted signal, estimate the channel, and perform zero-force equalisation in order to extract the symbols. A 2*10 Gigabit cable connects the USRP device to the 5G NR baseband processing server. The mmWave and VLC RX modules' input signals are handled by the USRP device. It converts the 3.48 GHz IF signal received into a baseband signal and sends it to the data processing server. Thirdly, mmWave TX and RX modules generate and receive 40 GHz RF signals. Fourthly, VLC Tx/Rx modules are included. Fifth component, a LO generator is needed to supply the 13 GHz signal to the mmWave TX and RX modules in order for them to function properly. Finally, the 13 GHz LO generator and the USRP device each receive a 10MHz reference signal [112]

Power levels, modulation schemes, bandwidth, and carrier frequencies of these six main components, as well as the system setup parameters for both the VLC and mmWave

measurements, are configured separately for each measurement type [112]

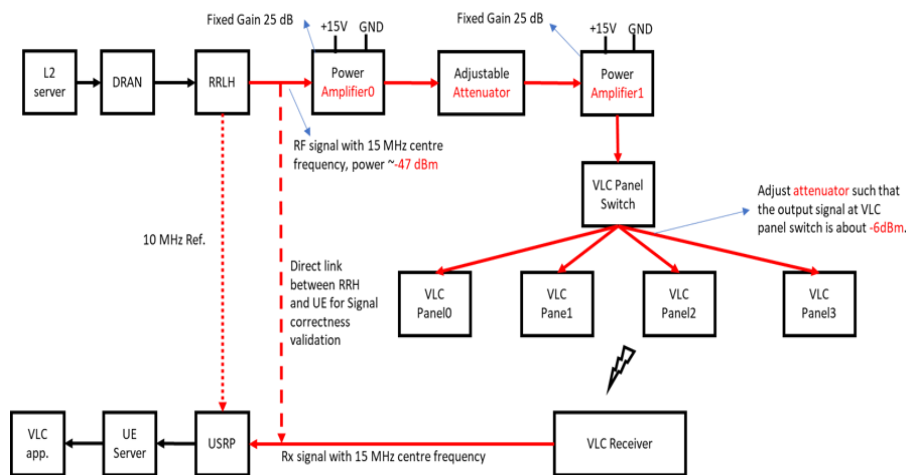


Figure 0-1: VLC Link

With regards to the VLC link, RRLH produces a signal with a centre IF frequency of 15 MHz and a power level of approximately -43 dBm from the 15 MHz RF port. The signal is then amplified to the appropriate power level and it is split by the switch into four VLC panels. The red line in the diagram above represents an RF cable with a SMA connector. Each VLC panel's VLC modulator is planned to accept a greater input power. Generally, the higher the input power of a VLC modulator, the better the signal quality. Nonetheless, there is a protective input power supply for the VLC modulator to prevent it from being damaged. As a result, the input power to the VLC panel should not exceed -6 dBm. To attain a good signal quality, the VLC panel requires a -6 dBm power level signal to be provided through two stage amplifiers. Additionally, an adjustable attenuator is plugged between the two amplifiers to compensate for variable cable attenuation [112]

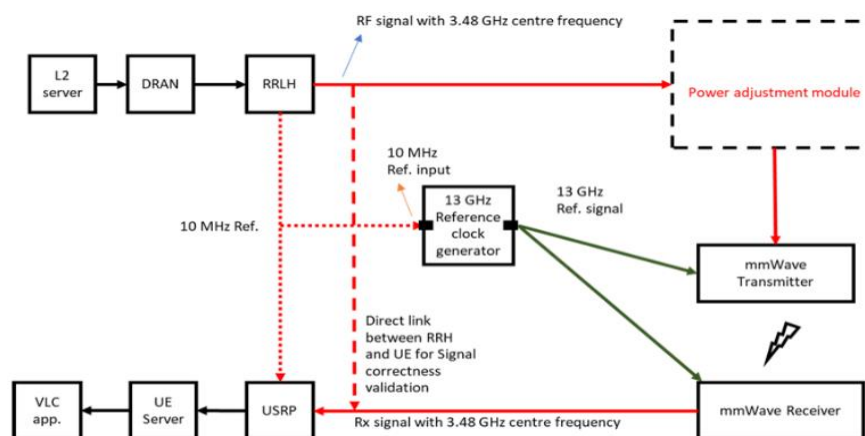


Figure 0-2: mmWave Link

The RRLH mmWave link generates a signal with a centre frequency of 3.48 GHz from the 3.48 GHz RF port at a power level of -27 dBm. The mmWave system requires an additional 13 GHz reference signal in addition to the signal path. This is generated by an external

frequency source that is powered by the RRLH reference signal at a frequency of 10 MHz. High-frequency cable is depicted by the dark green lines in this diagram. The remaining red lines represent cable that operates at frequencies lower than 6 GHz. Table 0-1 lists the transmitted signal parameters for mmWave and VLC links [112]

Table 0-1: Transmitted Signal Parameters

Parameter	mmWave link	VLC Link
RF Carrier frequency (Hz)	60 GHz or 40 GHz	Visible Light 400-800 THz
IF Carrier frequency (Hz)	3.48 GHz	15 MHz
Transmitted power out of RRLH (dBm)	-27	-45
Actual Bandwidth (MHz)	100	10
Modulation	64QAM	QPSK
RX USRP Gain (dB)	0	0
Cable loss (dB)	3	3

The mmWave and VLC link transmitter parameters are kept constant throughout the measurement collection process, but the transmission distance, angle, and location are varied.

Both the UE and the mmWave module require a 10 MHz reference signal, which is provided by the synchronisation clock system in conjunction with the RRLH. Figure 0-3, shows a diagram of a 10 MHz distribution as a point of reference [112].

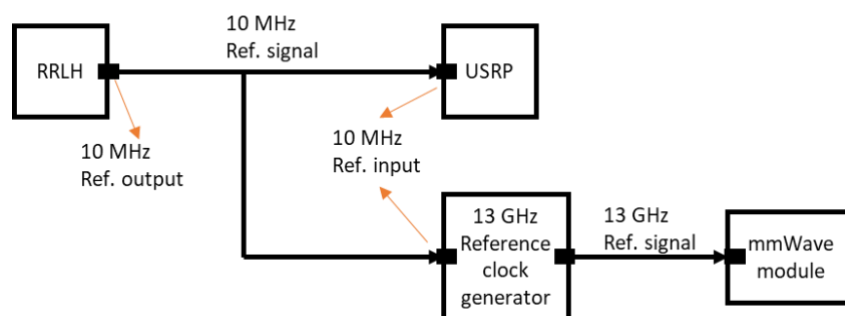


Figure 0-3: 10MHz Reference Distribution

4.3 Coverage Measuring Experimental Procedure

The practical indoor environment experimental setup consisted of an aluminium frame with (2.5 m*2.5 m*2.5 m) dimensions. Figure 4-4, shows the setup of the four LEDs used to conduct the testing. Also, the receiver gimbal on a ground level to point the receiver Photodiode towards the VLC LEDs. The testing strategy of the set up were always constant during data collection. The coverage tests were taken through MobaXterm which provided the EVM of the signal at different positions within the environment. The results were taken carefully after collecting approximately 100 EVM's, to make sure that the results obtained were as accurate as possible. The environment was unchanged to ensure that there are no external factors affecting the outcomes.

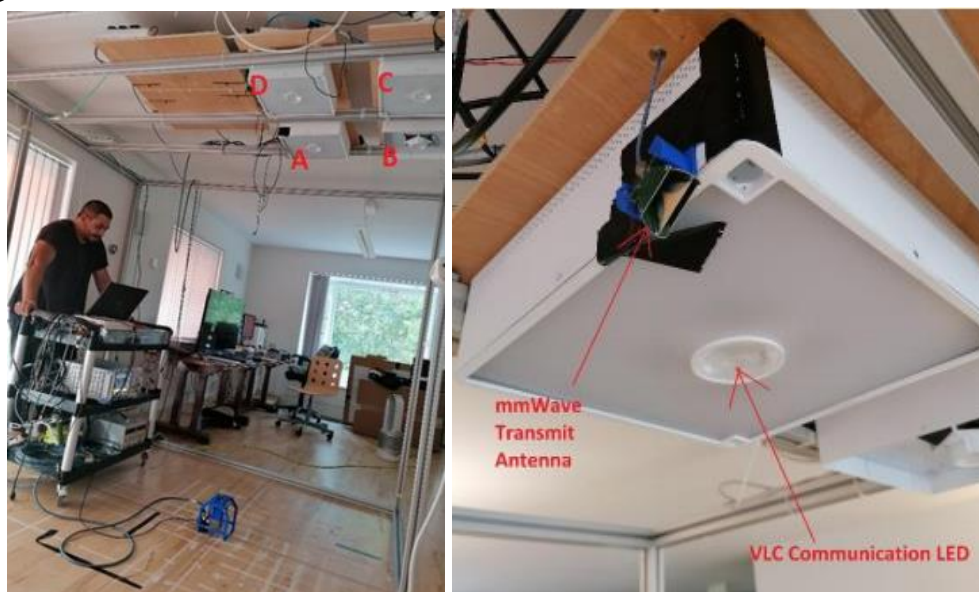


Figure 0-4: Experimental setup

4.3.1 VLC coverage

A plumb line is used to map the centre of each RRLH's communication light source onto a floor-level centimetre grid. As a result, the origin of each RRLH is designated at this location. In a vertical orientation, the VLC photodiode receiver module is fitted at the starting point, facing directly upwards [112]

The EVM signals measurements are taken at 6cm intervals, up to 54 cm in length, from the centre of the floor at each 45-degree angle. Before and after data recording, the EVM measurements are left to stabilise. Particularly, because the lens used to focus the received light has a long focal length, a slight horizontal translation away from the origin causes the received light path to 'miss' the receiver photodiode entirely, effectively eliminating any received signal. As a result, the Receiver for all VLC measurements is mounted on a custom gimbal. Keeping

the receiver photodiode's centre position along 2D floor grid while providing a way to angle receiver toward light source, thus ensuring long-distance LOS [112].

4.3.2 mmWave coverage

One mmWave polarised horn antenna was tested in this chapter. As shown in Figure 6, the antenna is attached to the side of an RRLH and is aimed downward. When the horn antenna's centre point was vertically lowered to floor level, the grid's starting point was established (origin point). For the reason of the antenna's orientation, the axes of each of the grids are aligned with the receiver and transmitter. Parallel to the long horn antenna, is the x-axis. An angle and a vertical orientation of the gimbal are used to examine the receiver module in both LOS and non-LOS (NLOS) scenarios. In order to achieve an 'angled orientation,' the receiver gimbal must be used. Between setting up the receiver and recording the data, the EVM measurements are allowed to stabilise. These tests were carried out both on the ground and at a height of 0.7 metres from the ground. This antenna is also set to 30 and 40 degrees from its vertical axis, but it remains at its base point in relation to that axis. The receiver is used in both a vertical and angled orientation during these angled transmitter experiments [112]. As the setups of VLC and mmWave's were established the results were as follows.

4.4 VLC Coverage Results

With the illumination LEDs turned off, the photodiode receiver was not angled toward the communication LED. The coverage for four VLC LED TXs EVM tests was determined at a distance of 2 m from the transmitter and with the Rx photodiode angled vertically up. The best performing Radio Light Head (RLH) is the RLH A, which has a 0.3 m radius of coverage [112].

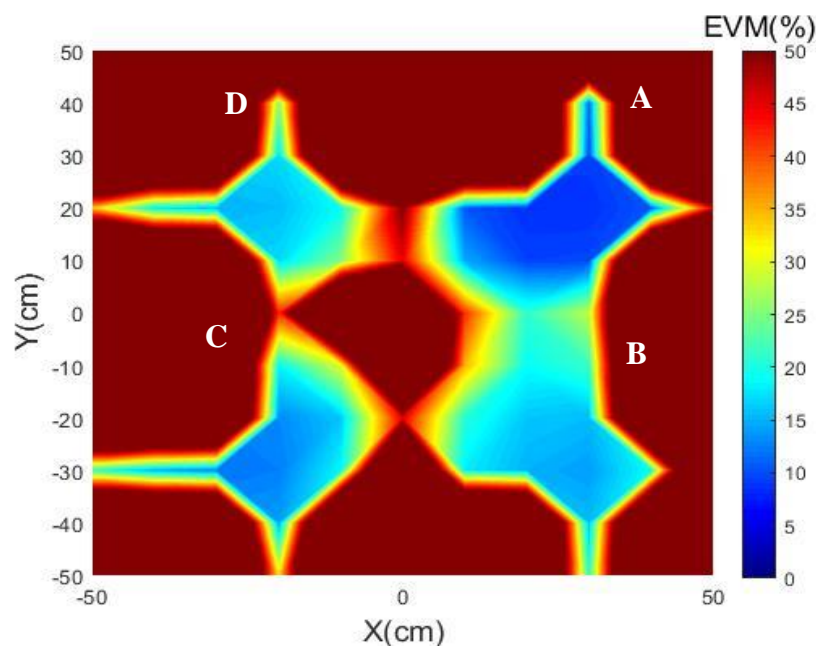


Figure 0-5: Four VLC TX LEDs pointing vertically down and Rx PD Non-Angled (pointing vertically up), EVM Test results at ground level

The results of the coverage of each of the four VLC LED TXs are shown in Figure 4-6. The test was performed at a distance of 2 m with the illumination LEDs turned off and the Rx PD angled toward the communication LED. The best performing RLH is A, as it provides a 0.5 m radius of coverage [112].

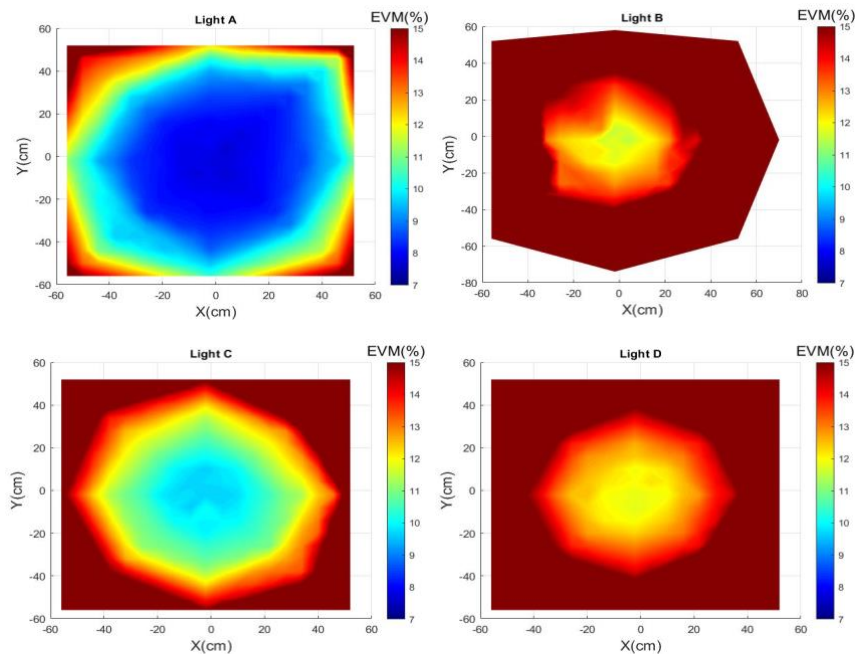
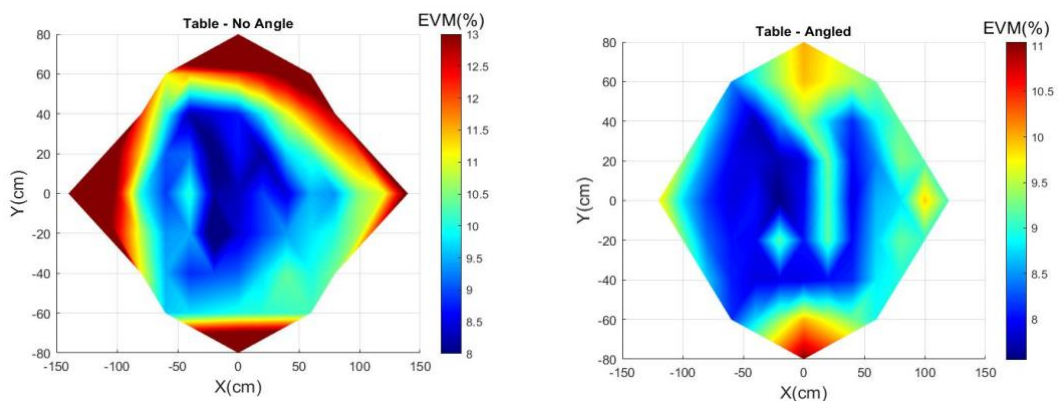


Figure 0-6: 4 Four VLC TX LEDs pointing vertically down and Rx PD Angled towards Tx, EVM Test results at ground level

4.5 mmWave Downlink Coverage Results

4.5.1 mmWave Transmit Antenna Pointing Vertically Down

The coverage for one mmWave Tx's EVM test at a height of 0.7 m above the ground is demonstrated in Figure 4-7. (1.3 m from the Tx antenna). The test was conducted with and without the Rx antenna angled toward the Tx antenna and the Tx pointed vertically downward.



(a) Without angling Rx toward Tx antenna

(b) With angling Rx toward Tx antenna

Figure 0-7: One mmWave Tx's, receiver at 0.7m above ground EVM Test

Most of the coverage region EVM was $\leq 8\%$ making, it suited for 64-QAM transmission (for 4-QAM this is 12% and for 16-QAM this is 10%). The propagation was greater in the x direction than in the y direction. As a result of the physical construction of the PCB Horn antenna, which only applies the horn slant in the x direction and not in the y direction, the x direction was 1.2 m and the y direction was 0.8 m [112].

Note: the antenna is polarised in one direction, both the transmit and receive antennas must face the same direction in order for the polarisations to align; otherwise, reception will be poor.

The sample results in Figure 4-8 shows the results of the coverage for one mmWave TXs EVM test at ground level (2.1 m from Tx antenna). The test was conducted with/without Rx antenna angled towards the Tx antenna, while the Tx pointing vertically down [112].

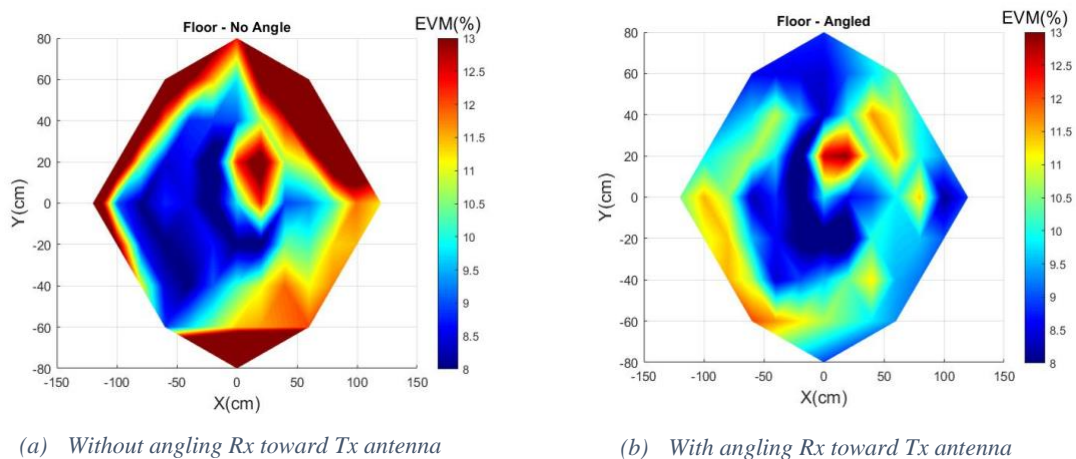


Figure 0-8: One mmWave TXs, receiver at 0m ground level EVM Test

The EVM in most of the coverage region was $\leq 8\%$ making it suited for 64-QAM transmission. The results show that angling the Rx towards Tx antenna shows better EVM than non-angled [112].

4.5.2 mmWave Transmit Antenna Point 30° from Vertical about antenna y-axis

The transmit antenna is angled 30 degrees along the room's x axis, and the receiving antenna is directed toward the transmitting antenna, resulting in a coverage area of at least 1.6 m in both the x and y directions, as illustrated in Figure 4-9b. Without directing, the receiver is limited to 0.8 m in the x direction and 1.2 m in the y direction. These measurements were taken on 17 September 2020 [112].

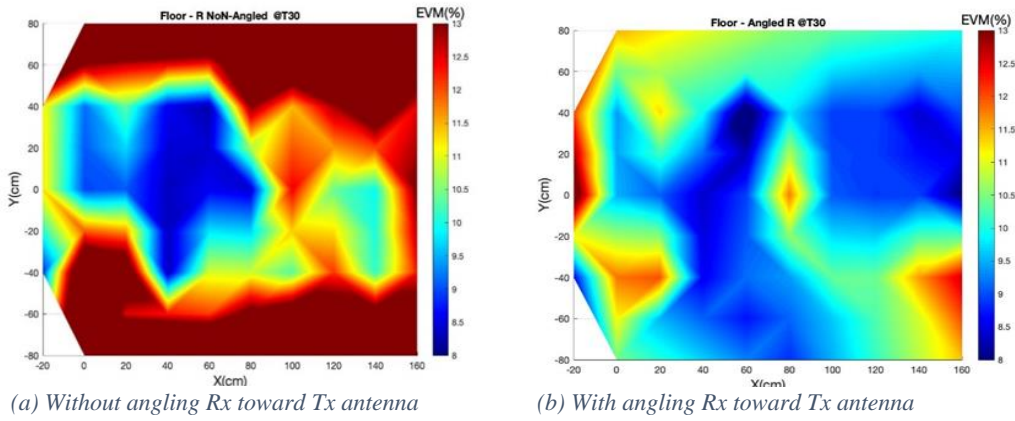


Figure 0-9: One mmWave TXs angled at 30o, receiver at 0m above ground EVM Test

The results were re-taken on 22nd September after the data was processed as shown in Figure 4-10; the new results were unexpectedly better. This, however, demonstrates that the mmWave system's performance is contingent on unknown external factors. As identical testbeds were used [112].

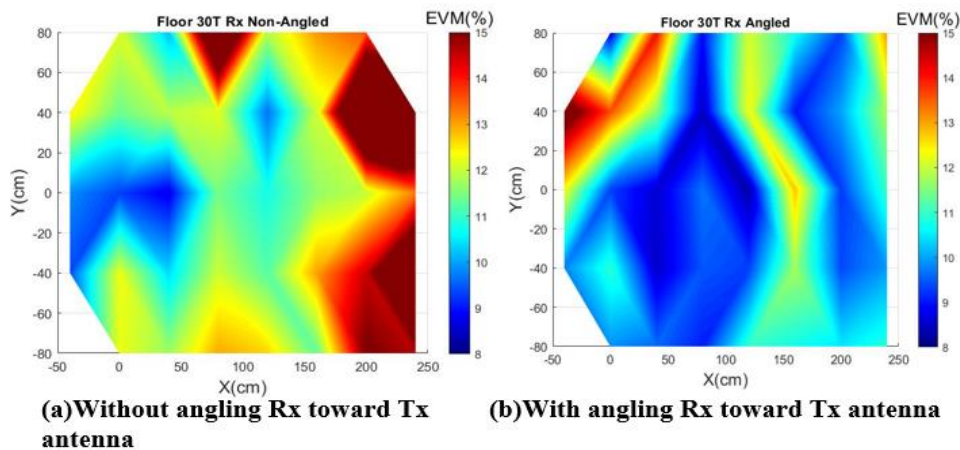


Figure 0-10: One mmWave TXs angled at 30, receiver at 0m above ground EVM Test

The measurements were tested once more, where the transmitting antenna was angled at 30 degrees, but at 0.7 m height above the ground as shown in Figure 4-11.

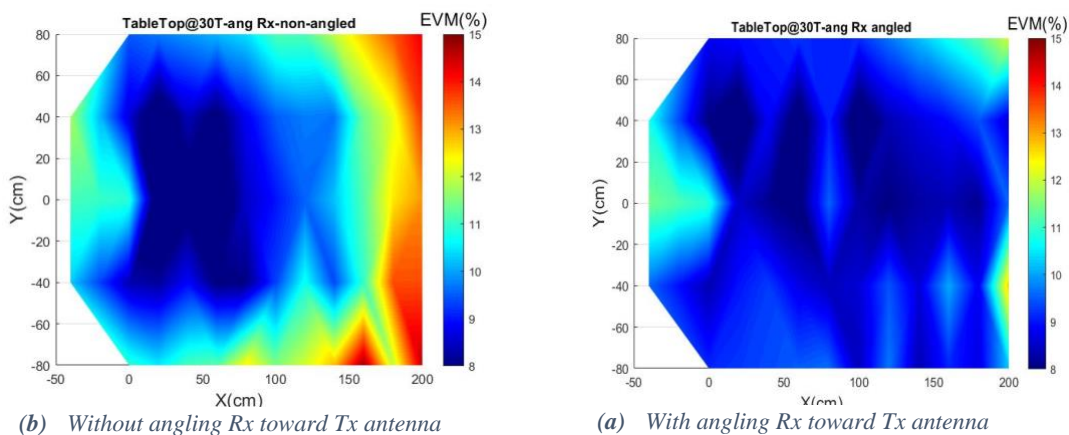
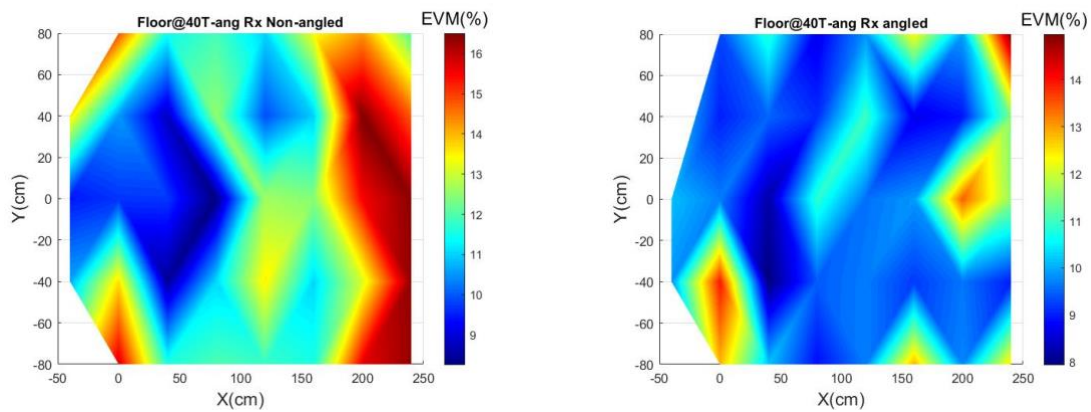


Figure 0-11: One mmWave TXs angled at 30°, receiver at 0.7m above ground EVM Test

The performance of the mmWave system does enhance when the Rx antenna is angled toward the Tx antenna and when the Tx antenna is located close to the Rx antenna.

4.5.3 mmWave Transmit Antenna Point 40° from Vertical about antenna y-axis

The transmit antenna is angled along the room in x direction by 40 degrees and the receiving antenna directed towards the transmitting antenna producing a coverage area of at least 1.6 m in both x and y direction as shown in Figure 0-12.



(a) Without angling Rx toward Tx antenna

(b) With angling Rx toward Tx antenna

Figure 0-12: One mmWave TXs angled at 40o, receiver at 0m above ground EVM Test

The results shown in Figure 0-12, shows that the performance of the mmWave system improves with Tx angling at 40 degrees.

4.6 Challenges (VLC and mmWave)

While measuring the coverage of the VLC and mmWave certain challenges were encountered. As expected, that the coverage of the four LED's was supposed to have the same coverage distance. Light A has shown a high performance compared to the other LED's as it provided 0.5 m of radius coverage, while Light C presented a less performing coverage. Whereas Lights B and D exhibited poor coverage results. The following results which showed a huge difference between the coverage areas of the different lights even though all of them were manufactured by the same company. Due to an unknown factor the three other lights did not show a high performance similarly to RLH A.

The mmWave coverage tests were taken while angling and without angling Rx antenna towards the Tx antenna. Without angling the antenna, it has shown less performing results as to with angling the antenna. While angling the transmitting antenna on the 17th of September 2020 at 30 degrees without angling the Rx, it showed very poor coverage results. The results were reconducted on the 22nd of September 2020 to try to discover why poor results were obtained. However, the new results were an unexpected improvement. As both results were

obtained in identical test beds. This conveys that the performance of the mmWave system is dependent on indefinite external factors. After discussing the results of the coverage for both technologies the following sections focuses on the accuracy procedure and its results.

4.7 Location Accuracy Measuring Procedure

4.7.1 System Architecture Diagram

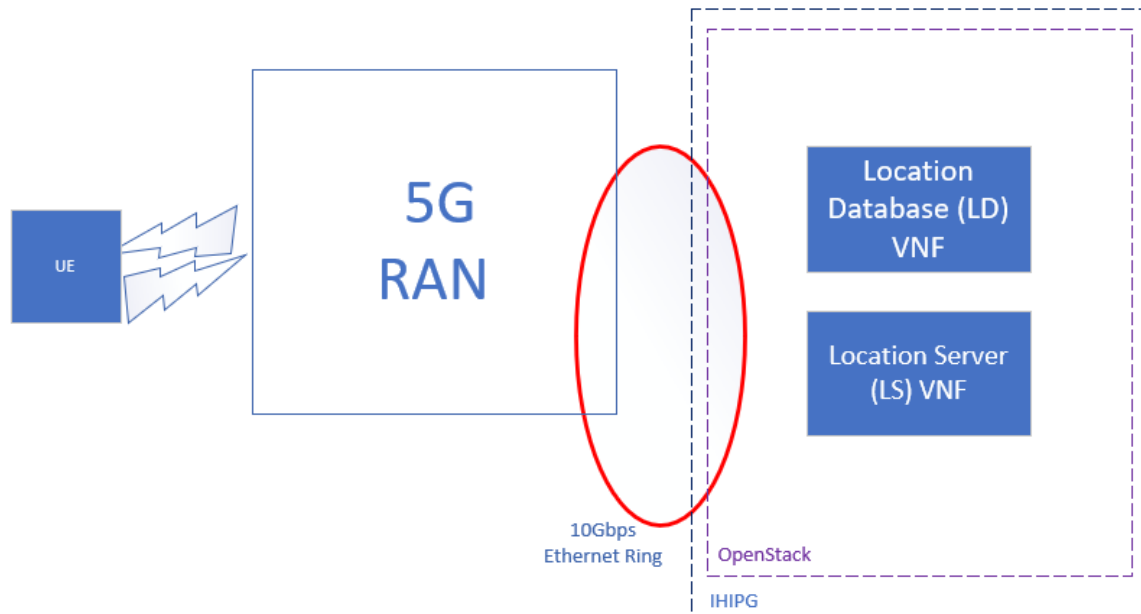


Figure 0-13: 5G positioning system architecture

The 5G positioning system diagram, shown in Figure 0-13, consists of two subsystems, namely: the 5G Radio access network (RAN) and the IHIPG. Both subsystems are linked together through 10 Gbps Ethernet ring. The 5G RAN consists of RRLH controller, VLC RRLHs (LEDs) as many as required up to 32 and any number of UEs in the room. The IHIPG consists of the OpenStack, that integrates the NFV technologies, which provide a flexible and extensible infrastructure. The Location Server (LS) is a VNF, that is implemented within the IHIPG to estimate the location (coordinates) of the UE. Also, another VNF that is implemented is the Location Database (LD), which stores three different sets of parameters; Received Signal Strength (RSS), Estimated Coordinates, Coordinates of all LEDs.

4.7.2 Experimental Setup

The Integer House Lab in the Building Research Establishment (BRE) at Watford was where the experiment was conducted. The aim was to evaluate both the localisation and coverage performance within a home scenario using the Indoor 5G system.

The coverage tests were obtained through MobaXterm program as it gives a live feed readout of the Error Vector Magnitude (EVM) of the signal at different positions within the

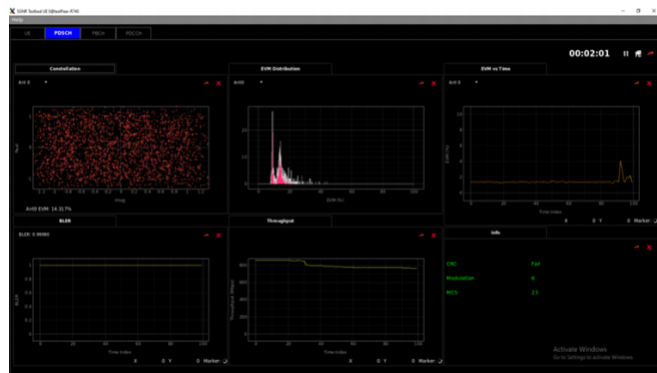


Figure 0-14: MobaXterm

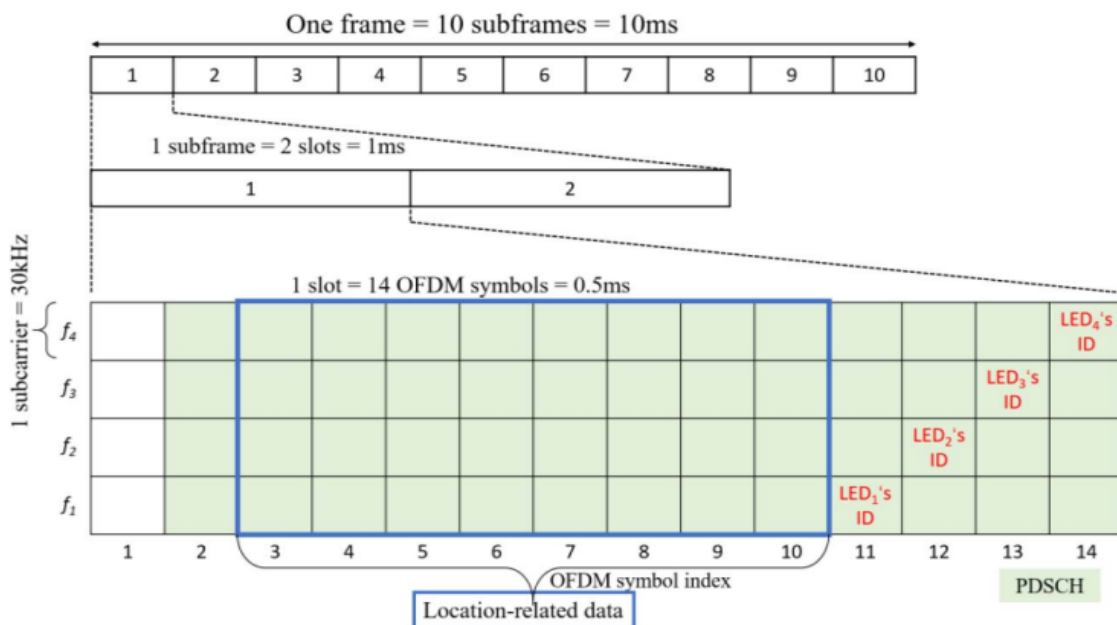


Figure 0-15: 14 OFDM symbols, the geographic data

environment as shown in Figure 4-14. Using the 5G compliant VLC LED access points, the Received Single Strength (RSS) VLC localisation measurements were recorded. This was performed using the last four OFDM symbols in a sub-frame slot to transmit geographic data from the four VLC LEDs (A, B, C and D) successfully as shown in Figure 4-15. In addition, the RSS geographic data can be carried by all of their 192 subcarrier frequencies.

4.7.2.1 Recording of distance from VLC RSS measurements from the Radio-Light Heads

The floor plan for the VLC measurement points coverage as demonstrated in Figure 4-16. The red lines were the measurement points used to obtain the data. The data was obtained through a live readout feed program called MobaXterm shown in Figure 4-14. The data was not only obtained in a “.CSV” format but also each file had about 100 Error Vector Magnitude (EVM) measurements that were captured. It was organised into

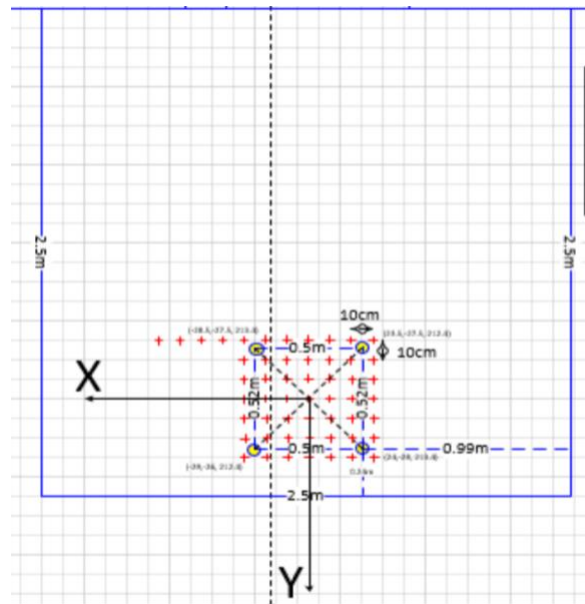


Figure 0-16: VLC floor measurement points

column x and column y. Column x presented the numerical order of how many EVMs were taken and column y presented the EVM value as shown Appendix 2

Appendix Appendix 2

Appendix 2

Appendix Appendix 2

Appendix Appendix . Each .csv file acquired manually and processed to get the average of all the EVMs captured so to perform this to 60-70 measurement files requires a lot of time, so a python script was developed to allow a fast data processing so the results can be processed quickly. This python script is explained in section 4.7.2.3.

4.7.2.2 mmWave location data

The floor plan for the VLC measurement points coverage was demonstrated in points. The red lines were the measurement points used to obtain the data. The data was obtained through a live readout feed program called MobaXterm shown in Figure 4-14. The data was not only obtained in a “.CSV” format but also each file had about 100 EVM that were captured. It was presented into columns *x* and *y*. Column *x* presented the numerical order of how many EVMs were taken and column *y* presented the EVM value as shown Appendix 1

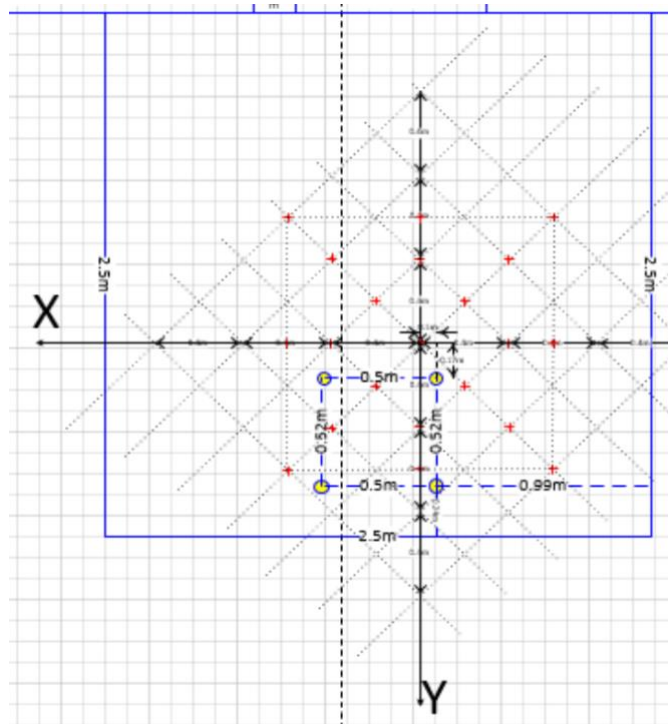


Figure 0-17: mmWave floor measurement points

Appendix Appendix 1

Appendix 2

Appendix Appendix Appendix 1

Appendix Appendix 1. Each .csv file required manually to get the average of all the EVMs captured and to do this to 60-70 measurement files requires a lot of time so a python script was developed to allow a fast data processing so the results can be acquired faster. The script is explained in section 4.7.2.3.

4.7.2.3 Data process script

The data process script was developed using python, where it adds all the files inside the test folder into a list and it reads the file name as it is named in coordinates X, Y and then calculate the average inside each .csv file and save them all into a .txt. The file would show the coordinates and a Z value, which is the average EVM as shown in Figure 4-18. The snippet of the python script is shown in Figure 4-19.

Floor@30T-ang Rx non-angled.txt - Notepad

```
File Edit Format View Help
| 20,80 Z=0.118562584164
120,-80 Z=0.12662963712000003
0,80 Z=0.121445648312
80,80 Z=0.17890628361799998
200,-80 Z=0.150832250236
160,-80 Z=0.11290714311500002
200,40 Z=0.19121223771899995
200,-40 Z=0.14520923411800007
80,0 Z=0.11433801341299997
240,0 Z=0.13279334307000001
-40,-40 Z=0.09384271627660001
-40,0 Z=0.09858033901630002
80,40 Z=0.12174661338400002
40,0 Z=0.08729511940490003
160,80 Z=0.13084328448300003
```

Figure 0-18: Script Output .txt file

```

import csv
import pandas as pd
import os
import glob

path = '/home/kareem/Desktop/csv_files' # use your path
allFiles = glob.glob(path + "/*.csv")
file_list= []

for file in allFiles:
    file_list.append(file) #Add all files to a list

d=0
while d<3:

    f=pd.read_csv(file_list[d])
    filename=os.path.splitext(os.path.split(file_list[d])[1])[0]
    y=filename.split(',')[1]
    x=filename.split(',')[1]

    with open(file_list[d]) as li:
        total=0
        li.readline()
        f = f.drop
        for row in csv.reader(li):
            total = total + float(row[1])

        average=total/1000
        print(average)

        text_file=open("output.txt", "a")
        text_file.write(str(d+1)+" ")

        text_file.write("X=" + str(x) + " " + "Y="+str(y) + " "+"Z="+ str(average)+"\n")
        text_file.close()

    d=d+1

```

Figure 0-19: Data processing Script

After

collecting the Received Signal Strength measurements for both technologies VLC and mmWave, they were used to find an optimal solution using simulated annealing algorithm, to discover the most accurate position of the light heads.

4.8 Data Optimisation for Location Measurements Accuracy

4.8.1 Positioning algorithm

The proposed algorithm assesses the estimated optimised solution of the data, is called Simulated Annealing-based Localisation (SAL). SAL was implemented in MATLAB. The localisation data was optimised for both the Rx and Tx.

The example shown in Figure 4-15, three out the four (f1, f2, f3) LED's ID are not only the dedicated subcarrier frequencies but also the three highest received powers. Thus, calculating the distance d between the UE and the LED can be achieved using the following equation (1).

$$d = \sqrt{\frac{(m+3) \left(\frac{(m+1)A_r h^{(m+1)} P_T}{2\pi} \right) \frac{P_T}{P_R}}{}} \quad (1)$$

A_r : the effective area of the receiving surface of the UE.

h : the vertical distance between the UE and LED, which is a constant.

$$m = \frac{-\ln 2}{\ln(\cos(\varphi_{1/2}))} \quad (2)$$

m : the order of Lambertian emission, which is relative to the semi-angle at half power of the LED denoted as $\varphi_{1/2}$.

$$P_R = H(0) * P_T \quad (3)$$

P_R : the received power of the UE

P_T : the transmitted light power of the LED

$H(0)$: the VLC Line of Sight (LOS) channel gain between the UE and LED, can be shown in equation (4).

$$H(0) = \frac{(m + 1)A_r \cos^m(\varphi) \cos(\theta)}{2\pi d^2} \quad (4)$$

where φ is the radiation angle between the UE and the LED, and θ is the angle of light incident to the receiving surface of the UE. Therefore, the distance d_1 , d_2 and d_3 can be attained correspondingly.

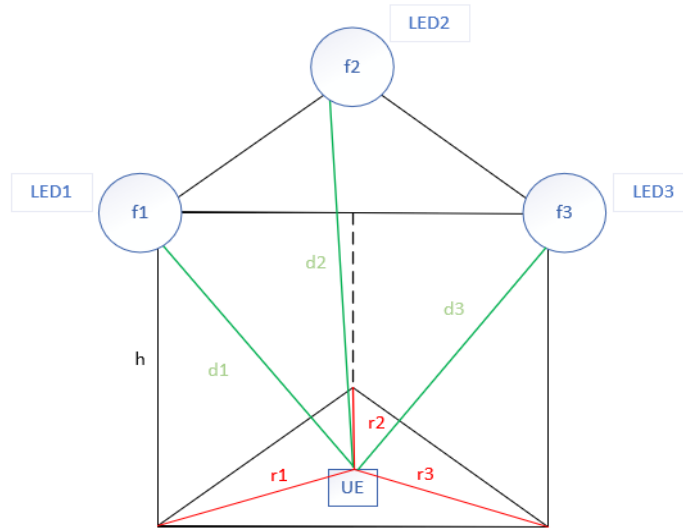


Figure 0-20: Positioning algorithm diagram

The projection distance r_1 , r_2 , and r_3 between the UE and LED can be expressed as shown in equation (5).

$$r = \sqrt{d^2 - h^2} \quad (5)$$

Thus, the estimated coordinates of UE can be calculated as shown in equation (6)

$$\begin{cases} (x_e - x_1)^2 + (y_e - y_1)^2 = r_1^2 \\ (x_e - x_2)^2 + (y_e - y_2)^2 = r_2^2 \\ (x_e - x_3)^2 + (y_e - y_3)^2 = r_3^2 \end{cases} \quad (6)$$

where, (x_1, y_1) , (x_2, y_2) and (x_3, y_3) are the known coordinates of three LED respectively. (6) can be formed in a matrix format as (7)

$$BX_e = C \quad (7)$$

where B , C and X_e are defined as

$$B = \begin{bmatrix} x_2 - x_1 & y_2 - y_1 \\ x_3 - x_1 & y_3 - y_1 \end{bmatrix}, X_e = \begin{bmatrix} X_e \\ Y_e \end{bmatrix} \quad (8)$$

$$C = \begin{bmatrix} \frac{d_1^2 - d_2^2 + x_2^2 + y_2^2 - x_1^2 - y_1^2}{2} \\ \frac{d_1^2 - d_3^2 + x_3^2 + y_3^2 - x_1^2 - y_1^2}{2} \end{bmatrix} \quad (9)$$

The estimated X_e can then be obtained by the linear least squares.

$$\widehat{X}_e = (B^T B)^{-1} B^T C \quad (10)$$

4.8.2 SA results and analysis

As the actual semi-angle of the LED's at half power and the best OFDM sub-carrier for the measurement of RSS was not known, the Artificial Intelligence (AI) simulated annealing algorithm was used to find the solution to the optimum parametrisation problem. Figure 4-21 and Figure 4-22 provide results with arbitrarily selected sub-carrier 4 and semi-angle with half power that produced a Lambertian mode $m=1$. By randomly selecting the semi-angle of the LED's at half power and the OFDM sub-carrier, the results of the average location error of x and y are 22.5 and 21.6 respectively.

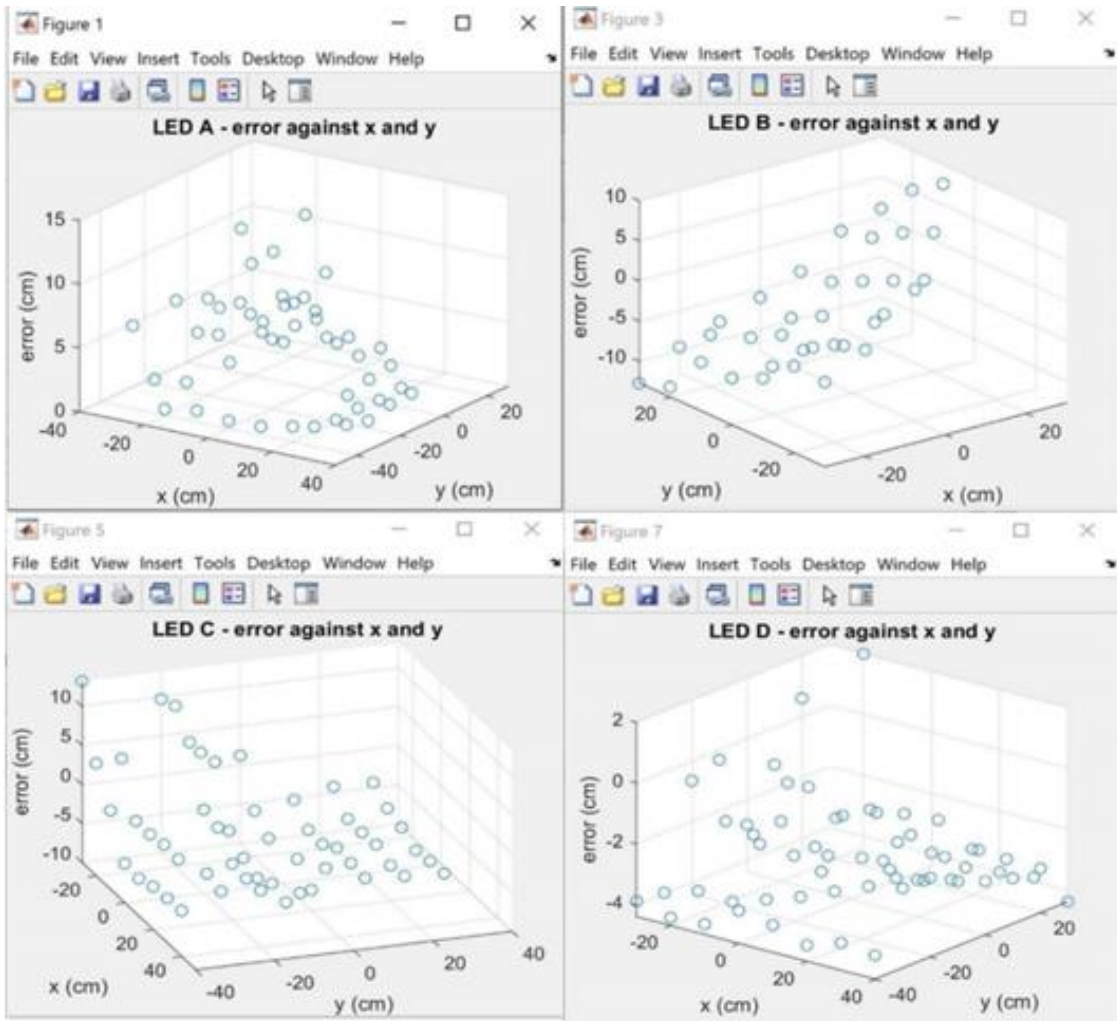


Figure 0-21: Error against x and y for LEDs A, B, C, D with $m=1$ and OFDM = 4

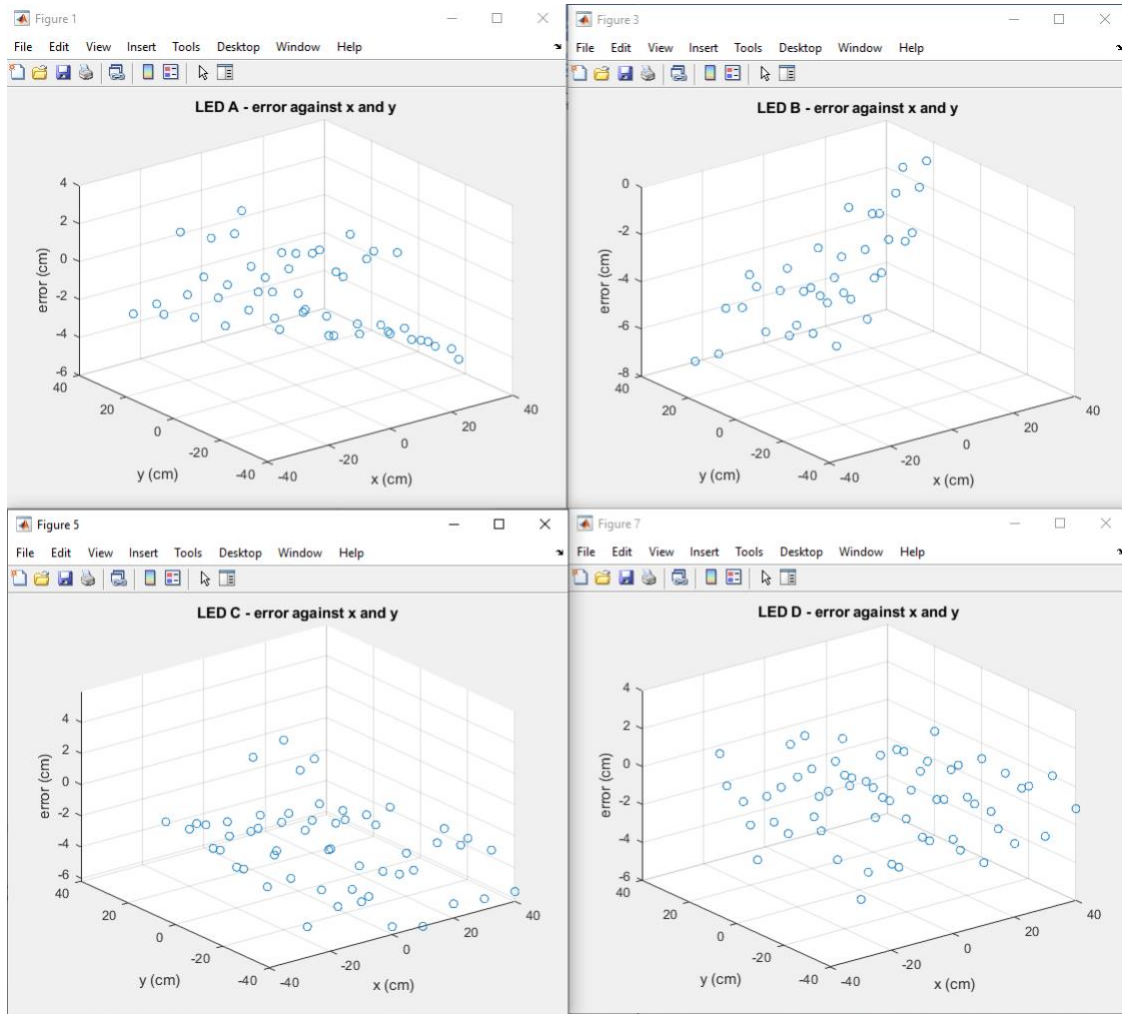


Figure 0-22: Error against angle from Communication LED for LEDs A, B, C, D with $m=1$ and OFDM = 4

The Simulated Annealing Solution (SAL) is constructed in an iteration process using data until the proposed data can no longer be improved. Once the localisation data had been optimised, the optimal sub-carrier and optimum 'm' for all LEDs are found. The results showed many improvements and that the problem was efficiently resolved based on the optimisation derivative. By selecting the best semi-angle LED at half power and OFDM sub-carrier, simulated annealing reduced the average location error to $x=11.09$ and $y=11.63$.

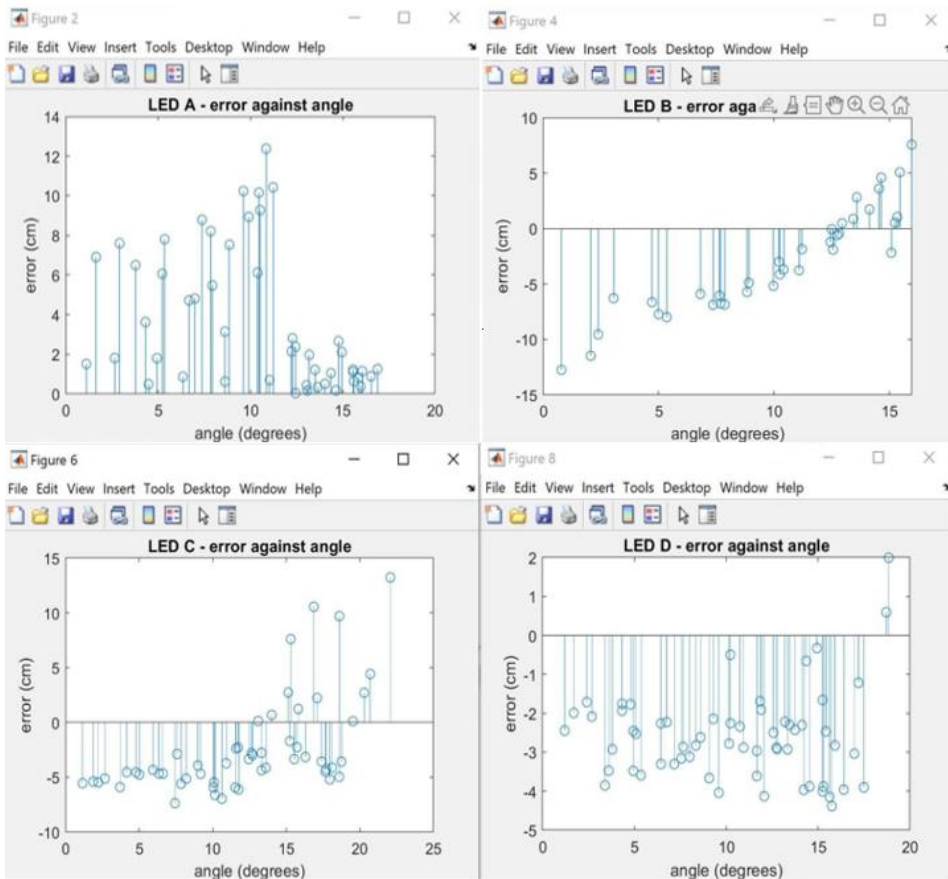


Figure 0-23: Error against x and y for LEDs A, B, C, D with simulated annealing optimised m and OFDM numbers

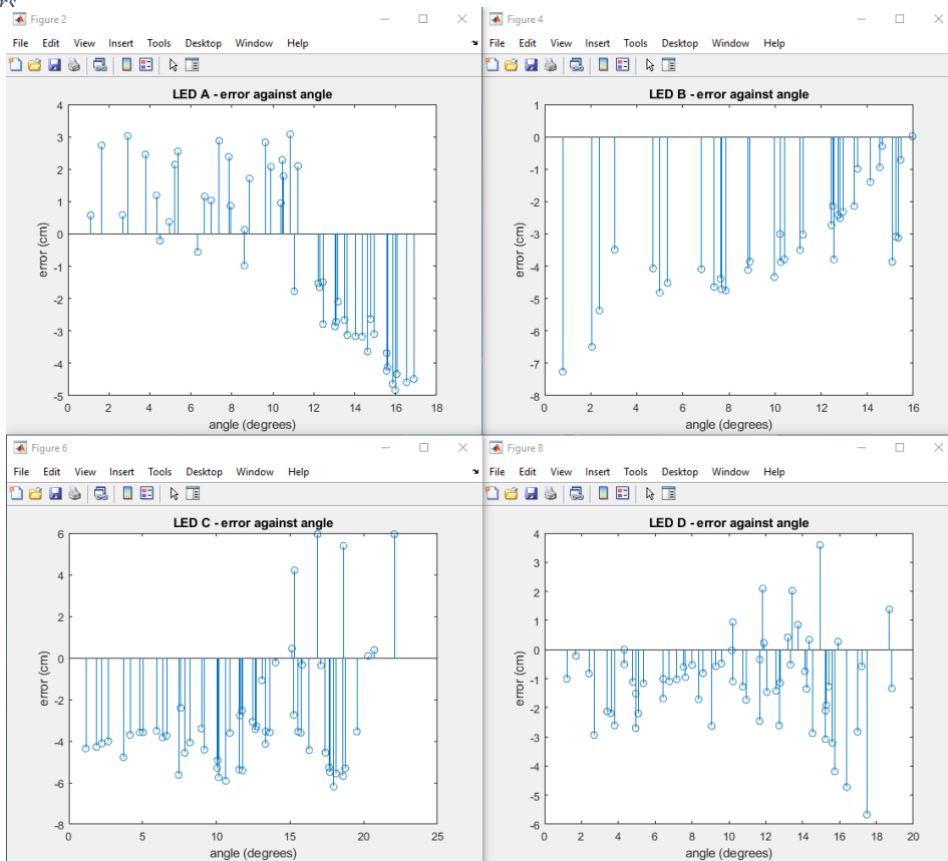


Figure 0-24: Error against angle from Communication LED for LEDs A, B, C, D simulated annealing optimised m and OFDM

After the SA algorithm has been implemented and the distance error has been reduced, the idea came of what if the number of iterations accepted gets changed, would it make a difference and improve the results? Initially, it was set to 20 iterations. Moreover, the maximum number of runs, rejections and accept has been altered to see if the average distance error could be further reduced. The number was set to go up 20 each time as shown in a Table 0-2.

Table 0-2: Average Distance Error based on change in Iterations

LED	ΔIteration	Average error
1: LED A	20	2.4361
	40	2.3696
	60	2.3475
	80	2.2809
2: LED B	20	3.3003
	40	3.3003
	60	3.1578
	80	3.1578
3: LED C	20	3.8187
	40	3.7359
	60	3.7359
	80	3.7359
4: LED D	20	2.1386
	40	1.9692
	60	1.6751
	80	1.6751

*ΔIterations: the change for iterations

Table 0-2, shows the four led lights and each was tested up to 80 iterations. The results concluded one of two of outcomes. Either the average error to decrease then goes flat or decreases. As shown above, LED A kept decreasing during all the iterations until it reached the average distance error it became 2.2809. LED B went flat in the 2nd iteration then it decreased to 3.1578 and went flat. LED C went flat in the 2nd iteration staying at 3.7359. Finally, LED D, which had the most reduction in the average distance error out of all the LEDs, which was 1.6751.

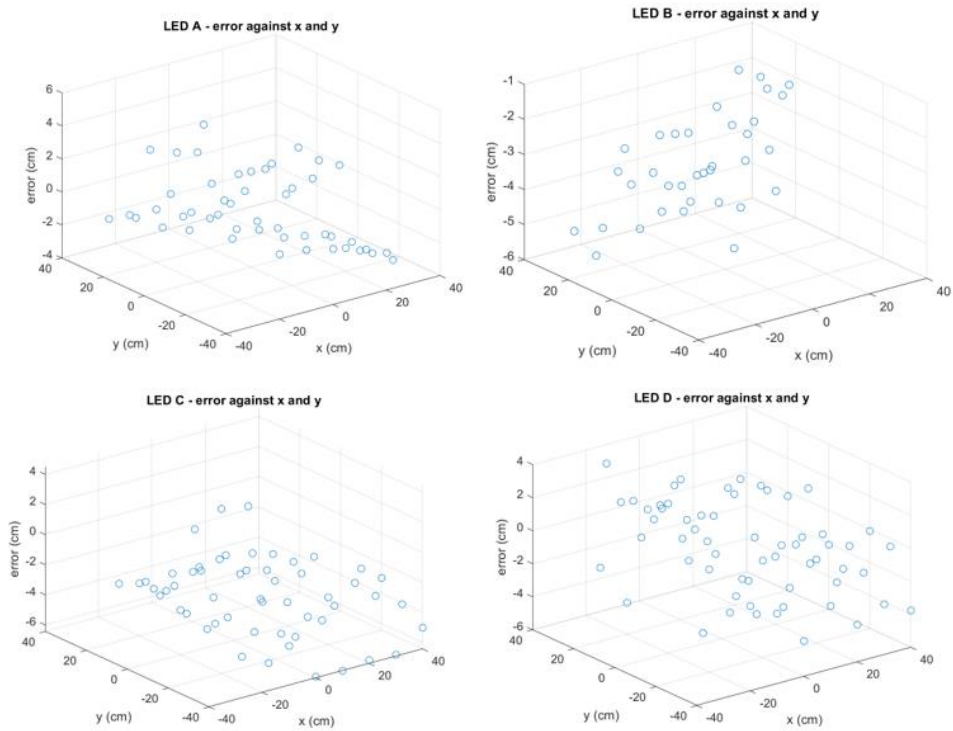


Figure 0-25: Error against x and y of 80 iterations for LEDs A, B, C, D with simulated annealing optimised m and OFDM numbers

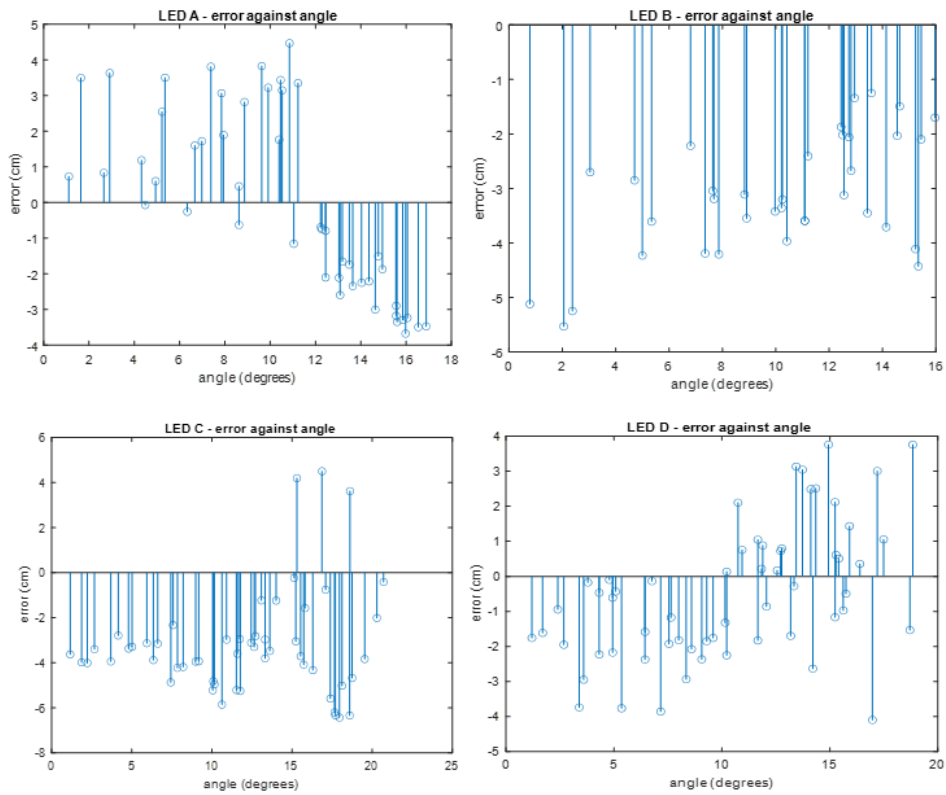


Figure 0-26: Error against angle from Communication LED for LEDs A, B, C, D simulated annealing optimised m and OFDM numbers

It is evident from Figure 4-25 and Figure 4-26, that the results obtained by using an iteration count of 80 are quite impressive. By arbitrarily selecting the semi-angle at half power of the LED and OFDM subcarrier the average distance of minimised error in x and y is 9.2741 and 13.2114 respectively.

4.9 Challenges

This chapter was not fully completed due to the time required to integrate the mmWave in the IoRL system implementation, which is current ongoing work. Due to the aforementioned challenge the mmWave accuracy was never obtained. The localisation data for the Rx and Tx of the average location error showed average results, however it was assumed that by manipulating the iteration process better average location results would be obtained. The iteration process was altered from 20 up to 80 iterations to test the proposed assumption. This concluded a reduction in the average distance error.

4.10 Summary

Many people rely on location-based application services, which must be accurate, dependable, and able to work in conjunction with outdoor positioning. It is therefore extremely difficult to deliver the same level of location accuracy and reliability as outdoors when using LBS. An indoor LBS could be useful for a variety of life-saving services, including security and emergency response.

The location positioning of the RRLHs from measurement data collection was successful in obtaining distance error accuracies as low as 2.37 cm and no larger than 3.74 cm. The localisation and coverage performance were evaluated. It has been possible to find the best parameters for the VLC LED Remote Signal Strength (RSS) estimates using simulated annealing technique. Due to the LED's actual half-power semi-angle, and the best OFDM subcarrier for measuring RSS being unknown, a simulated annealing algorithm was used to select the most optimal parameters.

Furthermore, after using the SA algorithm and manipulating the iterations, it was clear that some results improved while others remained unchanged. Overall, the average amount of error was reduced, through making a comparison between these outcomes and those obtained without making use of the SA algorithm. The results indicated significant improvements by finding that the method used could find an optimal solution, whilst surpassing the optimally localised estimates of distances.

The received signal strength measurements were used in a simulated annealing algorithm to populate the database with the most accurate position of the Light Heads. Once this is known, the triangulation can be used to determine the distance of the UE to each of the Radio Light Heads and saved on the location database. The location server uses the information and translates into the position of the UE which is stored on the location database. conclusively, the coverage and accuracy location data optimisation have shown promising results. The average distance of minimised error in $x = 9.2741$ and $y=13.2114$. The following chapter proposes an indoor location security architecture that aims to protect the system from DHCP starvation attack.

Chapter 5: 5G Contextual Aware Indoor Location Security

5.1 Chapter Outline

The objective of this chapter is to protect the network from malicious attacks (DHCP starvation attack) using VNF on the multiaccess edge cloud that provides a scalable solution to ensure user connectivity at all times. This chapter discusses the proposed solution with the evaluation of the implementation of the scripts to test its effectiveness. This chapter is structured as follows: Section 5.2 provides an introduction. Section 5.3 presents related work that is currently being implemented in the field. Section 5.4 provides the proposed security solution. Section 5.5 presents the implementation. Section 5.6 evaluates the testbeds strategy. Section 5.7 provides an analysis of the results. Section 5.8 provides a summary.

5.2 Introduction

Currently, 5G communication is the focus of industry, academia and governments all over the world. 5G is driving many new network capabilities requirements. As 5G aims to utilise a lot of the promising network technologies, including Software Defined Network (SDN), Network Function Virtualization (NFV), Network Slicing, Cloud Computing, Information Centric Networking (ICN), and Multi-Access Edge Computing (MEC). To be able to support a massive number of connected devices, integrating the aforementioned advanced technologies and innovating new techniques will undoubtedly bring significant challenges for security and privacy [113]. Hence, secure mechanisms, network architectures, and protocols are required as a basis to address the 5G problem and adhere to both security by operations and by design rules. Moreover, 5G networks will see greater volume of user data and network traffic than before. AI must be used for the big data security solutions to strive to handle the increased data quantities [113].

SDN has emerged as one of the most significant and promising networking paradigms in recent years [114]. SDN's primary advantage is the ability to decouple the data and control planes, which abstracts away the underlying network infrastructure from the applications. As a result, the network's management can be logically centralised. Apart from the numerous applications of SDN [114], it has recently emerged as an intriguing option for providing security in more effective and flexible ways in today's communication networks [115].

Additionally, the majority of network device manufacturers are already supporting SDN via the OpenFlow protocol with their physical and virtual equipment. SDN enables the management of heterogeneous networks to be standardised. Applications developed for the

SDN controller will run without modification on a variety of SDN-enabled devices in both physical and virtual environments [113].

Numerous papers discuss malware detection using SDN. Jin and Wang [116] examined the behaviour of malware on mobile devices. They proposed and implemented several detection algorithms for mobile malicious software using SDN on the basis of the acquired knowledge. Their system was capable of performing real-time traffic analysis and detecting malicious activity using only the packets used to establish connections. The authors of [117] designed and developed an SDN-based architecture for malware analysis with the goal of dynamically altering the network environment in response to malicious software actions. They demonstrated that this approach is capable of triggering significantly more malware events than conventional approaches [113].

5.3 Related work

According to [113], there are a limited number of papers, that are related to SDN and DHCP Security attack. In [118], it was proposed that an internal, specialised DHCP server is no longer required. The controller handles all DHCP requests and offers, and any other traffic is ignored. Unfortunately, this solution does not scale well, as the controller is required to manage IP leases and perform DHCP transactions, both of which require additional CPU resources and memory. This could have a detrimental effect on the network's overall performance and security [113].

The authors in [119] have proposed Network Flow Guard (NFG) to protect the system from rogue DHCP server. This solution is more scalable because it leverages the infrastructure's existing DHCP server rather than implementing the functionality in the controller. The NFG implements whitelisting of valid DHCP offers. Each time a server (legitimate or rogue) sends a DHCP offer, it is inspected and only whitelisted offers are allowed and forwarded to the client. Regrettably, examining each offer also creates scalability issues. Additionally, changing the DHCP server configuration will necessitate additional steps to reconfigure NFG, which may result in unexpected behaviour [113].

Finally, the authors of [120] propose a solution to the problems of rogue DHCP servers, starvation, and lease attacks. It works by inspecting each DHCP packet and comparing it to a hardcoded whitelist. Unfortunately, there was no mention of an appropriate research methodology or experimental results. All proposed solutions are incompatible with dynamic, scalable, virtualized or cloud environments. If any changes are made to the network infrastructure (additional hosts, DHCP reconfiguration, etc.), the network will behave

unpredictably without updating the applications listed above. This can result in additional problems, such as unstable work, or exposure to security threats [113].

5.3.1 Dynamic Host Configuration Protocol (DHCP)

In order to understand how DHCP starvation attack works, a complete understanding of the DHCP protocol is required. DHCP stands for Dynamic Host Configuration protocol, and the main purpose of this protocol is to provide an IP address for each client who connects to the network, as well as more important information such as the IP addresses of the gateway, DNS server, and much more.

This protocol consists of 4 stages that must occur for the successful assignment of an IP address for any device. The 4 stages consist of 4 messages being exchanged by the server and the client.

Figure 5-1 shows, the 4 stages of assigning an IP address to a client. The process is initiated with the client broadcasting a discover message where the client asks if there is any DHCP server, then waits for a reply. Subsequently, the server sends an offer message to the client offering them an IP address and many other information. Following, the client responds with a Request message to obtain the offered IP address, and lastly, the server replies with an Acknowledgement message assigning the client with the offered IP address. Moreover, DHCP has more additional messages such as DHCPDECLINE, DHCPRELEASE, and others [121].

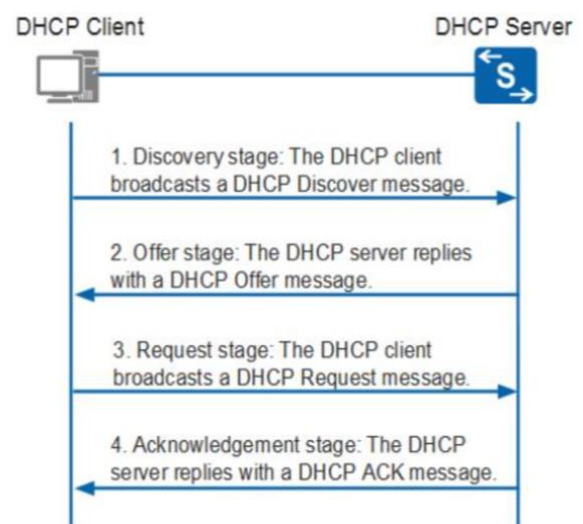


Figure 0-1: DHCP 4 Stages

It is a very simple protocol that is present in all types of networks, however, this protocol does not have any security measures implemented. Due to this fact, many malicious users were able to discover some vulnerabilities in it and were able to compromise them. The next section will be explaining how the DHCP protocol can be attacked leading to other security issues.

5.2.1.1 Current DHCP Mitigation Solutions

5.2.1.1.1 Port Security

Port security is a feature added by Cisco to their switches [122]. This feature has 3 different features included that could help in mitigating DHCP attacks.

5.2.1.1.1.1 Specifying trusted MAC-addresses

This method relies on specifying a list of the trusted MAC addresses. This list is saved in the DHCP server, and it only allows the trusted MAC addresses to communicate with it. However, this method has some drawbacks. This method cannot be applied in public networks as new clients connect to it on a daily basis. Also, attackers can overcome this solution by attacking one of the trusted machines and denying its service, then use its MAC address to communicate with the DHCP server [123].

5.2.1.1.1.2 Limiting number of MAC addresses per port (Port security):

This method is also referred to as port security, and it operates by assigning a limited number of MAC addresses on each port. For instance, each port could have maximum 3 MAC addresses allowed. If the attacker sends more than 3 DHCP Discover messages, the port will have 3 MAC addresses occupied, hence, any other packet will be discarded. However, the malicious client could still pass this security feature by changing his MAC address in the ethernet header, while still using a fake MAC address in the DHCP Discover packet [123].

5.2.1.1.1.3 Sticky MAC address:

This is one of the methods that are included in the port-security feature. Whenever a client connects to the switch on a specific port, the port saves the MAC address and does not accept any communication except from this MAC address. Any other machine that tries to connect to the same port will be denied access and the port will be disabled. However, the attacker can still overcome this feature by editing the MAC address in the ethernet header to match the same MAC address that is saved on it, and still send Discover messages using fake MAC addresses in the DHCP message.

5.2.1.1.1.4 Port Security and specifying trusted MAC addresses:

This method uses a combination of both solutions explained above. This approach makes it harder to an attacker to overcome it as it takes the advantages of both solutions and combines them. On the other hand, this solution is very rigid and cannot be applied in public networks [123].

5.2.1.1.1.5 Detecting DHCP message rate:

Another way of mitigating DHCP attacks is by having a system that counts the rate of DHCP messages in a time period. The system will have a threshold for the normal amount of DHCP messages that can be sent in a time period, however, if the rate goes higher than the threshold then the system should be able to detect an attack [124]. Following, more procedures could take place in order to stop the attack. Nonetheless, this system is unreliable as it can have

many false negatives due to times where there are many clients connecting to the network. Also, the attacker could reduce the rate of sending the DHCP messages in order to avoid being detected.

5.4 Indoor Location Security Application

This section demonstrates the proposed security architecture for 5G aware indoor location security.

5.4.1 Security architecture

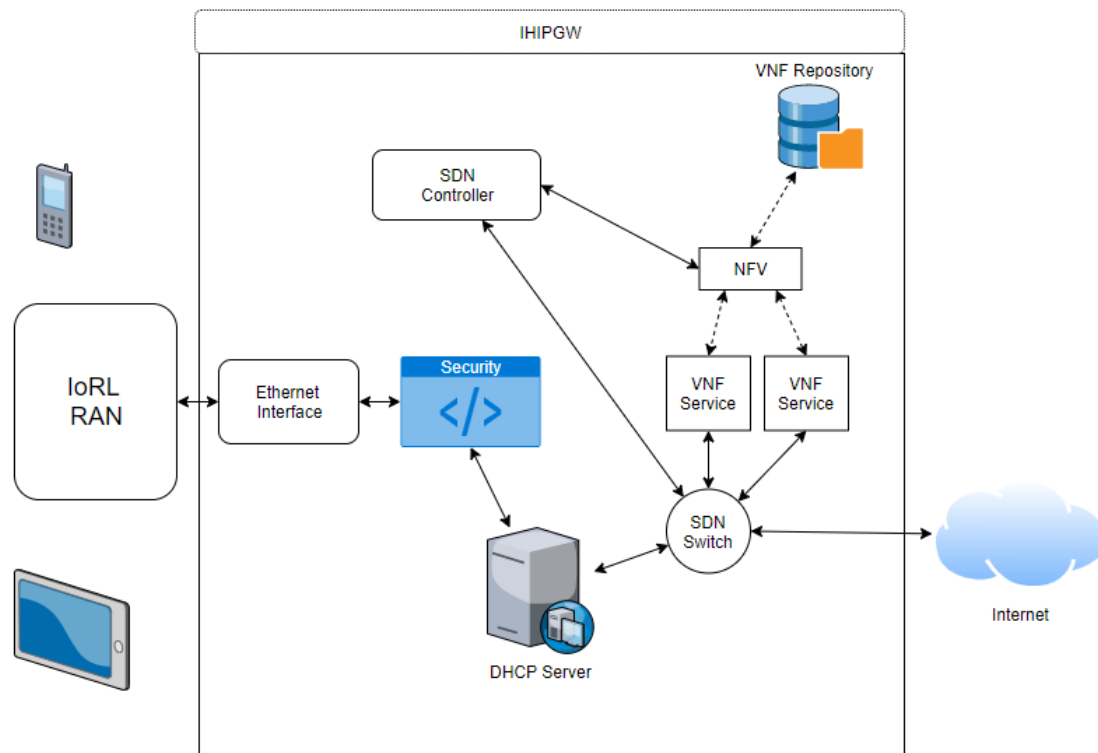


Figure 0-2: Security Architecture

Figure 5-2 shows, the proposed solution architecture. Any device or machine that connects to the network sends traffic to the Radio Access Network (RAN) first which is then redirected to an ethernet interface.

Following, the traffic passes through the security scripts that are developed to mitigate DHCP attacks. Detailed explanation about the security scripts are made in the sections below. As soon as the traffic passes through the security scripts, each packet is analysed to check for any potential information that might help detect if the traffic is safe or if it might be a DoS attack. Following the security check-ups, if the traffic is safe, it is redirected to the DHCP server which assigns an IP address to the device that is trying to connect. If the whole process is successful, the traffic is sent to the SDN switch, which then redirects it to the SDN controller.

SDN has been proven to simplify the process of controlling the whole network for multiple reasons. To begin with, normal networks do not separate the control plane and the

data plane, whereas, SDN has the control plane separated from the data plane [125]. The control plane is responsible for handling the traffic and deciding where it should go next, and the data plane forwards the traffic based on the decision taken by the control plane [125]. SDNs control routers, switches, or any other networking device using well-defined APIs [125]. An example of these APIs is OpenFlow which operates using a set of rules that are applied on each packet in order to determine what to do next [125].

After the traffic is sent to the SDN controller, the controller can send the traffic to NFV which stands for Network Functions Virtualization. NFV is a way of virtualizing network services, and it has numerous benefits. To begin with, NFV allows maximum flexibility and programmability that is needed in order to create multiple virtual networks [126]. Each network can be programmed according to its requirements, which means it is possible to develop many networks each having different purposes. Furthermore, NFV has a great benefit as there are no bespoke hardware requirements. Service providers can add network services or adjust any configurations without the need to have additional hardware resources [127].

5.5 Implementation

This section provides an overview of the security scripts previously discussed in section 5.4.1. The implementation of all the scripts is discussed in detail. Python was chosen as the programming language for the scripts due to its flexibility, simplicity, and because it includes a library called scapy which allows many operations in networking such as sniffing packets and manipulating them.

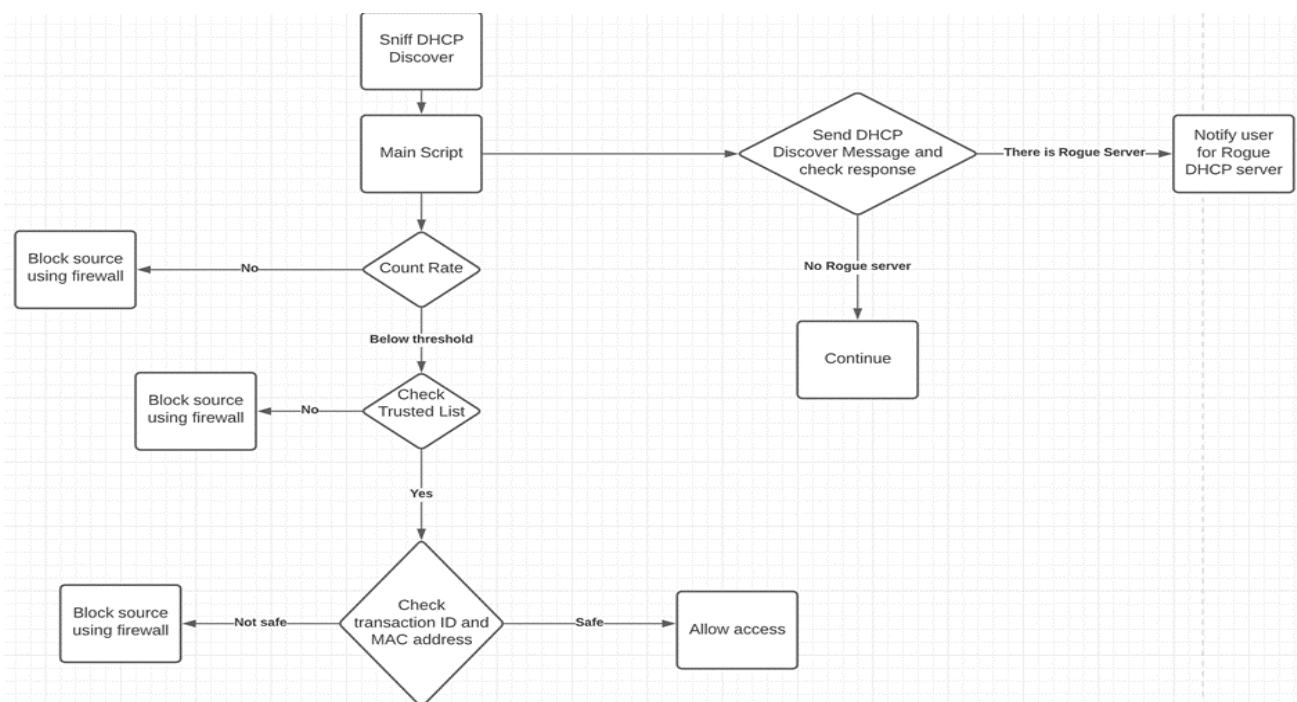


Figure 0-3: UML diagram

Figure 5-3, demonstrates the basic operations of each script, the checking conditions, and how they are linked together. Also, the flowchart shows how the script is contextual aware of what happens in the system. It has the ability to identify malicious attacks, gather information and save it to the database. The code is run through one script, called main script, that calls all the other scripts when needed. Each script will be explained in detail below.

5.5.1 Main Script

The main script consists of 3 functions which are handlepacket, keepcount, and stopfilter.

```
if __name__=="__main__":
    print("Started sniffing!")
    sniff(filter="udp and (port 67 or port 68)",count=0, prn=handlepacket, store=0, stop_filter=stopfilter)
```

Figure 0-4: sniffing

Figure 0-4, shows how the main script starts. Sniff is function from the library called scapy, and it is responsible for sniffing packets. It takes many arguments which helps sniff the packets that is required such as filter where we specify the protocol or the port we want to sniff on. Also, one of the arguments it takes is prn where we specify a function that does analysis on each packet sniffed. In this case, the function that does all the analysis is called handlepacket. The stop_filter argument is given so that if a specific condition occurs, it stops sniffing. More arguments were given such as store which is given the value 0, and this is to not store any packet sniffed, and the argument count which is also given value 0 as to sniff packets indefinitely until the stop condition is met.

```
def handlepacket(pkt):
    if pkt.haslayer(DHCP):
        EtherMac=pkt[Ether].src
        keepcount()

    #Check if mac address in trusted list
    trust=checkTrusted.check(pkt)
    if trust==True:
        print("source is trusted")
        print("")
    elif trust==False:
        print("Source is not trusted, further inspection will take place")
        print("")
        detectAttack.packetHandler(pkt)

s.enter(100,100,DiscoverRogue.check())
```

Figure 0-5 - Main Script HandlePacket

Figure 0-5, shows the function called handlepacket. Each packet sniffed passes through to this function where analysis is performed. The first if statement checks if it is a DHCP packet, if true it saves the MAC address of the source that the message was sent from in a variable called EtherMac. Following, the keepcount method is called which keeps count of the packets received. Then, the MAC address of the source is compared to check if it is in the list of trusted MAC addresses. If true, then the source is trusted, and the packet is allowed to pass. If false, further inspections must be made, and this is where the detectAttack script is called. The last line of code runs the DiscoverRogue script every couple of seconds.

```
def stopfilter(pkt):  
    x=keepcount()  
  
    if x<1000:  
        return False  
    else:  
        return True
```

Figure 0-6 - Stop filter

Figure 0-6, shows the method stopfilter, which calls another method called keepcount that returns the value of the packets captured, and the time they were captured in. Then an if statement was made to decide where the message rate is higher than the threshold or lower. If higher, a notification will be sent to indicate that the system might be under attack. If the message rate is lower than the threshold, then the code continues running.

5.5.2 Attack Detection Script

This script checks each packet for its transaction id and MAC address. It creates a text file to save the transaction id and the MAC address of each packet sniffed.

```
from scapy.all import *  
import os
```

Figure 0-7: Libraries

Figure 5-7, shows the libraries that were used to write the script. Scapy is used for packet sniffing and analyzation, while the OS library is used to interact with the operating system which in this case Linux.

```

xid=0
EtherMac=""
def packetHandler(pkt):

    if pkt.haslayer(DHCP):
        xid=pkt[BOOTP].xid
        EtherMac=pkt[Ether].src

    f=open("xid.txt", "r")
    readfile=f.read()

    if str(xid) in readfile:
        if EtherMac in readfile:
            print("Packet is safe")

        else:
            print("Potential attack!")
            print("")
            command="iptables -I INPUT -m mac --mac-source "+EtherMac+" -j DROP"
            os.system(command)
            print(EtherMac+" blocked by firewall")
            print("")

    else:
        print("safe")
        print("")

    f.close()

    f=open("xid.txt", "a")
    f.write("xid: "+str(xid)+" Ethernet mac: "+EtherMac+"\n")
    f.close

```

Figure 0-8: Attack Detection (detectAttack) Script

Figure 5-8, displays the rest of the script which is responsible for detecting an attack. Every time the main script is run, every packet sniffed is passed to this function above. The first condition is to check whether the packet contains DHCP in it as this is our concern. Following, if the packet contains DHCP, then the transaction ID and the source MAC address are stored in 2 variables. Then, the script creates a text file to save the 2 variables and check for them later. The second condition is if the transaction ID is saved in the text file, and if it is there then it checks for the MAC address. If both of them are saved then the packet is saved. If not, then there might be an attack as the transaction ID is not changing, while the MAC address

is, and as explained above, the attacker will generate fake MAC addresses to obtain different IP addresses, which exhausts the DHCP server. If the attack is detected, the firewall is updated to block the packet from this source and block any further communication with it. This is done using the `os.system()` command where any command is written between the brackets, and it is sent to the operating system to perform the command. Lastly, if the transaction ID is not in the text file, then the packet is safe. After checking it is safe, the transaction ID and the source MAC address are saved in the text file.

5.5.3 Check Trusted Script

This script is called by the main script before any other script. As explained above, one of the main checks is having a trusted list for MAC addresses and then check each packet if its source is trusted or not. If the source is not trusted, then further checks are performed using the `detectAttack` script.

```
def check(pkt):
    f=open("trusted.txt","r+")
    readfile=f.read()
    f.close()

    if pkt.haslayer(DHCP):
        EtherMac=pkt[Ether].src

    if EtherMac in readfile:
        return True
    else:
        return False

    f.close()
```

Figure 0-9: Check Trusted Script

The script shown in Figure 5-9 , opens the text file, which has the list of trusted MAC addresses in read mode. The script then checks if the packet contains DHCP, and if it does, it saves the MAC address in a variable called `EtherMac`. Following, it checks if the variable `EtherMac` is found in the text file, and it returns `True` if it is found, and if it is not found it returns `False`.

5.5.4 Discover Rogue Script

This script is responsible for checking if there is a rogue DHCP server in the network or not. The Scapy library is again used but for a different reason. It is used to forge a DHCP Discover message, send it, and wait for replies. If it receives more than the number of legitimate DHCP servers in the network, then there might be a rogue DHCP server. The random library is used to generate random numbers which will be used while forging the DHCP packet.

```
def randMac():
    mac=[random.randint(0x00, 0x00),
        random.randint(0x00,0x16),
        random.randint(0x00,0x3e),
        random.randint(0x00,0x7f),
        random.randint(0x00,0xff),
        random.randint(0x00,0xff)]
    return ':'.join(map(lambda x: "%02x" % x,mac))
```

Figure 0-10: Generate random MAC address

As explained in the sections above, each device that has a network card must have an identification number which is called MAC address. MAC addresses consist of six bytes, each written in the form of hexadecimal. Between each byte, a colon is inserted to make it easier to read. An example of a MAC address could be BE:82:6F:C2:A1:02. The function shown in Figure 5-10, is responsible for generating the MAC address using the random.randint function. Each byte is generated alone, and then joined together using .join, map, and lambda functions. The value is returned at the end.

```
def discoverpkt():
    transaction_id=random.randint(1,900000000)
    src_mac=randMac()
    ether=Ether(src=src_mac, dst='ff:ff:ff:ff:ff:ff', type=0x0800)
    ip=IP(src='0.0.0.0',dst='255.255.255.255')
    udp=UDP(sport=68, dport=67)
    bootp=BOOTP(chaddr=mac2str(src_mac), xid=transaction_id, flags=0xFFFF)
    dhcp=DHCP(options=[("message-type", "discover"), ("max_dhcp_size",1500), ("client_id", mac2str(src_mac)), ("lease_time", 10000), "end", "0"])

    dhcp_discover=ether/ip/udp/bootp/dhcp

    return dhcp_discover
```

Figure 0-11: create DHCP Discover

Upon generating a MAC address, the DHCP Discover message is created in the function called `discoverpkt` shown in Figure 5-11. To begin with, each parameter is generated and saved to variables. The transaction ID is generated using the `random.randint()`. The MAC address is given the generated MAC address from the function explained above.

Each packet consists of layers which are shown above. The first layer is the ether layer which carries the source MAC, the destination MAC which is given the value of `ff:ff:ff:ff:ff:ff` as it is a broadcast message. The second layer is the IP layer which carries the source IP address and the destination IP address. In DHCP Discover messages the source IP is always `0.0.0.0` as the device did not obtain an IP address from the DHCP server yet. Also, the destination IP address is always `255.255.255.255` as it is a broadcast message. The third layer is the protocol layer which is UDP in our case as DHCP messages are exchanged using the UDP protocol. This layer carries the port number of the sender and the receiver. DHCP operates on ports 67 and 68, where 68 is always the source port, and 67 is the destination port. Then, the BOOTP layer, which includes the source MAC address, the transaction ID, and flags. The method `mac2str()` is used to convert the MAC address to the form of string to be used in the packet. Lastly, the DHCP layer consisting of the message type as there are many types, which are explained in the sections above. It also carries the maximum size of the DHCP packet, the MAC address of the source, and the lease time. The function then joins all these layers together and stores the value in a variable called `dhcp_discover`. The variable is then returned when the function is called.

```
def check():
    packet=discoverpkt()
    ans=srp(packet, timeout=10)
    detect(ans)
```

Figure 0-12: Send Packet

Figure 5-12, shows another function called `check`. This function creates a variable called `packet`, and it calls the `discoverpkt()` function, which was explained above to get the value of the DHCP packet. Another value is then created, and the packet is sent using `srp` which is a method in `scapy` library that allows to send and wait for an answer for the packet. Another parameter was set to `timeout` if time exceeds 10 seconds. Lastly, the value of the received packet is then passed to another function called `detect`, which will be explained below.

5.6 Performance evaluation

5.6.1 Testbed description

In this section, detailed plan of the testing and the network configuration will be explained and implemented in order to check whether the built scripts will be able to mitigate DHCP attacks, to see how efficient they are.

5.6.1.1 Testing plan

- Create a network which must include a DHCP server, a client where the scripts will be running on, and a malicious client which will be running the attacks.
- Run the attack first in order to compare results before and after running the security scripts.
- Run the scripts and launch the attack to check whether they mitigate it or not.
- Analyse the results using Wireshark and checking DHCP bindings.

5.6.1.2 Developing the Network

A network was created in order to be able to perform the testing on. The network consists of the following:

1. A DHCP server running on a Cisco router
2. A switch which connects all devices to the DHCP server as the network uses ethernet to connect devices together
3. A normal VM running ubuntu which has the security scripts running on.
4. A malicious client running kali Linux in order to perform the attack from.

To build this network, a simulation software called GNS3, which stands for graphical network simulator, was used. GNS3 allows users to build and simulate all types of networks in order to test any scenario before implementing any network in real life. It is widely used by network professionals for testing.

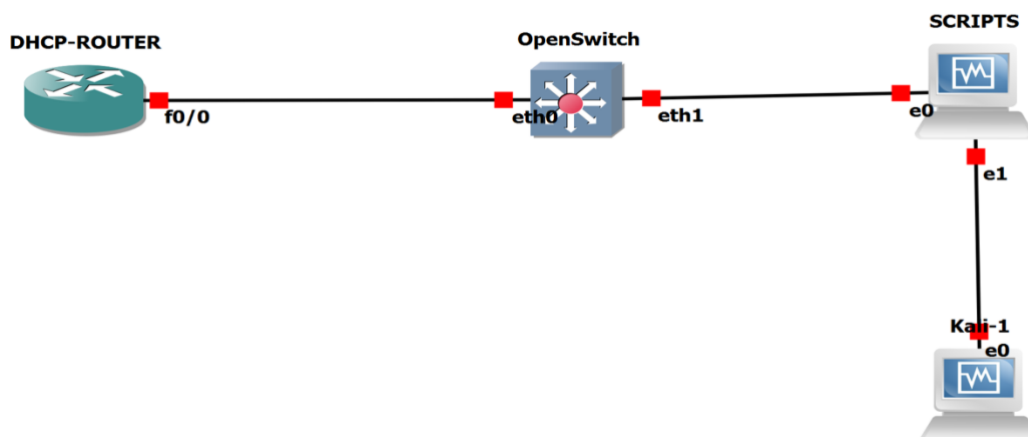


Figure 0-13: Network Model

Figure 0-13, demonstrates the network created using GNS3 which contains the 4 main components as described above. The DHCP server is connected to a switch using ethernet, and the ubuntu vm is connected to the switch as the scripts will be running on it and it is required to block malicious traffic before reaching the DHCP server. Lastly, the kali linux vm is connected to the Ubuntu vm using ethernet as well.

5.5.1.3 DHCP configuration

As discussed above, the main aim of the security scripts that were developed is to protect the DHCP server from DDoS attacks. Therefore, in order to test these scripts, a DHCP server must be configured correctly to function as it should. This section explains how the DHCP server is configured.

Firstly, the DHCP server is running on a 3725 Cisco router which allows having a DHCP running on it as well as allowing the administrator to configure the DHCP server as they want.

```
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.0.1 192.168.0.20
!
ip dhcp pool DHCP_Main
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 dns-server 192.168.0.1
 lease 8
!
```

Figure 0-14 - DHCP Configuration

Figure 5-14, demonstrates the characteristics of the DHCP server. A DHCP pool was created and name DHCP_Main. This DHCP pool has a subnet network number as 192.168.0.0 which means that any client that connects to the network will have an IP address that starts with 192.168.0.x, where the x changes according to the client. The subnet mask was also identified as 255.255.255.0. Following, the default-router and the DNS server's IP addresses was set to 192.168.0.1.

Based on this information, it can be concluded that as the DHCP server is running on the default-router, then the DHCP server's IP address is 192.168.0.1. Lastly, the lease time was set to 8 days, which means that if a client was assigned with an IP address, it can hold it for 8 days while the DHCP server marks the clients IP address as taken so that no other client can obtain the same IP address. However, after the lease time ends, the client should ask for a new IP address.

Upon configuring the DHCP server, all the devices were started to check whether they will be able to obtain an IP address from the DHCP server or not.

```
Kali#sh ip dhcp bind
R1#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/          Lease expiration    Type
                   Hardware address/
                   User name
192.168.0.2         0108.0027.05b0.0a  Mar 09 2002 12:05 AM Automatic
192.168.0.3         0108.0027.a61f.86  Mar 09 2002 12:06 AM Automatic
```

Figure 0-15: Device check

According to Figure 5-15, both devices running Ubuntu and Kali Linux were able to obtain an IP address from the DHCP server. This demonstrates all IP addresses leased from the DHCP server as well as their MAC address and their date of lease expiration which was explained above. The vm running Ubuntu was able to obtain 192.168.0.2 as its IP address, which is shown below in Figure 5-16 by running the command `ifconfig` to check the information for all its network interfaces. The same procedure was carried out for kali Linux, and it was able to obtain an IP address of 192.168.0.3 as shown in Figure 5-15.

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.2 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::c165:a2f7:bed0:88f4 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:05:b0:0a txqueuelen 1000 (Ethernet)
RX packets 545 bytes 37176 (37.1 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 594 bytes 50048 (50.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 0-16: Check for IP address

5.6.2 Testing the attack

After setting the DHCP server and ensuring that it was working properly by issuing IP addresses to both virtual machines, it is time to conduct an attack and see if it has any effect on the DHCP server's functionality. Another virtual PC is introduced to the network and the attack initiated to test this. The virtual PC is turned on after the attack is complete, and it attempts to obtain an IP address using the DHCP protocol. If the DHCP pool has issued all 254 addresses, it is unable to assign an IP address to any new client, making the attack successful. The tool used for running the DHCP starvation attack is called Yersinia, which is a software used for testing multiple types of attacks and it is available on kali Linux by default.

192.168.0.245	2db8.2b5f.1829	Mar 29 2020 10:59 AM	Automatic
192.168.0.246	4623.a670.f608	Mar 29 2020 10:59 AM	Automatic
192.168.0.247	59c8.ae18.6d12	Mar 29 2020 10:59 AM	Automatic
192.168.0.248	834e.f460.dfe9	Mar 29 2020 10:59 AM	Automatic
192.168.0.249	b99e.db2a.d1b7	Mar 29 2020 10:59 AM	Automatic
192.168.0.250	96c1.f858.bf7c	Mar 29 2020 10:59 AM	Automatic
192.168.0.251	f2ac.543f.3496	Mar 29 2020 10:59 AM	Automatic
192.168.0.252	5151.2d4e.5f96	Mar 29 2020 10:59 AM	Automatic
192.168.0.253	e94d.014f.c239	Mar 29 2020 10:59 AM	Automatic
192.168.0.254	3444.1619.b5ca	Mar 29 2020 10:59 AM	Automatic

Figure 0-17: DHCP Binding

Figure 0-17 , demonstrates the DHCP bindings after running the attack. As shown, all the IP addresses until 192.168.0.254 were leased to fake MAC addresses generated by the malicious client which exhausted the DHCP pool leading to the DHCP server having no more IP addresses to assign to any other client. Also, Wireshark was used to monitor the traffic flowing through the network to know whether the attack was successful or not.

Wireshark has discovered 254 Discover DHCP packets using bogus MAC addresses, and the DHCP server has supplied 178 IP addresses, as seen in Figure 5-18. Due to the high volume of traffic, Wireshark only caught 178 IP addresses; however, 254 IP addresses were provided, causing the DHCP pool to be totally exhausted, preventing any other client connecting to the network from obtaining an IP address. The attack was effective in draining all IP addresses from the DHCP server, based on the information above.

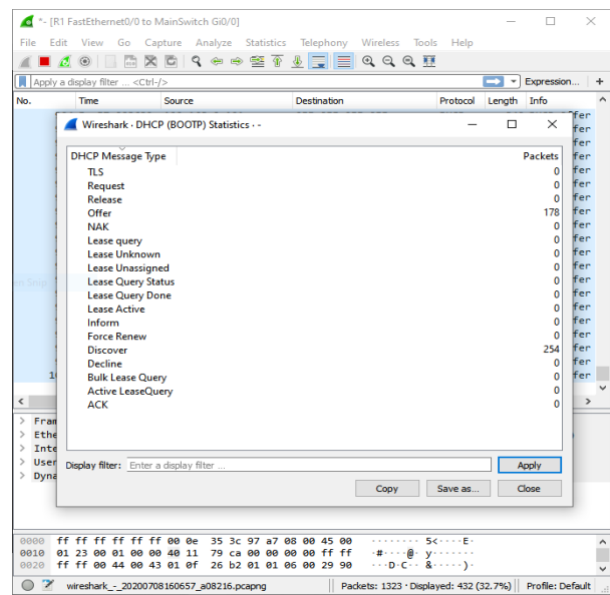


Figure 0-18: DHCP packets

Additionally, as mentioned above, a normal client was added to the network to test whether it can obtain an IP address after the attack has drained the DHCP pool or not.

```
PC1> dhcp
DDD
Can't find dhcp server
```

Figure 0-19: Console for PCI

Figure 5-19 above shows the console of PC1 when the command DHCP was entered in order to ask for a DHCP server, the DHCP server did not reply back leaving the machine without an IP address.

5.6.3 Testing the scripts

In this section, testing of the developed security scripts is taking place and demonstrated using Wireshark, checking the DHCP bindings, and checking the firewall of the machine running the scripts as it includes all the blocked requests.

First step was running the security scripts and making sure it is functioning correctly, then the DHCP starvation attack was run using Yersinia, and Wireshark was started between both machines to monitor the traffic flowing between them.

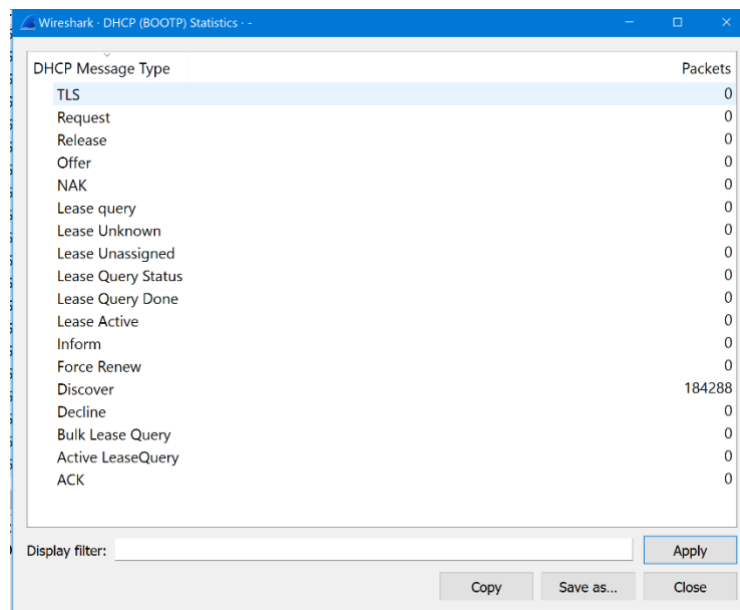


Figure 0-20: Wireshark with security

Figure 5-20 shows that Wireshark identified 184,288 DHCP Discover messages being sent from the kali Linux system; however, unlike the first attempt, no offer messages were received, indicating that the DHCP server did not provide any IP address.

```
R1#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/
                Hardware address/
                User name
192.168.0.2     0108.0027.05b0.0a    Mar 09 2002 12:00 AM    Automatic
192.168.0.3     0108.0027.a61f.86    Mar 09 2002 12:01 AM    Automatic
R1#
```

Figure 0-21: DHCP leased IP addresses

Furthermore, the DHCP bindings which is shown in Figure 5-21 demonstrates that only two IP addresses have been leased and none of the fake Discover messages received a response. Additionally, the security scripts detected the attack, and each packet was analysed to check for its MAC address in order to add it to the firewall and block the source.

```
Potential attack!  
The following mac: 00:13:24:62:b8:c5 is blocked by firewall for malicious activity!  
Potential attack!  
The following mac: 00:02:11:0a:bf:57 is blocked by firewall for malicious activity!  
Potential attack!  
The following mac: 00:06:21:06:a2:0c is blocked by firewall for malicious activity!  
Potential attack!  
The following mac: 00:15:18:42:62:55 is blocked by firewall for malicious activity!  
Potential attack!  
The following mac: 00:06:30:62:0e:16 is blocked by firewall for malicious activity!  
Potential attack!  
The following mac: 00:12:39:5d:86:ad is blocked by firewall for malicious activity!  
Potential attack!  
The following mac: 00:12:1e:11:cc:61 is blocked by firewall for malicious activity!
```

Figure 0-22: Detected malicious packets

As previously stated, the security scripts block every malicious packet received after performing a series of checks to determine whether the packet is safe to enter or not. Figure 5-22 shows the script after it detected the attack and continues to display the message "Potential attack," followed by the MAC address and confirmation that it has been stopped by the firewall for malicious activity. According to the data gathered during the testing of the security scripts, the scripts were capable of blocking the attack and saving the DHCP server from the malicious user who was attempting to take it down.

Furthermore, PC1 which was added to the network to test if a normal client was able to obtain an IP address while the attack was on, was started again and it tried to obtain an IP address from the DHCP server. As shown above in Figure 5-19 , the attack was running without the security scripts protecting the server, leading to PC1 not being able to acquire an IP address. However, upon running the scripts and the attack, the scripts successfully protected the server by blocking all the fake Discover messages, and PC1 was able to acquire an IP address from the DHCP server as shown in Figure 5-23.

```
PC1> dhcp  
DDORA IP 192.168.0.2/24 GW 192.168.0.1
```

Figure 0-23: PC1 acquires IP from the DHCP Server

Lastly, the security script called Discover which is responsible for checking if there is a rogue DHCP server in the network was tested for its functionality. Firstly, the script was run and only one DHCP server was in the network which was not rogue. Wireshark was also started to monitor the traffic going out and to the machine running the scripts.

```
Begin emission:
Finished sending 1 packets.
.....
Received 15 packets, got 0 answers, remaining 1 packets
DHCP offer received from 192.168.0.1 c2:01:3a:04:00:00
```

Figure 0-24: Discover Script

Figure 5-24, shows the output after running the Discover script which shows that one DHCP offer was received from the IP address 192.168.0.1 with MAC address c2:01:3a:04:00:00. These are the DHCP server's legit details which proves that there is not rogue DHCP server in the network.

Following, a rogue DHCP server was created in the network using the Yersinia tool which was explained above. The rogue DHCP server was given IP address of 192.168.0.10 and a MAC address of 00:02:16:1d:1f:3f. The Discover script was then run to check if it detects that there are 2 DHCP servers in the network or not.

```
Begin emission:
Finished sending 1 packets.
..
Received 2 packets, got 0 answers, remaining 1 packets
DHCP offer received from 192.168.0.1 c2:01:3a:04:00:00
DHCP offer received from 192.168.0.10 00:02:16:1d:1f:3f
```

Figure 0-25: Discover Script output

Figure 5-25, shows the output of the script which successfully detected 2 DHCP offer requests from 2 different DHCP servers where one of them is rogue and the other one is legit. As demonstrated in Figure 5-25, the script received an Offer request from 192.168.0.10 with the MAC address stated above which proves that it detected the rogue server. This process helps network administrators to be able to monitor the network and if there is a rogue server, they would have to take it down before it causes damage to the network and the clients using it.

5.7 Results and analysis

This section will discuss the results obtained after testing the security scripts in section. Also, these results will be analysed to check whether the security scripts that was developed were capable of denying a DHCP attack and were scripts protect the DHCP server, and how efficient were the scripts.

To begin with, based on Figure 5-20 **Error! Reference source not found.** above, Wireshark was able to sniff a huge amount of DHCP Discover messages that was generated and sent by the malicious client who was aiming to exhaust the DHCP server. However, no

DHCP Offer requests were sent back by the DHCP server which means that the server did not receive any of the fake DHCP Discover messages sent by the malicious user. Based on that information, the security scripts were successfully able to block most of those requests.

Table 0-1: CPU usage before running the scripts

Time (msec)	CPU Usage (%)
1000	10
2000	20
3000	80
4000	88
5000	89
6000	90

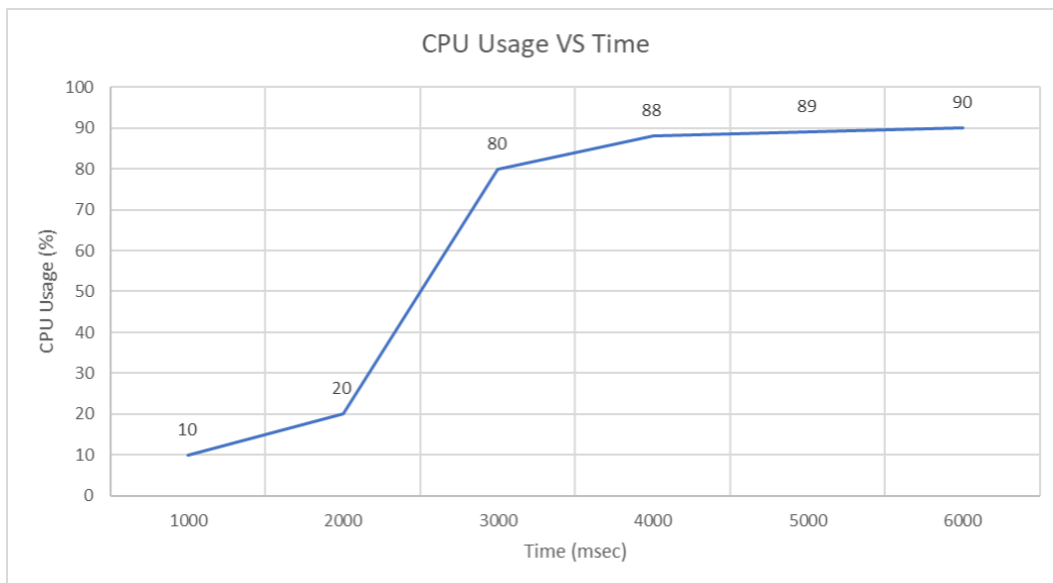


Figure 0-26: CPU usage of the DHCP server during an attack

Table 0-1 and Figure 5-26 demonstrates the CPU usage of the DHCP server during the

Time (msec)	CPU Usage (%)
1000	10
2000	20
3000	80
4000	88
5000	89
6000	90

attack but without running the proposed security scripts. According to these results, the CPU usage was almost stable in the first 2 seconds of running the attack, however, after 3 seconds there was a huge increase in the usage of the CPU due to the vast amount of DHCP Discover packets that was received by the server while simultaneously trying to send back DHCP Offer packets. This leads to the server not responding as it should, and the attack successfully took

down the DHCP server leaving legitimate clients unanswered when they try to obtain an IP address.

Table 0-2: CPU usage after running the scripts

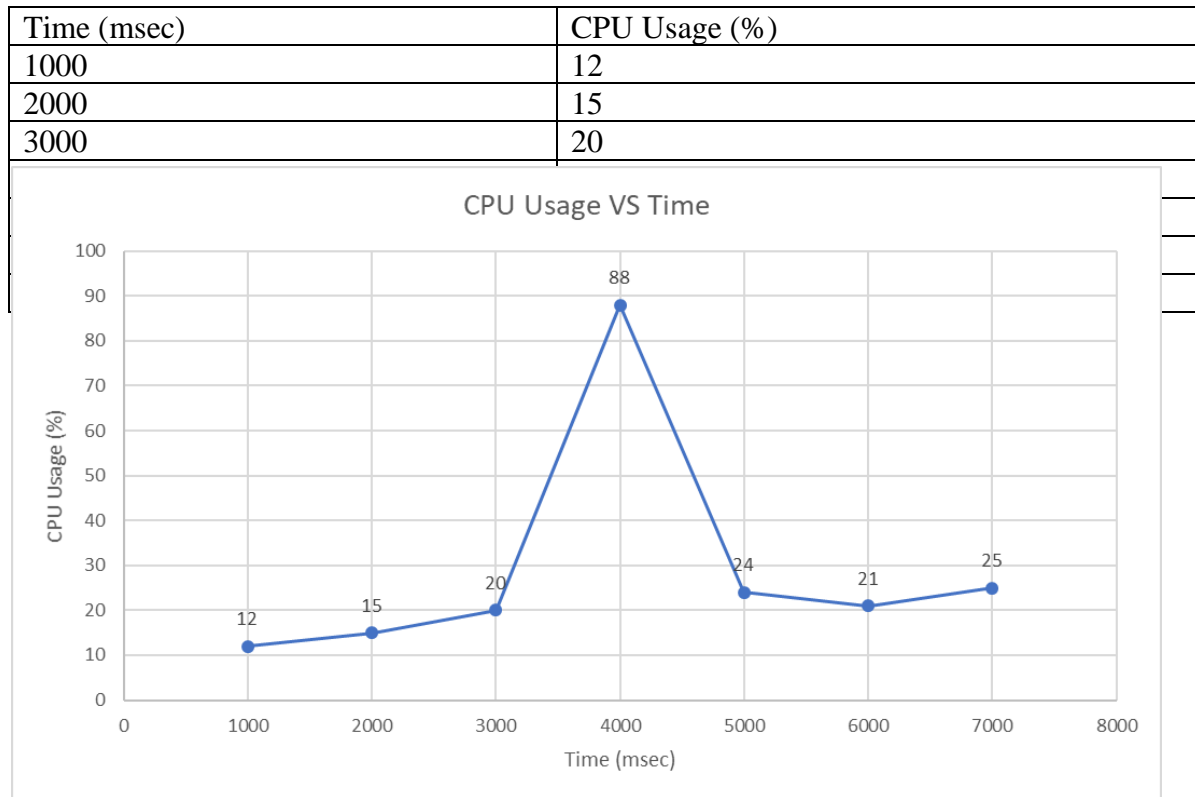


Figure 0-27: CPU usage of the DHCP server during an attack while running scripts

The same test was conducted again to see what happens while running the proposed security scripts. Table 0-2 , demonstrates that for the first 3 seconds the CPU usage was normal and stable, however, in the 4th second the usage of the CPU increased rapidly to 88%, but it dropped to 24% later. This shows that the security scripts developed were successful and protected the DHCP server from the DHCP starvation attack. Nonetheless, the DHCP server was still affected by the attack for 1 or 2 seconds due to the scripts getting overloaded and some of the DHCP Discover packets still reached the server.

Table 0-3: DHCP Attack without the running security scripts

Time (msec)	Number of DHCP Discover requests sent by attacker	Number of DHCP Discover requests received by DHCP server
1000	20	20
2000	50	50
3000	77	77
4000	130	130
5000	178	178
6000	199	199

7000	250	250
------	-----	-----

Another test was made to check how many packets passes through to the DHCP server before and after running the proposed security scripts. Firstly, before running the scripts, packets were monitored as soon as they leave the attackers machine, and when they reach the DHCP server. The table above shows that all the packets sent by the attacker reached the DHCP server causing the server to crash and be unresponsive to legitimate clients trying to connect to the network.

Table 0-4: DHCP Attack while running the security scripts

Time (msec)	Number of DHCP Discover requests sent by attacker	Number of DHCP Discover requests received by DHCP server
1000	20	15
2000	50	20
3000	77	32
4000	130	50
5000	178	23
6000	199	15
7000	250	0

However, upon running the security scripts that were developed, almost 90% of the fake DHCP Discover packets did not reach the DHCP server which was demonstrated in the table above. In the first 4 seconds some packets passed through to the server, but as at the end almost no packets were able to pass through to the DHCP server.

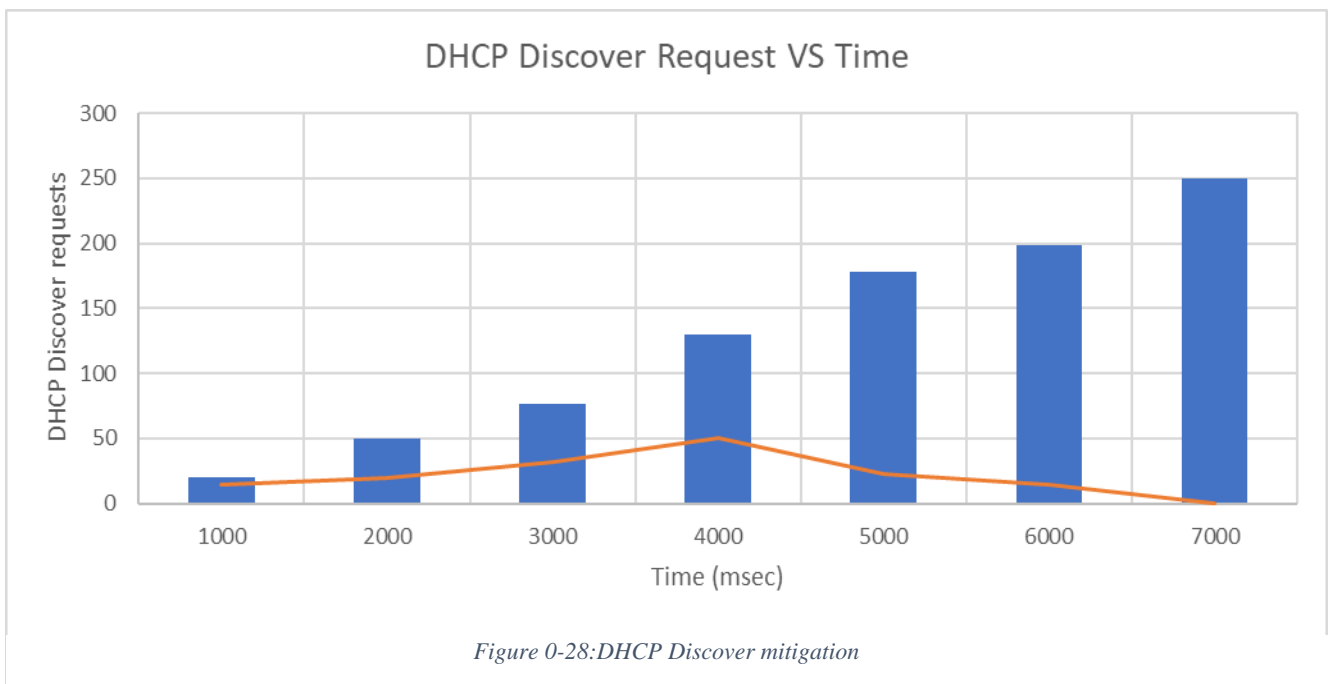


Figure 0-28:DHCP Discover mitigation

According to the results mentioned above, the proposed solution to mitigate DHCP starvation attacks is effective and can successfully protect DHCP servers from a DDoS attack which leads to it being unresponsive. However, the results show that the proposed solution is not 100% effective as some of the fake Discover packets reached the DHCP server. This is due to the high load of traffic passing through and the scripts not being able to block all of it.

Lastly, the Discover script which is responsible for detecting any rogue DHCP servers in the network was successfully able to perform its task with no limitations. It is a simple process where it sends a DHCP Discover message broadcasted in the network, and all DHCP servers will respond to it. Network administrators should know how many legit DHCP servers there are in the network, and if the received Offer messages exceeds that number, then they will know if there is an abnormal activity in the network and they will start investigating it.

5.8 Summary

Wireless communication's security flaws have existed since their inception. A more dynamic and complicated threat landscape was created as a result of the emergence of mobile networks. (5G) wireless networks will have more security vulnerabilities and a greater focus on user privacy.

The security scripts developed are of great use when it comes to protecting the network from DHCP attacks that could cause a lot of damage to the network. They have the ability to block fake DHCP Discover requests that drain the DHCP pool from all the IP addresses available. Consequently, normal clients will not be able to connect to the network.

Moreover, the scripts are also capable of detecting if there is any DHCP rogue server in the network, that could lead to more problems. Nevertheless, there are limitations to the scripts such as; the amount of fake Discover requests received, as well as the rate they are being sent. However, most of the requests can be blocked automatically until the network administrators take action to make sure the DHCP server is safe from any possible attacks.

Finally, the proposed indoor location security application is a promising solution as it provides a high scalability solution using VNF. Nearly 90% of the fake DHCP packets did not reach the DHCP server. After the scripts got alert that the DHCP discover packets are fake, it started blocking all the fake discover packets and none passed through to the DHCP server.

Chapter 6: Conclusion and future works

6.1 Conclusion

Internet of Things (IoT) is a promising technology that is expected to alter and connect the globe in the near future by seamlessly linking heterogeneous smart devices. 5G enables numerous technological breakthroughs that when combined with broadcasting services, have a significant transformational and impactful effect. The need for mobile data location broadcasting services from broadband networks has been growing tremendously. Managing networks has historically been challenging due to the high resource requirements. However, Software Defined Networking (SDN) and Network Function Virtualization (NFV) have emerged as the potential future of network management. Both provided substantial benefits including simplified management, increased resource utilisation, and lower operating expenses.

The design, implementation, experimental inspection, and assessment of 5G indoor location services were all scrutinized in this thesis. These services comprise of the location database, an interactive web interface, an interactive application, and a location server that streams real-time video in real time. The objective to build a multiaccess edge cloud was achieved successfully, whilst improving the streaming performance parameters. The performance characteristics of the streaming system revealed a high degree of Quality of Service (QoS), as the jitters and delays were kept at minimal during all the different streams. 4K stream showed, an average jitter of 0.07ms, and an average delay of 9.53 ms.

The mmWave and VLC link transmitters were used to obtain the required localisation coverage, and accuracy measurements. A world's first experiment to measure the coverage for both technologies was successfully achieved. A world's first experiments to measure the location accuracy of VLC was successful. However, the location accuracy of mmWave was not achieved due to integration challenges and time constraints. The data optimization for location measurement accuracy exhibited significant gains compared to the previous algorithm. After several iterations the average location error of x and y decreased dramatically from 22.5 and 21.6 to $x=11.09$ and $y=11.63$, which halved the original results. The distance error accuracies were as low as 2.37 cm and not greater than 3.74 cm.

The suggested indoor location security solution demonstrated remarkable results due to the fact it is a high scalability solution that makes use of VNF technology. The solution revealed that it was not 100% successful, as some of the fake discover packets still managed to reach the DHCP server after the scripts were running. This was brought by the large volume of traffic that passed through the network. Almost 90% of the fake DHCP packets did not reach the DHCP server, as the scripts started to block all the fake discover packets after perceiving it is an attack. The system was able to protect the network from malicious attacks using the VNF on the multiaccess edge cloud, whilst ensuring user connectivity.

6.2 Future works

In our society, people with disabilities are a diverse group. There are many ways to describe disability since "it denotes limitations on activity, participation and impairments" [128]. Some people are born with a disability, while others develop it because of a long-term illness or injury [128]. People with disabilities around the world will benefit from this project's development of a visible light communication system. A voice guiding system application, that could be used to assist people with disabilities, such as "Vision Disability," as they walk. I believe that 5G would be able to help provide new services to assist people with not only vision disabilities but also people with any other disability like hearing disability.

5G capabilities will allow a lot of technological advancements. As it can be used for remote surgery. A doctor would be sitting in a country performing an operation on a patient in another country remotely. This could be achieved due to the low latency that 5G provides. Furthermore, 5G systems can be used in cars to allow real time communication between cars, which would reduce car accidents. This does not only protect the environment, but it also saves lives. It would allow remote monitoring and data analysis of the cars on the road.

Bibliography

- [1] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6. Institute of Electrical and Electronics Engineers Inc., pp. 3619–3647, Dec. 02, 2017. doi: 10.1109/ACCESS.2017.2779844.
- [2] S. Sridharan, "A Literature Review of Network Function Virtualization (NFV) in 5G Networks," *International Journal of Computer Trends and Technology*, vol. 68, pp. 49–55, 2020, doi: 10.14445/22312803/IJCTT-V68I10P109.
- [3] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3. Institute of Electrical and Electronics Engineers Inc., pp. 1617–1655, Jul. 01, 2016. doi: 10.1109/COMST.2016.2532458.
- [4] A. Osseiran *et al.*, "Scenarios for 5G mobile and wireless communications: The vision of the METIS project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, May 2014, doi: 10.1109/MCOM.2014.6815890.
- [5] A. A. Ateya, A. Muthanna, M. Makolkina, and A. Koucheryavy, "Study of 5G Services Standardization: Specifications and Requirements," in *International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, Jan. 2019, vol. 2018-November. doi: 10.1109/ICUMT.2018.8631201.
- [6] M. B. Yassein, S. Aljawarneh, and A. Al-Sadi, "Challenges and features of IoT communications in 5G networks," in *2017 International Conference on Electrical and Computing Technologies and Applications, ICECTA 2017*, Jun. 2017, vol. 2018-January, pp. 1–5. doi: 10.1109/ICECTA.2017.8251989.
- [7] C. Liang and F. Yu, "Wireless virtualization for next generation mobile cellular networks," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 61–69, Feb. 2015, doi: 10.1109/MWC.2015.7054720.
- [8] J. J. Gimenez *et al.*, "5G new radio for terrestrial broadcast: A forward-looking approach for NR-MBMS," *IEEE Transactions on Broadcasting*, vol. 65, no. 2, pp. 356–368, Jun. 2019, doi: 10.1109/TBC.2019.2912117.
- [9] S. K. Ahn, K. J. Kim, S. Myung, S. I. Park, and K. Yang, "Comparison of Low-Density Parity-Check Codes in ATSC 3.0 and 5G Standards," *IEEE Transactions on Broadcasting*, vol. 65, no. 3, pp. 489–495, Sep. 2019, doi: 10.1109/TBC.2018.2874541.
- [10] F. Alvarez *et al.*, "An Edge-to-Cloud Virtualized Multimedia Service Platform for 5G Networks," *IEEE Transactions on Broadcasting*, vol. 65, no. 2, pp. 369–380, Jun. 2019, doi: 10.1109/TBC.2019.2901400.
- [11] S. Rommel, D. Perez-Galacho, J. M. Fabrega, R. Munoz, S. Sales, and I. Tafur Monroy, "High-Capacity 5G Fronthaul Networks Based on Optical Space Division Multiplexing," *IEEE Transactions on Broadcasting*, vol. 65, no. 2, pp. 434–443, Jun. 2019, doi: 10.1109/TBC.2019.2901412.
- [12] T. Cisco, "Cisco Visual Networking Index : Global Mobile Data Traffic Forecast Update , 2015 – 2020," pp. 2015–2020, 2020.
- [13] Y. Jeong, S. Cho, G. Kim, C. Ahn, S. Lee, and W. Kim, "Location based service based on digital multimedia broadcasting," in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 2006, vol. 2006, pp. 147–148. doi: 10.1109/ICCE.2006.1598353.

- [14] A. Basiri *et al.*, “Indoor location based services challenges, requirements and usability of current solutions,” *Computer Science Review*, vol. 24, no. c, pp. 1–12, 2017, doi: 10.1016/j.cosrev.2017.03.002.
- [15] S.-Philip. Oriyano and Robert. Shimonski, *Client-side attacks and defense*. Syngress, 2012.
- [16] P. Liu, T. F. LaPorta, and K. Kotapati, “Cellular Network Security,” in *Network and System Security: Second Edition*, Elsevier Inc., 2013, pp. 319–351. doi: 10.1016/B978-0-12-416689-9.00011-3.
- [17] A. D. Abioye, M. K. Joseph, and H. C. Ferreira, “Comparative Study of 3G and 4GLTE Network,” *Journal of Advances in Computer Networks*, vol. 3, no. 3, pp. 247–250, 2015, doi: 10.7763/jacn.2015.v3.176.
- [18] E. Ezhilarasan and M. Dinakaran, “A Review on Mobile Technologies: 3G, 4G and 5G,” *Proceedings - 2017 2nd International Conference on Recent Trends and Challenges in Computational Models, ICRTCCM 2017*, pp. 369–373, 2017, doi: 10.1109/ICRTCCM.2017.90.
- [19] S. Chen and J. Zhao, “The Requirements , Challenges , and Technologies for 5G of Terrestrial Mobile Telecommunication,” no. May, pp. 36–43, 2014.
- [20] J. Clement, “Global mobile data traffic 2022 | Statista,” Feb. 28, 2020. <https://www.statista.com/statistics/271405/global-mobile-data-traffic-forecast/> (accessed May 08, 2020).
- [21] “Ericsson Mobility Report June 2019.” <https://www.slideshare.net/MediatelecomPolicyan/ericsson-mobility-report-june-2019> (accessed May 08, 2020).
- [22] S. O’Dea, “Mobile subscriptions worldwide 1993-2019 | Statista,” Feb. 28, 2020. <https://www.statista.com/statistics/262950/global-mobile-subscriptions-since-1993/> (accessed May 08, 2020).
- [23] “What is 5G | Everything You Need to Know About 5G | 5G FAQ | Qualcomm.” <https://www.qualcomm.com/invention/5g/what-is-5g> (accessed May 07, 2020).
- [24] S. Papavassiliou, “Software defined networking (SDN) and network function virtualization (NFV),” *Future Internet*, vol. 12, no. 1, pp. 10–12, 2020, doi: 10.3390/fi12010007.
- [25] M. Scott, “The history of Heinrich Hertz and the discovery of radio waves - WHY?,” Jul. 15, 2016. <https://why.org/segments/the-history-of-heinrich-hertz-and-the-discovery-of-radio-waves/> (accessed May 06, 2020).
- [26] B. Carroll, “Chapter 1: Introduction to Wireless Networking Concepts | Network World,” Jan. 13, 2009. <https://www.networkworld.com/article/2272293/chapter-1--introduction-to-wireless-networking-concepts.html> (accessed May 06, 2020).
- [27] Brain Marshall, Wilson Tracy V., and Johnson Bernadette, “How WiFi Works | HowStuffWorks,” Apr. 30, 2001. <https://computer.howstuffworks.com/wireless-network.htm> (accessed May 02, 2020).
- [28] “Guide to Small Cells, HetNets and 5G.” <https://5g.co.uk/guides/small-cells-hetnets-5g/> (accessed Apr. 26, 2020).
- [29] Y. Liu, A. Y. Ding, and S. Tarkoma, “Software-Defined Networking in Mobile Access Networks,” 2013.
- [30] A. Hakiri, P. Berthou, A. Gokhale, and S. Abdellatif, “AN ARCHITECTURE FOR SOFTWARE DEFINED WIRELESS NETWORKING,” *IEEE Communications Magazine*, vol. 53, no. September, pp. 48–54, 2015, doi: 10.1109/MCOM.2015.7263372.

- [31] H. Kim and N. Feamster, “Improving network management with software defined networking,” *IEEE Communications Magazine*, vol. 51, no. 2, pp. 114–119, 2013, doi: 10.1109/MCOM.2013.6461195.
- [32] “ETSI - Standards for NFV - Network Functions Virtualisation | NFV Solutions.” <https://www.etsi.org/technologies/nfv> (accessed May 17, 2020).
- [33] C. Tipantuna and P. Yanchapaxi, “Network functions virtualization: An overview and open-source projects,” *2017 IEEE 2nd Ecuador Technical Chapters Meeting, ETCM 2017*, vol. 2017-Janua, pp. 1–6, 2018, doi: 10.1109/ETCM.2017.8247541.
- [34] “A Guide to Network Function Virtualization (NFV).” <https://www.fir3net.com/Networking/Concepts-and-Terminology/a-guide-to-network-function-virtualization-nfv.html> (accessed May 18, 2020).
- [35] “What’s Network Functions Virtualization (NFV)? - SDxCentral.” <https://www.sdxcentral.com/networking/nfv/definitions/whats-network-functions-virtualization-nfv/> (accessed May 18, 2020).
- [36] “Understanding OpenStack.” <https://www.redhat.com/en/topics/openstack> (accessed Apr. 22, 2021).
- [37] “What is OpenStack? | Opensource.com.” <https://opensource.com/resources/what-is-openstack> (accessed Apr. 22, 2021).
- [38] “OpenStack: Core Components - DZone Cloud.” <https://dzone.com/articles/openstack-core-components> (accessed Apr. 23, 2021).
- [39] H. Cramer, J. Müller, T. U. Berlin, J. Mueller@tu-, and -Berlin De, “Beyond the Bar: The places where location--based services are used in the city”, doi: 10.1007/s00779--014--0772--5.
- [40] H. S. Maghdid, I. A. Lami, K. Z. Ghafoor, and J. Lloret, “Seamless Outdoors-Indoors Localization Solutions on Smartphones: Implementation and Challenges,” *ACM Computing Surveys*, vol. 48, no. 4, Feb. 2016, doi: 10.1145/2871166.
- [41] A. Basiri *et al.*, “Indoor location based services challenges, requirements and usability of current solutions,” *Computer Science Review*, vol. 24, no. c, pp. 1–12, 2017, doi: 10.1016/j.cosrev.2017.03.002.
- [42] R. Mautz, “Indoor positioning technologies,” 2012, doi: 10.3929/ethz-a-007313554.
- [43] S. Shrestha, J. Talvitie, and E. S. Lohan, “Deconvolution-based indoor localization with WLAN signals and unknown access point locations,” 2013. doi: 10.1109/ICL-GNSS.2013.6577256.
- [44] H. Nurminen *et al.*, “Statistical path loss parameter estimation and positioning using RSS measurements in indoor wireless networks,” 2012. doi: 10.1109/IPIN.2012.6418856.
- [45] J. Xiao, K. Wu, Y. Yi, L. Wang, and L. M. Ni, “Pilot: Passive device-free indoor localization using channel state information,” in *Proceedings - International Conference on Distributed Computing Systems*, 2013, pp. 236–245. doi: 10.1109/ICDCS.2013.49.
- [46] M. Ciurana, D. López, and F. Barceló-Arroyo, “SofTOA: Software ranging for toa-based positioning of WLAN terminals,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, vol. 5561 LNCS, pp. 207–221. doi: 10.1007/978-3-642-01721-6_13.
- [47] S. Sendra, M. Garcia, C. Turro, J. Lloret, C. Vera, and V. , Spain, “WLAN IEEE 802.11a/b/g/n Indoor Coverage and Interference Performance Study,” Sep. 2011. Accessed: Mar. 13, 2021. [Online]. Available: www.iaria.org
- [48] G. Hejc, J. Seitz, and T. Vaupel, “Bayesian sensor fusion of Wi-Fi signal strengths and GNSS code and carrier phases for positioning in urban environments,” *Record - IEEE*

- PLANS, Position Location and Navigation Symposium*, pp. 1026–1032, 2014, doi: 10.1109/PLANS.2014.6851470.
- [49] X. Meng, Y. Gao, K. H. Kwok, and H. Zhao, “Assessment of UWB for ubiquitous positioning and navigation,” 2012. doi: 10.1109/UPINLBS.2012.6409783.
- [50] F. Zampella, M. Khider, P. Robertson, and A. Jiménez, “Unscented Kalman filter and Magnetic Angular Rate Update (MARU) for an improved Pedestrian Dead-Reckoning,” in *Record - IEEE PLANS, Position Location and Navigation Symposium*, 2012, pp. 129–139. doi: 10.1109/PLANS.2012.6236874.
- [51] A. K. M. M. Hossain and W. S. Soh, “A comprehensive study of bluetooth signal parameters for localization,” 2007. doi: 10.1109/PIMRC.2007.4394215.
- [52] R. K. Pateriya and S. Sharma, “The evolution of RFID security and privacy: A research survey,” in *Proceedings - 2011 International Conference on Communication Systems and Network Technologies, CSNT 2011*, 2011, pp. 115–119. doi: 10.1109/CSNT.2011.31.
- [53] F. Seco, C. Plogemann, A. R. Jiménez, and W. Burgard, “Improving RFID-based indoor positioning accuracy using Gaussian processes,” 2010. doi: 10.1109/IPIN.2010.5647095.
- [54] M. Fujimoto *et al.*, “A Broad-Typed Multi-Sensing-Range Method for Indoor Position Estimation of Passive RFID Tags,” 2011.
- [55] M. Hasani, J. Talvitie, L. Sydänheimo, E. S. Lohan, and L. Ukkonen, “Hybrid WLAN-RFID Indoor Localization Solution Utilizing Textile Tag,” *IEEE Antennas and Wireless Propagation Letters*, vol. 14, pp. 1358–1361, 2015, doi: 10.1109/LAWP.2015.2406951.
- [56] A. Basiri, P. Amirian, A. Winstanley, S. Marsh, T. Moore, and G. Gales, “Seamless Pedestrian Positioning and Navigation Using Landmarks,” *Journal of Navigation*, vol. 69, no. 1, pp. 24–40, Jan. 2016, doi: 10.1017/S0373463315000442.
- [57] J. Racko, P. Brida, A. Perttula, J. Parviainen, and J. Collin, “Pedestrian dead reckoning with particle filter for handheld smartphone,” Nov. 2016. doi: 10.1109/IPIN.2016.7743608.
- [58] J. Pinchin, C. Hide, and T. Moore, “The use of high sensitivity GPS for initialisation of a foot mounted inertial navigation system,” in *Record - IEEE PLANS, Position Location and Navigation Symposium*, 2012, pp. 998–1007. doi: 10.1109/PLANS.2012.6236841.
- [59] R. Harle, “A survey of indoor inertial positioning systems for pedestrians,” *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 1281–1293, 2013. doi: 10.1109/SURV.2012.121912.00075.
- [60] I. Skog *et al.*, “Zero-Velocity Detection-An Algorithm Evaluation Radio Frequency Measurement Technology View project Signal Processing View project Stockholm 2010 Signal Processing School of Electrical Engineering Zero-Velocity Detection-An Algorithm Evaluation,” *IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING*, vol. 57, no. 11, 2010, doi: 10.1109/TBME.2010.2060723.
- [61] T. le Nguyen, Y. Zhang, and M. Griss, “ProbIN: Probabilistic inertial navigation,” in *2010 IEEE 7th International Conference on Mobile Adhoc and Sensor Systems, MASS 2010*, 2010, pp. 650–657. doi: 10.1109/MASS.2010.5663779.
- [62] J. Torres-Solis, T. H., and T. Chau, “A Review of Indoor Localization Technologies: towards Navigational Assistance for Topographical Disorientation,” in *Ambient Intelligence, InTech*, 2010. doi: 10.5772/8678.
- [63] Y. Bai, W. Jia, H. Zhang, Z. H. Mao, and M. Sun, “Helping the blind to find the floor of destination in multistory buildings using a barometer,” in *Proceedings of the Annual*

- International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, 2013, vol. 2013, pp. 4738–4741. doi: 10.1109/EMBC.2013.6610606.
- [64] “ITU-T Newslog - IPTV Standardization on Track Say Industry Experts.” <https://web.archive.org/web/20110916031736/http://www.itu.int/ITU-T/newslog/IPTV+Standardization+On+Track+Say+Industry+Experts.aspx> (accessed Mar. 31, 2020).
- [65] M. Z. Afgani, H. Haas, H. Elgala, and D. Knipp, “Visible light communication using OFDM,” *2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, TRIDENTCOM 2006*, vol. 2006, pp. 129–134, 2006, doi: 10.1109/TRIDENT.2006.1649137.
- [66] R. D. Roberts, S. Rajagopal, and S. K. Lim, “IEEE 802.15.7 physical layer summary,” *2011 IEEE GLOBECOM Workshops, GC Wkshps 2011*, pp. 772–776, 2011, doi: 10.1109/GLOCOMW.2011.6162558.
- [67] J. Vucic, C. Kottke, S. Nerreter, K. D. Langer, and J. W. Walewski, “513 Mbit/s visible light communications link based on DMT-modulation of a white LED,” *Journal of Lightwave Technology*, vol. 28, no. 24, pp. 3512–3518, 2010, doi: 10.1109/JLT.2010.2089602.
- [68] L. Zeng *et al.*, “High data rate Multiple Input Multiple Output (MIMO) optical wireless communications using white LED lighting,” *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 9, pp. 1654–1662, Dec. 2009, doi: 10.1109/JSAC.2009.091215.
- [69] A. H. Azhar, T. A. Tran, and D. O’Brien, “A gigabit/s indoor wireless transmission using MIMO-OFDM visible-light communications,” *IEEE Photonics Technology Letters*, vol. 25, no. 2, pp. 171–174, 2013, doi: 10.1109/LPT.2012.2231857.
- [70] H. Elgala, R. Mesleh, and H. Haas, “Indoor optical wireless communication: Potential and state-of-the-art,” *IEEE Communications Magazine*, vol. 49, no. 9, pp. 56–62, Sep. 2011, doi: 10.1109/MCOM.2011.6011734.
- [71] M. Biagi and A. M. Vegni, “Enabling High Data Rate VLC via MIMO-LEDs PPM”.
- [72] J. Grubor, S. Randel, K. Langer, and J. Walewski, “Towards a 100 Gb/s visible light wireless access network,” *Optics Express*, Vol. 23, Issue 2, pp. 1627-1637, vol. 23, no. 2, pp. 1627–1637, Jan. 2015, doi: 10.1364/OE.23.001627.
- [73] “(2) (PDF) Application of simulated annealing in process optimization: A review.” https://www.researchgate.net/publication/329894300_Application_of_simulated_annealing_in_process_optimization_A_review (accessed Apr. 26, 2021).
- [74] S. Voß, “Meta-heuristics: The State of the Art.”
- [75] D. Henderson, S. H. Jacobson, and A. W. Johnson, “The Theory and Practice of Simulated Annealing,” in *Handbook of Metaheuristics*, Kluwer Academic Publishers, 2006, pp. 287–319. doi: 10.1007/0-306-48056-5_10.
- [76] J. C. Spall, *Introduction to Stochastic Search and Optimization*. John Wiley & Sons, Inc., 2005. doi: 10.1002/0471722138.
- [77] T. v. Šibalija and V. D. Majstorović, *Advanced multiresponse process optimisation: An intelligent and integrated approach*. Springer International Publishing, 2015. doi: 10.1007/978-3-319-19255-0.
- [78] I. Mukherjee and P. K. Ray, “A review of optimization techniques in metal cutting processes,” *Computers and Industrial Engineering*, vol. 50, no. 1–2, pp. 15–34, May 2006, doi: 10.1016/j.cie.2005.10.001.
- [79] M. Zandieh, M. Amiri, B. Vahdani, and R. Soltani, “A robust parameter design for multi-response problems,” *Journal of Computational and Applied Mathematics*, vol. 230, no. 2, pp. 463–476, Aug. 2009, doi: 10.1016/j.cam.2008.12.019.







































- [80] H. Baseri, "Simulated annealing based optimization of dressing conditions for increasing the grinding performance," *International Journal of Advanced Manufacturing Technology*, vol. 59, no. 5–8, pp. 531–538, Mar. 2012, doi: 10.1007/s00170-011-3518-9.
- [81] P. Martinez-Julia, E. T. Garcia, J. O. Murillo, and A. F. Skarmeta, "Evaluating video streaming in network architectures for the internet of things," in *Proceedings - 7th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2013*, 2013, pp. 411–415. doi: 10.1109/IMIS.2013.76.
- [82] "Internet of Things Grant – Apply Today | NSF SBIR." <https://seedfund.nsf.gov/topics/internet-of-things/> (accessed Apr. 25, 2021).
- [83] A. Sammoud, A. Kumar, M. Bayoumi, and T. Elarabi, "Real-time streaming challenges in Internet of Video Things (IoVT)," Sep. 2017. doi: 10.1109/ISCAS.2017.8050815.
- [84] P. S. Hage, "Discrete wavelet transform based video signal processing," 2015. doi: 10.1109/EIC.2015.7230722.
- [85] L. E. Tresa and M. Sundararajan, "Comparative analysis of different wavelets in DWT for video compression," in *2014 International Conference on Circuits, Power and Computing Technologies, ICCPCT 2014*, Mar. 2014, pp. 1512–1517. doi: 10.1109/ICCPCT.2014.7054859.
- [86] Wei-Chih Ting; Kun-Hsien Lu; Chi-Wen Lo; Shu-Hsin Chang; Pin-Chuan Liu, "Smart Video Hosting and Processing Platform for Internet-of-Things | IEEE Conference Publication | IEEE Xplore." <https://ieeexplore.ieee.org/document/7059658?arnumber=7059658> (accessed Apr. 25, 2021).
- [87] X. Liu and R. Buyya, "Performance-Oriented Deployment of Streaming Applications on Cloud," *IEEE Transactions on Big Data*, vol. 5, no. 1, pp. 46–59, Jun. 2017, doi: 10.1109/tbdata.2017.2720622.
- [88] M. WILBERT, "What Is MPEG DASH And Why Should We Use It?," Mar. 14, 2016. <https://www.dacast.com/blog/explaining-mpeg-dash/> (accessed Mar. 31, 2020).
- [89] B. Al-Madani, A. Al-Roubaiey, and Z. A. Baig, "Real-Time QoS-Aware video streaming: A comparative and experimental study," *Advances in Multimedia*, vol. 2014, 2014, doi: 10.1155/2014/164940.
- [90] "How the Application Layer Works: A Brief look at Network Infrastructure." <https://www.itprc.com/how-the-application-layer-works/> (accessed Mar. 08, 2021).
- [91] H. Mukhtar, K. Salah, and Y. Iraqi, "Mitigation of DHCP starvation attack," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1115–1128, Sep. 2012, doi: 10.1016/J.COMPELECENG.2012.06.005.
- [92] "DHCP exploitation guide," 2017.
- [93] A. Shaikh, R. Tewari, and M. Agrawal, "On the effectiveness of DNS-based server selection," *Proceedings - IEEE INFOCOM*, vol. 3, pp. 1801–1810, 2001, doi: 10.1109/INFCOM.2001.916678.
- [94] C. Rohner, S. Raza, D. Puccinelli, and T. Voigt, "Security in Visible Light Communication: Novel Challenges and Opportunities," 2015. Accessed: May 19, 2020. [Online]. Available: <http://www.sensorsportal.com>
- [95] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, *Robust Key Generation from Signal Envelopes in Wireless Networks*. 2007.
- [96] S. Jana, S. Nandha Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. v Krishnamurthy, *On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments * General Terms*.

- [97] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *2007 IEEE International Conference on Ultra-Wideband, ICUWB*, vol. 2, no. 3, pp. 270–275, 2007, doi: 10.1109/ICUWB.2007.4380954.
- [98] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3. Institute of Electrical and Electronics Engineers Inc., pp. 1617–1655, Jul. 01, 2016. doi: 10.1109/COMST.2016.2532458.
- [99] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017*, Oct. 2017, pp. 193–199. doi: 10.1109/CSCN.2017.8088621.
- [100] P. Kulkarni, R. Khanai, and G. Bindagi, "Security frameworks for mobile cloud computing: A survey," in *International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016*, Nov. 2016, pp. 2507–2511. doi: 10.1109/ICEEOT.2016.7755144.
- [101] S. S. Vikas, K. Pawan, A. K. Gurudatt, and G. Shyam, "Mobile cloud computing: Security threats," 2014. doi: 10.1109/ECS.2014.6892511.
- [102] H. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and privacy in mobile cloud computing," in *2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013*, 2013, pp. 655–659. doi: 10.1109/IWCMC.2013.6583635.
- [103] V. Sucasas, G. Mantas, and J. Rodriguez, "Security Challenges for Cloud Radio Access Networks," in *Backhauling/Fronthauling for Future Wireless Systems*, Chichester, UK: John Wiley & Sons, Ltd, 2016, pp. 195–211. doi: 10.1002/9781119170402.ch9.
- [104] K. Ali, A. Alkhatar, N. Jawad, and J. Cosmas, "IoRL Indoor Location Based Data Access, Indoor Location Monitoring Guiding and Interaction Applications," in *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, BMSB*, Aug. 2018, vol. 2018-June. doi: 10.1109/BMSB.2018.8436932.
- [105] J. Ozer, "Streaming 101: The Basics – Codecs, Bandwidth, Data Rate and Resolution – Streaming Learning Center," Feb. 05, 2009. <https://streaminglearningcenter.com/articles/streaming-101-the-basics-codecs-bandwidth-data-rate-and-resolution.html> (accessed May 09, 2020).
- [106] J. Cosmas, Y. Zhang, and X. Zhang, "Internet of Radio-Light: 5G Broadband in Buildings".
- [107] J. Cosmas, Y. Zhang, and X. Zhang, "Internet of Radio-Light: 5G broadband in buildings," 2017.
- [108] Q. Zhang, W. Zhu, and Y. Q. Zhang, "Resource allocation for multimedia streaming over the Internet," *IEEE Transactions on Multimedia*, vol. 3, no. 3, pp. 339–355, Sep. 2001, doi: 10.1109/6046.944477.
- [109] "VLC: Official site - Free multimedia solutions for all OS! - VideoLAN." <https://www.videolan.org/> (accessed Apr. 24, 2021).
- [110] "The cross-platform streaming solution - VideoLAN." <https://www.videolan.org/vlc/streaming.html> (accessed Apr. 24, 2021).
- [111] Y. Zhang *et al.*, "Internet of radio and light: 5G building network radio and edge architecture," *Intelligent and Converged Networks*, vol. 1, no. 1, pp. 37–57, Sep. 2020, doi: 10.23919/ICN.2020.0002.
- [112] K. Ali *et al.*, "Measurement Campaign on 5G Indoor millimeter Wave and Visible Light Communications Multi-Component Carrier System," 2021, Accessed: Nov. 17,

2021. [Online]. Available:
https://www.researchgate.net/publication/353308204_Measurement_Campaign_on_5_G_Indoor_millimeter_Wave_and_Visible_Light_Communications_Multi-Component_Carrier_System
- [113] K. Cabaj, M. Gregorczyk, W. Mazurczyk, P. Nowakowski, and P. Zórawski, “Network Threats Mitigation Using Software-Defined Networking for the 5G Internet of Radio Light System,” *Security and Communication Networks*, vol. 2019, 2019, doi: 10.1155/2019/4930908.
- [114] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-defined networking: A comprehensive survey,” *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.
- [115] S. A. Mehdi, J. Khalid, and S. A. Khayam, “Revisiting traffic anomaly detection using software defined networking,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011, vol. 6961 LNCS, pp. 161–180. doi: 10.1007/978-3-642-23644-0_9.
- [116] R. Jin and B. Wang, “Malware detection for mobile devices using software-defined networking,” in *Proceedings - 2013 2nd GENI Research and Educational Experiment Workshop, GREE 2013*, 2013, pp. 81–88. doi: 10.1109/GREE.2013.24.
- [117] J. M. Ceron, C. B. Margi, and L. Z. Granville, “MARS: An SDN-based malware analysis solution,” in *Proceedings - IEEE Symposium on Computers and Communications*, Aug. 2016, vol. 2016-August, pp. 525–530. doi: 10.1109/ISCC.2016.7543792.
- [118] R. Rietz, A. Brinner, and R. Cwalinsky, “Improving Network Security in Virtualized Environments with OpenFlow”, doi: 10.1145/1355734.1355746.
- [119] J. H. Cox, R. J. Clark, and H. L. Owen, “Leveraging SDN to improve the security of DHCP,” in *SDN-NFV Security 2016 - Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization, co-located with CODASPY 2016*, Mar. 2016, pp. 35–38. doi: 10.1145/2876019.2876028.
- [120] J. L. Wang and Y. C. Chen, “An SDN-based defensive solution against DHCP attacks in the virtualization environment,” in *2017 IEEE Conference on Dependable and Secure Computing*, Oct. 2017, pp. 529–530. doi: 10.1109/DESEC.2017.8073876.
- [121] “How DHCP works Explained with Examples.”
<https://www.computernetworkingnotes.com/ccna-study-guide/how-dhcp-works-explained-with-examples.html> (accessed Oct. 23, 2021).
- [122] J Footman, “Cisco Network Basics - Port Security,” *online*, 2017.
<https://www.ccieby30.com/post/cisco-network-basics-port-security> (accessed Jul. 17, 2021).
- [123] H. Mukhtar, K. Salah, and Y. Iraqi, “Mitigation of DHCP starvation attack,” *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1115–1128, Sep. 2012, doi: 10.1016/J.COMPELECENG.2012.06.005.
- [124] T. OConnor, “Detecting and Responding to Data Link Layer Attacks | SANS Institute,” Oct. 15, 2010. <https://www.sans.org/white-papers/33513/> (accessed Oct. 23, 2021).
- [125] N. Feamster, J. Rexford, E. Zegura, and G. Tech, “The Road to SDN: An Intellectual History of Programmable Networks”.
- [126] J. Ordóñez-Lucena, P. Ameigeiras, Di. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, “Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges,” *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80–87, May 2017, doi: 10.1109/MCOM.2017.1600935.

- [127] “What is NFV?” <https://www.redhat.com/en/topics/virtualization/what-is-nfv> (accessed Oct. 24, 2021).
- [128] “Assistive technologies to support people with disabilities - Think Tank.” [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI\(2015\)559513](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)559513) (accessed Nov. 28, 2021).

Appendix 1

-  0,0.csv
-  0,40.csv
-  0,-40.csv
-  0,80.csv
-  0,-80.csv
-  40,0.csv
-  -40,0.csv
-  40,40.csv
-  40,-40.csv
-  -40,40.csv
-  -40,-40.csv
-  40,80.csv
-  40,-80.csv
-  80,0.csv
-  80,40.csv
-  80,-40.csv
-  80,80.csv
-  80,-80.csv
-  120,0.csv
-  120,40.csv
-  120,-40.csv
-  120,80.csv
-  120,-80.csv
-  160,0.csv
-  160,40.csv
-  160,-40.csv
-  160,80.csv
-  160,-80.csv
-  200,0.csv
-  200,40.csv
-  200,-40.csv
-  200,80.csv
-  200,-80.csv
-  240,0.csv
-  240,40.csv
-  240,-40.csv
-  240,80.csv
-  240,-80.csv

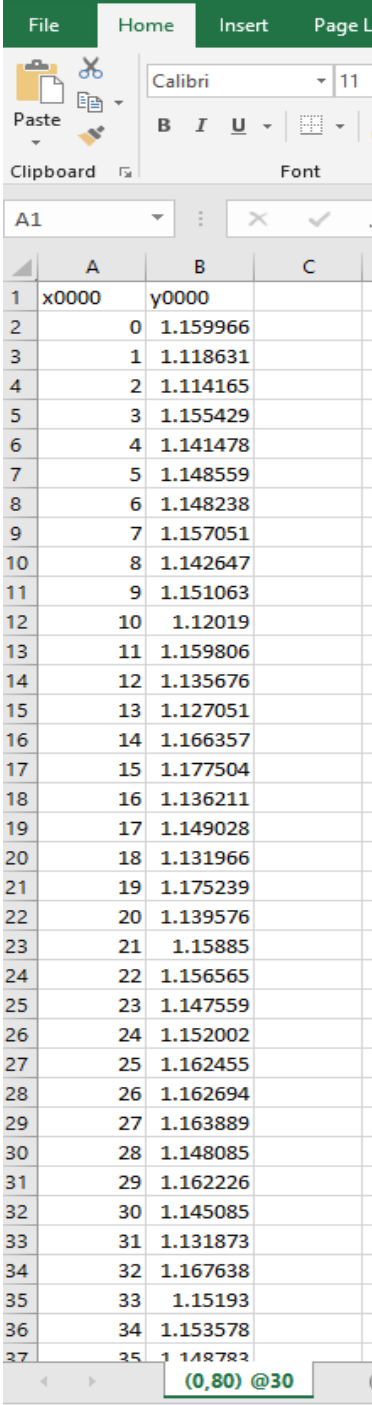
Appendix 1

Appendix Appendix 2

Appendix 2

Appendix Appendix Appendix 3

Appendix Appendix 4



	A	B	C
1	x0000	y0000	
2	0	1.159966	
3	1	1.118631	
4	2	1.114165	
5	3	1.155429	
6	4	1.141478	
7	5	1.148559	
8	6	1.148238	
9	7	1.157051	
10	8	1.142647	
11	9	1.151063	
12	10	1.12019	
13	11	1.159806	
14	12	1.135676	
15	13	1.127051	
16	14	1.166357	
17	15	1.177504	
18	16	1.136211	
19	17	1.149028	
20	18	1.131966	
21	19	1.175239	
22	20	1.139576	
23	21	1.15885	
24	22	1.156565	
25	23	1.147559	
26	24	1.152002	
27	25	1.162455	
28	26	1.162694	
29	27	1.163889	
30	28	1.148085	
31	29	1.162226	
32	30	1.145085	
33	31	1.131873	
34	32	1.167638	
35	33	1.15193	
36	34	1.153578	
37	35	1.148783	

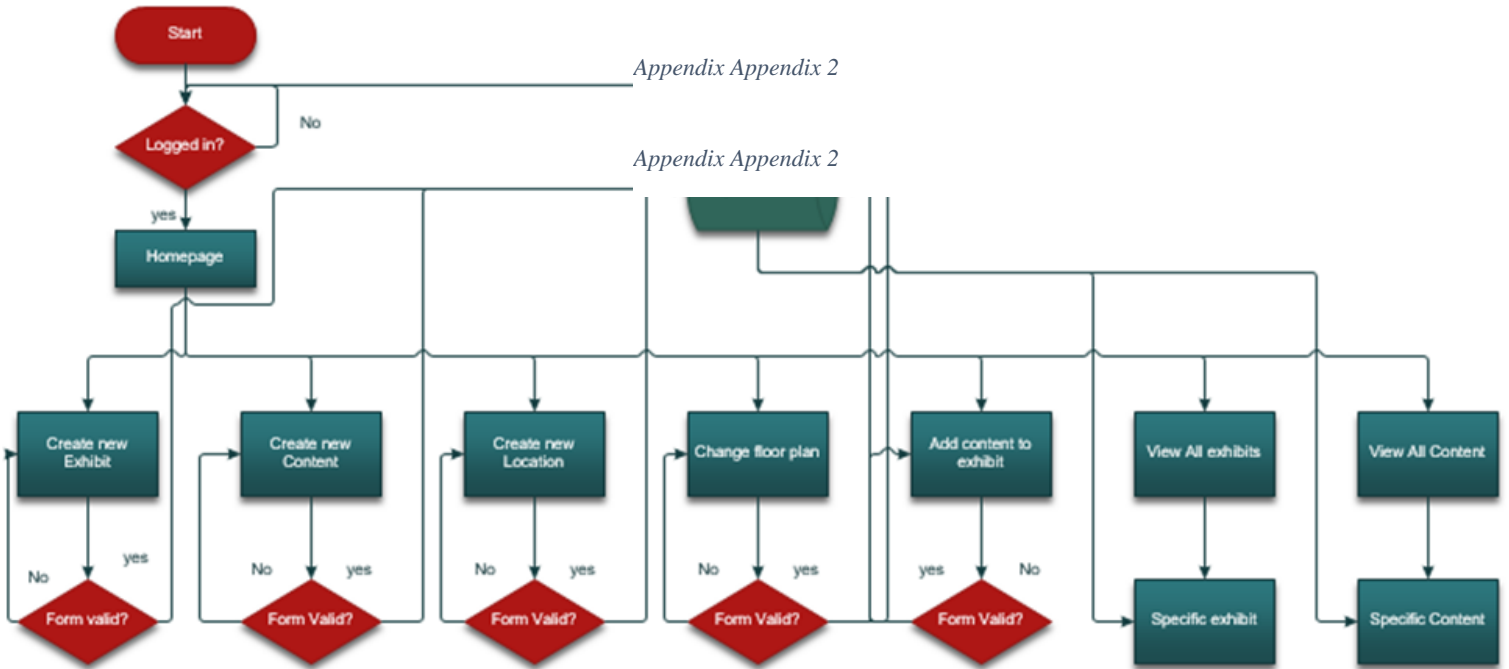
Appendix 2

Appendix Appendix 2

Appendix 2

Appendix Appendix 2

Appendix Appendix 2



Appendix 2

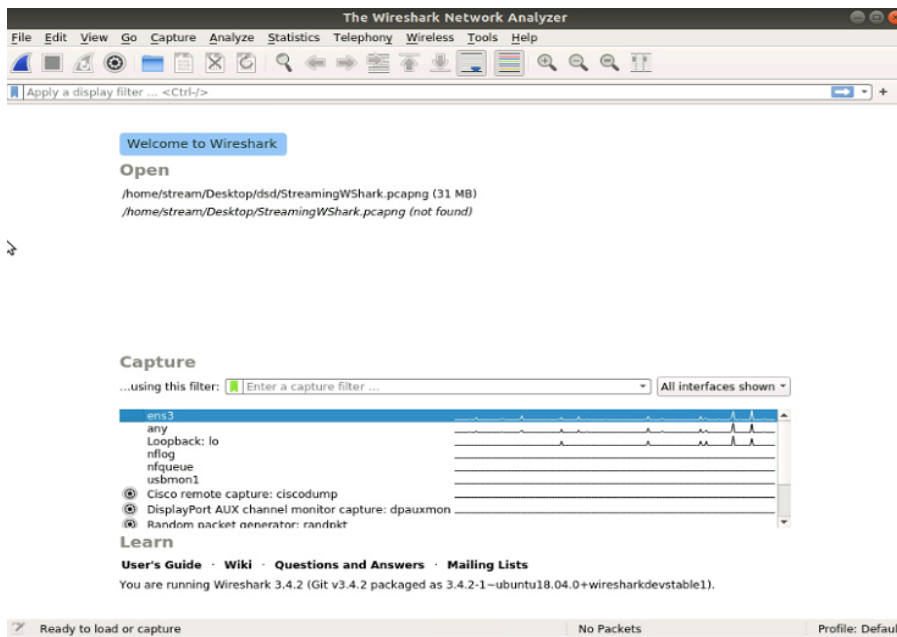
Appendix 2

Appendix 2

Appendix 2

Appendix 3 How to capture packets using Wireshark

1. Open Wireshark as root/administrator
2. You will need to pick the interface you want to listen too



3. Type ICMP (Internet Control Message Protocol) as your packet filter and double click on your interface for instance my interface is eno3.
4. Type UDP in the display filter and start streaming using your VLC
5. You will see the packets displayed with all the details as seen below

The screenshot displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets, all of which are UDP packets. The middle pane shows the detailed view of a selected packet, revealing its structure: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (UDP). The bottom pane shows the raw packet bytes in hexadecimal and ASCII.

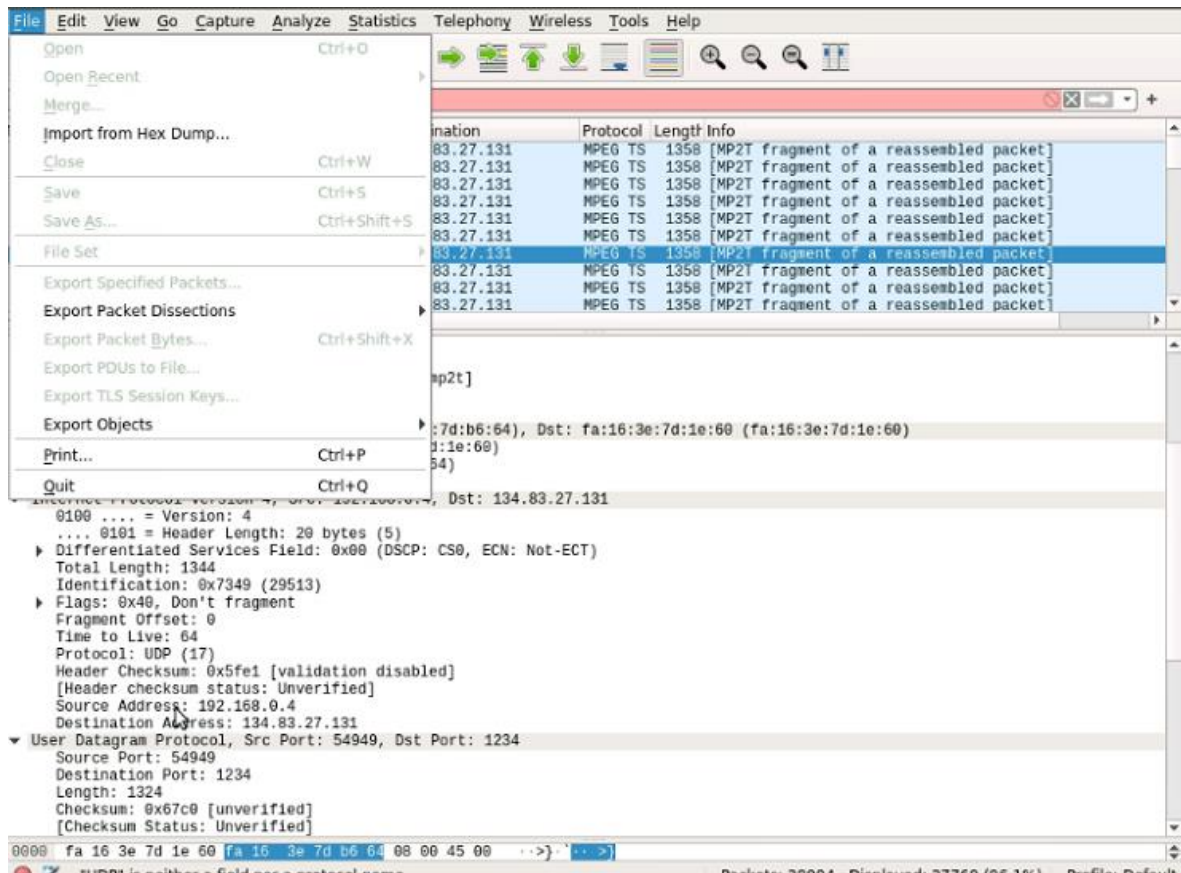
No.	Time	Source	Destination	Protocol	Length	Info
432	270.850310157	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
433	270.850324346	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
434	270.850336789	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
435	270.850348963	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
436	270.850361356	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
437	270.850370358	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
438	270.850378958	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
439	270.850390696	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
440	270.850400227	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
441	270.850408857	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
442	270.850421888	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
443	270.850433420	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
444	270.850442861	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
445	270.850451282	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
446	270.850459762	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
447	270.850470543	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
448	270.850484154	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
449	270.850496661	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
450	270.850506858	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
451	270.850535219	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
452	270.850550469	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
453	270.850573904	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]
454	270.850600000	192.168.0.4	134.83.27.131	MPEG TS	1358	[MP2T fragment of a reassembled packet]

```

[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:mp2t]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: fa:16:3e:7d:b6:64 (fa:16:3e:7d:b6:64), Dst: fa:16:3e:7d:1e:60 (fa:16:3e:7d:1e:60)
  Destination: fa:16:3e:7d:1e:60 (fa:16:3e:7d:1e:60)
  Source: fa:16:3e:7d:b6:64 (fa:16:3e:7d:b6:64)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 134.83.27.131
  0100 ... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1344
  Identification: 0x7349 (29513)
  Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x5fe1 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.4
  Destination Address: 134.83.27.131
User Datagram Protocol, Src Port: 54949, Dst Port: 1234
  Source Port: 54949
  Destination Port: 1234
  Length: 1324
  Checksum: 0x67c0 [unverified]
  [Checksum Status: Unverified]
0000 fa 16 3e 7d 1e 60 fa 16 3e 7d b6 64 00 00 45 00 ...
  
```

UDP is neither a field nor a protocol name. Packets: 28846 - Displayed: 27769 (96.3%) Profile: Default

6. Press File, Export to any format you want



Appendix 5