

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ  
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ  
Τμήμα Ηλεκτρολόγων & Ηλεκτρονικών Μηχανικών  
[www.eee.uniwa.gr](http://www.eee.uniwa.gr)

Θηβών 250, Αθήνα-Αιγάλεω 12241  
Τηλ. +30 210 538-1225, Fax. +30 210 538-1226



UNIVERSITY of WEST ATTICA  
FACULTY OF ENGINEERING  
Department of Electrical & Electronics Engineering  
[www.eee.uniwa.gr](http://www.eee.uniwa.gr)

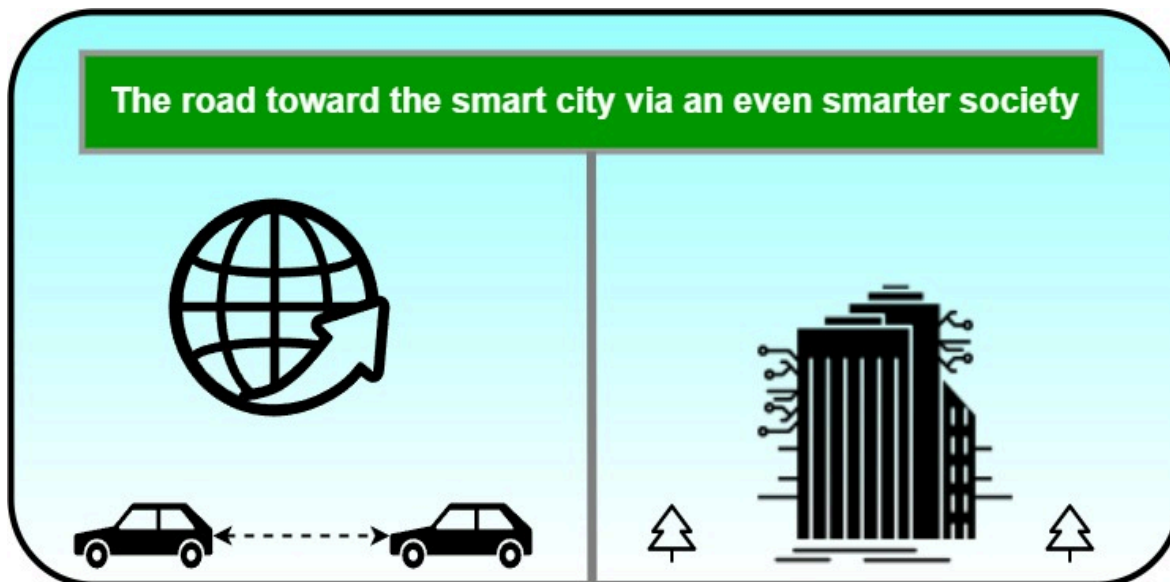
250, Thivon Str., Athens, GR-12241, Greece  
Tel:+30 210 538-1225, Fax:+30 210 538-1226

Πρόγραμμα Μεταπτυχιακών Σπουδών  
Ηλεκτρικές & Ηλεκτρονικές Επιστήμες μέσω Έρευνας

Master of Science By Research in  
Electrical & Electronics Engineering

## ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τίτλος (ελληνικά): Αυτοοργανούμενα δίκτυα LPWAN και 5G για την υποστήριξη αυτοματοποιημένων διαδικασιών για υπηρεσίες Έξυπνης Πόλης



Μεταπτυχιακός Φοιτητής: Αθανάσιος Τρίγκας, AM MSCRES-0055  
Επιβλέπων: Παναγιώτης Παπαγεώργας, Καθηγητής

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, 2/12/2023

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ  
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ  
Τμήμα Ηλεκτρολόγων & Ηλεκτρονικών Μηχανικών  
[www.eee.uniwa.gr](http://www.eee.uniwa.gr)

Θηβών 250, Αθήνα-Αιγάλεω 12241  
Τηλ. +30 210 538-1225, Fax. +30 210 538-1226



UNIVERSITY of WEST ATTICA  
FACULTY OF ENGINEERING  
Department of Electrical & Electronics Engineering  
[www.eee.uniwa.gr](http://www.eee.uniwa.gr)

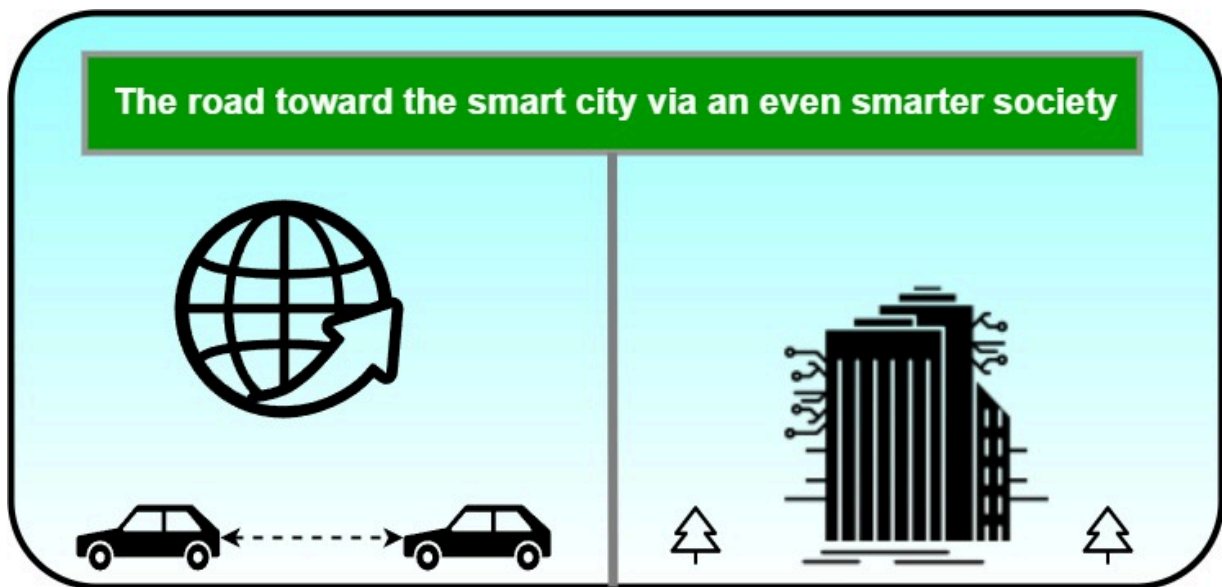
250, Thivon Str., Athens, GR-12241, Greece  
Tel:+30 210 538-1225, Fax:+30 210 538-1226

Πρόγραμμα Μεταπτυχιακών Σπουδών  
Ηλεκτρικές & Ηλεκτρονικές Επιστήμες μέσω Έρευνας

Master of Science By Research in  
Electrical & Electronics Engineering

## MSc Thesis

*Title (in English): Ad-hoc LPWAN and 5G Networks for the support of automated smart-city applications*



Student: Trigkas, Athanasios, Registration Number MSCRES-0055

MSc Thesis Supervisor: Prof. Papageorgas Panagiotis

ATHENS-EGALEO, 2/12/2023

Η Μεταπτυχιακή Διπλωματική Εργασία έγινε αποδεκτή, εξετάστηκε και βαθμολογήθηκε από την εξής τριμελή εξεταστική επιτροπή:

Επιβλέπων	Μέλος	Μέλος
Παναγιώτης Παπαγέωργας	Γεώργιος Χλούπης	Πέτρος Καραϊσάς
Καθηγητής	Αναπληρωτής Καθηγητής	Αναπληρωτής Καθηγητής
	Τμήμα Μηχανικών Τοπογραφίας και Γεωπληροφορικής	

## ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Τρίγκας Αθανάσιος του Δημητρίου με αριθμό μητρώου MSCRES-0055 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών «Ηλεκτρικές και Ηλεκτρονικές Επιστήμες μέσω Έρευνας» του Τμήματος Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής διπλωματικής εργασίας και κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος. Τέλος, βεβαιώνω ότι η εργασία αυτή δεν έχει κατατεθεί στο πλαίσιο των απαιτήσεων για τη λήψη άλλου τίτλου σπουδών ή επαγγελματικής πιστοποίησης πλην του παρόντος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών



Αθανάσιος Τρίγκας

**Copyright ©** Με επιφύλαξη παντός δικαιώματος. All rights reserved.

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ και Τρίγκας Αθανάσιος,**

**Φεβρουάριος, 2023**

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας Μεταπτυχιακής Διπλωματικής Εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον/την συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον/την συγγραφέα του και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις θέσεις του επιβλέποντος μέλους ΔΕΠ, της επιτροπής εξέτασης ή τις επίσημες θέσεις του Τμήματος και του Ιδρύματος.

## ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία μελετάει την υλοποίηση δικτύων LPWAN και 5G για την υποστήριξη αυτοματοποιημένων διαδικασιών έξυπνης πόλης. Παρουσιάζονται οι ανάγκες μίας πόλης οι οποίες μπορούν να εξυπηρετηθούν από αυτές τις τηλεπικοινωνιακές τεχνολογίες, στην συνέχεια οι τεχνολογίες αυτές μελετώνται με σκοπό να προσδιορισθεί η χρηστικότητα τους σε περιβάλλον πόλης.

Οι τεχνολογίες LPWAN βασίζονται σε μικρά πακέτα δεδομένων με σκοπό να παρέχουν ευρεία τηλεπικοινωνιακή κάλυψη με μικρές ενεργειακές απαιτήσεις και μικρό κόστος. Τα χαρακτηριστικά αυτά τις θέτουν ιδανικές για την ανάπτυξη εφαρμογών βασισμένες σε δίκτυα ασύρματων αισθητήρων (Wireless Sensor Network, WSN) στο πεδίο μίας πόλης. Ειδικότερα, σε σημεία στα οποία η παροχή τροφοδοσίας είναι δύσκολη. Εκτός αυτού, η ασφάλεια των δεδομένων των αισθητήριων κόμβων είναι ένα κρίσιμο σημείο το οποίο αξίζει να σταθούμε σε ένα πολυπληθές περιβάλλον όπως μία πόλη.

Το 5G είναι η πέμπτη γενιά κινητής τηλεφωνίας, η οποία με καινοτόμες τεχνολογίες έρχεται να εξελιχθεί από την υπάρχουσα τέταρτη γενιά (4G) με ρυθμούς δεδομένων μεγαλύτερων του 1 Gbps και παρέχοντας συνδεσιμότητα παντού και πάντα. Με τα δίκτυα 5G, γίνεται εφικτή η απομακρυσμένη μετάδοση μεγάλου όγκου δεδομένων με μικρή καθυστέρηση άρα και την ανάπτυξη σχετικών εφαρμογών στο πεδίο της πόλης. Οι εφαρμογές τέτοιου τύπου θα έχουν αρκετές ενεργειακές απαιτήσεις, ωστόσο η συνδεσιμότητα παντού και πάντα του 5G προτείνεται να προσφέρει λύσεις και στο πεδίο των ασύρματων αισθητήρων προσφέροντας εύκολη και έγκυρη σύνδεση στο δίκτυο.

Λαμβάνοντας υπόψιν τα παραπάνω, αξιολογούμε τις παραπάνω τεχνολογίες προσομοιώνοντάς τες σε σενάρια τα οποία μπορούν να αντιπροσωπεύουν πραγματικές υλοποιήσεις σε μία πόλη. Τέτοια σενάρια είναι η επικοινωνία Vehicle-to-vehicle (V2V) με την χρήση 5G σταθμών καθώς και ένα Early Warning System (EWS) σενάριο βασισμένο στην τεχνολογία LPWAN NB-IoT.

Τέλος υλοποιείται και παρουσιάζεται κόμβος NB-IoT ο οποίος επικοινωνεί μετρήσεις αισθητήριων μέσω του καινοτόμου πρωτοκόλλου MQTT το οποίο συνιστάται για λειτουργίες IoT. Ο κόμβος χρησιμοποιεί επίσης κρυπτογράφηση βασισμένη σε SSL/TLS για να εγγυηθεί την ασφάλεια των δεδομένων.

**ΛΕΞΕΙΣ – ΚΛΕΙΔΙΑ:** 5G, EWS, LPWAN, MQTT, NB-IoT, OMNeT++, SIM7000, SSL, V2V, WSN

# ABSTRACT

This thesis studies the implementation of LPWAN and 5G networking technologies to support automated smart city applications. The applications of a city that can be served by these telecommunication technologies are presented, then these technologies are studied in order to determine their usability in a city environment.

Modern LPWAN technologies are based on small data packets in order to provide wide telecommunication coverage with low energy requirements and low monetary cost. These characteristics make them ideal for the development of applications based on wireless sensor networks (Wireless Sensor Network, WSN) in the sphere of a city. In particular, in places where power supply is difficult. Besides, the data security of the sensor nodes is a critical point that should be considered in a crowded environment such as a city.

5G is the fifth generation of mobile telephony, which features innovative technologies in order to evolve from the existing fourth generation (4G). 5G promises data rates greater than 1 Gbps and to provide connectivity everywhere and always. 5G networks open the possibility for transmission of large volumes of data with little latency, and thus the development of relevant applications in the field of the city. Although, 5G applications will have several energy requirements, the «everywhere and always» connectivity of 5G is proposed to offer solutions in the field of WSN as well, offering an easy and validated connection to the network.

Considering the above, we evaluate these technologies by simulating them in case studies that can represent real city implementations. Such studies are Vehicle-to-vehicle (V2V) communication using 5G stations as well as an Early Warning System (EWS) based on the LPWAN NB-IoT technology.

Finally, an NB-IoT node is developed which communicates sensor measurements via the innovative application-layer MQTT protocol, recommended for IoT applications. The node also uses SSL/TLS based encryption to guarantee data security.

**KEYWORDS:** 5G, EWS, LPWAN, MQTT, NB-IoT, OMNeT++, SIM7000, SSL, V2V, WSN

## ΕΥΧΑΡΙΣΤΙΕΣ

Ευχαριστώ τον επιβλέπων καθηγητή μου κύριο Παναγιώτη Παπαγεώργα ο οποίος με μεράκι με καθοδήγησε στο Μεταπτυχιακό πρόγραμμα και απλόχερα παρείχε τους απαραίτητους πόρους και χρόνο για την ολοκλήρωσή του. Ευχαριστώ τους καθηγητές του Μεταπτυχιακού, τους συναδέλφους και τους καθηγητές του STRESQLab. Ευχαριστώ τους καθηγητές του Τμήματος Ηλεκτρονικών Μηχανικών Τ.Ε. που με την στήριξή τους κατάφερα να εισαχθώ στο πρόγραμμα και ιδιαίτερα τον κύριο Αθανάσιο Κοντογεώργο ο οποίος με έχει στηρίξει και καθοδηγήσει από προπτυχιακό επίπεδο. Ευχαριστώ την οικογένειά μου και ιδιαίτερα τις γιαγιάδες μου οι οποίες με μεγάλωσαν. Ευχαριστώ τον Κώστα ο οποίος με βοήθησε στην ολοκλήρωση του της κατασκευής του κόμβου. Ευχαριστώ τον φίλο μου τον Σταύρο που όσο άσχημα και αν του έχει φερθεί η ζωή, αυτός είναι πάντα έτοιμος να με στηρίξει. Ευχαριστώ όλους αυτούς που πρόσφεραν αφιλοκερδώς την βοήθειά τους αποδεικνύοντας ότι η ζωή δεν περιορίζεται σε ένα συγκαβατικό «Δούναι και Λαβείν» είτε αυτό ανταποκρίνεται σε υλικά ή πνευματικά αγαθά.



## ΠΙΝΑΚΑΣ ΣΥΜΒΟΛΩΝ-ΑΚΡΩΝΥΜΙΩΝ-ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

- LPWAN: Low-power wide-area network
- WSN: Wireless Senso Network
- PSM: power saving mode
- eDRx: extended Discontinuous Reception
- UE: User Equipment
- SC-FDMA: Single-Carrier Frequency Division Multiple Access
- OFDM: Orthogonal Frequency Division Multiplexing
- TLS: Transport Layer Security
- SSL: Secure Sockets Layer
- TCP: Transmission Control Protocol
- HTTP: Hypertext Transfer Protocol
- D2D: Device to device
- QoS: Quality of Service
- IIoT Industrial Internet of Things
- IoT: Internet of Things
- GNSS: Global Navigation Satellite System
- IP: Internet Protocol
- PDP: packet data protocol
- APN: access point name
- V2V: Vehicle-to-vehicle
- MQTT: Message Queuing Telemetry Transport
- V2X: Vehicle-to-Everything
- mIoT: Massive Internet of Things
- uRLLC: Ultra-Reliable and Low Latency Communication
- eMBB: Enhanced Mobile Broadband
- MEC: Mobile Edge Computing
- SDN: Software-Defined Networking
- AR: Augmented Reality
- VR: Virtual reality
- IDE: Integrated Development Environment
- SA: Standalone Access όπου το gNB
- NSA: Non-Standalone Access

- VANETs: Vehicular Ad Hoc Networks
- ITS: Intelligent Transportation System
- CSS : Chirp Spread Spectrum
- NB-IoT: Narrowband Internet of Things
- 3GPP: 3rd Generation Partnership Project
- FDMA: Frequency Division Multiple Access
- SMS: Short Message Service
- MMS: Multimedia Message Service
- LTE: Long-Term Evolution
- MIMO : Multiple Input Multiple Output
- mm-wave: Millimetre Wave
- DVR: Distance Vector Routing
- AODV: Ad Hoc On-Demand Distance Vector
- DSR: Dynamic Source Routing
- SC-FDMA: Single-Carrier Frequency Division Multiple Access
- AWGN: Additive white Gaussian noise
- LTE-A: Long Term Evolution Advanced
- NIC: Network Interface Card
- RLC: Radio Control Link
- PDPCP: Packet Data Convergence Protocol
- LCID: Logical Connection Identifier
- TTI: Transmission Time Interval
- RB: Resource Block
- WAVE: Wireless Access in Vehicular Environments
- POI: Point of Interest
- TraCI: Traffic Control Interface
- V2I: Vehicle-to-Infrastructure
- AT Commands: Attention Commands
- API: Application Programming Interface
- WS: WebSocket
- WSS: WebSocket Secure

## ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ.....	4
ΕΙΣΑΓΩΓΗ .....	13
ΚΕΦΑΛΑΙΟ 1: LPWAN, 5G ΚΑΙ Η ΕΞΥΠΝΗ ΠΟΛΗ.....	14
1. LPWAN .....	14
2. 5G.....	15
3. Εφαρμογές έξυπνης πόλης.....	18
3.1 Δίκτυα αισθητήρων και έξυπνη πόλη.....	19
3.2 Περαιτέρω εφαρμογές έξυπνης πόλης βασισμένες σε 5G .....	20
ΚΕΦΑΛΑΙΟ 2: ΜΕΛΕΤΗ LORAWAN ΚΑΙ NB-IOT.....	23
1. LoRa Wan.....	23
1.1 LoRa Mesh.....	25
1.2 LoRa 2.4 GHz .....	26
2. NB-IoT.....	26
2.1 Device to Device NB-IoT.....	29
2.2 NB-IoT και 5G.....	29
3. Σύγκριση LoRa Wan και NB-IoT για εφαρμογές πόλης .....	30
ΚΕΦΑΛΑΙΟ 3: Προσομοίωση δικτύων NB-IoT και 5G.....	33
1. Προσομοίωση NB-IoT με την χρήση του AWR Design Environment.....	33
1.1 AWR Design Environment .....	33
1.2 Προσομοίωση της NB-IoT κάλυψης του Πεντελικού όρους με το AWR Design Environment .....	34
1.3 Σύνοψη αποτελεσμάτων .....	38
2. Προσομοίωση σε οχήματα με το OMNeT++, το Simu5G και το SUMO.....	39
2.1 OMNeT++.....	39
2.2 Η βιβλιοθήκη INET .....	40
2.3 Η βιβλιοθήκη SimuLTE.....	42
2.4 Η βιβλιοθήκη Simu5G.....	45
2.5 Η βιβλιοθήκη Veins.....	48
2.6 SUMO.....	49
2.7 Προσομοίωση σεναρίου κίνησης με το Simu5G και το SUMO .....	51
2.8 Συμπεράσματα αποτελεσμάτων και σκέψεις.....	58
ΚΕΦΑΛΑΙΟ 4: Κατασκευή Ασφαλούς NB-IoT κόμβου .....	59
1. Σύνοψη των πρωτοκόλλων που θα χρησιμοποιηθούν.....	59
1.1. Πρωτόκολλο TCP/IP.....	59

1.2.	Πρωτόκολλο TLS.....	59
1.3.	Πρωτόκολλο MQTT (Message Queuing Telemetry Transport) .....	59
1.4.	AT Εντολές.....	60
1.5.	Arduino IDE.....	61
2.	Εργαλεία που χρησιμοποιήθηκαν.....	62
2.1.	EMQX MQTT Broker.....	63
2.2.	DFRobot SIM7000E.....	63
2.3.	OPENSSL.....	64
2.4.	EMnify SIM Cards.....	64
2.5.	Node-Red.....	65
3.	Υλοποίηση.....	65
3.1.	Εγκατάσταση του EMQX Broker στον Server.....	65
3.2.	Δημιουργία πιστοποιητικών με το OpenSSL.....	67
3.3.	Εγκατάσταση πιστοποιητικών στο SIM7000E .....	69
3.4.	Εγκατάσταση πιστοποιητικών στην Node-Red.....	70
3.5.	Προγραμματισμός και έλεγχος του SIM7000E με AT Commands .....	72
3.6.	Αυτοματοποιημένος MQTT SSL κόμβος.....	75
3.7.	Βελτιώσεις .....	78
	ΣΥΜΠΕΡΑΣΜΑΤΑ .....	79
	ΒΙΒΛΙΟΓΡΑΦΙΑ-ΠΗΓΕΣ.....	80

---

Στο Κεφάλαιο 1 γίνεται μία εισαγωγή στις τεχνολογίες LPWAN, το 5G και τις εφαρμογές μίας έξυπνης πόλης τις οποίες μπορούν να εξυπηρετήσουν. Μελετάται η έννοια LPWAN και τα χαρακτηριστικά της και παρουσιάζονται τεχνολογίες με τις οποίες μπορεί να υλοποιηθεί. Παρουσιάζεται το 5G ως η πέμπτη γενιά κινητής τεχνολογίας και αναλύονται τα χαρακτηριστικά τα οποία την ξεχωρίζουν από τις προηγούμενες. Τέλος, παρουσιάζονται σενάρια εφαρμογών έξυπνης πόλης τα οποία μπορούν να εξυπηρετηθούν είτε από εφαρμογές LPWAN είτε μέσω του 5G.

Στο Κεφάλαιο 2 αναλύονται οι LPWAN τεχνολογίες NB-IoT και LoRaWAN. Μελετώνται ως προς την αρχιτεκτονική τους, τα ραδιοηλεκτρικά χαρακτηριστικά τους, την δρομολόγησή των πακέτων τους και εξετάζεται η συνεργασία τους με 5G δίκτυα. Κατ' επέκτασιν αξιολογούνται ως προς την χρηστικότητα τους στο περιβάλλον έξυπνης πόλης.

Στο Κεφάλαιο 3 παρουσιάζονται τα εργαλεία προσομοίωσης AWR Design Environment, Simu5G στο OMNeT++ και SUMO. Παρουσιάζεται το σενάριο έγκυρης προειδοποίησης (Early Warning System) φωτιάς στο Πεντελικό όρος μέσω NB-IoT το οποίο εξετάζεται μέσω του AWR DE ως προς την χωρική διάταξη NB-IoT κόμβων καθώς και την αποφυγή ραδιοπαρεμβολών με το υπάρχον δίκτυο κινητής τηλεφωνίας. Στην συνέχεια, αναπτύσσεται δίκτυο οδικής κυκλοφορίας μέσω του SUMO και σε συνεργασία με το Simu5G αξιολογείται σενάριο V2V για την απόκρισή του μέσω 5G σε σύγκριση με την τέταρτη γενιά κινητής τηλεφωνίας (4G). Τα αποτελέσματα των προσομοιώσεων δείχνουν ότι η υλοποίηση των σεναρίων είναι δυνατόν να επιτευχθούν.

Στο Κεφάλαιο 4 περιγράφεται η ανάπτυξη ενός κρυπτογραφημένου NB-IoT κόμβου ο οποίος επικοινωνεί δεδομένα θερμοκρασίας και υγρασίας, καθώς και του server με τον οποίο επικοινωνεί. Περιγράφονται τα πρωτόκολλα τα οποία χρησιμοποιήθηκαν, τα εργαλεία με την κοστολόγησή τους και στην συνέχεια υλοποιείται η ανάπτυξη αυτού με σκοπό να αντιπροσωπεύει ένα κόμβο μίας πρακτικής εφαρμογής με όσο κατά το δυνατόν μικρότερο κόστος και μεγαλύτερης αυτοματοποίησης. Αξιολογείται και παρουσιάζονται πιθανές βελτιώσεις.

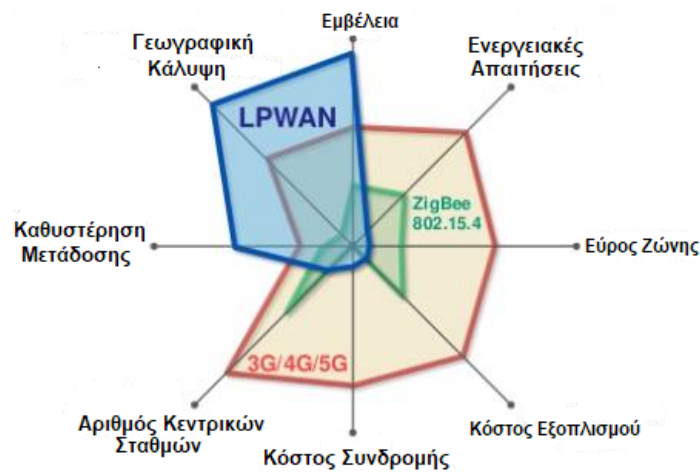
## 1. LPWAN

Πολλές από τις IoT συσκευές τις οποίες χρησιμοποιούμε σήμερα συμπεριλαμβάνουν στηρίζονται σε τηλεπικοινωνιακές τεχνολογίες οι οποίες έχουν μεγάλες απαιτήσεις ενέργειας και καταφέρνουν να μεταδίδουν δεδομένα μόνο σε μικρή εμβέλεια (πρωτόκολλα όπως Wi-Fi, Bluetooth, Zigbee). Αυτά τα χαρακτηριστικά θέτουν αυτές τις τεχνολογίες ακατάλληλες για καταστάσεις όπως απομακρυσμένη παρακολούθηση αισθητήριών όπου υπάρχει η ανάγκη κάλυψης μεγάλων αποστάσεων με πολύ μικρή κατανάλωση ενέργειας [1].

Οι τεχνολογίες LPWAN (low-power wide-area network) σκοπεύουν να λύσουν αυτό το πρόβλημα με εμβέλεια της τάξεως των 10 χιλιομέτρων και χρησιμοποιώντας μπαταρίες των 3V σε συσκευές μικρού κόστους, προτείνουν μία διάρκεια ζωής συσκευών της τάξεως των 10 χρόνων. Αυτό επιτυγχάνεται διότι οι τεχνολογίες αυτές αναλαμβάνουν να στέλνουν μικρά πακέτα δεδομένων με χαμηλό ρυθμό ενώ ενσωματώνουν μηχανισμούς κατά τους οποίους η συσκευή βρίσκεται σε κατάσταση ύπνου (sleep mode). Εφόσον η ενέργεια η οποία χρησιμοποιείται είναι λίγη, ανοίγει παράλληλα και ο δρόμος για μεθόδους συγκομιδή ενέργειας από το περιβάλλον (energy harvesting). Έτσι οι τεχνολογίες αυτές μπορούν να προσφέρουν λύσεις για ασύρματα δίκτυα αισθητήρων στο περιβάλλον πόλης καλύπτοντας κάθε άκρο της, ακόμα και σε σημεία όπου η παροχή ενέργειας είναι δύσκολη. Συνοψίζοντας, τα χαρακτηριστικά των τεχνολογιών αυτών είναι[1]:

- Επικοινωνία σε μεγάλες αποστάσεις
- Μικρή κατανάλωση ενέργειας
- Χαμηλός ρυθμός δεδομένων
- Χαμηλό κόστος συσκευών και εγκατάστασης
- Απλή τοπολογία δικτύου
- Ευρεία κάλυψη
- Επεκτασιμότητα δικτύου

Κάποιοι οργανισμοί οι οποίοι έχουν αναλάβει την ανάπτυξη τέτοιων τεχνολογιών είναι η LoRa, η SigFox, η Weightless, και η DASH7. Ωστόσο παρόμοιες τεχνολογίες αναπτύσσονται και για την κινητή τηλεφωνία όπως το NB-IoT και το eMTC[2]. Στο LoRa και το NB-IoT θα σταθούμε πιο αναλυτικά στο Κεφάλαιο 3.



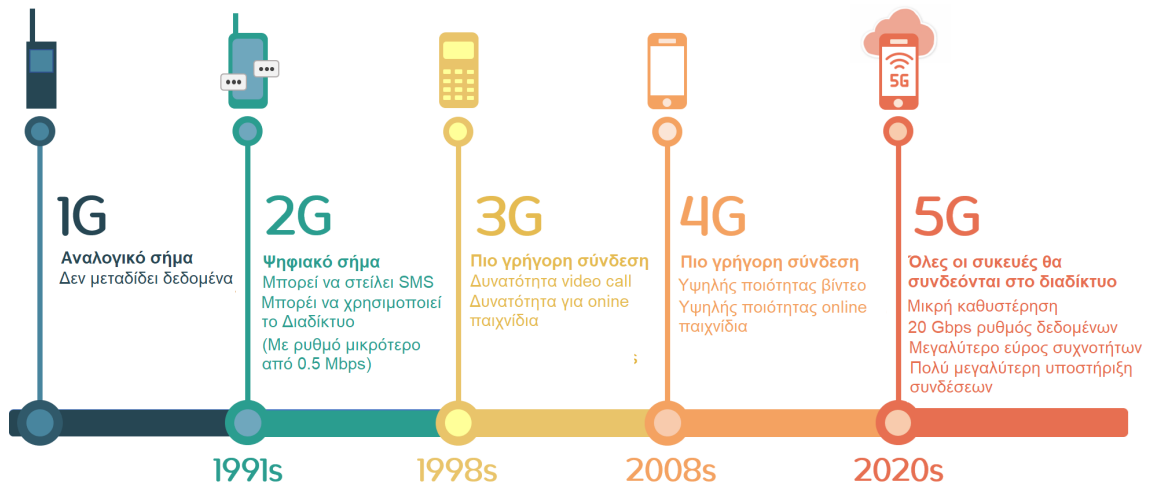
Εικόνα 1: LPWAN και άλλες τηλεπικοινωνιακές τεχνολογίες, [30]

## 2. 5G

Η έννοια 5G αντιπροσωπεύει την πέμπτη γενιά κινητής τηλεφωνίας η οποία έρχεται να προσφέρει λύσεις στο διαδίκτυο των πραγμάτων και να ανοίξει τον δρόμο για καινοτόμες εφαρμογές. Ακολουθεί μία σύντομη ιστορική αναδρομή των γενιών κινητής τηλεφωνίας [3][4].

1. Η πρώτη γενιά (1G) κινητής τηλεφωνίας παρουσιάστηκε στις αρχές της δεκαετίας του 1980 και χρησιμοποιούσε μόνο τηλεφωνικές κλήσεις. Στο 1G η αριθμολογία Frequency Division Multiple Access (FDMA) χρησιμοποιήθηκε η οποία χωρίζει την συχνότητα σε κανάλια και καταχωρεί το κάθε κανάλι σε κάθε χρήστη την φορά. Το 1G είχε κακή ποιότητα φωνής, δεν επέτρεπε την κρυπτογράφηση και ο μέγιστος ρυθμός δεδομένων ήταν της τάξεως των 2.4 Kbps.
2. Η δεύτερη γενιά (2G) εμφανίστηκε την δεκαετία του 1990 και πρόσφερε καλύτερες υπηρεσίες φωνής με ψηφιακά σήματα και μεγαλύτερο ρυθμό δεδομένων, της τάξεως των 35 Kbps. Εδώ συναντάμε το πρωτόκολλο GSM το οποίο έφερε την ενεργοποίηση υπηρεσιών όπως το Short Message Service (SMS) και το Multimedia Message Service (MMS).
3. Η τρίτη γενιά (3G) εμφανίστηκε στα τέλη της δεκαετίας του 2000. Το 3G έδωσε την δυνατότητα της παγκόσμιας περιαγωγής δεδομένων και σύνδεση των κινητών τηλεφώνων στα πολυμέσα του διαδικτύου με ρυθμούς δεδομένων της τάξεως των 3.1 Mbps.
4. Η τέταρτη γενιά (4G) και το πρωτόκολλο Long-Term Evolution (LTE) παρουσιάστηκε στις αρχές του της δεκαετίας του 2010. Σχήματα τα οποία εισήγαγε το 4G είναι η αριθμολογία Orthogonal Frequency Division Multiplexing (OFDM) και η μέθοδος Multiple Input Multiple Output (MIMO).

Με την τεχνική OFDM, ένα ψηφιακό σήμα μπορεί να διαχωριστεί σε μικρότερα κανάλια μικρού εύρους ζώνης με διαφορετικές συχνότητες. Με την τεχνική MIMO οι συσκευές 4G μπορούν να διαχειρίζονται δεδομένα με παραπάνω από μία πηγές διαθέτοντας πολλαπλές κεραιές. Και τα δύο αυτά σχήματα είχαν ως αποτέλεσμα ενισχυμένη κάλυψη και αντίθεση με το 3G, το 4G είναι βασισμένο ολοκληρωτικά στο πρωτόκολλο IP. Κατ' επέκτασιν, υπήρχε πλέον η δυνατότητα για την μετάδοση υψηλής ποιότητας βίντεο και πρόσβαση στο διαδίκτυο με ρυθμό δεδομένων μέχρι και 100 Mbps.



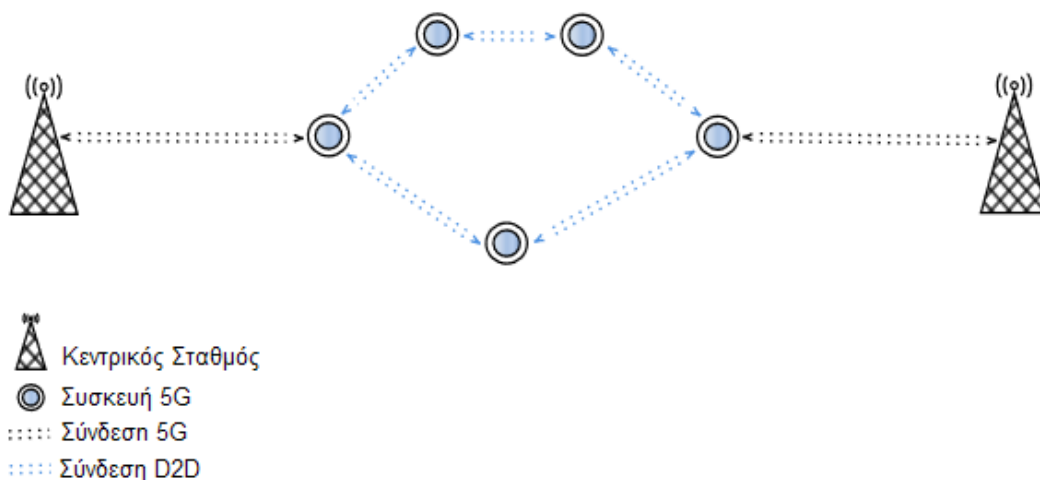
Εικόνα 2: Εξέλιξη γενεών κινητής τηλεφωνίας, [31]

Συγκριτικά με το 4G, το 5G υπόσχεται να υποστηρίξει 10 με 100 φορές υψηλότερους ρυθμούς δεδομένων, της τάξεως των 10 Gbps, καθώς και την υποστήριξη πολλών περισσότερων συσκευών με συνδεσιμότητα κάθε στιγμή και παγκόσμια γεωγραφική κάλυψη, παρέχοντας εξελιγμένη ασφάλεια και γρήγορη μετάδοση δεδομένων [3]. Επίσης το 5G θα χρησιμοποιεί 10 φορές λιγότερη ενέργεια, παρατείνοντας σημαντικά την διάρκεια ζωής μπαταρίας των συσκευών[3]. Η ιδέα λοιπόν πίσω από το 5G είναι η ιδέα δικτύωσης όλων το συσκευών στο δίκτυο κάθε στιγμή και παντού καθώς και εφαρμογών οι οποίες βασίζονται σε μεγάλους ρυθμούς δεδομένων [3]. Για να συμβεί αυτό, κάποιες τεχνολογίες οι οποίες θα ενεργοποιηθούν στα 5G δίκτυα είναι [3][5][6]:

- Η επικοινωνία της συσκευής προς συσκευή (Device to Device, D2D) κατά την οποία οι συσκευές θα μπορούν να συνδέονται μεταξύ τους χωρίς την άμεση επικοινωνία με κάποιον κεντρικό σταθμό. Εδώ η επικοινωνία μπορεί να είναι μόνο από συσκευή σε συσκευή ή κάποια συσκευή να αναλαμβάνει να επικοινωνήσει και να ενημερώσει τον κεντρικό σταθμό. Η επικοινωνία D2D θα προσφέρει κάλυψη χρηστών σε νεκρά σημεία, εξοικονόμηση ενέργειας διότι το πακέτων δεδομένων θα διανύει μικρότερες αποστάσεις μέχρι να φθάσει στον

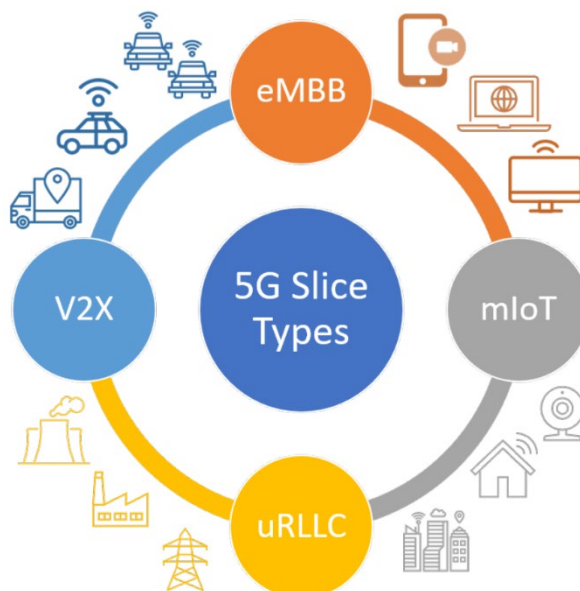


προορισμό και διαθεσιμότητα περισσότερων ραδιοφωνικών πόρων μιας και μόνο η τελική συσκευή συνδέεται στον κεντρικό σταθμό.



**Εικόνα 3: Επικοινωνία D2D**

- Την δικτύωση βάσει λογισμικού (Software-Defined Networking, SDN) όπου τα υπάρχοντα φυσικά δίκτυα θα διαχωριστούν σε μικρότερα εικονικά υποδίκτυα (Network Slices, NS) και το κάθε υποδίκτυο θα αναλαμβάνει να εξυπηρετήσει διαφορετικές διαδικασίες προσφέροντας ευελιξία στην διαχείριση πόρων οι οποίοι ικανοποιούν διαφορετικές ανάγκες. Πιο συγκεκριμένα, οι μορφές υποδικτύων οι οποίες έχουν προταθεί από τον οργανισμό 3GPP είναι[5]:
  1. Το υποδίκτυο Enhanced Mobile Broadband (eMBB), αυτό το υποδίκτυο θα καλύπτει τις ανάγκες της κινητής τηλεφωνία με μεγαλύτερο ρυθμό δεδομένων και ευρύτερη κάλυψη.
  2. Το υποδίκτυο Massive Internet of Things (mIoT), αυτό το υποδίκτυο θα μπορεί να καλύπτει μεγάλο εύρος συσκευών σε μια μικρή περιοχή. Οι εφαρμογές mIoT έχουν να κάνουν με συσκευές μικρού κόστους και μικρής κατανάλωσης ενέργειας που ανταλλάζουν μικρά πακέτα δεδομένων, συσχετίζονται λοιπόν με τα LPWAN.
  3. Το υποδίκτυο Ultra-Reliable and Low Latency Communication (uRLLC), αυτό το υποδίκτυο αφορά τις πιο κρίσιμες επικοινωνίες, όπως πχ περιπτώσεις έκτακτης ανάγκης όπου χρειαζόμαστε γρήγορη και αξιόπιστη μετάδοση δεδομένων .
  4. Το υποδίκτυο Vehicle-to-Everything (V2X), αυτό το υποδίκτυο δύναται να υποστηρίξει την επικοινωνία μεταξύ οχημάτων καθώς και την επικοινωνία των οχημάτων με το περιβάλλον.



**Εικόνα 4: Υποδίκτυα 5G, [3]**

- Η τεχνολογία Mobile Edge Computing (MEC). Η τεχνολογία θα χρησιμοποιεί μικρούς κινητούς σταθμούς όπου θα γίνεται η επεξεργασία στο σημείο που ανταλλάζονται τα δεδομένα, την άκρη (edge) δηλαδή του δικτύου χωρίς να χρειάζεται να μεταδοθούν τα δεδομένα στο κεντρικό νέφος του δικτύου. Αυτό έχει ως αποτέλεσμα την γρήγορη επεξεργασία δεδομένων και μετάδοση δεδομένων καθώς πλέον αυτή γίνεται από γειτονικούς κόμβους, ταυτόχρονα και την αποφόρτιση του δικτύου από υπολογιστικά καθήκοντα μεταφοράς δεδομένων και κατ' επέκτασιν και την εξοικονόμηση ενέργειας.
- Η ανάπτυξη ακόμα περισσότερων σχημάτων MIMO, το οποίο θα επιτρέψει σε σταθμούς και συσκευές να επικοινωνούν ταυτόχρονα στο ίδιο κανάλι συντηρώντας τον ίδιο ρυθμό δεδομένων.
- Οι ζώνες συχνοτήτων Millimetre Wave (mm-wave), ραδιοφωνικά κύματα τα οποία ανταποκρίνονται στις συχνότητες 30 and 300 GHz, σε αντίθεση με την χρήση συχνοτήτων κάτω από 6 GHz οι οποίες χρησιμοποιούνταν στην κινητή τηλεφωνία μέχρι το 4G. Αυτές οι συχνότητες υπόσχονται την γρήγορη μετάδοση μεγάλων πακέτων δεδομένων, ωστόσο μιας και τα μικρά κύματα δυσκολεύονται να διαδοθούν τους στον χώρο, θα πρέπει να συνδυαστούν με άλλες τεχνολογίες όπως η MEC για να αποφύγουν εμπόδια σε πυκνοκατοικημένες πόλεις.

### 3. Εφαρμογές έξυπνης πόλης

Θα μπορούσαμε να διαχωρίσουμε της εφαρμογές έξυπνης πόλης σε δύο σκέλη, το πρώτο σκέλος είναι τα συστήματα τα οποία βασίζονται στις εφαρμογές που βασίζονται στα ασύρματα δίκτυα αισθητήρων με μικρά πακέτα δεδομένων. Για το πρώτο σκέλος, λύσεις μπορούν να βρεθούν μέσω των τεχνολογιών LPWAN ενώ ανταποκρίνονται στο

υποδίκτυο mIoT του 5G. Το δεύτερο σκέλος έχει να κάνει με λύσεις τις οποίες μπορεί να προσφέρει το 5G σε περιπτώσεις όπου χρειαζόμαστε μεγάλο ρυθμό δεδομένων για εφαρμογές βασισμένες σε μεγάλο όγκο δεδομένων και άμεσης μετάδοσης.

### 3.1 Δίκτυα αισθητήρων και έξυπνη πόλη

Μία έξυπνη πόλη είναι αυτή η οποία χρησιμοποιεί το διαδίκτυο των πραγμάτων για να βελτιώσει τις υποδομές της και τις υπηρεσίες τις. Έτσι σκοπός μίας έξυπνης είναι να βελτιώσει την ποιότητα των υπηρεσιών της προς του πολίτες, να χρησιμοποιήσει με τον βέλτιστο τρόπο τα κοινά αγαθά και να μειώσει το κόστος των υπηρεσιών της [7]. Τα LPWAN ασύρματα δίκτυα αισθητήρων μπορεί να είναι δομικά στο να γίνει αυτό πραγματικότητα και να προσφέρουν υπηρεσίες όπως [7]:

- Την συντήρηση για παλιά ιστορικά κτίρια μιας πόλης με συνεχή παρακολούθηση και αναγνώριση. Υπολογίζοντας την δομική τους ακεραιότητα με αισθητήρες που παρακολουθούν παραμέτρους όπως η δόνηση.
- Την διαχείριση των απορριμμάτων και την ανακύκλωσή τους. Αισθητήρες μπορούν να προσδιορίζουν πότε ένας κάδος απορριμμάτων είναι γεμάτος και η θέση τους να προσδιορίζει τα δρομολόγια των απορριμματοφόρων.
- Παρατήρηση της ατμοσφαιρικής ρύπανσης. Αισθητήρες μπορούν να παρακολουθούν την ατμοσφαιρική ρύπανση σε διάφορα σημεία της πόλης και να προειδοποιούν τις αρχές αλλά και τους πολίτες ώστε να μπορούν να διαχειριστούν αυτές τις περιοχές.
- Διαχείριση τη ηχορύπανσης μίας πόλης. Ακουστικοί αισθητήρες μπορούν να παρατηρούν την ηχορύπανση μίας πόλης σε ώρες αιχμής και να διαχειρίζονται την κίνηση ώστε να την μειώσουν.
- Την κυκλοφοριακή συμφόρηση και το παρκάρισμα. Ένα σύστημα το οποίο λαμβάνει πληροφορίες για της κυκλοφοριακή συμφόρηση στον δρόμο, μπορεί να πληροφορεί τον οδηγό για εναλλακτικές οδούς ώστε να αποφύγει την συμφόρηση. Παρόμοια, αισθητήρες μπορούν να ενημερώνουν τον οδηγό για ελεύθερα parking κατά μήκος της πόλης.
- Ένα σύστημα με έξυπνους μετρητές μπορεί να παρακολουθεί την ενεργειακή κατανάλωση μίας πόλης ώστε να βρεθούν οι πηγές της κατανάλωσης και να τεθούν προτεραιότητες για την σωστή χρήση της. Π.χ. η διαχείριση των φωτών μίας πόλης μπορεί να εξαρτάται από συνθήκες όπως η ώρα της ημέρας, ο καιρός και την ύπαρξη ανθρώπων, η βέλτιστη διαχείριση αυτών μπορεί να αποδώσει σημαντική εξοικονόμηση ενέργειας. Παρόμοια, η βέλτιστη διαχείριση φρέσκου νερού και λυμάτων θα μπορούσε να βοηθήσει σημαντικά την υδραυλική κάλυψη μίας πόλης.



Εικόνα 5: Αισθητήρες και έξυπνη πόλη, [32]

### 3.2 Περαιτέρω εφαρμογές έξυπνης πόλης βασισμένες σε 5G

Εκτός από τα δίκτυα αισθητήρων και της μετρήσεις τις οποίες μπορούμε να πάρουμε για να υλοποιήσουμε έξυπνες εφαρμογές στην πόλη, μεγάλο ενδιαφέρον χρήζουν και οι εφαρμογές οι οποίες βασίζονται στην γρήγορη απόκριση και το μεγάλο όγκο δεδομένων που προσφέρει το 5G. Τα χαρακτηριστικά του αυτά μπορεί να είναι κρίσιμα για καταστάσεις έκτακτης ανάγκης, και ανοίγουν τον δρόμο και για την ευέλικτη χρήση τεχνολογιών όπως επαυξημένης (Augmented Reality, AR) και εικονικής (Virtual reality, VR) πραγματικότητας [3]. Κάποιες εφαρμογές μπορεί να είναι [3][4][6]:

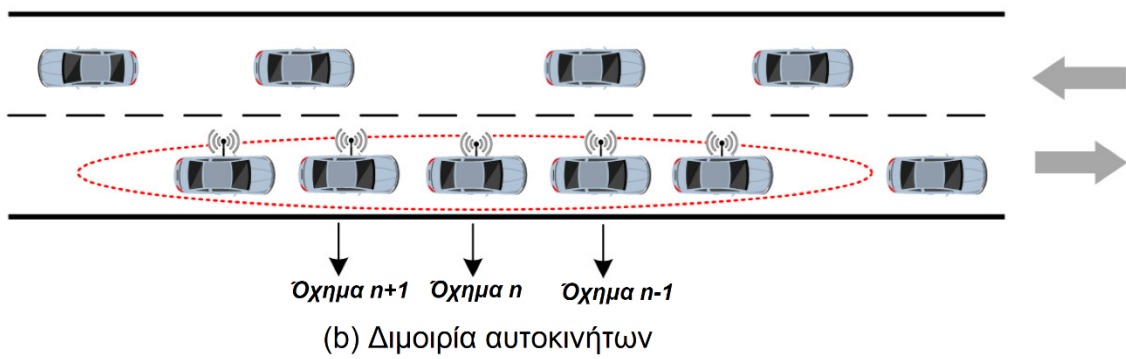
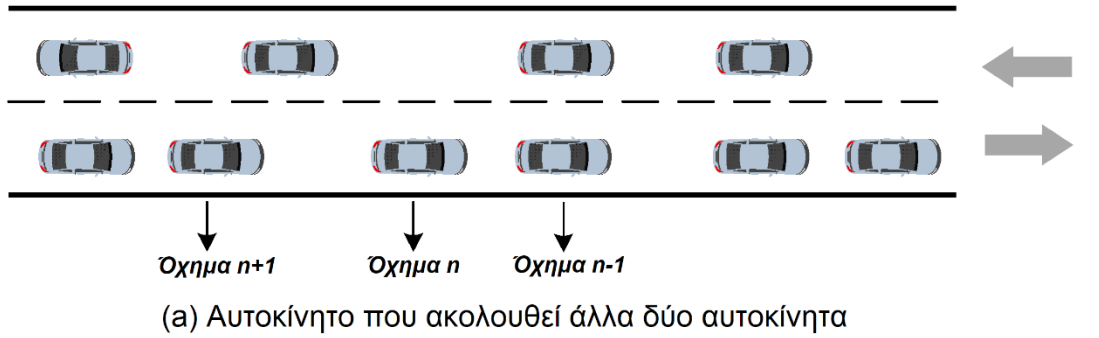
- Την τήλε-ιατρική και την αποκέντρωση των νοσοκομείων. Η δικτύωση των ασθενών και η παρακολούθησή τους από τους αρμόδιους γιατρούς συνεχόμενα με έγκυρες ειδοποιήσεις. Επίσης, την δυνατότητα μέσω υψηλής ποιότητας εικόνας και την χρήση AR και VR οι γιατροί να έχουν την δυνατότητα για κάποια απομακρυσμένη διάγνωση.
- Τον βιομηχανικό αυτοματισμό υποβοηθούμενο από τεχνολογίες όπως αυτόματα συγχρονισμένα οχήματα, επικοινωνία μέσω εφαρμογών τεχνητής νοημοσύνης, εφαρμογές AR και VR για να βοηθήσουν τους τεχνικούς να επισκευάσουν βλάβες.
- Των μετασχηματισμό των μέσων ψυχαγωγίας και διαφήμισης από μία απλή εικόνα στην δυνατότητα για την άμεση επικοινωνία με κινούμενες εικόνες σε εφαρμογές AR και VR.

Στο πλαίσιο μίας πόλης, ιδιαίτερο ενδιαφέρον παρουσιάζει η χρήση του 5G για την διαχείριση έξυπνων μέσων μεταφοράς, το υποδίκτυο V2X. Εκτός του ότι τα οχήματα μπορούν να συνδέονται με τους μαζεύουν μετρήσεις από τους διάσπαρτους αισθητήρες

μέσα στην πόλη, μέσα από την άμεση απόκριση του δικτύου για την επικοινωνία ενός οχήματος με άλλα οχήματα καθώς και με τους πεζούς μπορούμε να καταφέρουμε να αποτραπούν ατυχήματα. Π.χ. σε εφαρμογές όπως η πέδηση έκτακτης ανάγκης, η γρήγορη μετάδοση του 5G δείχνει να μειώνει την απόκριση φρεναρίσματος από 1.5 m στο 4G σε μόλις 2.5 cm[4]. Ο μεγάλος ρυθμός δεδομένων επίσης μπορεί να επιτρέψει στα οχήματα να διαμοιράζονται δεδομένα όπως ροή βίντεο στον δρόμο το οποίο για τη γρήγορη ενημέρωση και πλοήγησή τους. Επίσης ανοίγονται δρόμοι για εφαρμογές όπως:

- Απομακρυσμένη (remote driving) και αυτόνομη οδήγηση (autonomous driving). Δεδομένου ότι το όχημα θεωρείται πάντα συνδεδεμένο στο δίκτυο με μεγάλο ρυθμό δεδομένων, ο έλεγχός του μπορεί πλέον να γίνεται απομακρυσμένα με κατάλληλες εφαρμογές, π.χ. ο απομακρυσμένος έλεγχος αυτοκινήτου από μία εφαρμογή VR. Ταυτόχρονα η διαρκής επικοινωνία των αυτοκινήτων μεταξύ τους μπορεί να ενημερώνει όλα τα αυτοκίνητα για τις θέσεις τους στον δρόμο και τις διαδρομές που ακολουθούν. Έτσι με το 5G ανοίγονται δρόμοι όπου η όσο το δυνατόν πιο αυτόνομη οδήγηση δεν εξαρτάται μόνο από ισχυρούς υπολογιστές σε πολυτελή αυτοκίνητα αλλά είναι μέρος ενός μεγαλύτερου δικτύου. Και οι δύο αυτές εφαρμογές χρειάζονται πολύ μικρή καθυστέρηση μεταξύ των μηνυμάτων, της τάξεως των 5 ms [3], αξιοπιστία μηνυμάτων κοντά στο 100% [3] και ρυθμούς δεδομένων της τάξεως των 50 Mbps [3]. Οι εφαρμογές αυτές μπορεί να είναι ιδιαίτερα χρηστικές σε μέσα μαζικής μεταφοράς όπως τα λεωφορεία όπου η διαδρομή τους είναι προβλέψιμη αρά και πιο εύκολα διαχειρίσιμη.
- Μία εφαρμογή με μεγάλο ενδιαφέρον είναι η διαχείριση κίνησης σε διμοιρίες (Vehicles Platooning), με την εφαρμογή αυτή τα οχήματα θα επικοινωνούν έτσι ώστε να μπορούν να ταξιδεύουν οργανωμένα σε πολύ μικρή προσδιορισμένη απόσταση μεταξύ τους. Σε αυτήν την περίπτωση τα οχήματα θα μπορούν να συμμετέχουν σε μια διμοιρία ανταλλάζοντας μηνύματα με άλλα οχήματα και το δίκτυο για την ταχύτητά τους, το φρενάρισμα και τον προορισμό τους ώστε να οργανωθούν στον χώρο, και θα ενημερώνονται τακτικά για τα υπόλοιπα οχήματα της διμοιρίας. Λόγω της κοντινής τους απόστασης και της σταθερής του ταχύτητας θα μειώνεται η κίνηση, θα υπάρχει οικονομία στο καύσιμο, θα μειώνονται τα ατυχήματα και θα δίνουν τον χρόνο στον οδηγό να ασχοληθεί με άλλες δραστηριότητες. Για να επιτευχθεί αυτό η επικοινωνία πρέπει να γίνεται πολύ γρήγορα με καθυστέρηση μικρότερη από 10 με 25 milliseconds [3] και η αξιοπιστία των μηνυμάτων πρέπει να είναι της τάξεως 90 με 99.99% [3], όπου μικρότερη καθυστέρηση και μεγαλύτερη αξιοπιστία χρειαζόμαστε σε αυτοκίνητα τα οποία είναι ήδη αυτοματοποιημένα. Η θέση γεωγραφικού μήκους πρέπει να

δίνεται με ακρίβεια 0.5 m [3] ενώ τα μηνύματα που ανταλλάσσονται πρέπει να είναι της τάξεως 10 με 30 το δευτερόλεπτο [3]. Ιδιαίτερα για την Ελλάδα και ιδίως για την Αθήνα η οποία πάσχει από κυκλοφοριακή συμφόρηση, η οργάνωση της κίνησης σε διμοιρίες θα είχε ιδιαίτερη σημασία.

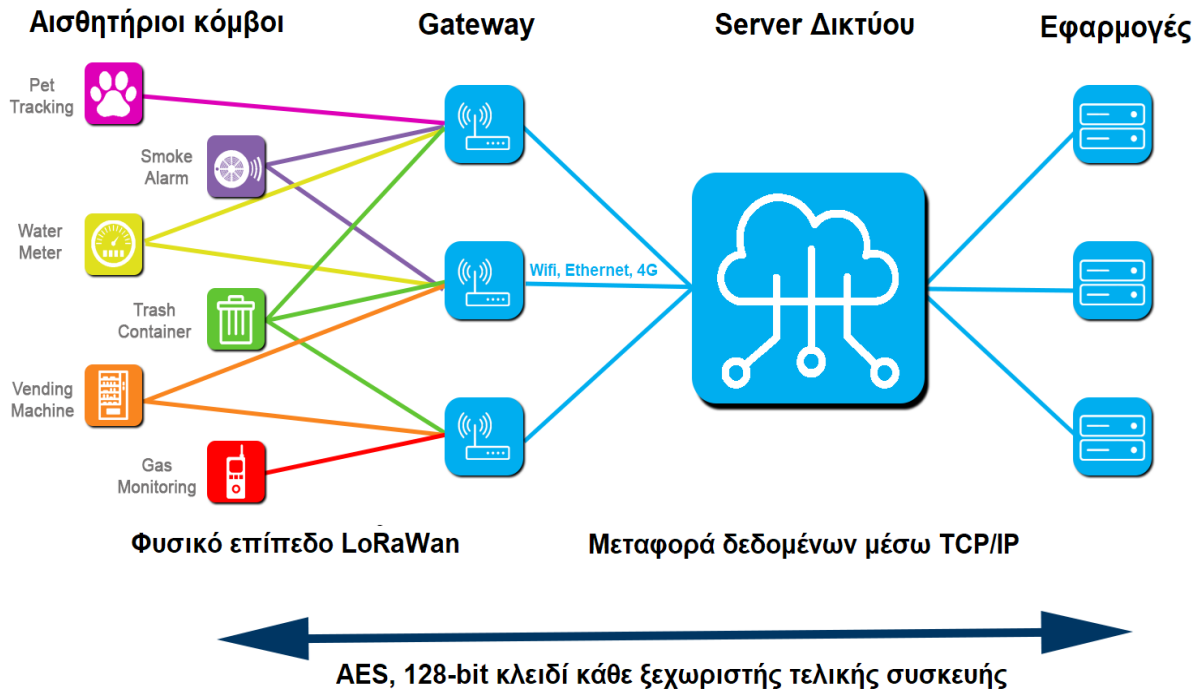


Εικόνα 6: Παράδειγμα Vehicles Platooning, [33]

## 1. LoRaWan

Το LoRaWan (Long Range) είναι μία LPWAN τεχνολογία η οποία αναπτύσσεται από την Semtech Corporation. Μία αρχιτεκτονική LoRaWan και μπορεί να διαχωριστεί σε δύο μέρη, το front end και το back end. Στο front end βρίσκουμε τους αισθητήριους κόμβους οι οποίοι ανταλλάζουν δεδομένα με ένα κεντρικό σταθμό gateway με ημι-αμφίδρομη επικοινωνία χρησιμοποιώντας το φυσικό επίπεδο του LoRa [8][9][10]. Στο back end τα δεδομένα αυτά μεταβιβάζονται για την επεξεργασία τους σε ένα κεντρικό server, συνήθως μέσω Wi-Fi[10]. Οι LoRaWan. Το φυσικό επίπεδο του LoRa κάνει χρήση της διαμόρφωσης Chirp Spread Spectrum (CSS), αυτός ο τρόπος διαμόρφωσης επιτρέπει την ανίχνευση σήματος σε πολύ μικρή ισχύ και έτσι καταφέρνουμε να καλύπτουμε πολύ μεγάλες αποστάσεις [8][10]. Σε ένα σύστημα LoRaWan, οι κόμβοι δεν έχουν δυνατότητες δρομολόγησης και χρησιμοποιούν το πρωτόκολλο ALOHAnet όπου τα δεδομένα τους συλλέγονται από το gateway σε τοπολογία αστέρα πριν αυτά μεταφερθούν στο back-end [8][10].

Το LoRaWan χρησιμοποιεί πολύ μικρό εύρος ζώνης, στο εύρος των 125 kHz. Η διαμόρφωση CSS χρησιμοποιεί συντελεστές διασποράς (spreading factors, SF) από 7 μέχρι 12 με ρυθμούς μετάδοσης από 0,3 Kbps μέχρι 50 Kbps. Χαμηλότεροι SF μας προσφέρουν υψηλότερο ρυθμό δεδομένων αλλά και χειρότερο σήμα προς θόρυβο (SNR). Ο μέγιστος όγκος δεδομένων ενός μηνύματος LoRaWan για SF 7 είναι 242 bytes ενώ για SF 12 είναι 51 bytes όπου τα 13 bytes χρησιμοποιούνται για την αναγνώριση της συσκευής από το back-end [8]. Οι αισθητήριοι κόμβοι του LoRaWan συνήθως αποτελούνται από μικροελεγκτές οι οποίοι ενεργοποιούνται από μπαταρίες χαμηλής ισχύος μέσο χρόνο ζωής τα 10 χρόνια και προτείνονται με εμβέλεια της τάξεως των 10 km ενώ μία μέση διάρκεια ζωής μπορούν να θεωρηθούν τα 10 χρόνια. Το κόστος ενός κόμβου LoRaWan κυμαίνεται γύρω στα 3-5 ευρώ ενώ το κόστος του gateway κυμαίνεται στα 300 ευρώ.



**Εικόνα 7: Αρχιτεκτονική LoRaWan, [34]**

Το LoRaWan ενεργοποιείται στις ύπο-GHz ISM συχνότητες οι οποίες έχουν περιορισμούς όπως 1% κύκλος καθηκόντων (duty cycle), 14 dBm μέγιστη εκπεμπόμενη ισχύ και 2.15 dbi μέγιστο κέρδος κεραίας. Αν δηλαδή ένας κόμβος εκπέμπει για 1 sec, πρέπει να περιμένει άλλα 99 sec για να εκπέμψει ξανά καθώς και δεν μπορεί να χρησιμοποιηθεί κατευθυντική κεραία για της εύρεση διαθέσιμου gateway[9]. Οι ύπο-GHz ISM συχνότητες για την Ευρώπη είναι:

- 863-870 MHz με κεντρικές συχνότητες: 868.10 MHz, 868.30 MHz, 868.50 MHz
- 433 MHz με κεντρικές συχνότητες: 433.175 MHz, 433.375 MHz, 433.575 MHz

Υπάρχουν τρεις τάξεις LoRaWan όπου η κλάση A είναι πιο αποδοτική στην εξοικονόμηση ενέργειας ενώ η κλάση C η λιγότερο αποδοτική [8][9][10]:

- Η κλάση A η οποία είναι σύγχρονη και όπου ο κόμβος ανοίγει πολύ μικρά παράθυρα για να λάβει ενημέρωση από το gateway αφού στείλει ένα μήνυμα.
- Η κλάση B η οποία είναι επίσης σύγχρονη αλλά ο κόμβος ανοίγει περισσότερα παράθυρα σε προγραμματισμένες χρονικές περιόδους.
- Η κλάση C η οποία είναι ασύγχρονη και ο κόμβος περιμένει συνεχώς ένα μήνυμα από το gateway.



**Πίνακας 1. Χαρακτηριστικά LoRaWan**

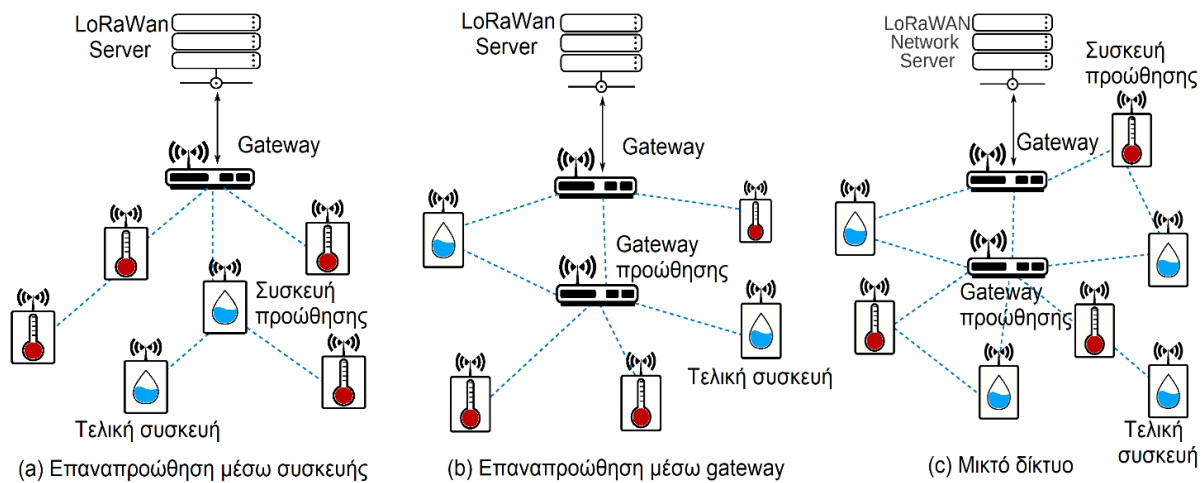
<b>LoRaWan</b>	
<b>Ανάπτυξη</b>	LoRaWan Κόμβοι, LoRaWan Gateway
<b>Κόστος</b>	300 ευρώ, Χρόνος
<b>Εμβέλεια</b>	10 km
<b>Διάρκεια Ζωής Μπαταρίας</b>	10+ χρόνια
<b>Συχνότητα<sup>1</sup></b>	868 MHz, 433 MHz
<b>Διαμόρφωση</b>	CSS
<b>Εύρος ζώνης</b>	125 kHz
<b>Κλάσεις</b>	Κλάση A, Κλάση B, Κλάση C
<b>Ρυθμός δεδομένων</b>	0.3 Kbps -50 Kbps
<b>Ισχύς στο Uplink</b>	14 dBm

<sup>1</sup> ISM συχνότητες για την Ευρώπη

## 1.1 LoRa Mesh

Μία διαφορετική προσέγγιση από το LoRaWan είναι η χρήση του φυσικού επιπέδου των κόμβων του LoRa για την δημιουργία δικτύων πλέγματος (mesh networks) [11], [12], [13], [14]. Σε αυτά τα δίκτυα, ο κάθε κόμβος επικοινωνεί με ενδιάμεσους κόμβους οι οποίοι έχουν τον ρόλο της επαναπροώθησης δεδομένων στο gateway και τελικά στον server. Διάφορα πρωτόκολλα δρομολόγησης μπορούν να υλοποιηθούν και να χρησιμοποιηθούν σε ένα τέτοιο σύστημα και να λύσουμε προβλήματα όπως την αδυναμία εύρεσης gateway από τους κόμβους, κάποια από τα προτεινόμενα είναι το Distance Vector Routing (DVR), Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR) Protocol [11].

Η διαδικασία δρομολόγησης στο LoRa μπορεί να λύσει προβλήματα σε ένα πυκνοκατοικημένο περιβάλλον πόλης όπου λόγω των υποδομών η τοπολογία αστέρα είναι δύσκολο να υλοποιηθεί, ωστόσο προϋποθέτει μεγαλύτερα πακέτα δεδομένων τα οποία περιέχουν πληροφορίες δρομολόγησης και πολλές ανταλλαγές πακέτων σε λίγο χρόνο ενώ όπως αναφέραμε ένα πακέτο LoRa μπορεί να περιέχει μόλις 242 bytes με μόλις 1% κύκλο καθυκόντων. Αν αναλογιστούμε πως μεγαλύτερα πακέτα αυξάνουν και το κύκλο καθυκόντων για να υπάρχει έγκυρη επικοινωνία, καταλαβαίνουμε πως οι εφαρμογές του LoRa στην δρομολόγηση δικτύων είναι πάρα πολύ περιορισμένες.



**Εικόνα 8 : LoRa-Mesh αρχιτεκτονικές, [35]**

## 1.2. LoRa 2.4 GHz

Μία νέα τεχνολογία της Semtech είναι το LoRa στις 2.4 GHz ISM συχνότητες [15]. Αυτή η τεχνολογία βασίζεται πάλι στην διαμόρφωση CSS και έτσι καταφέρνει να έχει μεγαλύτερη εμβέλεια από ότι άλλες τεχνολογίες στα 2.4 GHz όπως πχ WiFi, Bluetooth και Zigbee. Συστήνεται να καλύπτει αποστάσεις όπως 133 km στο κενό, 450 μέτρα σε ανοικτό περιβάλλον πόλης και 74 μέτρα σε εσωτερικούς χώρους [15]. Στις συχνότητες αυτές δεν υπάρχουν περιορισμούς σε ότι αφορά το duty cycle και τις κεραίες που μπορούμε να χρησιμοποιήσουμε και παρότι η συχνότητα των 2.4 GHz είναι λιγότερο ανθεκτική στα εμπόδια από ότι τα 868 MHz, η τεχνολογία αυτή μας δίνει εύκολα την δυνατότητα να αναπτύξουμε πρωτόκολλα δρομολόγησης και να ενισχύσουμε το με κατευθυντικές κεραίες. Επίσης η συχνότητα των 2.4 GHz είναι κοινή παγκοσμίως οπότε δεν έχουμε διαφορετικούς περιορισμούς ανά περιοχή, κάτι το οποίο δεν έχει ιδιαίτερη σημασία σε περιβάλλον πόλης αλλά μπορεί να είναι χρήσιμο για εφαρμογές παγκοσμίου εύρους.

## 2. NB-IoT

Το Narrow-band internet of things (NB-IoT) αναπτύσσεται από την 3GPP στο πλαίσιο του LTE 4G. Όπως και στο LoRaWAN, τα NB-IoT modules αναμένονται να διαρκούν 10 χρόνια με μία μπαταρία και να έχουν εμβέλεια της τάξεως εύρους των 10 km [8]. Τα NB-IoT modules μπορεί να κοστίζουν μόνο 20 €, σε αυτήν την περίπτωση όμως η σύνδεση εξαρτάται από τους πάροχους κινητής τηλεφωνίας μιας και το NB-IoT χρησιμοποιεί κανάλια μικρού εύρους ζώνης στο υπάρχον LTE δίκτυο συνυπάρχοντας με τους φορείς της κινητής τηλεφωνίας. Συσκευές βασισμένες σε NB-IoT μπορούν να ενσωματώνουν αισθητήρια ώστε να ενημερώνουν το δίκτυο κινητής τηλεφωνίας για τις μετρήσεις τους (uplink) ή να λαμβάνουν πληροφορίες για τελεστικές λειτουργίες και παραμετροποίηση της λειτουργίας τους (downlink) [8]. Για να επιτύχει χαμηλή

κατανάλωση ισχύος, το NB-IoT χρησιμοποιεί τους μηχανισμούς extended Discontinuous Reception (eDRx) καθώς και Power Saving Mode (PSM). Στο eDRx, η συσκευή είναι σε λειτουργία ύπνου για λίγα λεπτά ενώ στο PSM η συσκευή μπορεί να είναι σε λειτουργία ύπνου μέχρι και 413 μέρες [16]. Στην έκδοση 13 της 3GPP, ο μέγιστος ρυθμός δεδομένων ορίζεται στα 20 Kbps για το uplink και 100 Kbps για το downlink [17], σε νεότερες εκδόσεις σημαντικά βελτιώνουν τον ρυθμό δεδομένων στα 142.5 Kbps [17]. Για το 2021, οι συχνότητες κινητής τηλεφωνίας οι οποίες χρησιμοποιούνται στην Ευρώπη για NB-IoT είναι οι B3 (1800 MHz), B8 (900 MHz), and B20 (800 MHz), στην Ελλάδα μόνο η B20 υποστηρίζεται.

**Πίνακας 2. Χαρακτηριστικά NB-IoT**

NB-IoT	
Ανάπτυξη	Κάρτα SIM, Plug n' Play
Κόστος	Συνδρομή, Αισθητήριοι κόμβοι
Εμβέλεια	10 km
Διάρκεια Ζωής Μπαταρίας	5-10 χρόνια
Συχνότητα <sup>1</sup>	B20 (800 MHz), B8 (900 MHz), B3 (1800 MHz)
Διαμόρφωση	QPSK, BPSK <sup>3</sup>
Αριθμολογία	SC-FDMA <sup>3</sup> , OFDMA <sup>4</sup>
Εύρος ζώνης	180 kHz, 200 kHz <sup>2</sup>
Uplink λειτουργίες	In-band, Guard-band, Stand-alone
Διαχείριση ενέργειας	eDRx, PSM
SC-FDMA σχήματα	Single-tone, Multi-tone (3, 6, 12)
Ρυθμός δεδομένων	20 Kbps <sup>3,5</sup> , 100 Kbps <sup>4,5</sup>
Ισχύς στο Uplink	23 dBm <sup>5</sup> , 20 dBm, 14 dBm

<sup>1</sup> Ευρώπη για το 2021, μόνο η B20 για την Ελλάδα

<sup>2</sup> Stand-alone λειτουργία

<sup>3</sup> Uplink

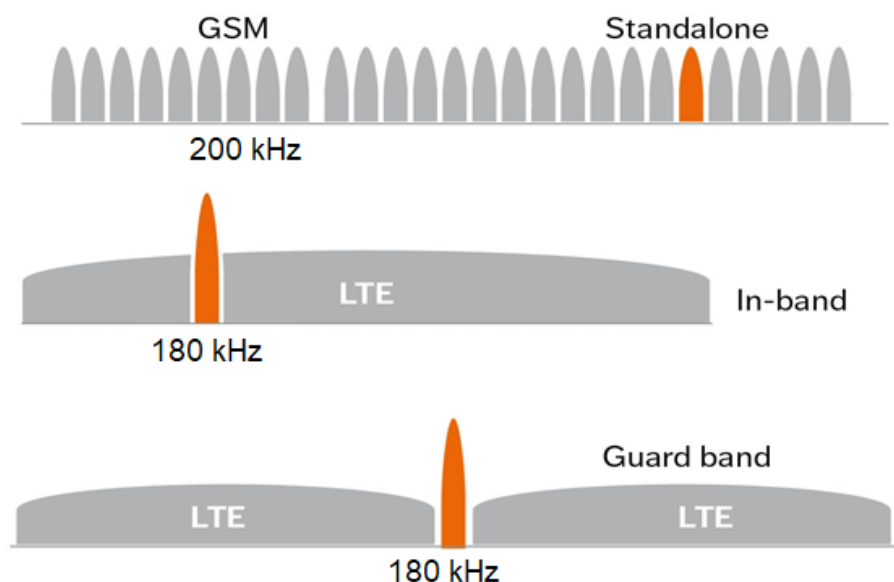
<sup>4</sup> Downlink

<sup>5</sup> Έκδοση 13 της 3GPP

Για το uplink, το NB-IoT χρησιμοποιεί 3εις διαφορετικές λειτουργίες, την λειτουργία stand-alone όπου το NB-IoT σήμα χρησιμοποιεί ένα κανάλι 200 kHz στις συχνότητες GSM, την λειτουργία guard-band όπου το NB-IoT χρησιμοποιεί την 180 kHz πλαϊνή

ζώνη συχνοτήτων ενός φορέα LTE, και την in-band ειρουργία όπου χρησιμοποιεί μία 180 kHz ζώνη συχνοτήτων ενσωματωμένη στον φορέα LTE[18]. Για να αυξήσει την φασματική απόδοση και για να αποφύγει συγκρούσεις στο uplink, το NB-IoT χρησιμοποιεί ένα κανάλι τυχαίας προσπέλασης (NPRACH) και από την έκδοση 15 της 3GPP χρονοδιαμετρική αμφίδρομη επικοινωνία (Time Division Duplexing, TDD) [16]. Το NB-IoT χρησιμοποιεί QPSK ή BPSK διαμόρφωση και την αριθμολογία Single-Carrier Frequency Division Multiple Access (SC-FDMA) για το uplink, για το downlink χρησιμοποιεί QPSK και την αριθμολογία Orthogonal Frequency Division Multiplexing (OFDM) όπως οι τυπικοί φορείς κινητής τηλεφωνίας στο LTE.

Αντίθετα με τους φορείς κινητής και για να αυξήσει την επεκτασιμότητα, το NB-IoT χρησιμοποιεί σχήματα πολλαπλών τόνων (multitone) στο SC-FDMA uplink όπου πολλά NB-IoT nodes μπορούν να χρησιμοποιούν τον ίδιο φορέα για συγκεκριμένες περιόδους. Μία μετάδοση ενός τόνου (single-tone) μπορεί να ορίζεται από διαστήματα 15 kHz όπως οι άλλοι φορείς LTE ή από 3.75 kHz, το 3.75 kHz προτείνει μια πιο ισχυρή μετάδοση αλλά κακή ενσωμάτωση με τους άλλους φορείς LTE, οπότε περιορίζεται στην λειτουργία standalone. Η multitone μετάδοση ορίζεται από διαστήματα 15 kHz και μπορεί να είναι 3,6 ή 12 τόνων, μικρότερος αριθμός τόνων εγγυάται πιο ισχυρή μετάδοση αλλά μειώνει την επεκτασιμότητα. Μέχρι και την έκδοση 13 της 3GPP, δύο τιμές εκπομπής ισχύος υπήρχαν στο uplink, 20 and 23 dBm [16]. Σε μεταγενέστερες εκδόσεις, η ισχύς μειώθηκε στα 14 dBm, συντηρώντας ωστόσο την ίδια ενέργεια ανά bit [16]. Το NB-IoT σχεδιάστηκε αρχικά μόνο για τις LTE συχνότητες αλλά τελευταία αναπτύσσεται και το NB-IoT-U το οποίο μπορεί να χρησιμοποιεί τις ISM συχνότητες [18], [19].



Εικόνα 9: Λειτουργίες NB-IoT, [36]

## 2.1 Device to Device NB-IoT

Η επικοινωνία D2D για το NB-IoT εφαρμόζεται από την έκδοση 15 της 3GPP. Όπως αναφέραμε το D2D επιτρέπει σε συσκευές NB-IoT να επικοινωνούν χωρίς απευθείας σύνδεση με τον κεντρικό σταθμό, [17], [20], η οποία φαίνεται να είναι πολλά υποσχόμενη στην εποχή του 5G για την διασύνδεση των πραγμάτων [3]. Και για το NB-IoT, η D2D επικοινωνία επιτυγχάνεται όταν συσκευές χρησιμοποιούν άλλες συσκευές στο δίκτυο σαν relays για να επαναπροωθήσουν τα δεδομένα του στο κεντρικό σταθμό, μιλάμε δηλαδή για multi-hop δρομολόγηση πακέτων. Μέσω της δρομολόγησης αυτής, οι συσκευές μπορούν να τοποθετηθούν έτσι ώστε να παρέχουν δεδομένα για σημεία χωρίς κάλυψη κινητής τηλεφωνίας και μίας και το σήμα διανύει μικρότερες αποστάσεις, μπορούμε να πετύχουμε εξοικονόμηση ενέργειας. Εκτός αυτού, το NB-IoT δεν χρειάζεται να στηρίζεται μόνο σε άλλους NB-IoT κόμβους για να φθάσει στον κεντρικό σταθμό αλλά μπορεί επίσης να χρησιμοποιεί και κινητά τηλέφωνα τα οποία υπάρχουν στην ζώνη LTE [20], [21]. Πειράματα για D2D τόσο για την κινητή τηλέφωνα όσο και για το NB-IoT δείχνουν ότι καλύτερη εξοικονόμηση ενέργειας μπορεί να επιτευχθεί αλλά και καλύτερη κατανομή ραδιοφωνικών πόρων εφόσον πολλές ζώνες συχνοτήτων παραμένουν ελεύθερες, χρησιμοποιούνται μόνον από την τελική συσκευή της δρομολόγησης [19], [20], [21]. Η D2D επικοινωνία δεν εξελίσσεται μόνο για τις συχνότητες της κινητής τηλεφωνία αλλά προτείνεται επίσης και για τις ISM συχνότητες [19].

## 2.2 NB-IoT και 5G

Το NB-IoT είναι μπορεί να συνεχίσει να συνυπάρχει και να εξελίσσεται και με τα δίκτυα 5G ικανοποιώντας τις συνθήκες που έχει θέσει η 3GPP για το υποδίκτυο mMTC [22]. Μίας και το 5G και το NB-IoT χρησιμοποιούν παρόμοιες τεχνικές διαμόρφωσης, η συνύπαρξη των δύο χωρίς παρεμβολές σήματος μπορεί να επιτευχθεί [22]. Οι νέες τεχνολογίες οι οποίες ενεργοποιούνται με τις λειτουργίες 5G τις οποίες περιγράψαμε όπως τα σχήματα MIMO και οι νέες συχνότητες οι οποίες ανοίγουν από το 5G δίνουν την ευκαιρία στο NB-IoT να χρησιμοποιήσει ακόμα περισσότερους πόρους [22][23]. Μεγάλο ενδιαφέρον δείχνουν και τα υποδίκτυα SDN όπου συσκευές NB-IoT μπορούν να καλύπτουν διαφορετικές ανάγκες με διαφορετικές απαιτήσεις, την οργάνωση δηλαδή NB-IoT συσκευών κατάλληλα ανάλογα με τις ανάγκες του δικτύου [23], π.χ. η καθημερινή παρατήρηση της ατμοσφαιρικής ρύπανσης μπορεί να μην είναι όσο σημαντική όσο μια φωτιά στο κέντρο της πόλης, έτσι λοιπόν το δίκτυο λοιπόν μπορεί να προσαρμόζεται κατάλληλα ώστε να δίνεται προτεραιότητα σε συγκεκριμένα περιστατικά. Η λειτουργία MEC όπου μικροί σταθμοί μπορούν να προσφέρουν τοπικούς άρα και περισσότερους πόρους για τις NB-IoT συσκευές μειώνοντας την

κίνηση στα κανάλια ενώ οι μικρότερες αποστάσεις μπορούν να προσφέρουν εξοικονόμηση ενέργειας μιας και η επικοινωνία είναι άμεση [23]. Εκτός αυτού, οι σταθμοί αυτοί μπορούν να διαμορφώνονται κατάλληλα για να καλύπτουν διάφορες εφαρμογές στο πεδίο της πόλης.

**Πίνακας 3. Παράμετροι της 3GPP για το υποδίκτυο mMTC, [22]**

Παράμετρος	mMTC	Απόδοση NB- 5G
Πλήθος Συνδέσεων	$10^6$ συσκευές/km <sup>2</sup>	$1.2 \cdot 10^6$ συσκευές/km <sup>2</sup>
Ρυθμός Μετάδοσης	160 bps	281 bps
Καθυστέρηση Μετάδοσης	10 sec	5.8 sec
Διάρκεια Ζωής Μπαταρίας	10 χρόνια	11.8 χρόνια
Μέγιστη Απώλεια Ζεύξης	164 dB	164 dB

### 3. Σύγκριση LoRaWan και NB-IoT για εφαρμογές πόλης

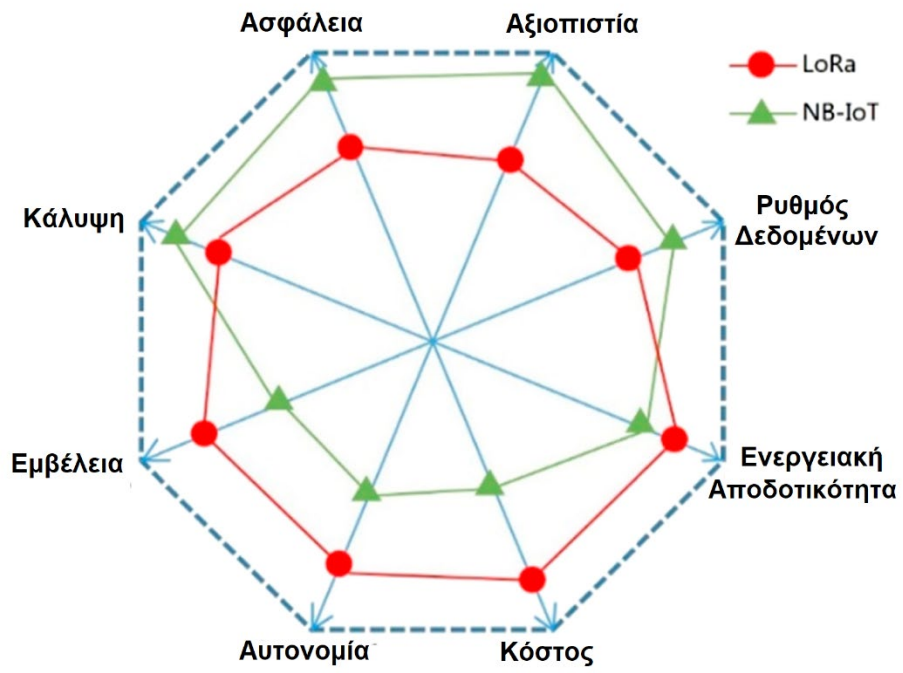
Διάφορες παράμετροι μπορούν να ληφθούν υπόψη για την σύγκριση των δύο αυτών LPWAN τεχνολογιών. Το LoRaWan προσφέρει αυτονομία μιας και η συνδεσιμότητά του στο δίκτυο δεν εξαρτάται από κάποιο εξωτερικό πάροχο κινητής τηλεφωνίας. Ωστόσο η χρήση των υπο-GHz ISM συχνοτήτων και η αδυναμία δρομολόγησης θέτουν την υλοποίηση του δύσκολη στο πυκνοκατοικημένο περιβάλλον πόλης καθώς και ο περιορισμός του duty cycle το θέτουν ακατάλληλο για ένα μεγάλο εύρος εφαρμογών, σε αντίθεση το NB-IoT φαίνεται να είναι η κατάλληλη τεχνολογία για να αφομοιωθεί σε μία πόλη συνυπάρχοντας με την κινητή τηλεφωνία στο LTE και να εξελιχθεί με τις νέες υποδομές 5G. Άλλες συγκρίσεις οι οποίες φαίνεται να έχουν ενδιαφέρον για περιβάλλον πόλης είναι:

- Γεωγραφική κάλυψη. Πειραματικές μελέτες δείχνουν ότι οι εφαρμογές LoRaWan καταφέρνουν να έχουν μεγαλύτερη εμβέλεια στον ελεύθερο χώρο [24]. Ωστόσο, τα δεδομένα αλλάζουν σε περίπτωση που οι κόμβοι βρίσκονται εντός κτηρίων όπου το NB-IoT υπερτερεί. Για ένα συνωστισμένο περιβάλλον πόλης, το NB-IoT προσφέρει καλύτερη κάλυψη [24], [25].
- Ποιότητα κάλυψης (Quality of Service, QoS) και επεκτασιμότητα. Το NB-IoT φαίνεται να υπερτερεί ξεκάθαρα του LoRaWan σε ότι έχει να κάνει με την ποιότητα κάλυψης. Χρησιμοποιώντας το πρωτόκολλο TCP μπορεί να εγγυηθεί την αξιοπιστία των απεσταλμένων πακέτων [26]. Εκτός αυτού, πειραματικές μελέτες δείχνουν ότι οι συσκευές NB-IoT, ιδιαίτερα η λειτουργία 12 τόνων, μπορούν να υποστηρίξουν υπερδεκαπλάσια μηνύματα από το LoRaWan το

λεπτό με πολύ μεγαλύτερη επιτυχία. Της τάξεως των 25000 μηνυμάτων το λεπτό έναντι των 2000 του LoRaWan [27].

- Ασφάλεια. Το NB-IoT φαίνεται να υπερτερεί του LoRaWan στο θέμα της ασφάλειας χρησιμοποιώντας το εξελιγμένο δίκτυο LTE, μελέτες θέτουν το πρώτο να είναι μέχρι και τρεις φορές πιο ασφαλές έναντι του δεύτερου [28]. Πιο συγκεκριμένα μία επίθεση στο NB-IoT βασίζεται πάνω στις κλασσικές μεθόδους επίθεσης IP (port scanning, ARP spoofing, DNS spoofing). Έναντι οι LoRaWan κόμβοι χρησιμοποιούν ένα κλειδί 128 bit για την επικοινωνία τους με τον server το οποίο μπορεί να μην είναι ισχυρό έναντι μεγάλης υπολογιστικής ισχύος, πιο ευάλωτοι σε επιτηδευμένες παρεμβολές στα 868 MHz και καθώς τα πακέτα δεδομένων τους είναι μικρότερα, θα μπορούσε κάποιος να το αναλύσει [29]. Η ασφάλεια η οποία χρειάζεται είναι ανάλογη της εφαρμογής η οποία στηρίζεται από την κάθε τεχνολογία, σε ένα περιβάλλον πόλης οι εφαρμογές οι οποίες χρειάζονται ασφάλεια είναι πολλές καθώς και η πιθανότητα να βρεθούν κακόβουλοι χρήστες είναι μεγάλη.
- Κατανάλωση ενέργειας. Οι κόμβοι LoRaWan καταναλώνουν λιγότερη ενέργεια από ότι οι κόμβοι NB-IoT καθώς οι δεύτεροι χρειάζονται κάποιο χρόνο για να συγχρονιστούν με το δίκτυο [27]. Η κατανάλωση εξαρτάται από τον όγκο δεδομένων με κάποιες προσεγγιστικές τιμές να είναι 0.001-7 mJ για μία uplink εκπομπή ενός κόμβου LoRaWan και 29.4-89.6 mJ για uplink εκπομπή κόμβου NB-IoT [8]. Ωστόσο, κάτι τέτοιο ισχύει σε ιδανικές συνθήκες όπου ένα πακέτο χρειάζεται να σταλεί μόνο μία φορά για να ληφθεί από τον εν λόγω gateway ή από τον σταθμό κινητής τηλεφωνίας. Σε συνθήκες πόλης, κάτι τέτοιο μπορεί να είναι δύσκολο να επιτευχθεί.

Θεωρούμε λοιπόν ότι μεταξύ αυτών των δύο τεχνολογιών, το NB-IoT δείχνει να ενσωματώνεται αρκετά καλύτερα στο περιβάλλον μίας πόλης καθώς και φαίνεται να είναι αρκετά υποσχόμενο να υποστηρίξει το mMTC κομμάτι των δικτύων 5G. Σε αντίθεση το LoRaWan, φαίνεται να υστερεί σε ότι αφορά την δρομολόγηση των κόμβων του, την ασφάλεια και την εγκατάστασή του σε περιβάλλον πόλης. Ωστόσο, δεν πρέπει να παραλείψουμε χαρακτηριστικά όπως αυτονομία, η κάλυψη σε εξωτερικούς χώρους και η μικρότερη κατανάλωση ενέργειας τα οποία μπορούν να το θέσουν ως λύση για σε μεμονωμένες εφαρμογές όπως αυτές απομακρυσμένων εξωτερικών χώρων.



Εικόνα 10: Χαρακτηριστικά LoRaWan και NB-IoT, [37]

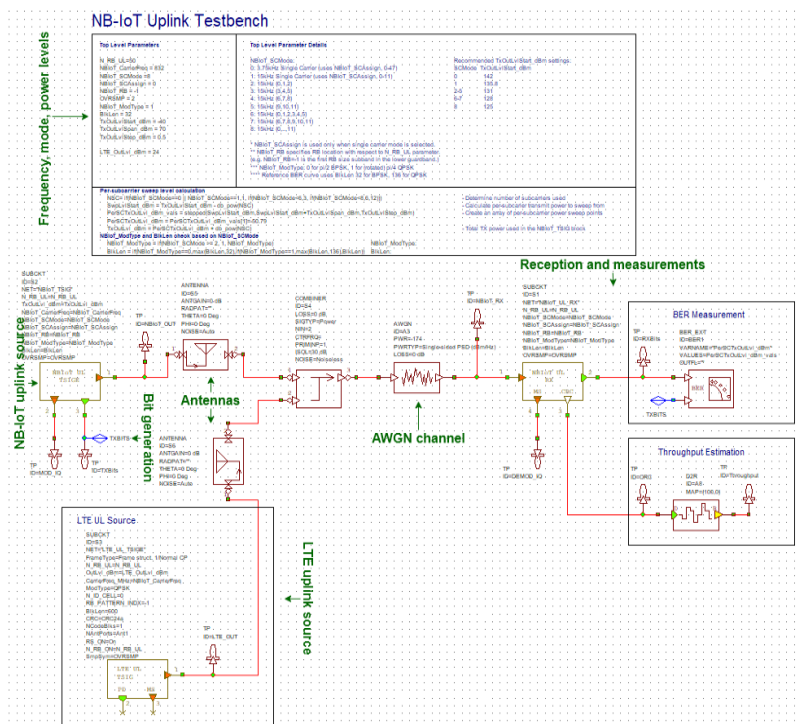


## 1. Προσομοίωση NB-IoT με την χρήση του AWR Design Environment

Στο κεφάλαιο αυτό θα επικεντρωθούμε στην προσομοίωση διαφορετικών διατάξεων NB-IoT για να εκτιμήσουμε τον τρόπο που αυτές θα μπορούσαν να εγκατασταθούν για να εξυπηρετήσουν σενάρια εγκατάστασης NB-IoT κόμβων σε ένα περιβάλλον πόλης. Για να πραγματοποιηθεί η προσομοίωση αυτή, γίνεται χρήση του λογισμικού AWR Design Environment [38].

### 1.1 AWR Design Environment

Το AWR Design Environment αποτελείται από 3 μέρη, το Microwave Office για την σχεδίαση RF κυκλωμάτων και πλακετών, το Visual System Simulation όπου μπορεί να γίνει η προσομοίωση μίας ολοκληρωμένης RF διάταξης συμπεριλαμβανομένων και των παραμέτρων διαμόρφωσης σήματος, καθώς και τους προσομοιωτές AXIEM και Analyst για την εύρεση της ηλεκτρομαγνητικής απόκρισης του σχεδιασμένου υλικού. Στο πεδίο του VSS, το AWR προσφέρει NB-IoT testbenches βασισμένα στην έκδοση 13 της 3GPP [39], με την χρήση αυτών και με την προσθήκη κατάλληλων εξαρτημάτων όπως κεραίες και θόρυβος, μπορούμε να βγάλουμε συμπεράσματα για την απόκριση των διαφορετικών deployments του NB-IoT και κατά πόσο είναι δυνατόν αυτό να συνεργαστεί με τα υπάρχοντα LTE κανάλια κινητής τηλεφωνίας.



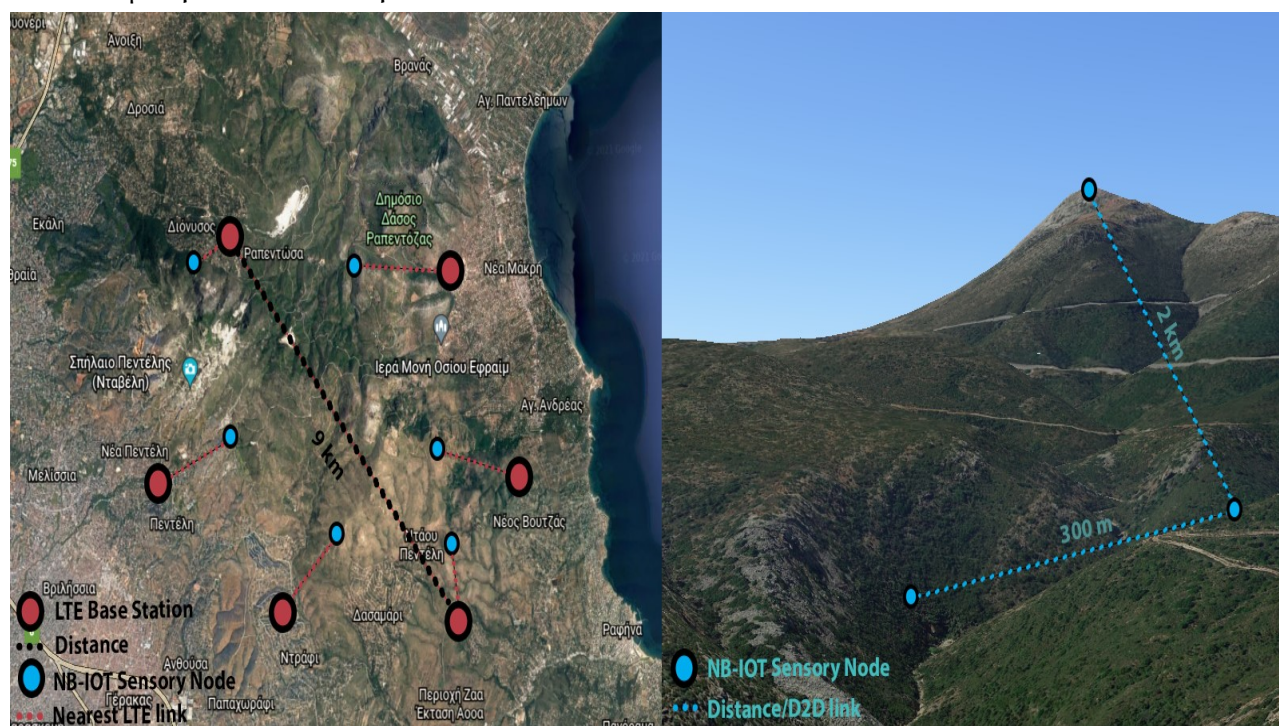
**Εικόνα 11: Το NB-IoT Testbench στο AWR DE**

Στην εικόνα 11 φαίνεται η διάταξη του NB-IoT testbench, όπου φαίνεται οι παράμετροι που μπορούμε να θέσουμε όπως ο τρόπος λειτουργίας του, η συχνότητα, η ισχύς. Στην συνέχεια παρατηρούμε τους δύο πομπούς (NB-IoT και LTE) να οδηγούνται από κεραιές σε ένα κοινό κανάλι θορύβου και τελικά να γίνεται η εκτίμηση των ληφθέντων bits του NB-IoT και της απόδοσης σε ένα δέκτη.

## 1.2 Προσομοίωση της NB-IoT κάλυψης του Πεντελικού όρους με το AWR Design Environment

Θα μελετήσουμε την κάλυψη με NB-IoT στο Πεντελικό όρος ως ένα τοπίο το οποίο βρίσκεται κοντά σε πυκνοκατοικημένες περιοχές της Αθήνας και έχει πληγεί κυρίως από φωτιές αρκετές φορές οι οποίες έχουν καταστρέψει και τον φυσικό πλούτο του αλλά και περιουσίες των κατοίκων των γύρω περιοχών. Η κάλυψή του με NB-IoT θα μπορούσε να προβλέψει τόσο τις μελλοντικές φωτιές, ή και περιστατικά όπως κατολισθήσεις, με αποτέλεσμα την ανάπλασή του και την προστασία των κατοίκων. Είναι επίσης ένα τοπίο το οποίο περιέχει διάφορες κορυφές και κοιλάδες, για το οποίο θα μπορούσα να προταθεί η χρήση D2D σε περίπτωση που το σήμα από τους NB-IoT κόμβους παρεμβάλλεται από εμπόδια. Είναι ωστόσο μία περιοχή κοντά στην Αθήνα η οποία καλύπτεται επαρκώς από την κινητή τηλεφωνία.

Στην εικόνα 12 παρατηρούμε τους LTE σταθμούς βάσης (eNB) ενός φορέα κινητής τηλεφωνίας καθώς και ένα θεωρητικό σενάριο D2D μέσω της εφαρμογής Google Earth [46], όπου παρατηρούμε ότι η μέγιστη απόσταση μεταξύ ενός NB-IoT κόμβου και ενός eNB δεν μπορεί να είναι παραπάνω από 4.5 km.

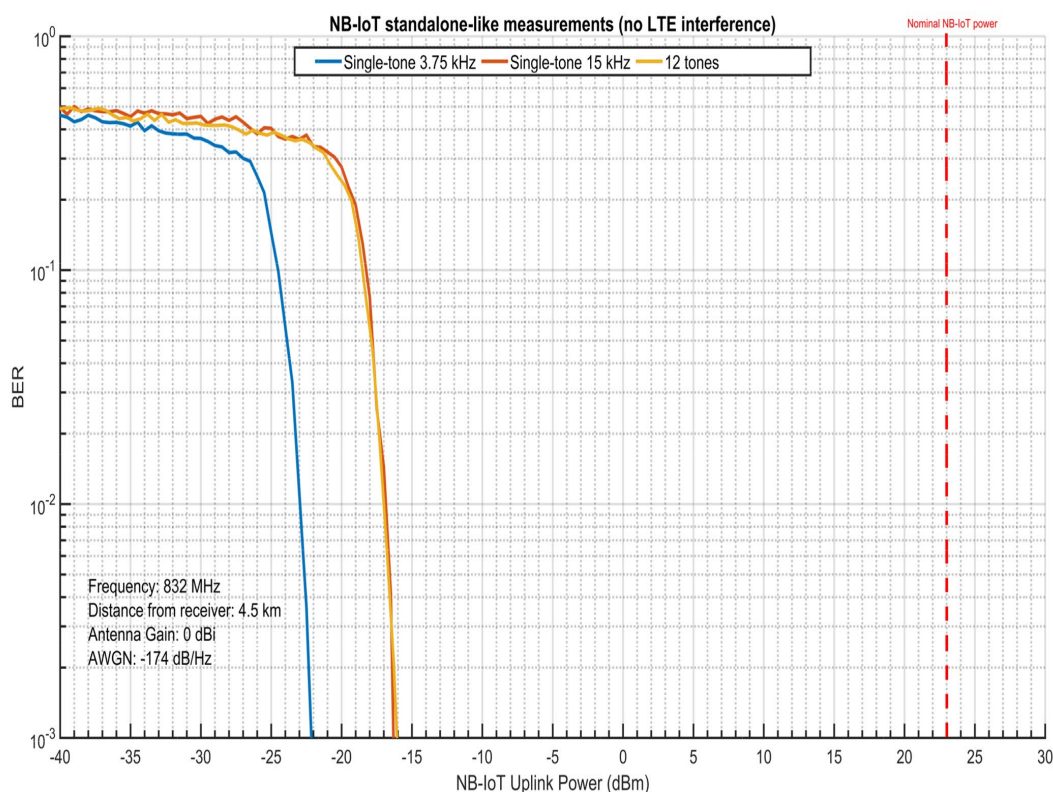


Εικόνα 12: Σταθμοί LTE και προτεινόμενο σχήμα D2D επικοινωνίας.

Ορίζουμε κάποια σενάρια τα οποία θα μπορούσαν να αντιπροσωπεύουν την τοποθέτηση των κόμβων στο Πεντελικό έτσι ώστε να ελέγξουμε την απόκριση NB-IoT

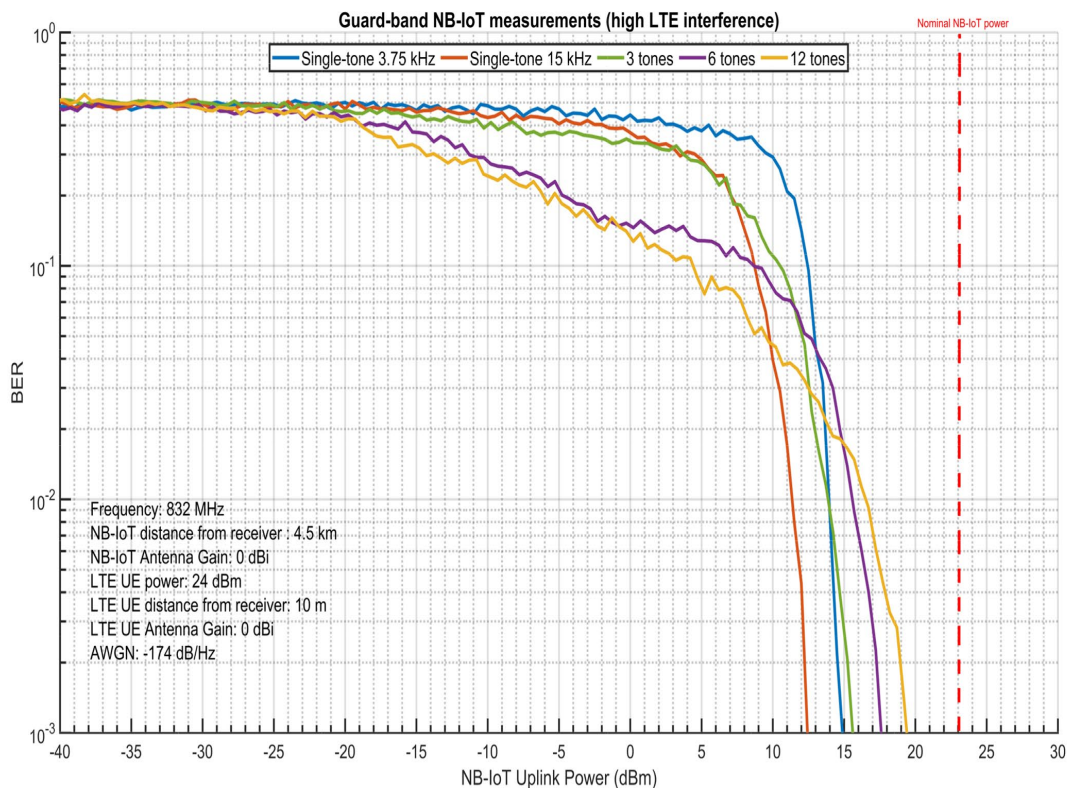
κόμβων σε διαφορετικά deployments αλλά και την επιρροή του σε LTE φορείς κινητής τηλεφωνίας, αλλά και την επιρροή LTE φορέων στους NB-IoT κόμβους, με σκοπό να μπορούμε να εγγυηθούμε την αξιόπιστη επικοινωνία και των δύο σε κάποιο περιστατικό έκτακτης ανάγκης όπως μία πιθανή φωτιά.

Στο AWR Design Environment τοποθετούμε τον NB-IoT πομπό σε απόσταση 4.5 km από τον σταθμό βάσης (eNB), ενώ ο φορέας LTE εκπέμπει μόλις σε απόσταση 10 μέτρα από τον σταθμό βάσης με σταθερή ισχύ τα 24 dBm. Και οι δύο πομποί εκπέμπουν στην συχνότητα των 832 MHz (uplink της B20), οι δύο κεραίες θεωρούνται να είναι ιστροπικές (0 dBi) ενώ θεωρούμε και λευκό θόρυβο (AWGN) με ισχύ τα -172 dBm για να εκπροσωπήσει τυχαίες παρεμβολές στην φύση, θεωρούμε πως δεν έχουμε περαιτέρω παρεμβολές μεταξύ των κόμβων και τον σταθμό βάσης. Πάρθηκαν μετρήσεις για όλους τους τρόπους deployment δηλαδή standalone, guard-band, and in-band τόσο σε single-tone όσο και σε multi-tone modes. Αγνοήθηκαν τα 3-tone and 6-tone modes καθώς οι αποκλίσεις είναι πολύ μικρές, είναι σημαντικό να σημειώσουμε ότι η συχνότητα των 832 MHz δεν είναι ρεαλιστική για standalone deployment καθώς αυτός ο τρόπος λειτουργίας βρίσκεται στις GSM συχνότητες ωστόσο εκπροσωπεί μία καλή αναφορά για συγκρίσεις. Ελέγχουμε την ισχύ του πομπού NB-IoT από τα -40 dBm μέχρι τα 30 dBm και θεωρώντας ότι η τυπική ισχύς εκπομπής του NB-IoT είναι 23 dBm, παίρνουμε τα παρακάτω αποτελέσματα.

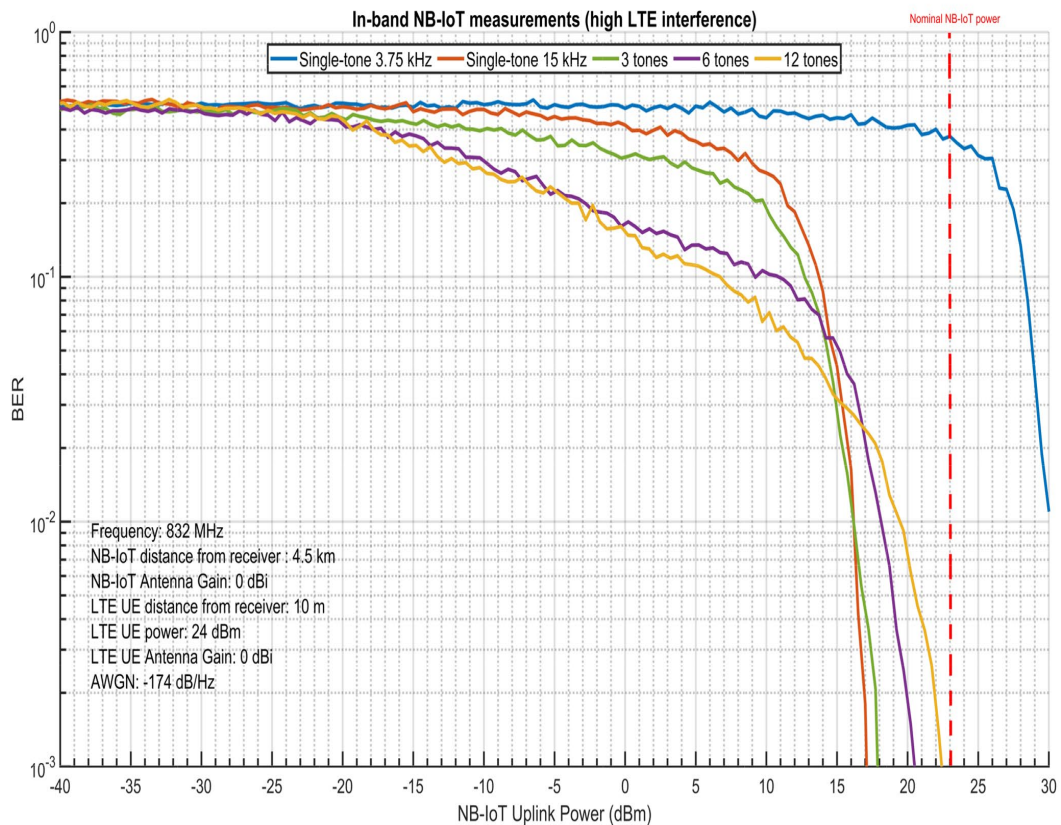


Εικόνα 13: Αποτελέσματα προσομοίωσης stand-alone, χωρίς παρεμβολές LTE





**Εικόνα 14: Αποτελέσματα προσομοίωσης guard-band, ισχυρές παρεμβολές LTE**



**Εικόνα 15: Αποτελέσματα προσομοίωσης in-band, ισχυρές παρεμβολές LTE**

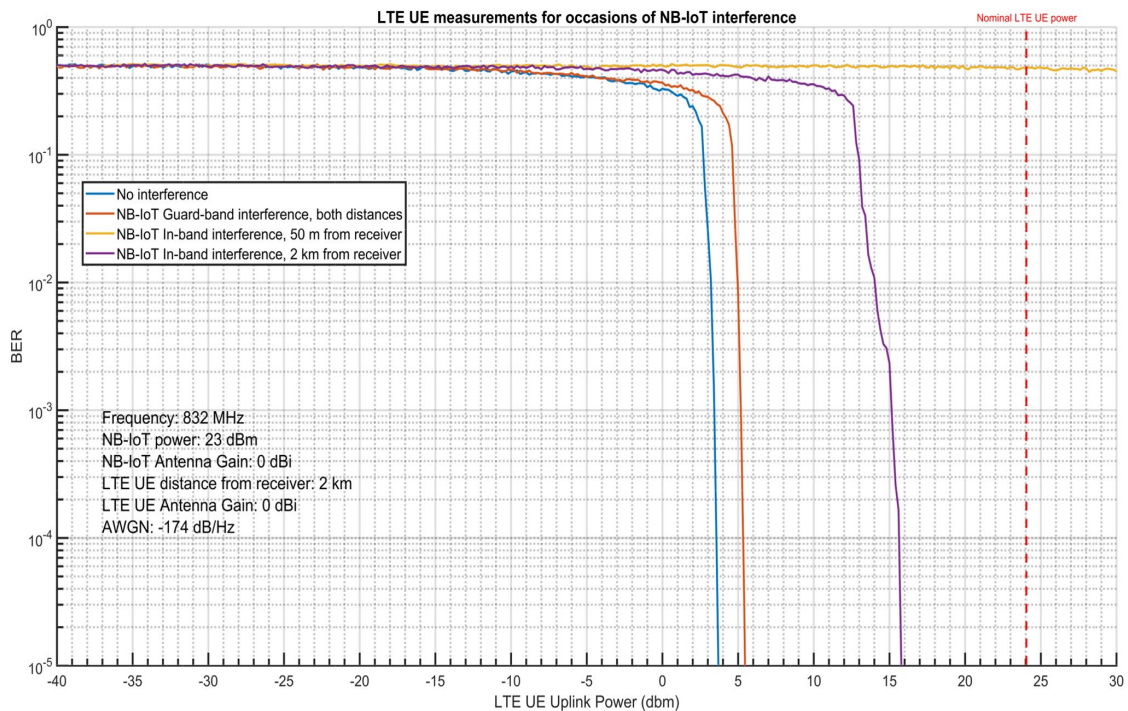
**Πίνακας 4 . Αποτελέσματα προσομοίωσης για το σεναρίο μας θεωρώντας τυπική ισχύ 23 dBm για το NB-IoT.**

<b>Mode</b>	<b>Power for sustainable BER (dBm)</b>	<b>Noise Tolerance (dBm)</b>
Standalone 3.75 kHz	-22	45
Standalone 15 kHz	-16	39
Standalone 12 tones	-15.8	38.8
Guard-band 3.75 kHz	15	8
Guard-band 15 kHz	12.5	10.5
Guard-band 3 tones	15.7	7.3
Guard-band 6 tones	17.7	5.3
Guard-band 12 tones	19.7	4.3
In-band 3.75 kHz	> 30	< 0
In-band 15 kHz	17.5	5.5
In-band 3 tones	18.2	4.8
In-band 6 tones	20.7	2.3
In-band 12 tones	22.7	0.3

Με τις ίδιες παραμέτρους σε σχέση με την συχνότητα, το AWGN και τις κεραιές, από το testbench μπορούμε να δούμε επίσης τον θόρυβο που δημιουργεί το NB-IoT σε LTE φορείς όπως τα κινητά τηλέφωνα. Σε αυτή την περίπτωση, ο φορέας LTE έχει τοποθετηθεί 2 km μακριά από τον σταθμό βάσης eNB και παρατηρούμε τα επίπεδα ισχύος του LTE φορέα θεωρώντας την τυπική uplink ισχύ να είναι τα 24 dBm. Οι κόμβοι NB-IoT έχουν τοποθετηθεί σε αποστάσεις είτε 50 m ή 2 km μακριά από τον σταθμό βάσης και μεταδίδουν στην ισχύ των 23 dBm. Αρχικά, παρατηρούμε το uplink του LTE χωρίς NB-IoT παρεμβολές και στην συνέχεια με τον θόρυβο ο οποίος προκαλείται από τις guard-band και τα in-band modes. Παρατηρούμε ότι και για τις δύο περιπτώσεις απόστασης, ο θόρυβος που προκαλείται από το guard-band δεν είναι περισσότερος από 1.5 dBm, κάτι το οποίο μας προτείνει την αρμονική συνύπαρξη μεταξύ LTE και NB-IoT φορέων ανεξάρτητα από την τοποθέτηση των κόμβων στον χώρο. Αυτή ωστόσο δεν είναι η περίπτωση με το in-band mode καθώς στα 50m ο θόρυβος μπλοκάρει το σήμα του LTE φορέα και ακόμα και στην περίπτωση των 2 km, απώλειες μεγαλύτερες των 10 dBm μπορούν να παρατηρηθούν.

Πίνακας 5. Αποτελέσματα προσομοίωσης για τις αποστάσεις θεωρώντας τυπική ισχύ LTE τα 24 dBm.

Mode	Power for sustainable BER (dBm)	Noise Tolerance (dBm)
No interference	3.5	20.5
Guard-band 50 m	5.5	18.5
Guard-band 2 km	5.5	18.5
In-band 50 m	< 30	> 0
In-band 2 km	16	8



Εικόνα 16: Επίδραση NB-IoT modes σε φορείς LTE

### 1.3 Σύνοψη αποτελεσμάτων

Τα αποτελέσματα της προσομοίωσης δείχνουν ότι αποστάσεις όπως για το σενάριο μας, μπορούν να καλυφθούν με οποιαδήποτε deployment NB-IoT ακόμα και σε περίπτωση που υπάρχουν παρεμβολές από φορείς LTE όπως στο in-band και το guard-band mode. Πιο συγκεκριμένα, το guard-band mode δείχνει να μπορεί να συνυπάρξει αρμονικά με τους LTE φορείς με σχετικά μικρές αποκλίσεις ισχύος τόσο σε 3-tone mode όσο και σε 12-tone, το οποίο μας εξασφαλίζει την χρήση πολλών κόμβων στις ίδιες συχνότητες χωρίς να επηρεάζεται η LTE κινητή τηλεφωνία, κάτι αρκετά σημαντικό σε περιπτώσεις επείγουσας ανάγκης. Το in-band mode δείχνει και αυτό ικανό να καλύψει μεγάλες αποστάσεις ακόμα και με τις παρεμβολές LTE φορέων, ωστόσο φαίνεται να έχει χειρότερα αποτελέσματα από το guard-band mode και σε κάποιες περιπτώσεις

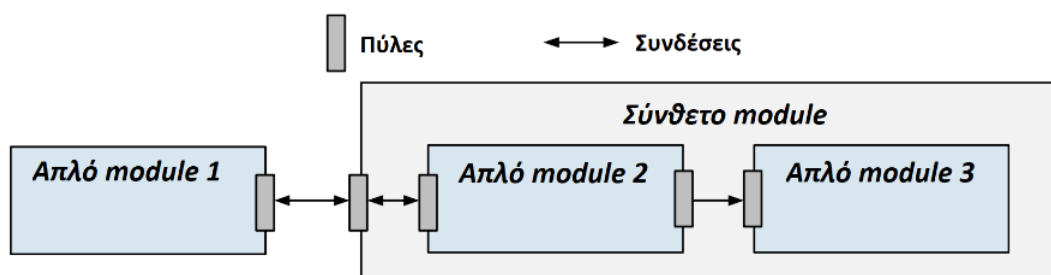
ισχυρές παρεμβολές στους LTE φορείς. Το stand-alone φαίνεται να μπορεί να καλύψει τις μεγαλύτερες αποστάσεις, ωστόσο χρησιμοποιεί GSM συχνότητες οι οποίες χρειάζονται στην κινητή τηλεφωνία. Τα συμπεράσματά μας είναι ότι το guard-band deployment είναι το κατάλληλο NB-IoT deployment για το σενάριο του Πεντελικού όρους. Πρέπει να σημειώσουμε ότι στην προσομοίωση δεν λάβαμε υπόψιν την τοποθέτηση των κόμβων και κατ' επέκτασιν παρεμβολές από φυσικά εμπόδια, καθώς και οι κεραιές μας θεωρήθηκαν ιστροπικές το οποίο δεν αντιπροσωπεύει ένα ρεαλιστικό σενάριο.

## 2. Προσομοίωση σε οχήματα με το OMNeT++, το Simu5G και το SUMO

Στο κεφάλαιο αυτό θα επικεντρωθούμε στην προσομοίωση οχημάτων και θα εξεταστεί η απόκρισή τους σε ένα σενάριο ρεαλιστικής κίνησης είτε με σταθμούς 5G είτε με LTE. Για να συντάξουμε το σενάριο, θα γίνει η χρήση της πλατφόρμας OMNeT++ σε συνεργασία με την βιβλιοθήκη Simu5G και το λογισμικό SUMO.

### 2.1 OMNeT++

Το OMNeT++ είναι ένα λογισμικό discrete-event simulation το οποίο μπορεί να χρησιμοποιηθεί για να μοντελοποιήσει κάθε είδους δικτύου όπως ενσύρματο, ασύρματο, αισθητηρίων κλπ. [40]. Το περιβάλλον του OMNeT++ βασίζεται σε μοντέλα τα οποία είναι συνδεδεμένα μεταξύ τους με πύλες (gates) και μπορούν να είναι απλά και σύνθετα, να περιέχουν δηλαδή αλλά υπομοντέλα [40]. Τα μοντέλα αυτά ανταλλάζουν μηνύματα με σκοπό να εκπροσωπήσουν διάφορες παραμέτρους όπως κόμβους και πρωτόκολλα στο δίκτυο. Στην κορυφή της ιεραρχίας βρίσκεται το μοντέλο network το οποίο περιέχει όλα τα υπόλοιπα υπόμοντέλα χωρίς εξωτερικές πύλες και αντιπροσωπεύει το τελικό μοντέλο που θέλουμε να προσομοιώσουμε. Το OMNeT++ είναι open-source ώστε κάθε χρήστης να μπορεί να εξελίξει το δικό του μοντέλο προσομοίωσης [40].

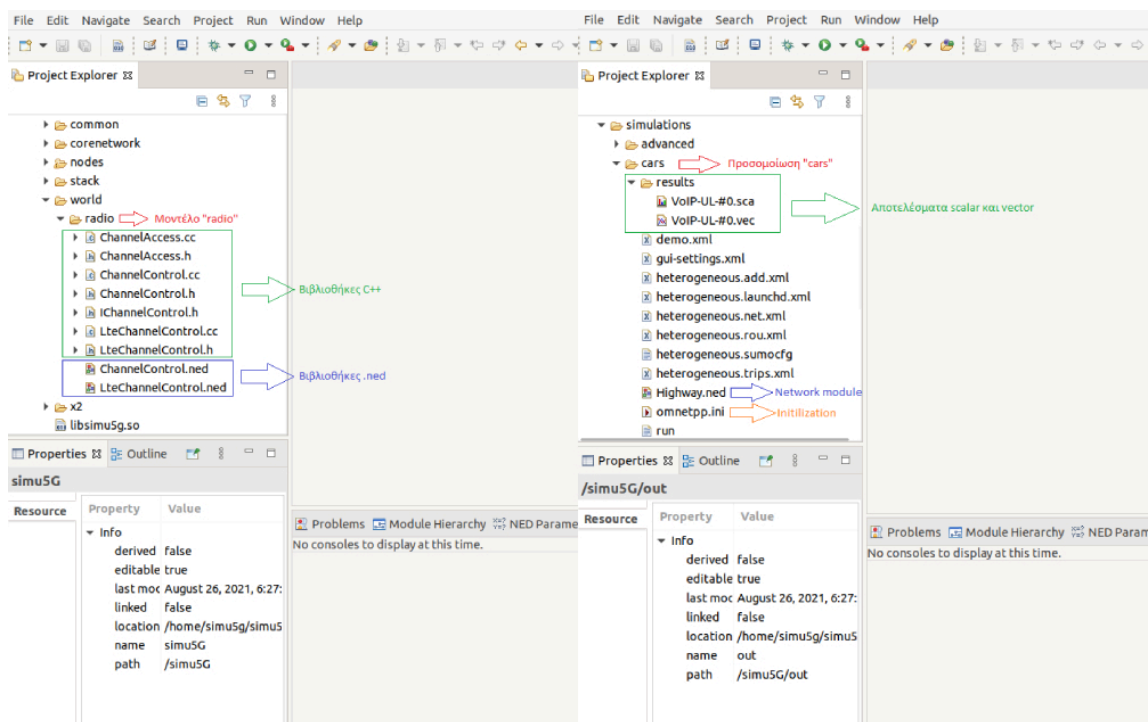


Εικόνα 17: Μοντελοποίηση στο OMNeT++

Το OMNeT++ ξεχωρίζει την συμπεριφορά του μοντέλου, την περιγραφή του και τις παραμέτρους του. Η συμπεριφορά του κάθε μοντέλου εκφράζεται στην γλώσσα C++. Η περιγραφή (πύλες, συνδέσεις και ο ορισμός των παραμέτρων) εκφράζεται σε αρχεία της Network Description (NED) γλώσσα. Οι τιμές των παραμέτρων εκφράζονται με



initialization (INI) αρχεία. Με την γλώσσα NED μπορείς ο χρήστης να εξελίξει σενάρια προσομοίωσης, είτε γραφικά μέσω ενός GUI είτε μέσω κειμένου όπως σε μία κλασική γλώσσα προγραμματισμού [40]. Το OMNeT++ βασίζεται στο περιβάλλον Eclipse Integrated Development Environment (IDE) το οποίο ευκολύνει το debugging αφήνοντας τον χρήστη να ελέγξει τα μοντέλα του κατά την εκτέλεση της προσομοίωσης με την γραφική απεικόνιση του μοντέλου και των μηνυμάτων που ανταλλάσσονται στο δίκτυο καθώς και αναφορές στα γεγονότα της προσομοίωσης σε σχέση με τον χρόνο που τρέχει η προσομοίωση. Παραπάνω από μία προσομοιώσεις μπορούν να τρέξουν παράλληλα σε έναν υπολογιστή με περισσότερους από έναν επεξεργαστικό πυρήνα. Μετά το τέλος μίας προσομοίωσης, οι παράμετροι που είχαμε ορίσει να αποθηκεύει το δίκτυο, π.χ. packet loss, uplink latency αναλύονται ανάλογα με την φύση τους σε βαθμωτά (scalar) είτε σε διανυσματικά (vector) μεγέθη, το OMNeT++ στην συνέχεια δίνει την δυνατότητα απεικόνισης των παραμέτρων σε γραφήματα [40]. Στην εικόνα 17 φαίνονται οι διάφορες βιβλιοθήκες οι οποίες χρησιμοποιούνται όπως το module radio το οποίο περιέχει αρχεία C++ και .ned, ενώ η προσομοίωση cars περιέχει το αρχείο .ned του module network (κορυφή της ιεραρχίας) καθώς και το INI αρχείο για να θέσουμε τις παραμέτρους της προσομοίωσης, διακρίνονται επίσης τα αρχεία κάποιων αποτελεσμάτων.



Εικόνα 18: Περιβάλλον IDE του OMNeT++ και βιβλιοθήκες για την μοντελοποίηση προσομοίωσης

## 2.2 Η βιβλιοθήκη INET

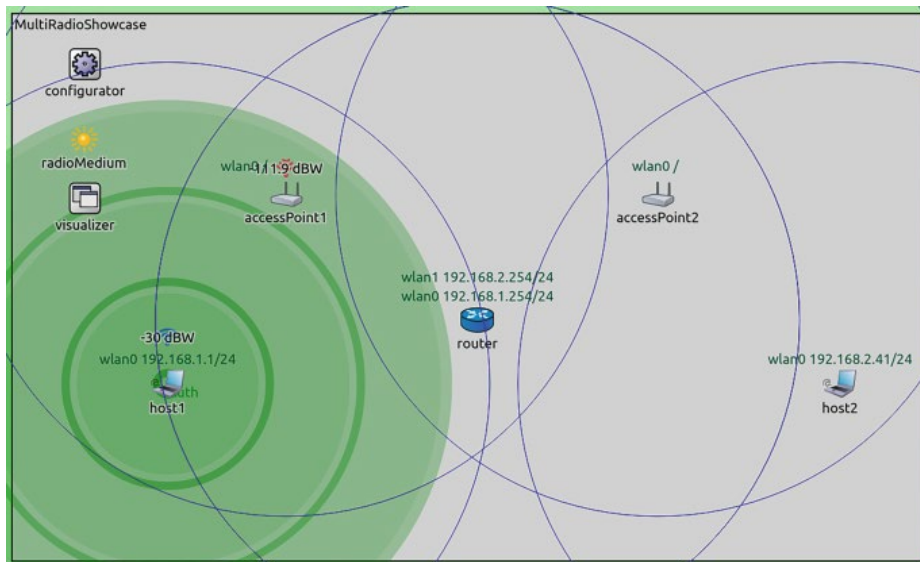
Η βιβλιοθήκη είναι μία από τις παλιότερες βιβλιοθήκες για το OMNET++, ξεκινώντας από το 2000 και την προσομοίωση του IP (Internet Protocol) πρωτόκολλου και εξελισσόμενη ταυτόχρονα μαζί με το OMNET++ για να συμβαδίζει με τα νέα μοντέλα



επικοινωνίας [42]. Είναι αρκετά χρήσιμη βιβλιοθήκη και αποτελεί την βάση για τον σχεδιασμό και προσομοίωση νέων πρωτοκόλλων και δικτύων επικοινωνίας, χρησιμοποιείται ευρέως τόσο από την ακαδημαϊκή κοινότητα όσο και από την βιομηχανία. Η βιβλιοθήκη INET ξεκίνησε από τις πρώτες μοντελοποιήσεις για το πρωτόκολλο IP (π.χ. IPV4, TCP και UDP) και σταδιακά έχει αναπτυχθεί για την προσομοίωση πεδίων όπως το Ethernet, το Wi-fi (802.11), μηχανισμοί QoS (Quality of Service), πρωτόκολλα routing όπως για MANET (Mobile Ad Hoc Network), ασύρματα MAC πρωτόκολλα όπως 4G/5G, υπηρεσίες IPv6 και πολλά άλλα. Οι τελευταίες πρόοδοι στις INET επιτρέπουν την μοντελοποίηση του φυσικού επιπέδου (physical layer) καθώς και του φυσικού μέσου (physical medium) με γραφική απεικόνιση και βελτιωμένες δυνατότητες εξομοίωσης (emulation). Η INET είναι open-source, στηρίζεται σε μία μεγάλη κοινότητα και έχει χρησιμεύσει ως την βάση για τις βιβλιοθήκες SimuLTE, Simu5G και Veins της οποίες θα εξετάσουμε στην συνέχεια [42].

Για την προσομοίωση ασύρματων δικτύων, η INET περιέχει μοντέλα για την προσομοίωση του 802.11 καθώς και για άλλα ασύρματα πρωτόκολλα. Η προσομοίωση των ασύρματων δικτύων μπορεί να είναι αρκετά πιο πολύπλοκη από τα ενσύρματα δίκτυα, καθώς ένα ασύρματο κανάλι είναι ένα κοινόχρηστο μέσο το οποίο οδηγεί σε πιο περίπλοκα πρωτόκολλα MAC από τις ενσύρματες επικοινωνίες, καθώς μεγάλο ρόλο παίζει και το φυσικό περιβάλλον [42]. Σε ένα ενσύρματο περιβάλλον η ισχύς κατά την μετάδοση δεν επηρεάζεται αρκετά από το περιβάλλον και οι απώλειες είναι εύκολο να μοντελοποιηθούν, στα ασύρματα δίκτυα σε αντίθεση είναι αναγκαίο να προσδιοριστούν οι απώλειες λόγω απόστασης (path loss), οι απώλειες λόγω εμποδίων (obstacle loss), οι παρεμβολές του περιβάλλοντος (background noise), και άλλες παρεμβολές [42]. Επίσης, στα ενσύρματα μέσα, δύο σήματα ταυτόχρονα που φτάνουν ταυτόχρονα στον δέκτη μπορούν εύκολα να αναγνωριστούν σαν μία σύγκρουση, στα ασύρματα δίκτυα λόγω του ότι το φυσικό μέσο είναι κοινό, οι συγκρούσεις είναι δύσκολο να αναγνωριστούν και όσο αυξάνονται οι κόμβοι τόσο αυξάνεται και η πολυπλοκότητα του μοντέλου. Γι' αυτούς τους λόγους, παράμετροι όπως η ισχύς μετάδοσης, η απολαβή του δέκτη και του πομπού, η ευαισθησία του κάθε δέκτη κλπ. πρέπει να αναλύονται σε κάθε επίπεδο του μοντέλου, από το μοντέλο του δικτύου που θέλουμε να προσομοιώσουμε μέχρι και το ξεχωριστό μοντέλο του κάθε κόμβου, αλλά και με τρόπο έτσι ώστε να υπάρχει η κατάλληλη επεκτασιμότητα. Οι υποδομές που η INET προσφέρει για ασύρματα δίκτυα περιέχουν τρία βασικά μέρη [42]:

1. Το μοντέλο του πομποδέκτη για κάθε κόμβο, το οποίο περιέχει επίσης την κατάλληλη κεραία.
2. Το μοντέλο του γενικότερου μέσου (global transmission medium) το οποίο καταγράφει όλες τις αναμεταδόσεις που συμβαίνουν στο δίκτυο και την αλληλεπίδρασή τους.
3. Το μοντέλο του φυσικού περιβάλλοντος (εμπόδια, έδαφος κλπ.).

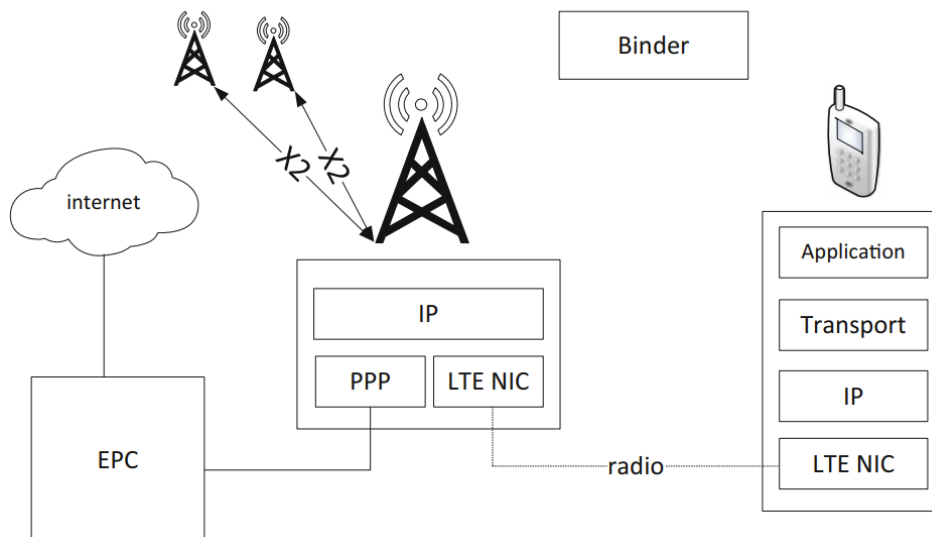


**Εικόνα 19: Απεικόνιση ασύρματου δικτύου 802.11 στο OMNET++ μέσω της INET, [40]**

Για να πραγματοποιηθεί αυτή η μοντελοποίηση, κάθε ένα από αυτά τα μέρη αποτελείται από διάφορα modules τα οποία μπορούν να παραμετροποιηθούν για να συντάξουν το τελικό module του δικτύου που θέλουμε να προσομοιώσουμε. Αυτό συμβαίνει και με τις βιβλιοθήκες SimuLTE και Simu5G οι οποίες βασισμένες στην INET συντάσσουν μοντέλα προσομοίωσης δικτύων LTE και 5G NR, και θα μελετήσουμε στο επόμενο υποκεφάλαιο. Είναι επίσης σημαντικό να σταθούμε στο ότι λόγω της πολυπλοκότητας των ασύρματων μοντέλων, οι απαιτήσεις του υπολογιστή είναι μεγαλύτερες από ότι σε ένα ενσύρματο δίκτυο.

## 2.3 Η βιβλιοθήκη SimuLTE

Η βιβλιοθήκη SimuLTE για το OMNeT++ προσφέρει την δυνατότητα προσομοίωσης 4G LTE και Long Term Evolution Advanced (LTE-A) δικτύων [43]. Το SimuLTE έχει σχεδιαστεί επικεντρωμένο στο επίπεδο δεδομένων (data plane) του LTE έτσι ώστε το δίκτυο και ο κάθε κόμβος να καλεί τις απαραίτητες LTE λειτουργίες από το σχεδιασμένο module Binder, χωρίς να χρειάζεται η επί μέρους μοντελοποίηση του κάθε κόμβου ξεχωριστά. Το SimuLTE περιέχει κάθε επίπεδο πρωτοκόλλου του LTE, και δίνει την δυνατότητα μοντελοποίησης του φυσικού επιπέδου υπολογίζοντας το SINR (Signal-to-Interference plus-Noise-Ratio) στους δέκτες λαμβάνοντας υπόψιν όλους τους ταυτόχρονους πομπούς τους δικτύου. Επιτρέπει την προσομοίωση τόσο των LTE φορέων (UE) προς τους σταθμούς βάσης 4G (eNB) καθώς και την επικοινωνία D2D. Οι λειτουργίες LTE αναθέτονται στο NIC (Network Interface Card) καθενός UE, όπου επιτρέπεται και η ταυτόχρονη χρήση LTE με άλλες ασύρματες επικοινωνίες όπως το Wi-fi [43].

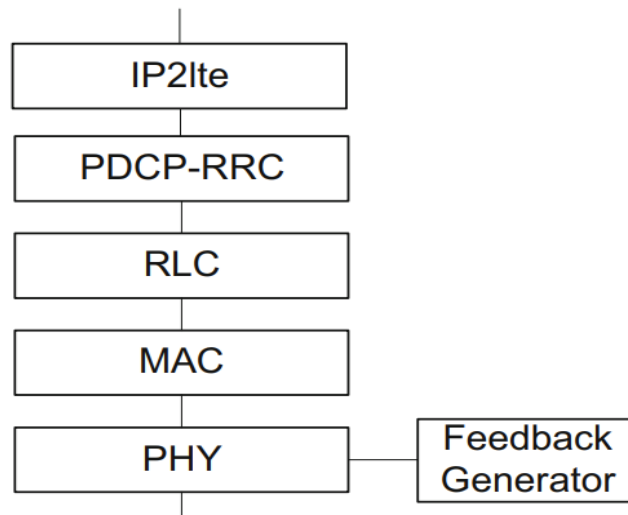


Εικόνα 20: Δίκτυο LTE στο OMNeT++, [43]

Το SimuLTE βασίζεται σε λειτουργίες της INET και αποτελείται από τα παρακάτω κομμάτια [43]:

- Τους κόμβους (nodes). Οι δύο βασικοί κόμβοι είναι ο σταθμός βάσης LTE (eNB) και οι φορείς (UE). Ωστόσο το SimuLTE προσθέτει τον κόμβο Binder για τον συσχετισμό της κάθε επικοινωνίας μεταξύ των κόμβων. Πιο συγκεκριμένα:
  1. Το eNB είναι το μέσο επικοινωνίας από και προς τα UEs. Χρησιμοποιεί το Point-to-Point Protocol (PPP) interface προς το EPC (Evolved Packet Core), και μία LTE NIC κάρτα για να επικοινωνεί με τα Ues. Επίσης υπάρχει και η δυνατότητα της χρήσης PPP interface για την X2 επικοινωνία με γειτονικά eNBs.
  2. Το UE node συμπεριφέρεται όπως ένα LTE-based cellphone. Είναι μία συνέχεια του module Standarhost της INET και επιτρέπει την επικοινωνία μέσω του πρωτόκολλου TCP καθώς και UDP. Το SimuLTE παρέχει μοντέλα για αληθινές LTE εφαρμογές (π.χ., VoIP και VoD), αλλά μπορεί να περιέχει κάθε TCP/UDP εφαρμογή του OMNeT++. Το IP module χρησιμοποιείται επίσης μέσω της INET. Μία LTE NIC κάρτα χρησιμοποιείται για την επικοινωνία του UE με το eNB ή με άλλα UEs στην περίπτωση των D2D επικοινωνιών.
  3. Τον κόμβο Binder ο οποίος περιέχει και καταγράφει πληροφορίες για κάθε LTE κόμβο στο δίκτυο. Ο σκοπός του είναι να καλύπτει όλες τις λειτουργίες οι οποίες δεν μοντελοποιούνται απλά ως μία ανταλλαγή μηνυμάτων έτσι ώστε να απλοποιήσει το μοντέλο και να κάνει την προσομοίωση πιο γρήγορη. Λειτουργίες όπως ο συσχετισμός των κόμβων μεταξύ τους είτε είναι eNBs είτε είναι UEs, περιέχει πλάνα για την επικοινωνία D2D κτλπ. Κάθε κόμβος εγγράφεται στο Binder κατά την εκκίνηση της προσομοίωσης.

- Το LTE NIC. Το LTE NIC module είναι αυτό το οποίο ενεργοποιεί τα επίπεδα του LTE πρωτοκόλλου (protocol stack) στα eNBs και τα UEs. Το LTE NIC module είναι μία συνέχεια του module IWirelessNic της INET, και επιτρέπει την εύκολη τοποθέτηση του LTE σε κόμβους ή ακόμα και σε συνδυασμό με το Wi-fi για υβριδικά μοντέλα επικοινωνίας [43]. Το LTE NIC είναι παρόμοιο και στα UEs και τα eNBs και αποτελείται από τα παρακάτω submodules [43]:
  1. Το PHY module το οποίο βρίσκεται χαμηλά στο LTE protocol stack για λειτουργίες του φυσικού επιπέδου όπως η προσομοίωση του ασύρματου καναλιού (air channel), την μετάδοση δεδομένων, την ισχύ μετάδοσης και το προφίλ της κεραίας.
  2. Το MAC module, το οποίο διαχειρίζεται τα πακέτα τα οποία έρχονται από το κατώτερο layer (PHY) και ζητά δεδομένα για την μετάδοση από τα πιο πάνω επίπεδα όπως το RLC που θα δούμε στην συνέχεια. Το MAC module είναι αυτό το οποίο καθορίζει την χρονοδρομολόγηση των πακέτων και ορίζει την κωδικοποίηση και την διαμόρφωση αυτών (AMC-Adaptive Modulation and Coding). Οι περισσότερες λειτουργίες είναι κοινές στο eNB και το UE, ωστόσο παράμετροι όπως η δρομολόγηση των πακέτων τείνουν να διαφέρουν.
  3. Το RLC (Radio Control Link) module το οποίο επιτρέπει την πολυπλεξία και την αποπολυπλεξία από και προς το MAC επίπεδο, και επαναπροωθεί πακέτα από και προς το PDCP (Packet Data Convergence Protocol) επίπεδο. Το RLC είναι παρόμοιο και στο eNB και στο UE.
  4. Το PDCP module μοντελοποιεί τις λειτουργίες στο υψηλότερο επίπεδο του LTE πρωτοκόλλου. Λαμβάνει δεδομένα από το IP2LTE module (κατά το downstream) και από το RLC (στο upstream). Στην πρώτη περίπτωση, το PDCP αναθέτει το κατάλληλο LCID (Logical Connection Identifier), έτσι ώστε το πακέτο να επαναπροωθηθεί στην κατάλληλη RLC πόρτα. Στην δεύτερη περίπτωση, το πακέτο το οποίο φθάνει από το RLC ταυτοποιείται ώστε τελικά να φτάσει στο ανώτερο επίπεδο.
  5. Το IP2LTE module είναι η διεπαφή (interface) μεταξύ του επιπέδου δικτύου (IP) και της LTE NIC κάρτας. Στην μετάδοση (downstream), εξάγει τα στοιχεία IP και τις θύρες δικτύου (ports) για την προέλευση (source) και το προορισμό (destination), και τις εισάγει στο πακέτο πριν αυτό μεταφερθεί στα κατώτερα layers. Στην λήψη (upstream), το IP2LTE απλά επαναπροωθεί το πακέτο το οποίο έρχεται από το PDCP στο επίπεδο δικτύου χωρίς περαιτέρω επεξεργασία. Εκτός από αυτές τις διαδικασίες, το IP2LTE είναι υπεύθυνο για να καταγράφει το κάθε LTE NIC στο Binder κατά την εκκίνηση της προσομοίωσης.



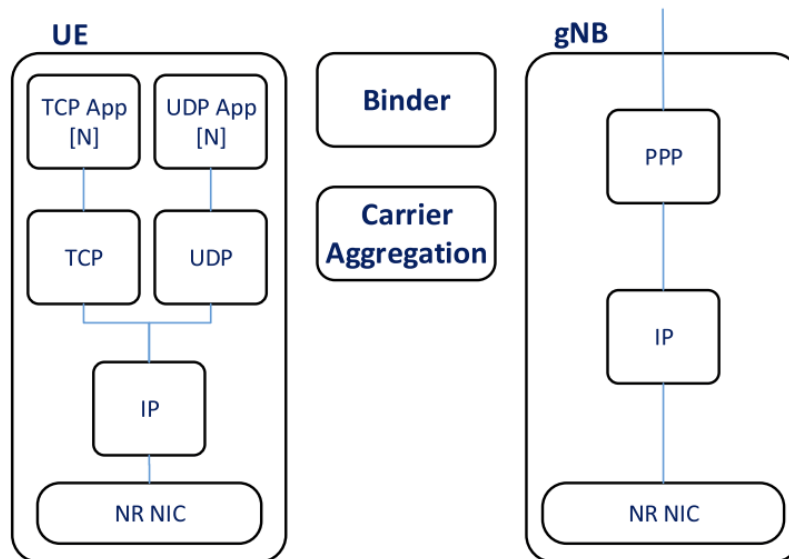
**Εικόνα 21 : Μοντελοποίηση του LTE stack στο OMNeT++, [43]**

- Τις κεντρικές συναρτήσεις (Main Functions), οι οποίες διαχωρίζονται ως εξής [43]:
  1. Την χρονοδρομολόγηση (scheduling). Η χρονοδρομολόγηση είναι η διαδικασία για να αποφασιστεί πως θα διανεμηθούν τα RB (Resource Blocks) στα UEs, και κατά το downlink και κατά το uplink. Η διαδικασία γίνεται στο MAC επίπεδο και την αναλαμβάνουν τα eNBs κάθε χρονικό διάστημα μετάδοσης (Transmission Time Interval – TTI). Στο SimuLTE, οι διαδικασίες χρονοδρομολόγησης χρησιμοποιούν την κλάση «LteSchedulerEnb» η οποία ορίζει όλες τις διαδικασίες οι οποίες είναι κοινές και στο downlink και στο uplink, όπως η διαμόρφωση των δεδομένων (data structure initialization), η διανομή των RBs (allocation management) και η συλλογή στατιστικών.
  2. Η επικοινωνία μεταξύ eNBs (Inter-eNB Communication). Η αλληλεπίδραση μεταξύ των eNBs είναι σημαντική για τις διαδικασίες όπως το handover, δηλαδή την άμεση σύνδεση του UE από ένα eNB στο άλλο, και την αποφυγή παρεμβολών στο δίκτυο (interference coordination). Για την επικοινωνία των eNBs χρησιμοποιείται το interface X2, το οποίο και μοντελοποιείται στο SimuLTE με την κλάση LTeX2App η οποία διαχειρίζεται τα μηνύματα από κάθε LTE NIC του eNB προς ένα άλλο και αντίστροφα.
  3. Την επικοινωνία D2D. Το SimuLTE υποστηρίζει και την ένας-προς-έναν και την ένας-προς-πολλούς D2D επικοινωνία. Στην ένας-προς-έναν επικοινωνία, η σύνδεση γίνεται μόνο μεταξύ δύο συζευγμένων UEs. Ο Binder καταγράφει όλες τις πληροφορίες οι οποίες σχετίζονται με όσα UEs έχουν την δυνατότητα να επικοινωνήσουν μεταξύ τους και επίσης όλης της δρομολόγησης από κάθε D2D UE μέχρι το πακέτο να φθάσει στο eNB.

## 2.4 Η βιβλιοθήκη Simu5G

Η βιβλιοθήκη Simu5G είναι μία επέκταση της βιβλιοθήκης SimuLTE για δίκτυα 5G, η οποία ενσωματώνει τις λειτουργίες του SimuLTE που περιγράψαμε όπως το X2 για

handover και την D2D επικοινωνία. Το Simu5G προσθέτει το Carrier Aggregation module για την ταυτόχρονη χρήση ραδιοπόρων RBs (resource blocks) από τους κόμβους. Επίσης, εισάγει τα modules NrUe και gNodeB, τα οποία είναι επεκτάσεις των modules Ue και eNodeB του SimuLTE. Υπάρχουν δύο διαφορετικοί τρόποι με τις οποίες μπορεί να αναπτυχθεί ένα δίκτυο 5G στο Simu5G, η πρώτη είναι η SA (Standalone Access) όπου το gNB λαμβάνει δεδομένα από τα διάφορα UEs και τις μεταβιβάζει κατευθείαν στον server ενώ η δεύτερη είναι NSA (Non-Standalone Access) όπου το gNB εφόσον λάβει τα δεδομένα από τα UEs τα μεταβιβάζει σε ένα eNB το οποίο έχει τον ρόλο του MN (Master Node) και αυτό αναλαμβάνει τα μεταβιβάζει στον server [44]. Όπως και μεταξύ δύο eNBs στο SimuLTE, η λειτουργία αυτή πραγματοποιείται με την χρήση του interface X2. Μία άλλη λειτουργία την οποία προσφέρει το Simu5G είναι τα SB (Split Bearers), σε αυτή την λειτουργία ένα UE επικοινωνεί ταυτόχρονα με το eNB και gNB [44].



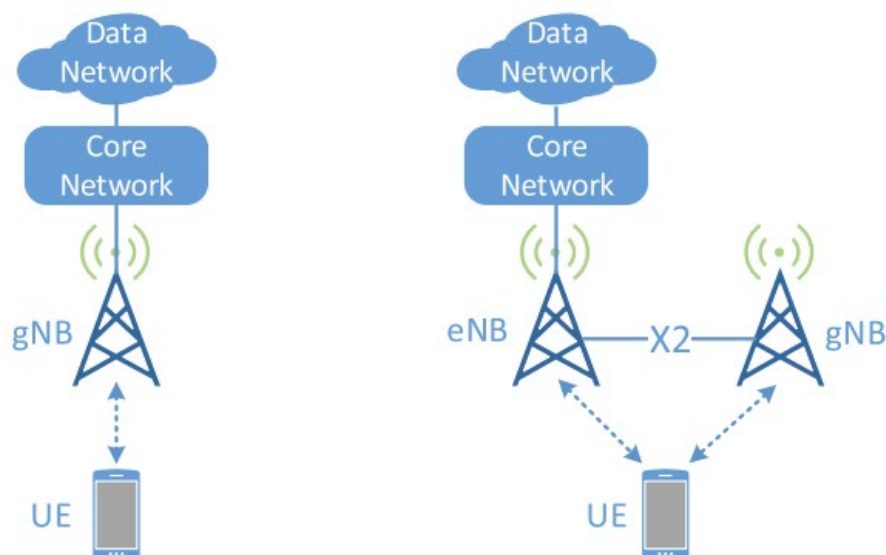
Εικόνα 22: Βιβλιοθήκες του Simu5G, [44].

Στην περίπτωση του Simu5G, οι κάρτες LTE NIC αντικαθιστούν τις αντίστοιχες για 5G NR, NrNicUe και NrNicGnb. Οι κάρτες NR NIC περιέχουν το 5G NR protocol stack, η αντιστοιχία με τις κάρτες LTE βρίσκεται στα παρακάτω επίπεδα [44]:

1. Το επίπεδο PHY είναι όμοιο με αυτό του SimuLTE.
2. Το επίπεδο MAC είναι σε μεγάλο βαθμό όμοιο με αυτό του SimuLTE, ωστόσο μπορεί να υποστηρίξει διαμορφώσεις σήματος μεγαλύτερης τάξης, μέχρι και 256 QAM.
3. Το επίπεδο RLC είναι όμοιο με αυτό του SimuLTE.
4. Το επίπεδο PDCP είναι επέκταση του ανάλογου PDCP του SimuLTE, έχει την δυνατότητα να κατευθύνει πακέτα στο RLC με τελικό προορισμό είτε το eNB είτε το gNB μέσω του interface X2. Ταυτόχρονα είναι και αυτό που αναλαμβάνει να

οργανώσει τα πακέτα που έρχονται είτε από το LTE RLC είτε από το NR RLC σε περίπτωση σύνδεσης SB πριν τα παρουσιάσει στο επίπεδο IP2LTE.

5. Το επίπεδο IP2LTE είναι ίδιο όπως και στο SimuLTE, ήδη από αυτό το επίπεδο καθορίζεται ποια πακέτα έχουν ως τελικό προορισμό είτε το eNB είτε το gNB.

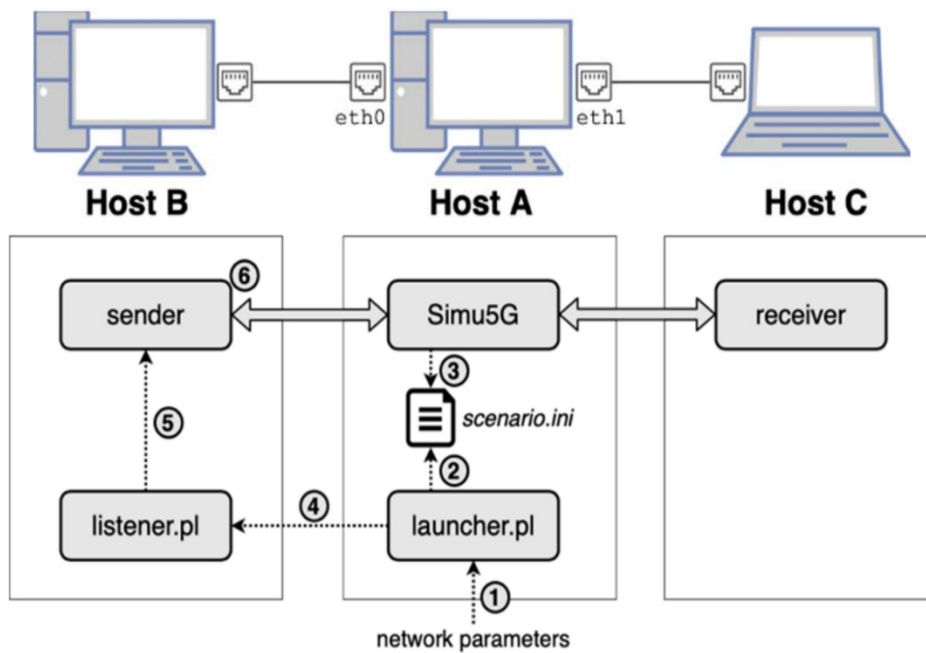


**Εικόνα 23: 5G NR SA και NSA deployments, [44]**

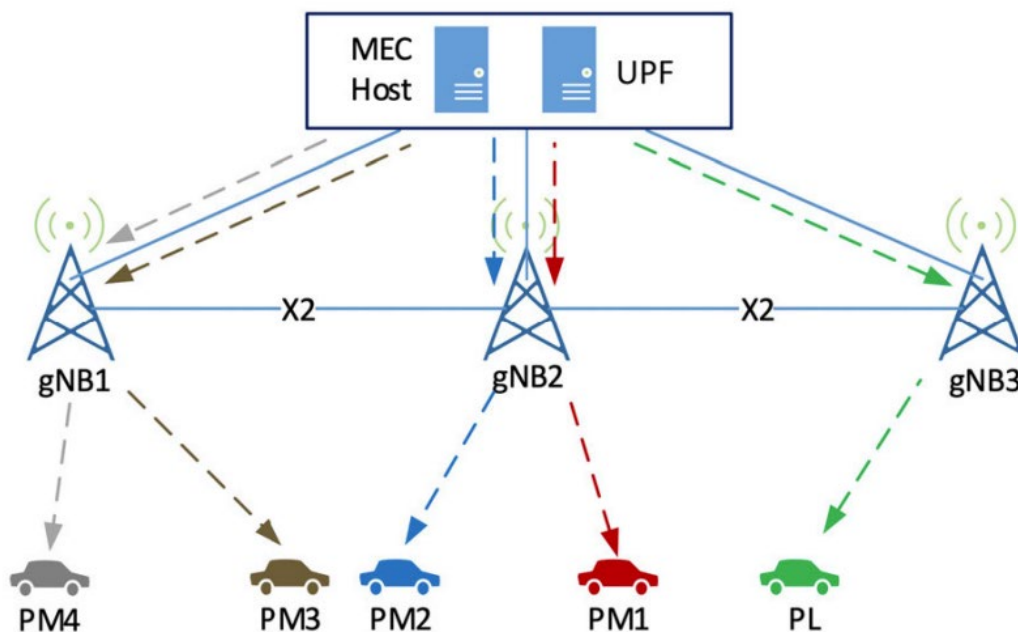
Το Simu5G προσφέρει την δυνατότητα και έτοιμα παραδείγματα για την προσομοίωση πολλών λειτουργιών 5G, κάποιες από τις οποίες είναι:

- Λειτουργίες MEC. Για την προσομοίωση εφαρμογών με MEC, το Simu 5G χρησιμοποιεί το module MechHost το οποίο περιέχει και δίνει στον χρήστη την δυνατότητα να αναπτύξει MEC Apps για να διαχειρίζεται τα δεδομένα τα οποία φτάνουν από τα UEs από το edge [40][45].
- Την ανάπτυξη εφαρμογών V2V και V2I, αυτό επιτυγχάνεται με την συνεργασία του Simu5G με άλλες βιβλιοθήκες του OMNET++, όπως είναι η Veins και την οποία θα δούμε στο επόμενο κεφάλαιο [40][45].
- Την δυνατότητα εξομοίωσης (emulation). Με αυτήν την δυνατότητα του Simu5G, τρεις συνδεδεμένοι υπολογιστές μπορούν να συνδεθούν μεταξύ τους μέσω ethernet έτσι ώστε να παρουσιάσουν ένα σενάριο 5G. Δύο υπολογιστές έχουν τον ρόλο του πομπού και του δέκτη ενώ ανάμεσά τους βρίσκεται ο τρίτος είναι αυτός στον οποίο αναπτύσσεται το σενάριο του δικτύου. Ένας υπολογιστής π.χ. μπορεί να κάνει streaming ένα βίντεο, στον ενδιαμέσο υπολογιστή ορίζεται το σενάριο που θέλουμε να προσομοιώσουμε (π.χ. επικοινωνία V2V) και στον τρίτο υπολογιστή μπορούμε να δούμε τα αποτελέσματα όπως π.χ. η αλλοίωση του βίντεο [45].





Εικόνα 24: Διάταξη emulation στο Simu5G, [45].



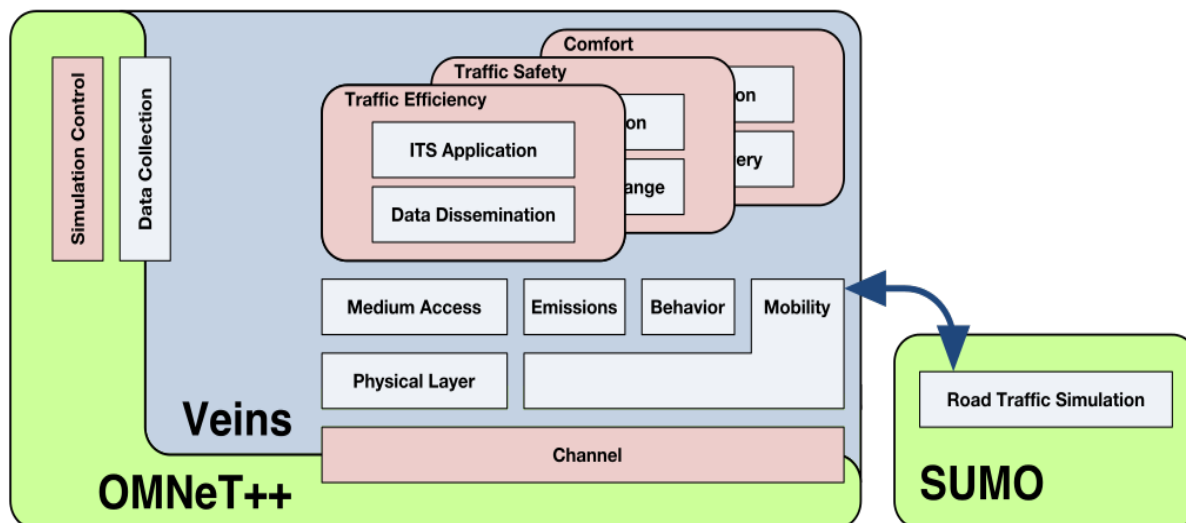
Εικόνα 25: Σενάριο Vehicles Platooning στο Simu5G, [44].

## 2.5 Η βιβλιοθήκη Veins

Η βιβλιοθήκη Veins του OMNeT++, επιτρέπει την προσομοίωση οχημάτων που επικοινωνούν μεταξύ τους. Είναι Open-Source και χρησιμοποιείται συχνά στον τομέα των Vehicular Ad Hoc Networks (VANETs) και Intelligent Transportation System (ITS). Κάποιες από τις εφαρμογές στις οποίες χρησιμοποιείται είναι η οδική ασφάλεια, η επικοινωνία οχημάτων με τα φανάρια, το platooning, η διαχείριση κίνησης και άλλες. Η βιβλιοθήκη περιέχει πολλά μοντέλα προσομοίωσης για να εξεταστούν οι εν λόγω επικοινωνίες, όπως π.χ. το IEEE WAVE (Wireless Access in Vehicular Environments)



αλλά ταυτόχρονα μπορεί να χρησιμοποιηθεί και σαν βάση για την μοντελοποίηση άλλων κόμβων όπως πεζοί, ποδήλατα, τρέινα και UAV, αλλά και πρωτόκολλα επικοινωνιών όπως το LTE και το 5G NR. Η βιβλιοθήκη δεν δίνει την δυνατότητα σχεδιασμού σεναρίων κίνησης δρόμου από μόνη της αλλά έχει σχεδιαστεί έτσι ώστε να συνδέει το OMNeT++ με τον προσομοιωτή κίνησης SUMO (Simulation of Urban Mobility) τον οποίο θα δούμε στο επόμενο κεφάλαιο. Θα μπορούσαμε να πούμε ότι στην περίπτωση που εξετάζουμε λειτουργεί σαν τον μεσάζοντα για να ενσωματώσει το Simu5G και το SUMO.



Εικόνα 26: Σύνδεση του OMNeT++ με το SUMO μέσω του Veins, [41]

## 2.6 SUMO

Το SUMO είναι ένας open-source προσομοιωτής κίνησης δρόμου, ο οποίος διανέμεται μέσω της άδειας Eclipse Public License V2 [41]. Το SUMO χρησιμοποιείται διεθνώς και με πάνω από 35.000 χρήστες κάθε χρόνο. Το SUMO είναι ένα μικροσκοπικός προσομοιωτής, γενικότερα υπάρχουν τέσσερα είδη προσομοιωτές κίνησης δρόμου [41]:

- Μακροσκοπικοί (Macroscopic): Όπου πολύ γενικά στοιχεία όπως η πυκνότητα της κίνησης μπορούν να προσομοιωθούν [41].
- Μικροσκοπικοί (Microscopic): Όπου κάθε όχημα και οι παράμετροι του μπορούν να μοντελοποιηθούν ξεχωριστά [41].
- Μεσοσκοπικοί (Mesoscopic): Μία μίξη μακροσκοπικών και μικροσκοπικών μοντέλων [41].
- Υπομικροσκοπικοί (Submicroscopic): Κάθε όχημα αλλά και παράμετροι μέσα στο όχημα, π.χ. αλλαγή ταχυτήτων μπορούν να προσομοιωθούν εκτεταμένα.

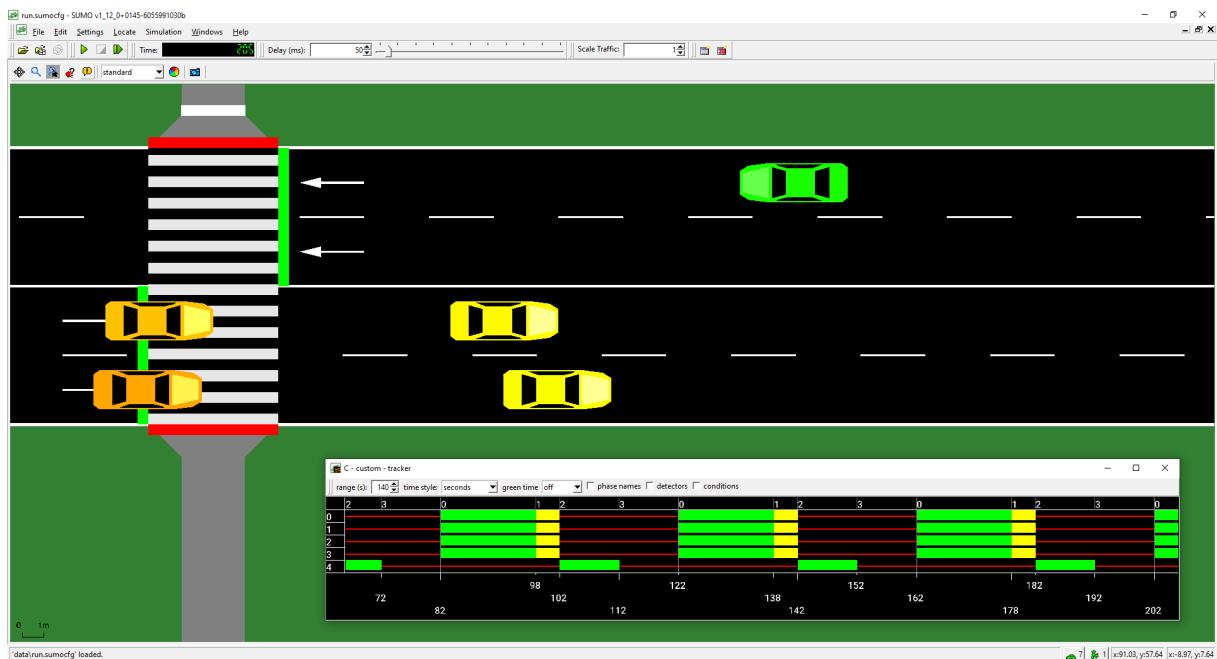
Για να πραγματοποιηθεί μία προσομοίωση στο SUMO, μπορούμε να ορίσουμε διάφορα στοιχεία όπου τα τρία πιο σημαντικά είναι το δίκτυο (π.χ. διαθέσιμοι δρόμοι, μονοπάτια), άλλες υποδομές της κίνησης (π.χ. τα φανάρια) και η ποσότητα της κίνησης [41]. Μαζί αυτά τα στοιχεία ορίζουν ένα σενάριο προσομοίωσης, όπου στο τέλος της μπορούμε να βγάλουμε στατιστικά συμπεράσματα σχετικά με την ταχύτητα και την θέση των οχημάτων, τα πρωτόκολλα με τα οποία μπορούν να αλλάζουν τα φανάρια

του δρόμου, στοιχεία για τις εκπομπές των καυσαερίων και άλλα. Τόσο η προσομοίωση όσο και τα αποτελέσματα μπορούν να αναπαρασταθούν γραφικά με την χρήση του SUMO-GUI [41].

Το δίκτυο του SUMO αποτελείται από κόμβους και λωρίδες κυκλοφορίας οι οποίες μπορούν να αντιπροσωπεύουν δρόμους, κανάλια νερού, ράμπες τραίνων, ποδηλατοδρόμους και πεζοδρόμια [41]. Χαρακτηριστικά όπως το πλάτος του δρόμου, το όριο ταχύτητας και προσβάσεις (π.χ. μία λωρίδα κυκλοφορίας η οποία είναι αποκλειστικά για λεωφορεία) ορίζονται στο πρόγραμμα. Ως αποτέλεσμα, ένα οδικό δίκτυο πρέπει να μοντελοποιηθεί σαν ένα σύνολο λωρίδων κυκλοφορίας με συγκεκριμένα χαρακτηριστικά [41]. Για την δημιουργία ενός δικτύου, το SUMO μπορεί να χρησιμοποιήσει δύο εφαρμογές οι οποίες είναι το NETCONVERT και το NETEDIT. Το NETCONVERT είναι ένα εργαλείο command-line το οποίο μπορεί να χρησιμοποιηθεί για να εισάγουμε οδικά δίκτυα από διάφορες πηγές όπως είναι το OpenStreetMap (OSM), το OpenDrive, το Shapefile ή και από άλλους προσομοιωτές κίνησης όπως το MATSim και το Vissim [41]. Το NETEDIT είναι ένας γραφικός τρόπος έτσι ώστε ο χρήστης να δημιουργήσει, επεξεργαστεί και να αναλύσει τα αρχεία οδικού δικτύου, έτσι δίνεται η δυνατότητα και για την δημιουργία ενός οδικού δικτύου από την αρχή αλλά και η δυνατότητα προσαρμογής και επεξεργασίας ενός υπάρχοντος δικτύου, μερικά από τα στοιχεία τα οποία μπορεί να ορίσει ο χρήστης είναι [41]:

- Βασικά στοιχεία του δικτύου (Διασταυρώσεις και λωρίδες κυκλοφορίας).
- Περαιτέρω στοιχεία του δικτύου (π.χ. φανάρια).
- Επιπλέον υποδομές (π.χ στάσεις λεωφορείων).
- Συγκεκριμένα σημεία ενδιαφέροντος (points of interest-POI).

Εκτός από το δίκτυο, μία ικανότητα του SUMO είναι να παρέχει τα δεδομένα κυκλοφορίας στο κάθε δίκτυο. Η κυκλοφορία σε ένα δίκτυο μπορεί να οριστεί σαν ταξίδια (trips), ροές (flows) και διαδρομές (routes) [41]. Οι βασικές πληροφορίες που πρέπει να περιέχονται είναι ο χρόνος αναχώρησης, η προέλευση, ο προορισμός, και το μέσο κυκλοφορίας το οποίο μπορεί να οριστεί ως διαφορετικά είδη οχημάτων και πεζών [41]. Όταν η κυκλοφορία ορίζεται ως διαδρομή, δεν είναι αναγκαίο να ορίσουμε την προέλευση και τον προορισμό [41]. Το κεντρικό στοιχείο για να μοντελοποιηθεί η κίνηση με διαφορετικά μέσα κυκλοφορίας είναι οι πεζοί [41]. Κάθε πεζός στο SUMO μπορεί να έχει ένα διαφορετικό πλάνο για το πότε με ποιο μέσο θέλει να κινηθεί, και το μέσο που θα χρησιμοποιήσει μπορεί να αλλάζει από ταξίδι σε ταξίδι [41]. Τα υποστηριζόμενα μέσα στο SUMO είναι το περπάτημα, τα ιδιωτικά οχήματα (αυτοκίνητο, μοτοσυκλέτα κλπ.), τα ΜΜΕ (Μέσα Μαζικής Μεταφοράς) αλλά και άλλες δραστηριότητες όπως οι στάσεις λεωφορείων [41]. Το SUMO δεν ξεχωρίζει κάθε μοναδικό όχημα από μόνο του, προσφέρει στους πεζούς μία λίστα από διαθέσιμα οχήματα και ο χρήστης ορίζει τον τύπο αυτών των οχημάτων, οπότε κάθε πεζός μπορεί να έχει πολλά οχήματα στην διαθεσιμότητα του [41].



**Εικόνα 27 : Περιβάλλον SUMO**

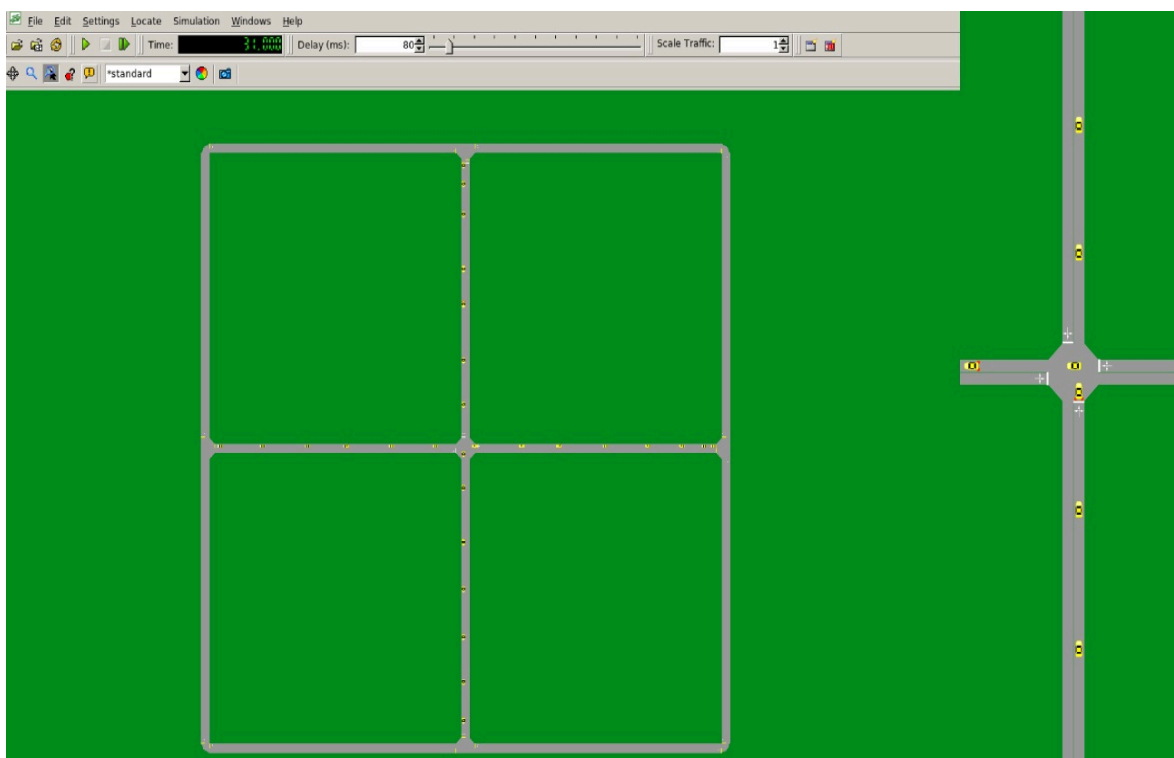
Με το SUMO είναι δυνατόν να προσομοιωθούν πολλά χαρακτηριστικά κίνησης, υπάρχουν όμως και περιορισμοί, π.χ. για την δικτυακή επικοινωνία μεταξύ οχημάτων χρειάζονται δύο ειδών εξειδίκευση [41]. Πρώτα η επικοινωνία μεταξύ οχημάτων πρέπει να μοντελοποιηθεί και δεύτερον οι διαδρομές που τα οχήματα θα ακολουθήσουν [41]. Δεδομένου ότι η μία διαδικασία μπορεί να επηρεάσει την άλλη, είναι αναγκαίο να συνδέσουμε το SUMO με άλλους προσομοιωτές για να παράγουμε ικανοποιητικά αποτελέσματα. Για την σύζευξη δύο ή περισσότερων προσομοιωτών, πρέπει να υπάρχει ένα interface για να μπορούν να συνδεθούν μεταξύ τους [41]. Αυτό το interface παρέχεται στο SUMO μέσω του TraCI (Traffic Control Interface), όπου ο χρήστης μπορεί να συνδέσει δύο προσομοιωτές μέσω μίας δικτυακής θύρας [41]. Το TraCI έχει χρησιμοποιηθεί σε projects όπως το iCS (iTETRIS Control System) για να συνδέσει το ns3 με το SUMO για επικοινωνία vehicle-to-vehicle (V2V) και vehicle-to-infrastructure (V2I) [41]. Ένα άλλο πρόγραμμα που μπορεί να συνεργαστεί με το TraCI είναι η βιβλιοθήκη Veins στο OMNeT++, την οποία θα χρησιμοποιήσουμε και στην παρακάτω προσομοίωση [41].

## 2.7 Προσομοίωση σεναρίου κίνησης με το Simu5G και το SUMO

Σε αυτό το υποκεφάλαιο προχωράμε στην προσομοίωση ενός σεναρίου κίνησης με το SUMO το οποίο εξετάζουμε στην συνέχεια με το Simu5G ως προς τις δικτυακές του παραμέτρους, τόσο σε συνδεσιμότητα LTE όσο και σε συνδεσιμότητα 5G.

Αρχικά στο SUMO ορίζουμε το σενάριο κίνησης το οποίο θέλουμε να προσομοιώσουμε, για την συγκεκριμένη προσομοίωση εξετάζεται μία διασταύρωση οι οποία αποτελείται από δύο δρόμους (lanes) μονής κυκλοφορίας όπου ο καθένας έχει μήκος 400 μέτρα. Στον δρόμο αυτό τοποθετούνται όμοια αυτοκίνητα τα οποία εκτελούν διαδρομές (trips) από την μία άκρη του δρόμου προς την άλλη, συνολικά 40 αυτοκίνητα ή 20 σε κάθε δρόμο. Τα αυτοκίνητα αυτά έχουν μήκος 4 μέτρα και ξεκινούν κάθε

δευτερόλεπτο το ένα μετά το άλλο με επιτάχυνση 3,5 m/sec μέχρι να φθάσουν την τελική ταχύτητα των 22.2 m/sec (~80 km/h) όπου και συνεχίζουν την πορεία τους στην έξοδο του δρόμου. Η προσομοίωση ολοκληρώνεται όταν όλα τα αυτοκίνητα έχουν ολοκληρώσει τις διαδρομές τους, περίπου 60 sec.

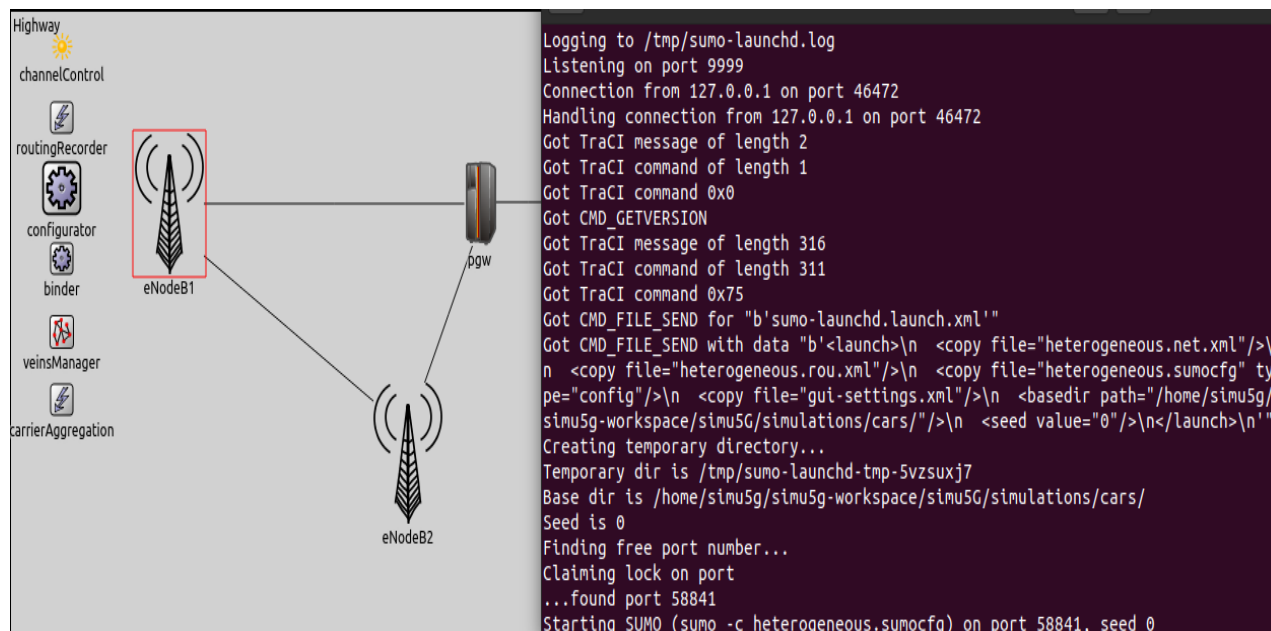


Εικόνα 28: Προσομοίωση κίνησης, τα αυτοκίνητα κινούνται από τα δεξιά προς τα αριστερά και από πάνω προς τα κάτω.

Πίνακας 5. Παράμετροι σεναρίου κίνησης

Μήκος δρόμου	400 m κάθε λωρίδα κυκλοφορίας
Σύνολο Αυτοκινήτων	40
Αυτοκίνητα σε κάθε λωρίδα ενδιαφέροντος	20
Μήκος Αυτοκινήτων	4 m για κάθε αυτοκίνητο
Αρχική Ταχύτητα	0 m/sec
Εκκίνηση νέου αυτοκινήτου	Ένα αυτοκίνητο/sec
Επιτάχυνση	3.5 m/sec
Τελική ταχύτητα	22.2 m/sec
Τύπος κίνησης	Διαδρομές (trips)
Διάρκεια προσομοίωσης	60 sec

Για να χρησιμοποιηθεί το σενάριο αυτό σε συνδυασμό με την δικτυακή προσομοίωση στο Simu5G, πρέπει να υπάρξει επικοινωνία μεταξύ του SUMO και του OMNeT++, πρέπει δηλαδή να εκκινήσουμε τον TraCI server (εικόνα 22) και εφόσον έχουμε επικοινωνία, αρχίζουμε να σχεδιάζουμε τις παραμέτρους των σεναρίων που θέλουμε να εξετάσουμε.

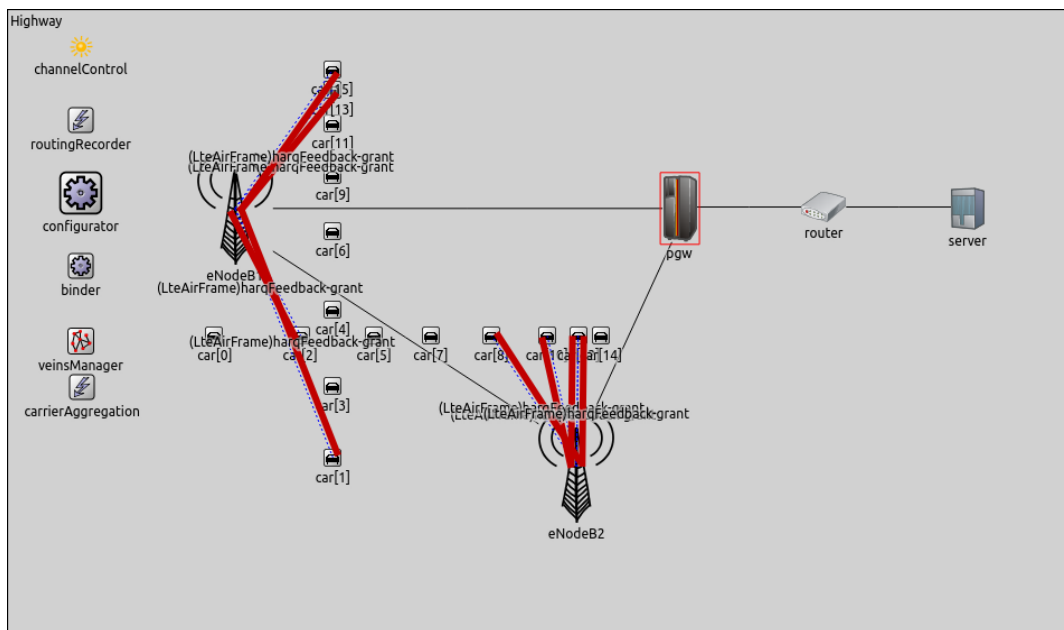


**Εικόνα 29: Επικοινωνία SUMO και OMNET++ μέσω του TraCI server**

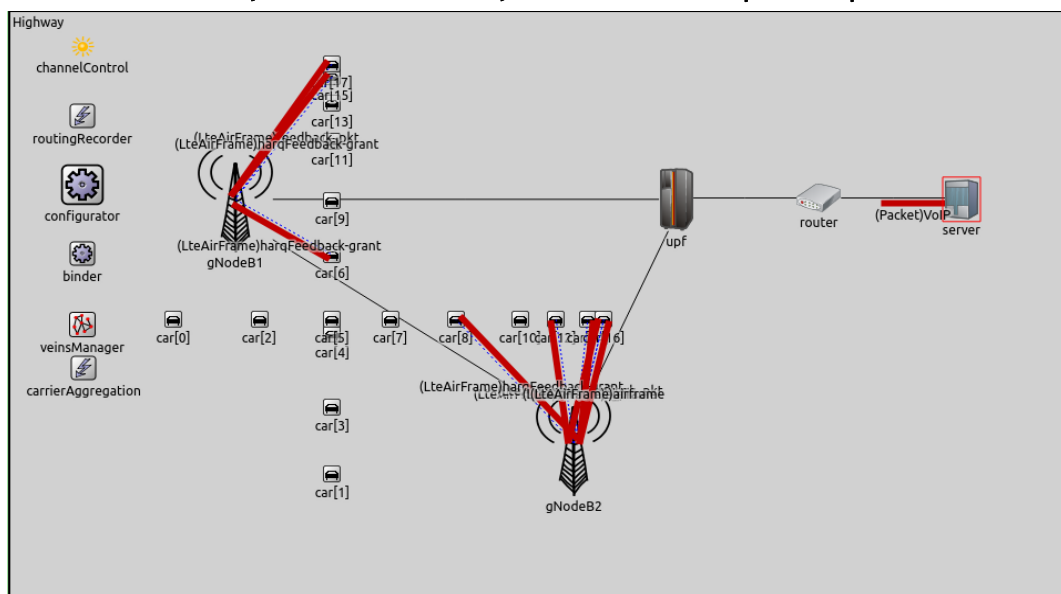
Στην συγκεκριμένη περίπτωση θα εξετάσουμε την καθυστέρηση της μεταφοράς των πακέτων (uplink latency) από τα αυτοκίνητα, ως ασύρματοι κόμβοι προς τον server του δικτύου, δεδομένου ότι η ασύρματη επικοινωνία πραγματοποιείται είτε μέσω σταθμών LTE (eNB) είτε μέσω 5G NR (gNB), ταυτόχρονα μπορούμε να ελέγξουμε και την καθυστέρηση μεταφοράς πακέτων από τους σταθμούς προς τα αυτοκίνητα (downlink latency). Στο σενάριο A, δύο σταθμοί LTE (eNB) τοποθετούνται κατά μήκος της διασταύρωσης σε 100 m μεταξύ τους απόσταση, και οι δύο αυτοί σταθμοί είναι συνδεδεμένοι άμεσα με τον server αλλά χρησιμοποιούν επίσης και το interface X2 για την μεταξύ τους επικοινωνία ώστε τα πακέτα που λαμβάνουν να βρίσκουν την πιο σύντομη διαδρομή, μεταδίδουν μηνύματα με ισχύ 46 dBm στην συχνότητα 2 GHz ενώ είναι εξοπλισμένοι με κεραιές απολαβής 18 dBi. Τα αυτοκίνητα ως δικτυακοί κόμβοι είναι εξοπλισμένα με κάρτες LTE NIC και στέλνουν συνεχόμενα μηνύματα VoIP μεγέθους 40 bytes, που θα μπορούσαν να εκπροσωπούν την ενημέρωση για την γεωγραφική τους θέση, προς στους δύο σταθμούς βάσης στην συχνότητα των 2GHz, με ισχύ 26 dBm μέσω ισοτροπικών (0 dBi) κεραιών. Το σενάριο B χρησιμοποιεί τις ίδιες παραμέτρους, ωστόσο οι σταθμοί είναι 5G NR (gNB) και τα αυτοκίνητα είναι εξοπλισμένα με κάρτες NR NIC. Και σε αυτή την περίπτωση οι δύο σταθμοί επικοινωνούν κατευθείαν με τον server (5G SA) αλλά και μεταξύ τους μέσω του X2 interface.

Και στα δύο σενάρια, η απόσταση του κάθε αυτοκινήτου από τον κάθε σταθμό βάσης κυμαίνεται μεταξύ των 64 m και 324 m με την μέση απόσταση να είναι ~120 m,

ενώ και στις δύο περιπτώσεις τα μηνύματα που ανταλλάσσονται από το κάθε αυτοκίνητο είναι  $\sim 1000$ . Η προσομοίωση όπως και στην περίπτωση του SUMO διαρκεί μέχρι κάθε αυτοκίνητο να έχει εγκαταλείψει την λωρίδα κυκλοφορίας, δηλαδή  $\sim 60$  sec. Πρέπει να σημειώσουμε ότι ενώ η απώλεια διαδρομής (path loss) υπολογίζεται στην κάθε θέση, δεν θεωρούνται άλλα ενδιάμεσα εμπόδια καθώς και χρήστες που θα μπορούσαν να απασχολούν τους δύο σταθμούς. Εφόσον έχει ολοκληρωθεί η προσομοίωση, μπορούμε να εξετάσουμε το uplink και το downlink latency παρατηρώντας το RLC layer του κάθε αυτοκινήτου, τόσο ως διανυσματικά (vector) μεγέθη για το κάθε πακέτο σε σχέση με τον χρόνο όσο και τον μέσο όρο καθυστέρησης όλων των πακέτων κάθε αυτοκινήτου σε βαθμωτά (scalar) μεγέθη.



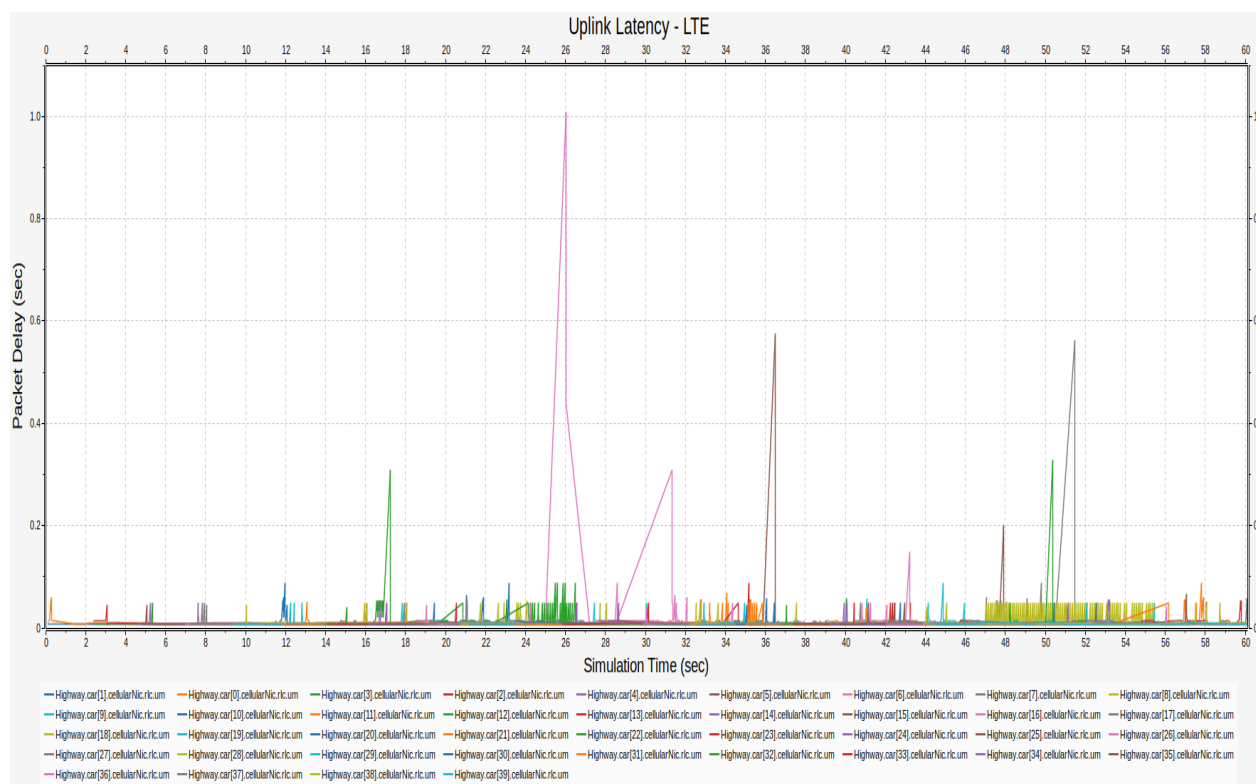
Εικόνα 30: Σενάριο A, τα αυτοκίνητα επικοινωνούν με σταθμούς LTE eNB



Εικόνα 31: Σενάριο B, τα αυτοκίνητα επικοινωνούν με σταθμούς 5G NR gNB

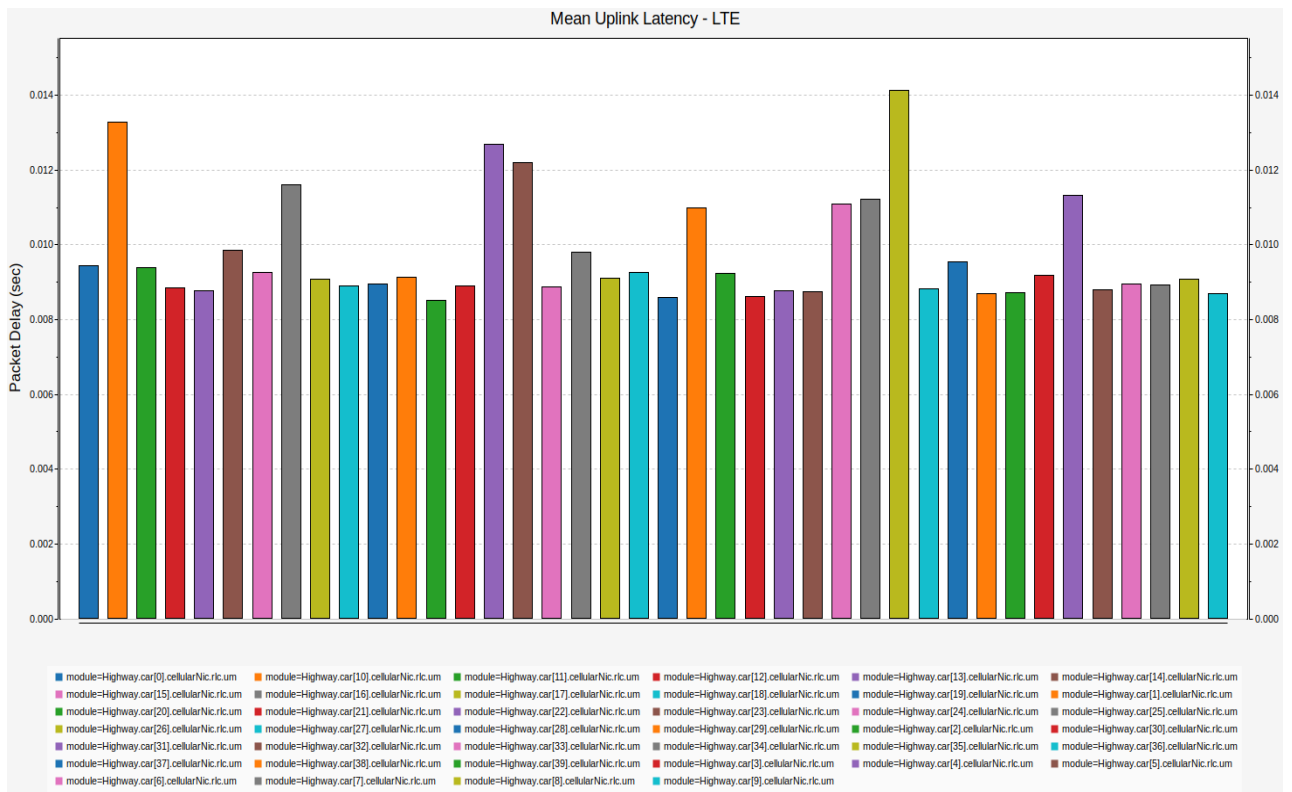
Πίνακας 6. Παράμετροι του δικτύου

Συχνότητα	2GHz
Ισχύς eNB και gNB	46 dBm
Απολαβή κεραίας eNB και gNB	18 dBi
Απολαβή κεραίας αυτοκινήτου	0 dBi
Μέγεθος μηνύματος	40 bytes
Επικοινωνία	VoIP
Απόσταση αυτοκινήτων από eNB/gNB	Περίπου 120 m
Ροή μηνυμάτων	Συνεχόμενη
Σύνολο πακέτων αυτοκινήτων	Περίπου 1000
Διάρκεια προσομοίωσης	60 sec

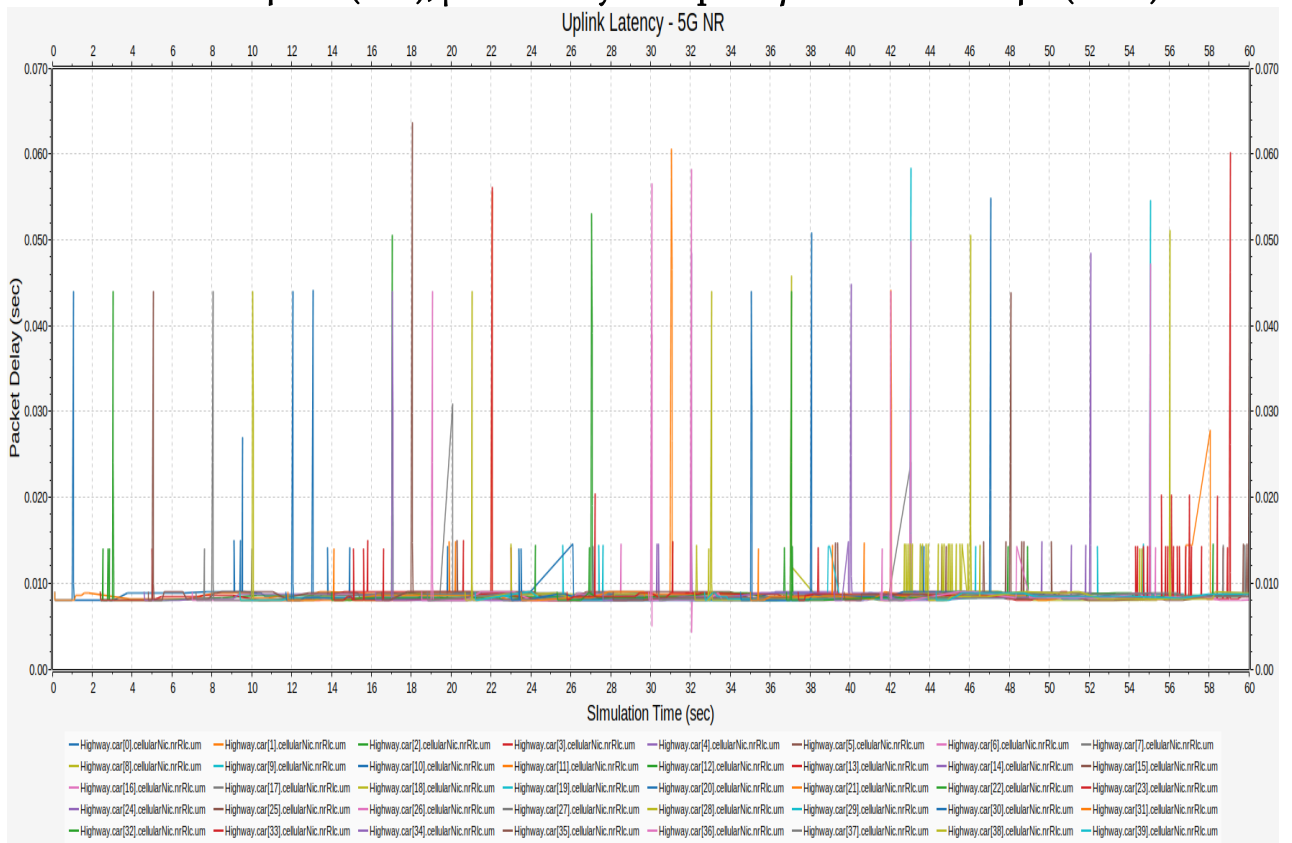


Εικόνα 32: Σενάριο A (LTE), στιγμιαίο latency στο uplink για κάθε μήνυμα αυτοκινήτου (vector)



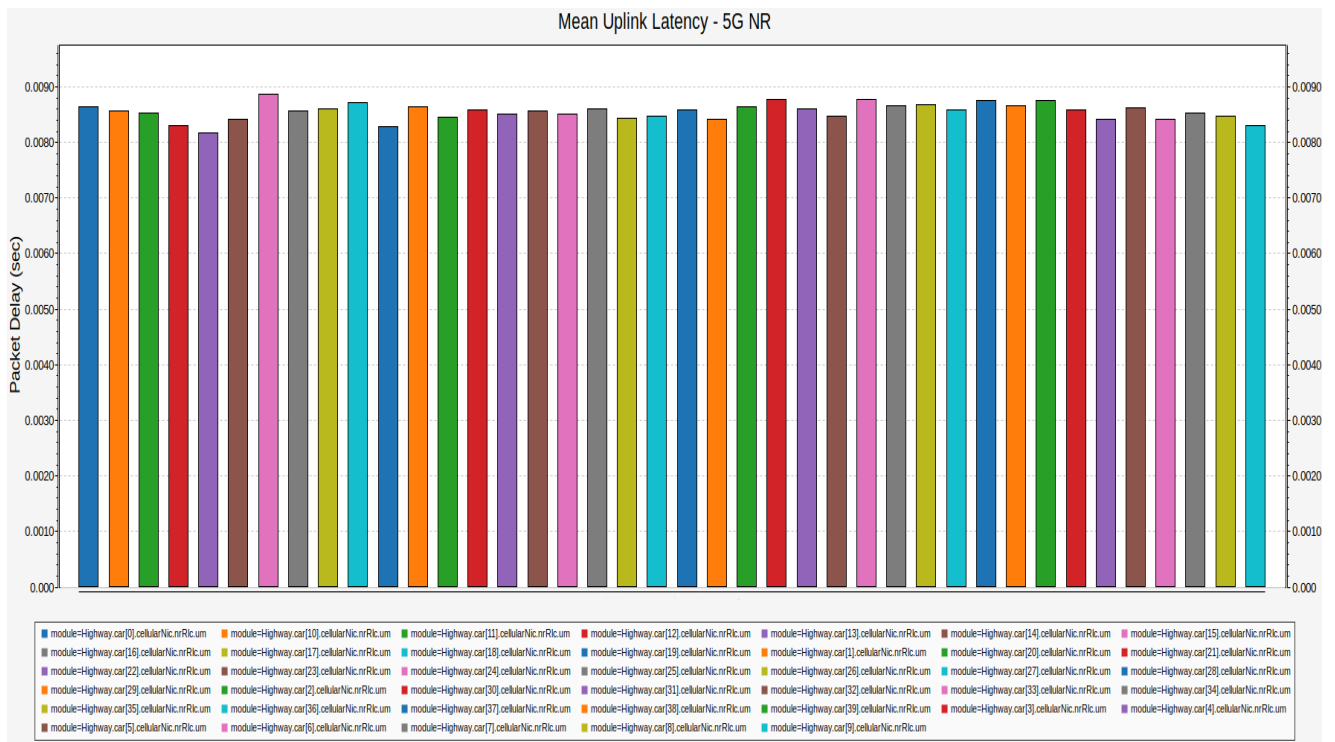


Εικόνα 33: Σενάριο A (LTE), μέσο latency στο uplink για κάθε αυτοκίνητο (scalar).

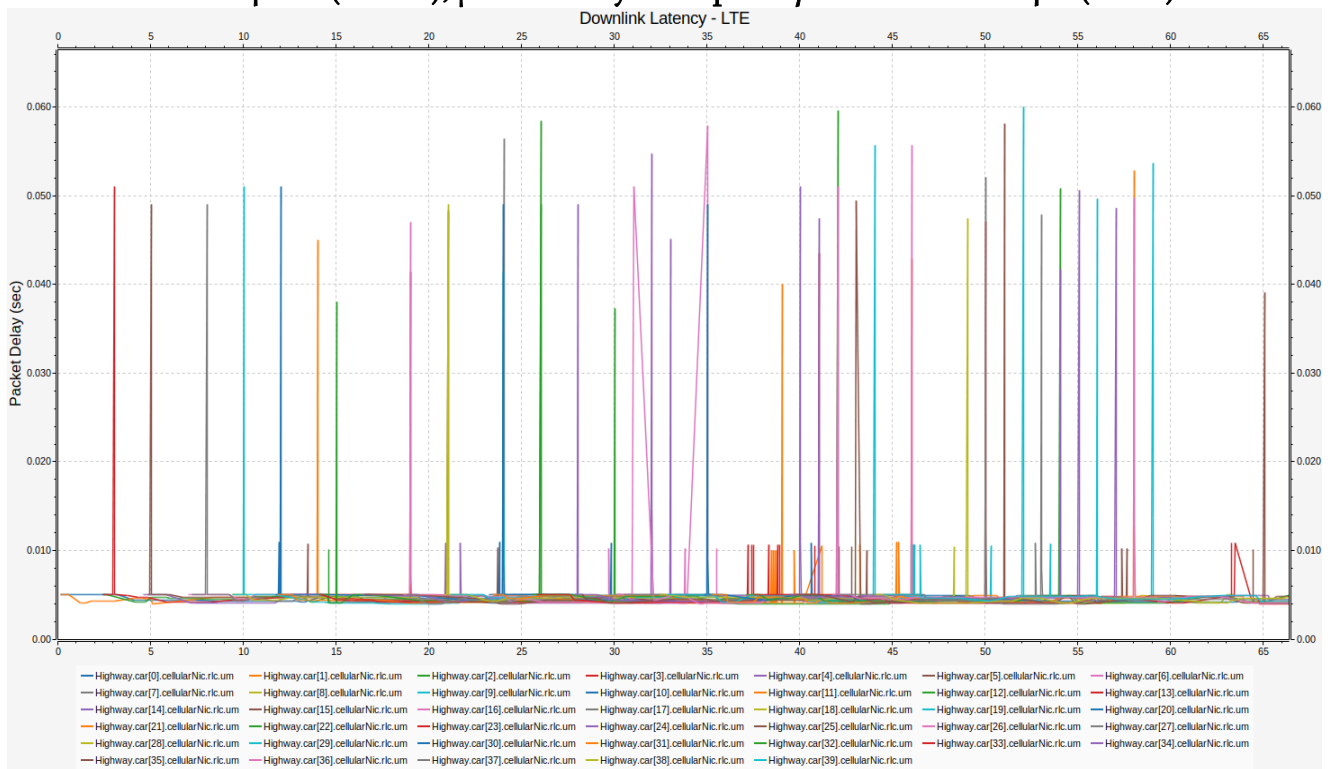


Εικόνα 34: Σενάριο B (5G NR), στιγμιαίο latency στο uplink για κάθε μήνυμα αυτοκινήτου (vector).

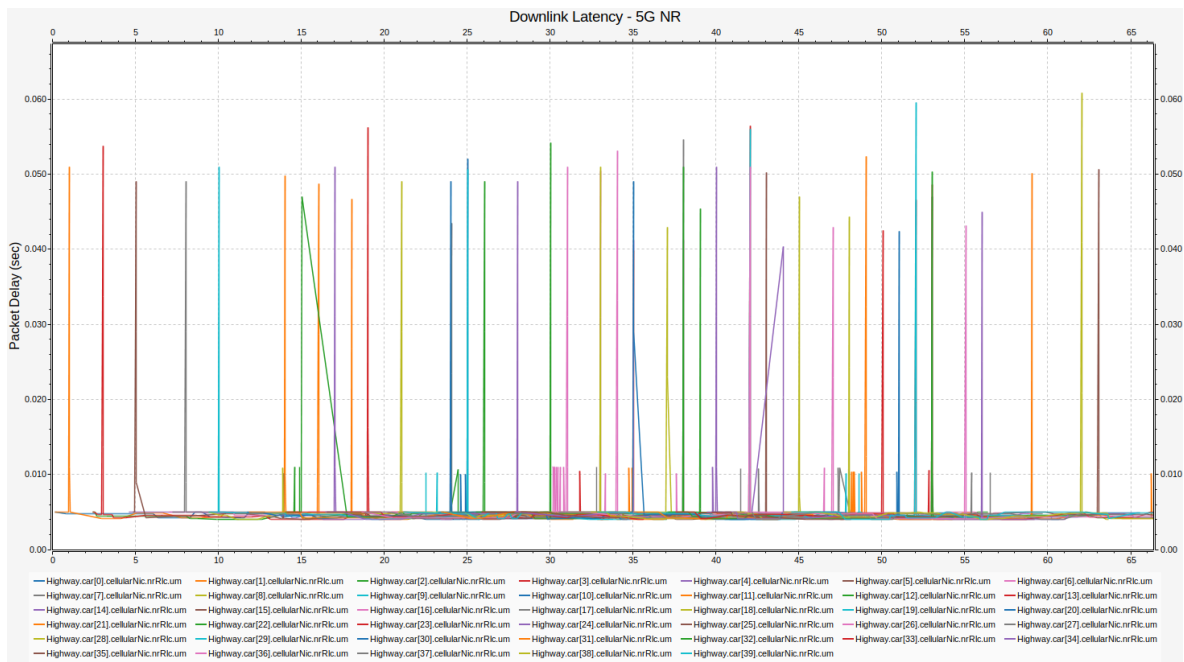




Εικόνα 35: Σενάριο B (5G NR), μέσο latency στο uplink για κάθε αυτοκίνητο (scalar).



Εικόνα 36: Σενάριο A (LTE), στιγμιαίο latency στο downlink για κάθε εισερχόμενο μήνυμα προς κάθε αυτοκίνητο (vector).



**Εικόνα 37: Σενάριο B (5G NR), στιγμιαίο latency στο downlink για κάθε εισερχόμενο μήνυμα προς κάθε αυτοκίνητο (vector).**

## 2.8 Συμπεράσματα αποτελεσμάτων και σκέψεις

Από τα αποτελέσματα συμπεραίνουμε ότι το μέσο uplink latency όσο και το στιγμιαίο downlink latency δεν είναι σημαντικά διαφορετικά τόσο στο σενάριο LTE όσο και στο σενάριο 5G NR, το οποίο είναι και ο λόγος που δεν εξετάστηκε το μέσο downlink latency. Ωστόσο, στο στιγμιαίο LTE uplink latency του παρατηρούμε ότι οι διακυμάνσεις είναι αρκετά μεγάλες με κάποια αυτοκίνητα να καθυστερούν να ενημερώσουν για τη θέση τους έως και 1 sec ενώ το στιγμιαίο 5G NR uplink latency δεν ξεπερνάει ποτέ τα 65 msec. Δεδομένου ότι η ταχύτητα των αυτοκινήτων είναι 22,2 m/sec, αυτό σημαίνει ότι στην περίπτωση LTE ένα αυτοκίνητο μπορεί να κινηθεί για 22,2 μέτρα χωρίς να έχει ενημερώσει για την θέση του ενώ στην περίπτωση 5G NR τα αυτοκίνητα θα κινηθούν το πολύ 1,443 μέτρα, ενώ με μέσο uplink latency τα 10 msec τα αυτοκίνητα προλαβαίνουν να κινηθούν μόλις 0,222 μέτρα πριν προλάβουν να ενημερώσουν για την θέση τους. Τα αποτελέσματα μας δείχνουν λοιπόν ότι το 5G NR και η άμεση διαχείριση πόρων σε σχέση με το LTE, θα μπορούσαν να εξυπηρετήσουν σενάρια platooning και αυτόνομων αυτοκινήτων με ένα αρκετά πιο αξιόπιστο τρόπο.

Το δίκτυο θα μπορούσε να ενισχυθεί με σταθμούς MEC και D2D επικοινωνία μεταξύ των αυτοκινήτων για ακόμα πιο άμεση ανταλλαγή δεδομένων. Πρέπει να λάβουμε ωστόσο υπόψιν ότι σε ένα αληθινό σενάριο δρόμου είναι πολύ πιθανόν να υπάρξουν και άλλοι παράγοντες όπως γεγονότα που εμποδίζουν την μετάδοση των μηνυμάτων (obstacle loss, jamming), οι σταθμοί πρέπει να είναι ενεργοί συνεχώς για να εξυπηρετήσουν τα αυτοκίνητα ενώ πρέπει να προστατεύονται από περιπτώσεις καταστροφής και κλοπής. Τέλος, για να υλοποιηθεί ένα σενάριο αυτόνομων αυτοκινήτων πρέπει να επιτρέπεται από αντίστοιχο νομοθετικό πλαίσιο και να υπάρχει η διαθεσιμότητα των αυτοκινήτων αυτών προς τους πολίτες.

## 1. Σύνοψη των πρωτοκόλλων που θα χρησιμοποιηθούν.

Στο κεφάλαιο αυτό θα αναλυθούν τα πρωτόκολλα τα οποία θα χρησιμοποιηθούν για την δημιουργία του NB-IoT κόμβου.

### 1.1. Πρωτόκολλο TCP/IP

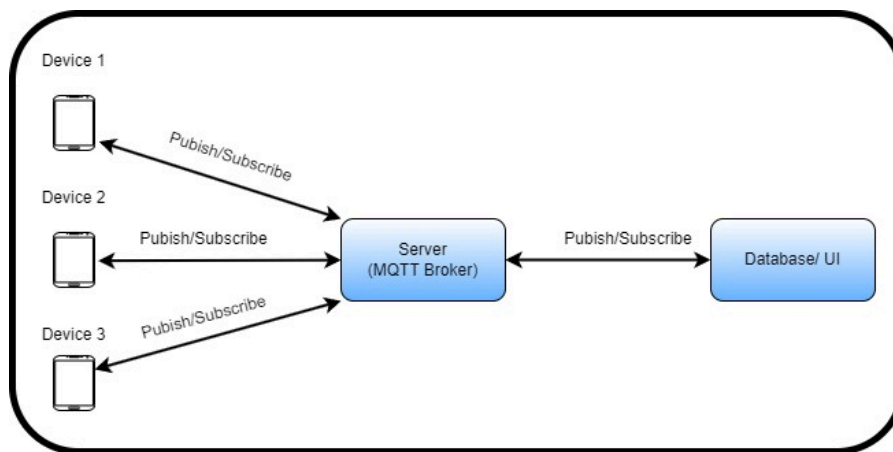
Το πρωτόκολλο IP (Internet Protocol) έχει τον ρόλο της επικοινωνίας μεταξύ χρηστών οι οποίοι αναγνωρίζονται από τις καθορισμένες IP διευθύνσεις τους [55]. Το πρωτόκολλο TCP (Transmission Control Protocol) παρέχει μια αξιόπιστη μεταφορά δεδομένων μεταξύ δύο κεντρικών μονάδων [55]. Επιτρέπει τον διαχωρισμό των πακέτων τα οποία δέχεται ώστε να φθάσουν στον οργανωμένα στον αποστολέα και περιμένει την αναγνώριση από αυτό για την περίπτωση που χρειαστεί να τα ξαναστείλει [55]. Το πρωτόκολλο IP από μόνο του δεν μπορεί να παρέχει αξιοπιστία και γι' αυτό τον λόγο συμπληρώνεται από το πρωτόκολλο TCP, οι επικοινωνίες τύπου TCP/IP είναι σε λειτουργία από την δεκαετία του 1970[55].

### 1.2. Πρωτόκολλο TLS

Το πρωτόκολλο TLS (Transport Layer Security) επιτρέπει την ασφαλή επικοινωνία μεταξύ δύο χρηστών χρησιμοποιώντας κρυπτογραφία για την αυθεντικοποίησή τους[56]. Το TLS είναι ένα πρακτικά ένα πρωτόκολλο το οποίο βρίσκεται πάνω από το TCP, όταν πραγματοποιείται η σύνδεση μεταξύ δύο μηχανών το TLS ορίζει τον τρόπο που αυτές οι μηχανές θα αναγνωριστούν[56]. Για ακόμα καλύτερη ασφάλεια, το TLS χρησιμοποιεί αλγορίθμους cipher κατά την διάρκεια της σύνδεσης[56]. Μία εφαρμογή με την οποία μπορούμε να χειριστούμε το TLS είναι το OpenSSL και θα δούμε αργότερα στην εργασία.

### 1.3. Πρωτόκολλο MQTT (Message Queuing Telemetry Transport)

Το MQTT εφευρέθηκε από την IBM, έχει σχεδιαστεί για να είναι ένα ιδιαίτερα ελαφρύ πρωτόκολλο στο επίπεδο εφαρμογής (Application Layer). Διαθέτει σταθερό μέγεθος κεφαλίδας (Header Size) μόλις 2 byte, και κατ' επέκταση είναι κατάλληλο για IoT διαδικασίες ασύρματων δικτύων αισθητήρων (WSN) και επικοινωνίες M2M. Το MQTT βασίζεται στην διαδικασία Publish/Subscribe, όπου οι Publishers και οι Subscribers συνδέονται σε έναν κεντρικό MQTT broker που λειτουργεί ως server. Οι Publishers δημοσιεύουν μηνύματα σε καθορισμένα θέματα (topics) που είναι αποθηκευμένα στον broker, οι Subscribers εγγράφονται στα ανάλογα topics ώστε μέσω του sever να ενημερώνονται για κάθε νέο μήνυμα. Στην Εικόνα 38 απεικονίζεται στο διάγραμμα ροής MQTT.



**Εικόνα 38: Διάγραμμα ροής MQTT.**

Το πρωτόκολλο MQTT έχει σχεδιαστεί για να στέλνει μικρά μηνύματα (0-256 Mb) σε μία ή πολλές συσκευές με μικρή καθυστέρηση και είναι κατάλληλο για την ανταλλαγή μηνυμάτων σε ασταθή δίκτυα. Συνιστάται η χρήση αυτού του πρωτοκόλλου σε ασύρματα δίκτυα για την ανταλλαγή μηνυμάτων χωρίς υψηλές απαιτήσεις δεδομένων και εύρους ζώνης. Όσον αφορά την ασφάλεια, οι MQTT Publishers και Subscribers μπορούν να επικοινωνούν με τον MQTT broker επικυρώνοντας ένα πιστοποιητικό SSL/TLS, το οποίο είναι αποθηκευμένο στον server του broker. Διαδοχικά, οι Publishers και οι Subscribers παρέχουν τα δικά τους πιστοποιητικά στον broker MQTT, ο οποίος τα ελέγχει για την πιστοποίηση[57][58].

Τα χαρακτηριστικά του MQTT περιλαμβάνουν QoS (Quality of Service), LWT (Last Will and Testament) και Retain Flag [58][59]. Το QoS καθορίζει τον τρόπο επικοινωνίας των μηνυμάτων μεταξύ του Publisher/Subscriber και του broker. Πιο συγκεκριμένα, με QoS 0 μεταδίδεται ένα μήνυμα χωρίς εγγύηση παράδοσης (χρησιμοποιείται κυρίως σε δίκτυα UDP), με QoS 1 το μήνυμα μεταδίδεται όσες φορές χρειαστεί μέχρι να υπάρξει επιβεβαίωση από τον δέκτη, με QoS 2 το μήνυμα μεταδίδεται ακριβώς μία φορά μέχρι να υπάρξει επιβεβαίωση δέκτη, [50][59]. Το LWT είναι ένα χαρακτηριστικό που ειδοποιεί τους Subscribers για μια ξαφνική αποσύνδεση του Publisher, όπως π.χ. βλάβη δικτύου [58]. Με το Retain Flag, ο broker αποθηκεύει το τελευταίο διατηρημένο μήνυμα και το μεταδίδει ξανά για ενημέρωση στους νέους Subscribers, μια δυνατότητα που αποδεικνύεται χρήσιμη σε καταστάσεις επανασύνδεσης συσκευών.

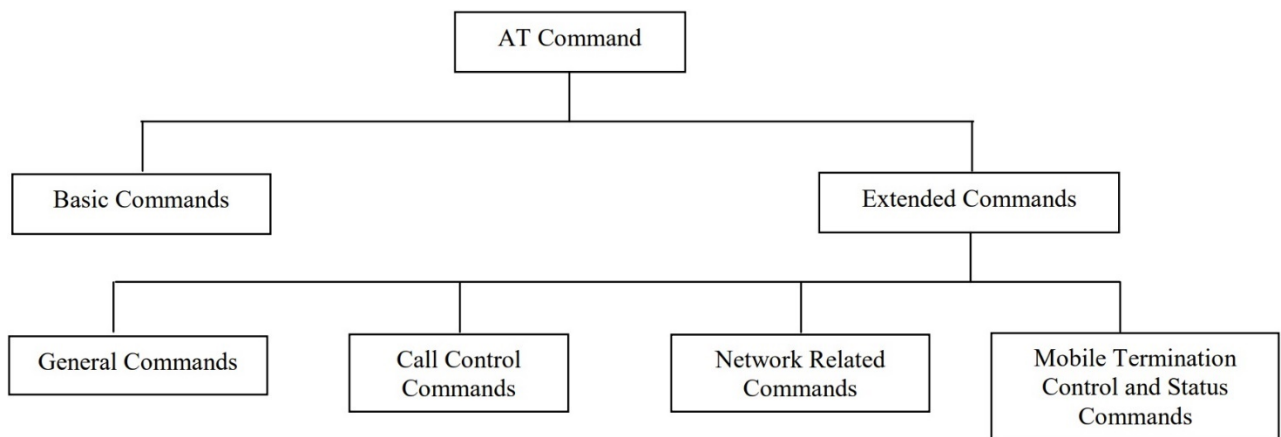
#### 1.4. AT Εντολές

Οι AT εντολές (AT Commands) προέρχονται από την λέξη «Attention», και είναι εντολές οι οποίες χρησιμοποιούνται για την παραμετροποίηση των GPRS/GSM μόντεμ, για τον λόγο αυτό οι εντολές αυτές είναι επίσης γνωστές ως εντολές μόντεμ. Στέλνοντας τις εντολές αυτές μέσω ενός τερματικού στο μόντεμ μπορούμε να καθοδηγήσουμε και να ελέγξουμε το τρόπο που ένα μόντεμ θα επικοινωνήσει στο δίκτυο ή και να αλλάξουμε κάποια χαρακτηριστικά του. Παρότι είναι καθιερωμένες στα κινητά τηλέφωνα, οι εντολές αυτές μπορεί να είναι διαφορετικές από μόντεμ σε μόντεμ ανάλογα με τον κατασκευαστή. Κάποιες από τις διαδικασίες που μπορούμε να εκτελέσουμε με τα AT Commands είναι οι επόμενες[47]:

- Να λάβουμε βασικές πληροφορίες για το κινητό τηλέφωνο. Για παράδειγμα το όνομα κατασκευαστή, τον αριθμό μοντέλου, τον αριθμό IMEI και την έκδοση λογισμικού.
- Να γνωρίζουμε τρέχουσα κατάσταση του του μόντεμ GSM/GPRS. Για παράδειγμα την κατάσταση εγγραφής σε δίκτυο κινητής τηλεφωνίας, την ισχύ του σήματος, το επίπεδο φόρτισης μπαταρίας.
- Να διαβάσουμε, να γράψουμε, να διαγράψουμε και να στείλουμε SMS, όπως και να λάβουμε ειδοποιήσεις για τη λήψη του νέου SMS.

Στα AT commands Η γραμμή εντολών ξεκινά με "AT" ή "at" και στην συνέχεια ακολουθεί η εντολή που θέλουμε να εκτελέσουμε. Κατά αυτό τον τρόπο οι εντολές AT χωρίζονται σε δύο είδη:

- Βασικές εντολές (Basic Commands) είναι εκείνες οι εντολές που δεν ξεκινούν με «+». Για παράδειγμα, ATD (Για κλήση), ATAN (Για απάντηση).
- Οι εκτεταμένες εντολές (Extended Commands) είναι εκείνες οι εντολές που ξεκινούν με «+». Για παράδειγμα, AT+CMGS (Για την αποστολή SMS). Ανάλογα οι εκτεταμένες εντολές διαχωρίζονται σε είδη ανάλογα τις παραμετροποιήσεις που εκτελούν (Εικόνα 39).



Εικόνα 39: Διάταξη των AT εντολών[47].

## 1.5. Arduino IDE

Το Arduino IDE (Integrated Development Environment) είναι open-source λογισμικό το οποίο αναπτύσσεται από την Arduino[60]. Χρησιμοποιείται για την επεξεργασία, σύνταξη και την εφαρμογή κώδικα στις πλατφόρμες της Arduino[60]. Είναι διαθέσιμο για λειτουργικά συστήματα όπως MAC, Windows, Linux και εκτελείται στην πλατφόρμα Java με ενσωματωμένες λειτουργίες και εντολές για τον εντοπισμό σφαλμάτων, την επεξεργασία και σύνταξη κώδικα[60]. Το περιβάλλον υποστηρίζει γλώσσες C και C++ και ο κώδικας μεταφέρεται στον μικροελεγκτή σε δεκαεξαδική μορφή [60]. Για την εκτέλεση συγκεκριμένων συναρτήσεων και τον εύκολο έλεγχο ενσωματωμένων συσκευών στο μικροελεγκτή προσφέρονται ενσωματωμένες

βιβλιοθήκες[60]. Ο Serial Monitor είναι ένα πολύ βοηθητικό εργαλείο καθώς μας δίνει την δυνατότητα σειριακής επικοινωνίας με τον μικροελεγκτή και κατ' επέκτασιν τον έλεγχο σφαλμάτων[60]. Αν π.χ. θέλουμε να χρησιμοποιήσουμε μία οθόνη για ένα σύστημα αλλά δεν είμαστε σίγουροι ότι θα δουλέψει, μπορούμε πρώτα να πάρουμε την επιβεβαίωση παρατηρώντας την απόκριση στον Serial Monitor.

## 2. Εργαλεία που χρησιμοποιήθηκαν.

Στο υποκεφάλαιο αυτό θα περιγράψουμε τα εργαλεία τα οποία χρησιμοποιήσαμε σε λογισμικό και υλικό επίπεδο για να υλοποιήσουμε τον κόμβο μας. Το υλικό το οποίο χρησιμοποιήθηκε είναι το Arduino UNO, το DFRobot SIM7000E, ο αισθητήρας DHT11, κάρτα EMnify τροφοδοσία 12V DC, καλώδιο σύνδεσης USB type B για την σύνδεση του Arduino σε υπολογιστή, jumper cables για την σύνδεση του αισθητηρίου στο Arduino, ο server του Πανεπιστημίου όπου εγκαταστάθηκε ο broker, ισοτροπική κεραία κοντά στην B20 του LTE (800 MHz). Στον πίνακα 7 φαίνεται το κόστος για τα υλικά.

Πίνακας 7. Κόστος Υλικών

Arduino UNO+USB Type B	~20 EUR
DFRobot SIM7000E	~50 EUR
EMnify SIM	7.5 EUR/SIM+0.24 EUR/MB
DHT11	~3 EUR
Τροφοδοσία 12V DC	~3 EUR
Υπολογιστής Server	~500-1000 EUR
Jumper Cables	Αμελητέο
Κεραία	~10 EUR



Εικόνα 40: Υλικά τα οποία χρησιμοποιήθηκαν.



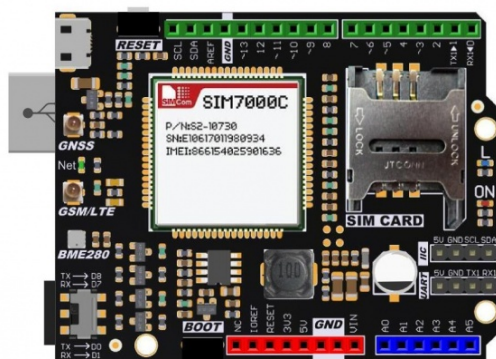
Σε επίπεδο λογισμικού χρησιμοποιήθηκαν ο EMQX broker, το Arduino IDE, η εφαρμογή Node-RED, η εφαρμογή OpenSSL και η εφαρμογή QPST. Όλες οι εφαρμογές διατίθενται δωρεάν.

## 2.1. EMQX MQTT Broker.

Ο EMQX Broker είναι ένας δημοφιλής MQTT broker που έχει αναπτυχθεί στην γλώσσα Erlang, φημίζεται για την επεκτασιμότητα του σε παράλληλα και κατακευματμένα συστήματα με υψηλή απόδοση όπως ένα εκατομμύριο μηνύματα το λεπτό με καθυστέρηση μικρότερη του msec. Ο EMQX υποστηρίζει πολλά πρωτόκολλα όπως MQTT, HTTP, QUIC, και WebSocket. Είναι συμβατός με το MQTT 5.0 και το 3.x standard, ενώ υποστηρίζει την αμφίδρομη MQTT επικοινωνία μέσω TLS/SSL και άλλων μηχανισμών ταυτοποίησης. Με ενσωματωμένες SQL δυνατότητες, ο EMQX μπορεί να εξάγει, να φιλτράρει και να παραμετροποιήσει IoT δεδομένα σε πραγματικό χρόνο. Επιπλέον διαθέτει φιλικό περιβάλλον προς τον χρήστη για την εύκολη παραμετροποίηση του και την επισκόπηση των δεδομένων. Ο EMQX χρησιμοποιείται πολύ συχνά στην βιομηχανία, κάποιες από τις εταιρείες οι οποίες των χρησιμοποιούν είναι οι HPE, VMware, Verifone, SAIC Volkswagen, και Ericsson[48][49].

## 2.2. DFRobot SIM7000E.

Το SIM7000 NB-IoT/LTE/GPRS HAT είναι ένα module επέκτασης για μικροελεγκτές Arduino το οποίο παράγεται από την DFRobot και είναι βασισμένο στο SIMCom SIM7000 chip. Υποστηρίζει την ασύρματη επικοινωνία σε επίπεδο LTE-FDD, GPRS/EDGE και NB-IoT. Το module μπορεί να υποστηρίζει και κάρτες GSM όπως για τηλεφωνική επικοινωνία και SMS αλλά και NB-IoT για την μετάδοση δεδομένων. Το module υποστηρίζει επικοινωνία μέσω GNSS (Global Navigation Satellite System) και είναι συμβατό με το Αμερικάνικο GPS, Ρωσικό GLONASS, Ευρωπαϊκό Galileo, Γιαπωνέζικο QZSS και το Κινέζικο BeiDou Navigation Satellite System, κάτι το οποίο είναι χρήσιμο σε deployments απομακρυσμένου χώρου [50].



Εικόνα 41: SIM700 HAT

Το SIM7000E είναι ο κωδικός «E» της σειράς SIM7000 ο οποίος υποδεικνύει ότι αυτό το module υποστηρίζει τις GNSS λειτουργίες στην Ευρώπη, την Αφρική, την Αυστραλία, και την Νοτιοανατολική Ασία [51]. Τα UART pins για TX και RX έχουν σχεδιαστεί για να ελέγχονται σειριακά, το οποίο πραγματοποιείται μέσω των AT εντολών. Το

SIM7000E υποστηρίζει συναρτήσεις για να μειώσει την κατανάλωση ενέργειας όπως η λειτουργία πτήσης, PSM, και e-DRX [51].

### 2.3. OPENSLL

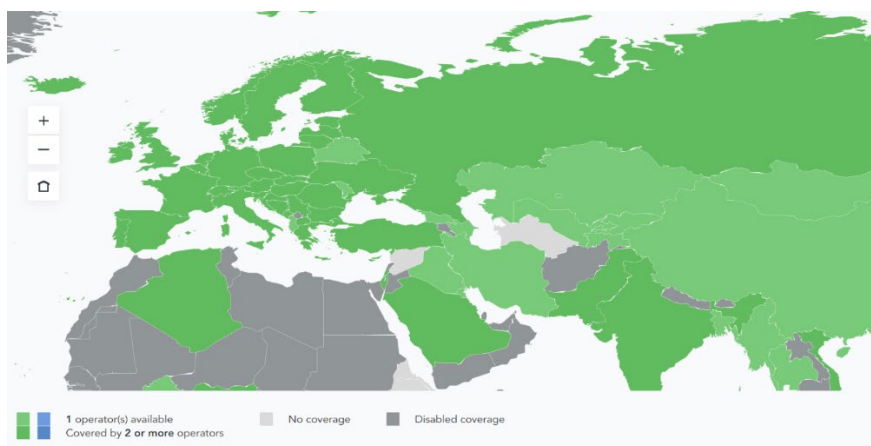
Το OpenSSL είναι μία εφαρμογή ανοιχτού κώδικα η οποία αναπτύσσεται από το “The OpenSSL Project” για την δημιουργία πιστοποιητικών στα πρωτόκολλα SSL και TLS. [52] Η βασική βιβλιοθήκη είναι γραμμένη στην γλώσσα C και εφαρμόζει τις βασικές κρυπτογραφικές συναρτήσεις [52]. Το OpenSSL υποστηρίζει διάφορους κρυπτογραφικούς αλγόριθμους όπως [52]:

- Cyphers - Blowfish, DES, RC2, RC4, IDEA, AES.
- Hashing functions - MD5, MD2, SHA, MDC-2.
- Public-key cryptography (Asymmetric) - RSA, DSA, Diffie-Hellman key exchange, ECC.

Με την χρήση του OpenSSL μπορούμε να δημιουργήσουμε πιστοποιητικά για να δημιουργήσουμε τα πιστοποιητικά ώστε ο κόμβος να επικοινωνεί πιστοποιημένα.

### 2.4. EMnify SIM Cards

Η EMnify είναι μία εταιρεία η οποία παρέχει ειδικές IoT SIM κάρτες και eSIM με σκοπό την συνδεσιμότητα σε διάφορα δίκτυα παγκοσμίως. Πιο συγκεκριμένα, μία EMnify SIM επιτρέπει το roaming σε παραπάνω από 540 δίκτυα σε περισσότερες από 195 χώρες, τα δίκτυα αυτά μπορεί να είναι 2G, 3G, 4G, LTE-M και NB-IoT. Επιπλέον, οι κάρτες αυτές μπορεί να είναι κατασκευασμένες με ειδικά υλικά για να αντέχουν σε βιομηχανικό περιβάλλον [53]. Για την Ελλάδα, η EMnify επιτρέπει το roaming στις εταιρείες Wind, Cosmote και Vodafone σε επίπεδο 2G, 3G, 4G και NB-IoT καθώς για το τελευταίο επιτρέπει τις λειτουργίες PSM και eDRX [53].



**Εικόνα 42: Κάλυψη της EMnify στην Ευρώπη**

Εκτός των καρτών, η EMnify παρέχει ένα IoT Dashboard για την παρακολούθηση των συνδεδεμένων καρτών, ένα REST API για την ανάπτυξη και ενσωμάτωση εφαρμογών, καθώς και την εύκολη σύνδεση με βάσεις δεδομένων και το cloud [53].

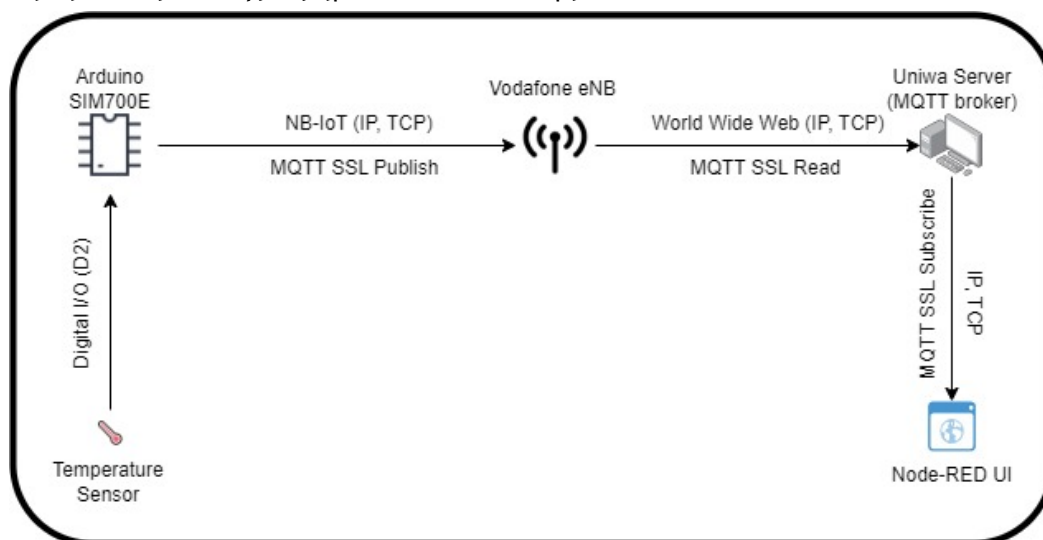


## 2.5. Node-Red

Η Node-RED είναι μία open source πλατφόρμα βασισμένη σε διαγράμματα (flows) για την διαχείριση IoT κόμβων, APIs και διαδικτυακών εφαρμογών η οποία αναπτύσσεται από την IBM[61]. Η Node-RED είναι ένα ευέλικτο και ισχυρό εργαλείο για να φτιάξουμε πρωτότυπα αφού επιτρέπει την εύκολη υλοποίηση εφαρμογών και ιδιαίτερα εφαρμογών IoT οι οποίες εξαρτώνται από κάποιο συμβάν (π.χ. την ανάγνωση ενός αισθητήρα)[13]. Χρησιμοποιεί γραφικό περιβάλλον με διαγράμματα (flows) όπου ο χρήστης μπορεί να συνδυάσει κόμβους (nodes) οι οποίοι αντιπροσωπεύονται από εικονίδια και με τεχνικές drag n' drop μπορεί να τους προσθέσει και να τους συνδυάσει στο flow καθώς και να εισάγει κώδικα Javascript[61]. Επιτρέπει την διασύνδεση μεταξύ διαδικτυακών εφαρμογών μέσω nodes τα οποία έχουν σχεδιαστεί να κάνουν συγκεκριμένες διαδικασίες (π.χ. την προώθηση δεδομένων από μία IoT συσκευή σε ένα e-mail)[13].

## 3. Υλοποίηση

Σε αυτό το υποκεφάλαιο περιγράφονται τα βήματα τα οποία ακολουθηθήκαν για την υλοποίηση του κρυπτογραφημένου MQTT κόμβου.



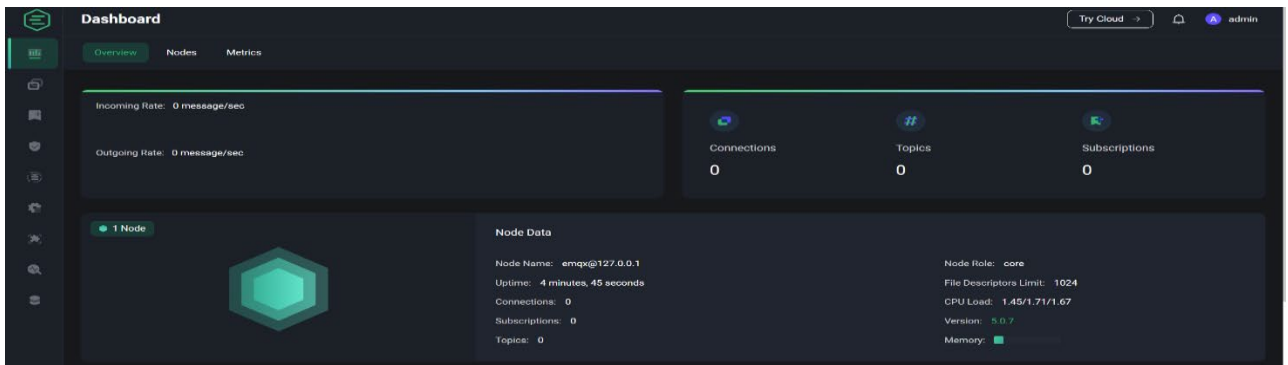
Εικόνα 43: Διάγραμμα υλοποίησης.

### 3.1. Εγκατάσταση του EMQX Broker στον Server

Έγινε εγκατάσταση της version 5.0.7 του EMQX ο οποίος υποστηρίζει TLS v1.3 σε λειτουργικό Linux Ubuntu κατεβάζοντας το πακέτο του EMQX και ακολουθώντας τις οδηγίες οι οποίες προβλέπονται [49]. Στην συνέχεια μέσω του τερματικού του Linux χρησιμοποιήσαμε την εντολή «emqx start» για να ξεκινήσουμε τον broker, αντίστοιχα με την εντολή «emqx stop» μπορούμε να τον σταματήσουμε. Μετά την εντολή start ο broker έχει εκκινήσει στο background και μπορούμε πλέον να κλείσουμε το τερματικό και να κατευθύνουμε στην θύρα 18083 του server όπου έχει εκκινήσει και το user interface της εφαρμογής.

```
root@restq1-PowerEdge-T440:/home/restq1# emqx start
EMQX 5.0.7 is started successfully!
root@restq1-PowerEdge-T440:/home/restq1#
```

Εικόνα 44: Έναρξη λειτουργίας του EMQX broker.



Εικόνα 45: Interface EMQX broker.

The screenshot shows the EMQX Listeners interface. It features a table with the following columns: Name, Type, Bind, Connections, Acceptors, Enable, and Actions. There are four rows of listener configurations, all with 'default' as the Name and 'Enable' as a toggle switch.

Name	Type	Bind	Connections	Acceptors	Enable	Actions
default	ssl	:8883	0	16	<input checked="" type="checkbox"/>	Settings Delete
default	tcp	:1884	0	16	<input checked="" type="checkbox"/>	Settings Delete
default	ws	:8083	0	16	<input checked="" type="checkbox"/>	Settings Delete
default	wss	:8084	0	16	<input checked="" type="checkbox"/>	Settings Delete

Εικόνα 46: Συνδέσεις EMQX broker

Στο user interface το οποίο μας παρέχει ο EMQX μπορούμε να παρακολουθούμε την κίνηση του Broker, το πόσες και ποιες συσκευές είναι συνδεδεμένες και σε ποια topics ενώ παράλληλα να θέσουμε κάποιες συνθήκες όπως για τον αριθμό των μηνυμάτων τα οποία επιτρέπεται να υποστηρίζονται από τον broker ή ακόμα και alarms τα οποία δημιουργεί ο broker σε περιπτώσεις όπως μη καλής χρήσης της επεξεργαστικής δυνατότητας και μνήμης του υπολογιστή. Στην εικόνα 46 μπορούμε επίσης να δούμε τις θύρες του EMQX οι οποίες είναι ανοιχτές αυτήν την στιγμή, όπου παρατηρούμε ότι η θύρα 1884 είναι ανοικτή για να χρησιμοποιήσει το πρωτόκολλο MQTT απλά με TCP, η θύρα 8883 είναι η MQTT θύρα η οποία χρησιμοποιεί το πρωτόκολλο SSL μαζί με το TCP και το MQTT για την κρυπτογράφηση των μηνυμάτων. Οι θύρες 8083 και 8084 είναι για το πρωτόκολλο WebSocket (WS) και το πρωτόκολλο WebSocket Secure (WSS) αντίστοιχα. Το ποιες θύρες θα χρησιμοποιήσει ο broker καθώς και τα πιστοποιητικά τα οποία θα χρησιμοποιήσει τα έχουμε ορίσει στο configuration file του broker όπως φαίνεται στην εικόνα 47. Η δημιουργία των πιστοποιητικών θα περιγράψει στο επόμενο κεφάλαιο.

```

listeners.tcp.default {
  bind = "0.0.0.0:1884" MQTT PORT
  max_connections = 1024000
}

listeners.ssl.default {
  bind = "0.0.0.0:8883" MQTT SSL PORT
  max_connections = 512000
  ssl_options {
    keyfile = "/etc/emqx/certs/emqx.key"
    certfile = "/etc/emqx/certs/emqx.pem"
    cacertfile = "/etc/emqx/certs/ca.pem"
  }
}

listeners.ws.default {
  bind = "0.0.0.0:8083" WS PORT
  max_connections = 1024000
  websocket.mqtt_path = "/mqtt"
}

listeners.wss.default {
  bind = "0.0.0.0:8084" WSS PORT
  max_connections = 512000
  websocket.mqtt_path = "/mqtt"
  ssl_options {
    keyfile = "/etc/emqx/certs/key.pem"
    certfile = "/etc/emqx/certs/cert.pem"
    cacertfile = "/etc/emqx/certs/cacert.pem"
  }
}

```

Εικόνα 47: Configuration file του EMQX broker

### 3.2. Δημιουργία πιστοποιητικών με το OpenSSL

Για την δημιουργία των πιστοποιητικών, εγκαταστήσαμε το λογισμικό OpenSSL στον server μας, στην συνέχεια ακολουθήσαμε τα παρακάτω βήματα για την δημιουργία αυτών θέτοντας ένα directory της επιλογής μας:

- Με την εντολή «openssl genrsa -out ca.key 2048» δημιουργούμε ένα ιδιωτικό κλειδί το οποίο υπογράφει το πιστοποιητικό CA (Certificate Authority).
- Στην συνέχεια χρησιμοποιώντας την εντολή «openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.pem» δημιουργούμε το πιστοποιητικό CA όπου εισάγουμε τα στοιχεία του οργανισμού μας τα οποία περιέχουν την χώρα, την περιοχή, την πόλη, το όνομα του οργανισμού, το όνομα της μονάδας του οργανισμού μας, το όνομά μας καθώς και ένα e-mail.

```

restq1@restq1-PowerEdge-T440:~/Documents/thanostrig/certs$ openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.pem
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GR
State or Province Name (full name) [Some-State]:Attica
Locality Name (eg, city) []:Athens
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UNIWA
Organizational Unit Name (eg, section) []:STRESQLab
Common Name (e.g. server FQDN or YOUR name) []:ATrigkas
Email Address []:mscres-55@uniwa.gr

```

Εικόνα 48: Δημιουργία πιστοποιητικού Certificate Authority.

- Με την εντολή «openssl genrsa -out emqx.key 2048» δημιουργούμε ένα ιδιωτικό κλειδί το οποίο θα το χρησιμοποιήσουμε για να δημιουργήσουμε το

πιστοποιητικό για τον EMQX broker. Πριν όμως δημιουργήσουμε το πιστοποιητικό, θα φτιάξουμε το αρχείο αναφοράς «openssl.cnf» με τα αρχεία τα οποία δηλώσαμε παραπάνω έτσι ώστε το πιστοποιητικό να βασίζεται στο Certificate Authority.

```
/home/restq1/Documents/thanostrig/certs/openssl.cnf
File Edit Search View Document Help
[req]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = req_ext
x509_extensions = v3_req
prompt = no
[req_distinguished_name]
countryName = GR
stateOrProvinceName = Attica
localityName = Athens
organizationName = UNIWA
commonName = ATrigkas
[req_ext]
subjectAltName = @alt_names
[v3_req]
subjectAltName = @alt_names
[alt_names]
IP.1 = ██████████
```

**Εικόνα 49:** Αρχείο αναφοράς στοιχείων πιστοποιητικού.

- Με την εντολή «openssl req -new -key ./emqx.key -config openssl.cnf -out emqx.csr» κάνουμε request για την δημιουργία του πιστοποιητικού χρησιμοποιώντας το αρχείο παραπάνω και με την εντολή «openssl x509 -req -in ./emqx.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out emqx.pem -days 3650 -sha256 -extensions v3\_req -extfile openssl.cnf» χρησιμοποιούμε το request παραπάνω και επικαλούμαστε το κλειδί CA για να δημιουργήσουμε το πιστοποιητικό για τον EMQX broker.
- Σε αυτό το επίπεδο έχουμε φτιάξει ένα πιστοποιητικό για τον broker, αυτό που μας λείπει είναι να δημιουργήσουμε πιστοποιητικά για τις συσκευές οι οποίες θέλουμε για την ταυτοποίησή τους με τον broker. Πρώτα δημιουργούμε ένα κλειδί client με την εντολή «openssl genrsa -out client.key 2048», στην συνέχεια κάνουμε ένα request με την εντολή «openssl req -new -key client.key -out client.csr -subj "/C=GR/ST=Attica/L=Athens/O=Atrigkas/CN=client"» όπου χρησιμοποιούμε τα στοιχεία τα οποία υπάρχουν και στο πιστοποιητικό CA. Τελικώς δημιουργούμε το πιστοποιητικό client με την εντολή «openssl x509 -req -days 3650 -in client.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out client.pem» επικαλούμενοι το πιστοποιητικό CA.

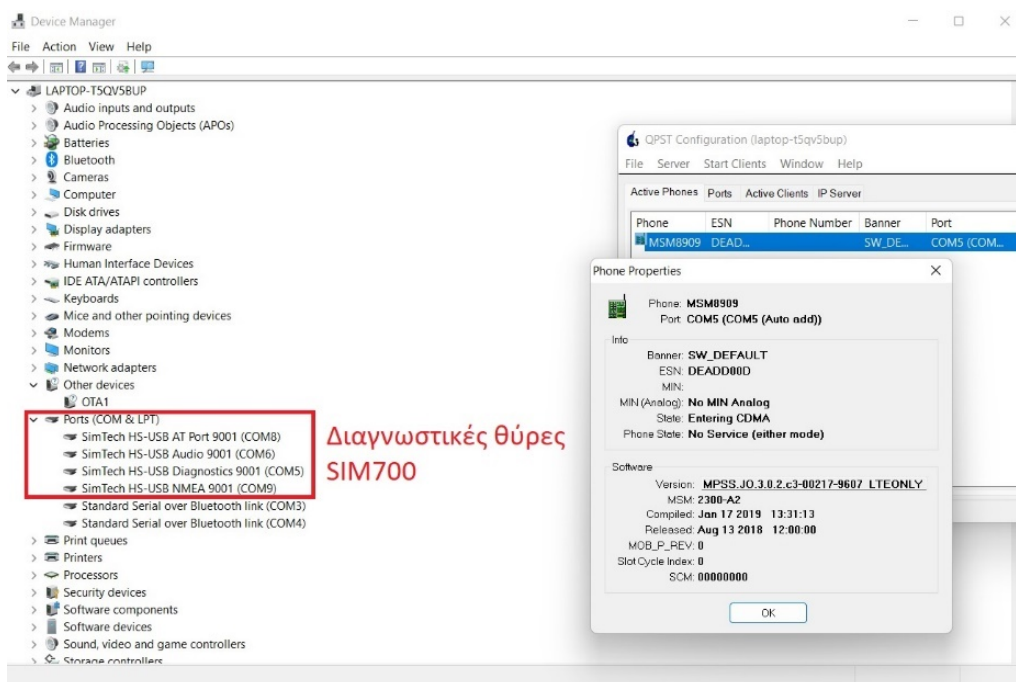
Σε αυτό το επίπεδο τα πιστοποιητικά μας τόσο για τον κεντρικό broker όσο και για τις διάφορες συσκευές μας έχουν δημιουργηθεί και μπορούν να χρησιμοποιηθούν για την ταυτοποίηση μεταξύ τους. Για τον broker χρειαζόμαστε τα πιστοποιητικά «ca.pem», «emqx.key» και «emqx.pem» ενώ για τους clients θα χρειαστούμε τα πιστοποιητικά «ca.pem», «client.key» και «client.pem».

Name	Size	Modified	Star
ca.key Κλειδί Certificate Authority	1,7 kB	21:27	☆
ca.pem Πιστοποιητικό Certificate Authority	1,4 kB	21:30	☆
ca.srl Request Certificate Authority	41 bytes	22:08	☆
client.csr Request Client	976 bytes	22:07	☆
client.key Κλειδί Client	1,7 kB	22:06	☆
client.pem Πιστοποιητικό Client	1,2 kB	22:08	☆
emqx.csr Request EMQX	1,0 kB	21:56	☆
emqx.key Κλειδί EMQX	1,7 kB	21:35	☆
emqx.pem Πιστοποιητικό EMQX	1,3 kB	21:56	☆
openssl.cnf Αρχείο Αναφοράς	405 bytes	21:56	☆

Εικόνα 50: Τα δημιουργημένα πιστοποιητικά.

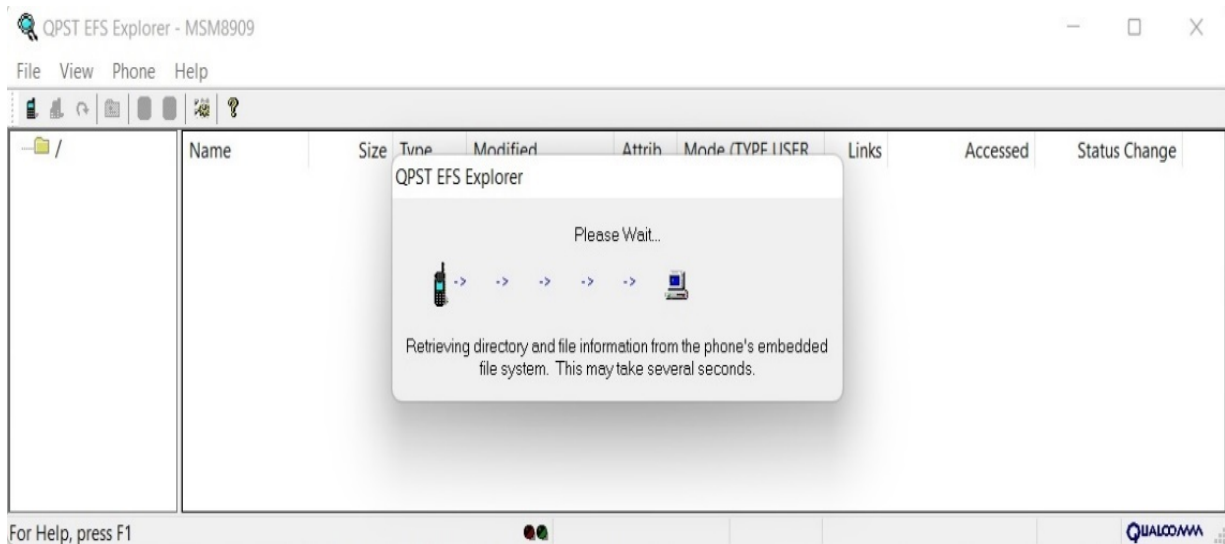
### 3.3. Εγκατάσταση πιστοποιητικών στο SIM7000E

Για να αποθηκευτούν τα πιστοποιητικά στο SIM7000e πρέπει να αποθηκευτούν στην μνήμη του chipset. Για να πραγματοποιηθεί αυτό, το SIM7000e διαθέτει την θύρα διαγνωστικών ώστε να μπορούμε να έχουμε πρόσβαση στην μνήμη του. Εφόσον εγκαταστήσουμε τους ανάλογους drivers στον υπολογιστή μας, μπορούμε να έχουμε πρόσβαση σε αυτήν. Εκτός αυτού και για να μπορούμε να διαχειριστούμε αυτήν την μνήμη, θα χρειαστούμε να εγκαταστήσουμε στον υπολογιστή μας ένα λογισμικό που σε αυτήν την περίπτωση είναι το λογισμικό QPST Tool της εταιρείας Qualcomm το οποίο ευρύτερα χρησιμοποιείται για την διαχείριση τηλεφωνικών συσκευών[54]. Αναγνωρίζει το SIM700 ως μία από αυτές και μπορούμε να έχουμε πρόσβαση στην μνήμη μέσω του QPST EFS Explorer.



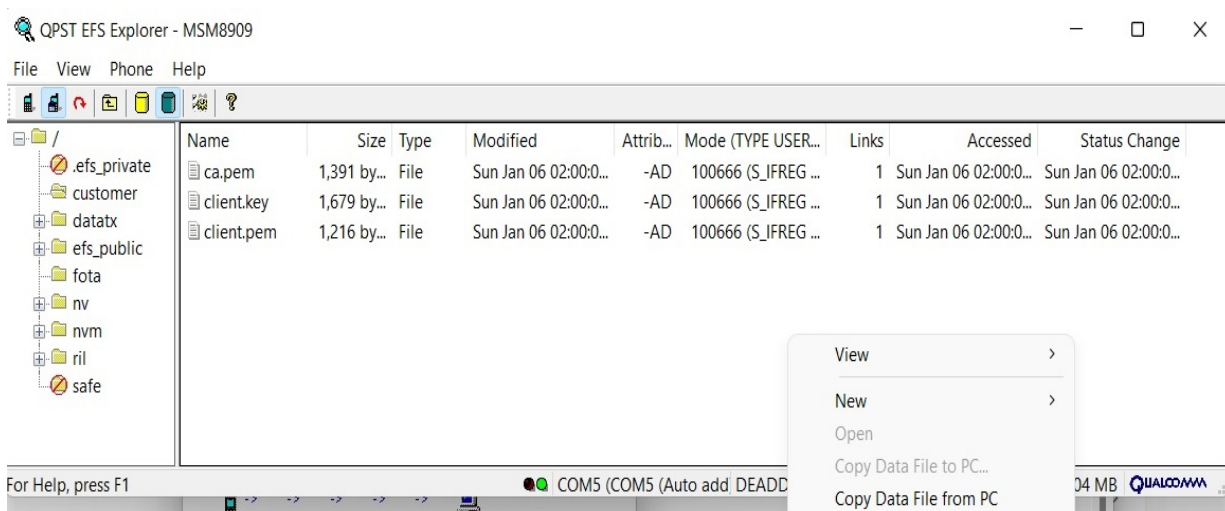
Εικόνα 51: Αναγνώριση του SIM7000E ως κινητής συσκευής από το QPST





**Εικόνα 52: Πρόσβαση στην μνήμη του SIM7000E μέσω του EFS explorer**

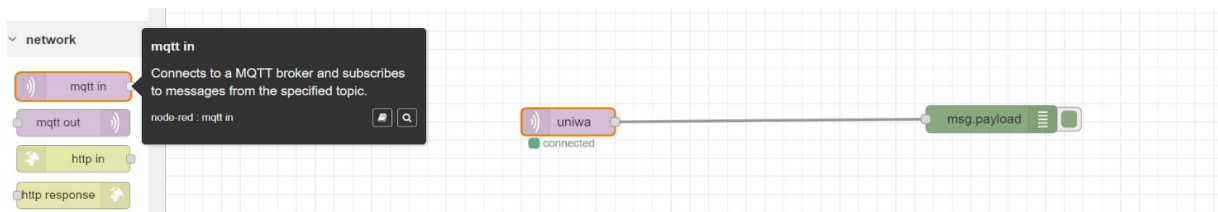
Το επόμενο βήμα είναι η εισαγωγή των πιστοποιητικών client τα οποία δημιουργήσαμε νωρίτερα στην μνήμη του SIM7000E. Έχοντας πλέον πρόσβαση στην μνήμη του SIM7000e αρκεί να αντιγράψουμε τα ανάλογα πιστοποιητικά από τον υπολογιστή μας στον εσωτερικό φάκελο customer του chip. Για την πιστοποίηση του SIM7000E θα χρειαστούμε τα πιστοποιητικά «ca.pem» για την πιστοποίηση με το Certificate Authority καθώς και το «client.pem» και «client.key» για την αναγνώριση της συσκευής.



**Εικόνα 53: Τα πιστοποιητικά αντιγραμμένα στην μνήμη του SIM7000E.**

### 3.4. Εγκατάσταση πιστοποιητικών στην Node-Red

Χρησιμοποιώντας την Node-Red ως τον subscriber ο οποίος θα δέχεται και θα παρουσιάζει τα δεδομένα τα οποία στέλνουμε από το SIM7000E, θα χρειαστεί επίσης να εγκαταστήσουμε τα ανάλογα πιστοποιητικά. Έχοντας εγκαταστήσει την Node-Red, θα χρησιμοποιήσουμε τον κόμβο «mqtt-in» για να συνδεθούμε στον MQTT broker μας και τον κόμβο «debug» για να δείξουμε τα δεδομένα.



**Εικόνα 54: MQTT κόμβος της Node-RED.**

Στην συνέχεια θα πρέπει να κάνουμε τις ανάλογες παραμετροποιήσεις στον κόμβο «mqtt-in» ώστε να ανταποκρίνεται στην διεύθυνση του broker μας, στο ανάλογο topic (σε αυτήν την περίπτωση το topic uniwa) καθώς και να δηλώσουμε το ότι επιθυμούμε να χρησιμοποιήσουμε το πρωτόκολλο TLS εισάγοντας τα κατάλληλα πιστοποιητικά. Όπως και στην περίπτωση του SIM7000E, και σε αυτήν την περίπτωση θα χρειαστούμε τα πιστοποιητικά client.

**Εικόνα 55: Δήλωση server και topic.**

**Εικόνα 56: Επιθυμία χρήσης TLS .**

**Εικόνα 57: Χρήση πιστοποιητικών «client».**

Τώρα μπορούμε να ελέγξουμε αν ο subscriber Node-RED είναι συνδεδεμένος με τον broker μέσω του interface του EMQX καθώς και σε πιο topic, ανάλογα βλέπουμε και έναν ενεργό χρήστη στην θύρα SSL του broker.

Client ID	Topic	QoS	No Local	Retain as Published	Retain Handling
Node-RED_Uniwa	uniwa	1	False	False	0

Name	Type	Bind	Connections	Acceptors	Enable	Actions
default	ssl	:8883	1	16	<input checked="" type="checkbox"/>	Settings Create

Εικόνα 58: Ο subscriber και το topic στο interface του EMQX.

### 3.5. Προγραμματισμός και έλεγχος του SIM7000E με AT Commands

Σε αυτό το υποκεφάλαιο θα εξετάσουμε την χρήση του SIM7000E με AT commands. Εφόσον εισαγάγουμε την κάρτα της EMnify στο DFRobot SIM7000E και το συνδέσουμε στο Arduino, θα το προγραμματίσουμε στο Arduino IDE με τον κώδικα «DFRobotSIM7000ATTest» ο οποίος παρέχεται από την DFRobot και κάνει χρήση της βιβλιοθήκης της.

```
#include <DFRobot_SIM7000.h>

#define PIN_TX 7
#define PIN_RX 8
SoftwareSerial mySerial(PIN_RX, PIN_TX);
DFRobot_SIM7000 sim7000(&mySerial);

void setup() {
  Serial.begin(9600);
  mySerial.begin(19200);
  Serial.println("Turn ON SIM7000.....");
  if(sim7000.turnON()){ //Turn ON SIM7000
    Serial.println("Turn ON !");
  }

  Serial.println("Set baud rate.....");
  while(1){
    if(sim7000.setBaudRate(19200)){ //Set SIM7000 baud rate from 115200 to 19200 reduce the baud rate to avoid distortion
      Serial.println("Set baud rate:19200");
      break;
    }else{
      Serial.println("Faile to set baud rate");
      delay(1000);
    }
  }
  mySerial.begin(19200);
  Serial.println("For example, if you type AT\r\n, OK\r\n will be responded!");
  Serial.println("Enter your AT command :");
}
```

Εικόνα 59: Κώδικας ATTest της DFRobot.

Στην συνέχεια ανοίγοντας την εφαρμογή Serial Monitor του Arduino IDE μπορούμε να στέλνουμε AT commands όπως προβλέπεται για το SIM7000E σύμφωνα με το manual του κατασκευαστή. Κάποιες πρώτες εντολές που μπορούμε να δοκιμάσουμε είναι η βασική εντολή «ATI» για να αναγνωρίσουμε την συσκευή, με την σύνθετη εντολή «AT+GSN» μπορούμε να δούμε το IMEI της συσκευής και με την εντολή «AT+CPIN?» να ελέγξουμε αν η SIM είναι έτοιμη για χρήση με το PIN το οποίο έχουμε θέσει.



```

COM18
Turn ON SIM7000.....
Turn ON !
Set baud rate.....
Set baud rate:19200
For example, if you type AT\r\n, OK\r\n will be responded!
Enter your AT command :
ATI
SIM7000E R1351 Μοντέλο Συσκευής
OK
AT+GSN
865234032468513 IMEI Συσκευής
OK
AT+CPIN?
+CPIN: READY Επιβεβαίωση SIM PIN
OK

```

**Εικόνα 60: Αναγνώριση της συσκευής με AT Commands.**

Θα ακολουθήσουμε τις παρακάτω σύνθετες εντολές για να συνδέσουμε το SIM7000 στο δίκτυο:

- «AT+CREG=1», για να ενεργοποιήσουμε την σύνδεση σε δίκτυα.
- «AT+COPS=?», για να δούμε ποιοι Network Operators είναι ενεργοί στην περιοχή μας.
- «AT+COPS=1,2,20205,9», για να συνδεθούμε στο δίκτυο NB-IoT της Vodafone, ο κωδικός 20205 αντιστοιχεί στο δίκτυο της Vodafone και ο κωδικός 9 συγκεκριμένα στο NB-IoT.
- «AT+CGDCONT=1,"IP","emnify"» για να θέσουμε το APN της Emnify από το οποίο θέλουμε να ενεργοποιήσουμε το PDP (Packet Data Protocol) που θα μας δώσει την IP
- «AT+CNACT», για να λάβουμε την IP από το δίκτυο

Έχουμε συνδεθεί στο δίκτυο NB-IoT της Vodafone κάτι το οποίο παρουσιάζεται και από το site διαχείρισης της Emnify.

```

OK
AT+COPS=?
+COPS: (1,"202 10","202 10","20210",0), (1,"202 05","202 05","20205",0), (1,"202 01","202 01","20201",0), (1,"202 05","202 05","20205",9), (0,1,2,3,4), (0,1,2)

```

**Εικόνα 61: Διαθέσιμοι παρόχοι, εντολή «AT+COPS=?».**

The screenshot shows the Emnify management interface for a device named 'Trigkas'. The device status is 'Enabled' and 'Online (NB-IoT)'. The IP address is highlighted as 10.188.166.83. Other details include Device ID 11917951, IMEI lock 8652340324685107, and various service policies.

**Εικόνα 62: Interface της EMnify, φαίνεται η IP της συσκευής.**

Εφόσον η συσκευή έχει συνδεθεί στο δίκτυο, η επόμενη κίνηση είναι να δοκιμάσουμε την σύνδεση με τον MQTT Broker, για να πραγματοποιηθεί αυτό θα πρέπει να ακολουθήσουμε τις εντολές για MQTT SSL σύνδεση με τον Broker οι οποίες περιγράφονται παρακάτω:

- «AT+SMCONF=" CLIENTID"," UNIWA\_SIM7000"», θέτουμε το όνομα που θέλουμε το SIM7000E να εμφανίζεται στο δίκτυο, σε αυτή την περίπτωση ως «UNIWA\_SIM7000».
- «AT+SMCONF="URL",117.131. 85.139,8883», ορίζουμε στο SIM7000E την διεύθυνση του MQTT broker (η συγκεκριμένη IP δεν ανταποκρίνεται στην αληθινή του Πανεπιστημίου).
- «AT+SMCONF="KEEPTIME",60», δίνουμε στο SIM7000E κάποιο χρόνο για να συνδεθεί στον broker, σε αυτήν την περίπτωση 60 δευτερόλεπτα.
- «AT+CSSLCFG=convert,2,ca.pem», λέμε στο SIM7000E να διαβάσει το πιστοποιητικό «ca.pem» το οποίο αποθηκεύσαμε από την μνήμη του
- «AT+CSSLCFG=convert,1,client.pem,client.key», λέμε στο SIM7000E να διαβάσει τα πιστοποιητικά «client.pem» και «client.key» το οποία αποθηκεύσαμε από την μνήμη του
- «AT+SMSSL=1,ca.pem,client.pem», για να ενεργοποιήσουμε τα πιστοποιητικά.
- «AT+SMCONN», για να συνδεθούμε στον broker.
- «AT+SMSUB="uniwa",1» για να κάνουμε subscribe στο topic «uniwa».
- «AT+SMPUB="uniwa","5",1,1» για να κάνουμε publish στο topic «uniwa» ένα μήνυμα το οποίο θα περιέχει 5 χαρακτήρες και το πληκτρολογούμε στον serial monitor.
- «AT+SMDISC» για να αποσυνδεθούμε από τον broker.

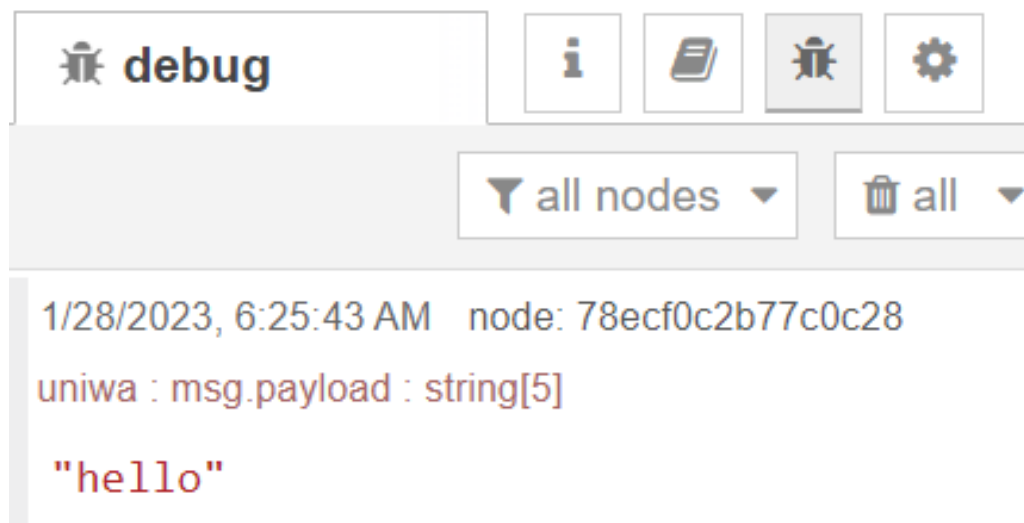
Σε αυτό το σημείο μπορούμε να κάνουμε publish ένα μήνυμα όπως το hello, να δούμε το SIM7000E στον EMQX broker και να λάβουμε το μήνυμα από την Node-Red μέσω της κρυπτογραφημένης SSL/TLS θύρας.

```
AT+SMCONF="CLIENTID", "UNIWASIM7000"  
OK  
AT+SMCONF="URL",195.251.95.14,8883  
OK  
AT+SMCONF="KEEPTIME", 60  
OK  
AT+CSSLCFG=convert, 2, ca.pem  
OK  
AT+CSSLCFG=convert, 1, client.pem, client.key  
OK  
AT+SMSSL=1, ca.pem, client.pem  
OK  
AT+SMCONN  
OK  
AT+SMPUB="uniwa", "5", 1, 1  
> hello  
OK
```

**Εικόνα 63: Εντολές MQTT στον Serial monitor και δημοσίευση του μηνύματος «hello».**

Client ID	Username	Status	IP Address	Keepalive	Connected At	Actions
Node-RED_Uniwa		Connected	90.53323	60	2023-01-28 06:20:29	Kick Out
UNIWASIM7000		Connected	.137:3433	60	2023-01-28 06:20:15	Kick Out

Εικόνα 64: Εμφάνιση της Node-RED και του SIM7000 στον broker.



Εικόνα 65: Το μήνυμα που έφθασε στον subscriber της Node-RED

Έχουμε πλέον μία ολοκληρωμένη και κρυπτογραφημένη MQTT επικοινωνία στο δίκτυο NB-IoT, ωστόσο τα μηνύματα τα οποία δημοσιεύουμε εισέρχονται μόνο μέσω του Serial Monitor και τα μηνύματα αυτά δεν αντιπροσωπεύουν μετρήσεις αισθητηρίων. Ένα αυτοματοποιημένο σύστημα θα υλοποιηθεί στο επόμενο κεφάλαιο.

### 3.6. Αυτοματοποιημένος MQTT SSL κόμβος

Σε αυτό το κεφάλαιο θα αυτοματοποιήσουμε το σύστημα το οποίο περιγράψαμε παραπάνω ώστε να επικοινωνεί μετρήσεις αισθητηρίων και να παρακολουθούμε τις μετρήσεις αυτές από ένα interface της Node-RED.

Για να το πραγματοποιήσουμε αυτό, θα ενσωματώσουμε στο SIM700E το αισθητήριο DHT11 το οποίο είναι δυνατόν να αναγνωρίζει μετρήσεις υγρασίας και θερμοκρασίας. Για να δούμε τις μετρήσεις από αυτό το αισθητήριο στο Arduino χρησιμοποιούμε την βιβλιοθήκη «DHT.h» η οποία δίνει την δυνατότητα να διαβάζουμε θερμοκρασίες είτε από αισθητήρια DHT11, DHT22 ή DHT21. Εφόσον συνδέσουμε στο αισθητήριο στην τροφοδοσία του Arduino καθώς και στην θύρα «D2», χρησιμοποιούμε τον κώδικα της βιβλιοθήκης και μπορούμε να πάρουμε τα πρώτα αποτελέσματα για τις μετρήσεις μας από τον Serial Monitor. Στην παρακάτω εικόνα 66 φαίνονται τα στοιχεία και οι μετρήσεις του αισθητηρίου DHT11, τα στοιχεία του καθώς και κομμάτι του κώδικα ο οποίος χρησιμοποιήθηκε.

```

DHT_Unified_Sensor
// DHT Temperature & Humidity Sensor
// Unified Sensor Library Example
// Written by Tony DiCola for Adafruit Industries
// Released under an MIT license.

// REQUIRES the following Arduino libraries:
// - DHT Sensor Library: https://github.com/adafruit/DHT-sensor-library
// - Adafruit Unified Sensor Lib: https://github.com/adafruit/Adafruit\_Sensor

#include <Adafruit_Sensor.h>
#include <DHT.h>
#include <DHT_U.h>

#define DHTPIN 2 // Digital pin connected to the DHT sensor
// Feather HUZZAH ESP8266 note: use pins 3, 4, 5, 12, 13 or 14 --
// Pin 15 can work but DHT must be disconnected during program upload.

// Uncomment the type of sensor in use:
#define DHTTYPE DHT11 // DHT 11
// #define DHTTYPE DHT22 // DHT 22 (AM2302)
// #define DHTTYPE DHT21 // DHT 21 (AM2301)

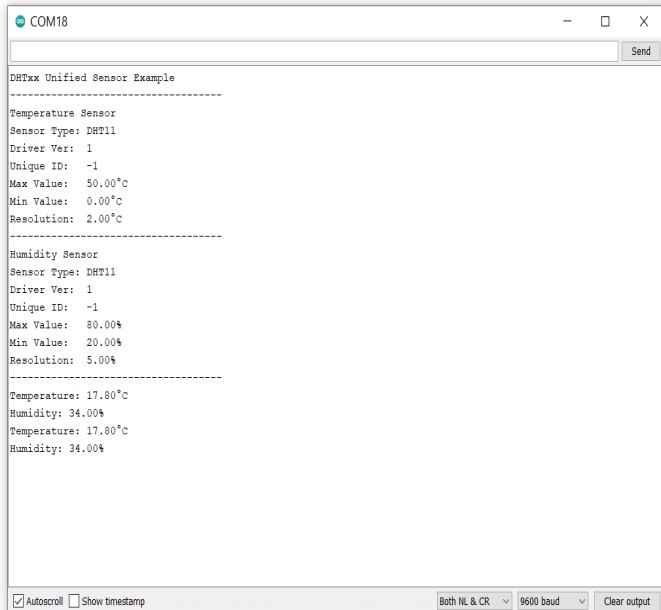
// See guide for details on sensor wiring and usage:
// https://learn.adafruit.com/dht/overview

DHT_Unified dht(DHTPIN, DHTTYPE);

uint32_t delayMS;

void setup() {
  Serial.begin(9600);
  // Initialize device.
  dht.begin();
  Serial.println(F("DHTxx Unified Sensor Example"));
  // Print temperature sensor details.
  sensor_t sensor;
  dht.temperature().getSensor(&sensor);
  Serial.println(F("-----"));
  Serial.println(F("Temperature Sensor"));
  Serial.print (F("Sensor Type: ")); Serial.println(sensor.name);
  Serial.print (F("Driver Ver: ")); Serial.println(sensor.version);
  Serial.print (F("Unique ID: ")); Serial.println(sensor.sensor id);
}

```



**Εικόνα 66: Κώδικας και μετρήσεις DHT11**

Στην συνέχεια θέλουμε αυτές οι μετρήσεις να κοινοποιούνται αυτόματα στα topics του EMQX broker και να φαίνονται στην Node-RED, για να το πραγματοποιήσουμε αυτό θα χρησιμοποιήσουμε την βιβλιοθήκη «ATcommands.h». Μέσω αυτής της βιβλιοθήκης μπορούμε να ορίσουμε τις εντολές AT που θα λαμβάνει το SIM7000E να στέλνονται κατευθείαν από το Arduino με την ενεργοποίησή του χωρίς να χρειαστεί η ενδιάμεση χρήση του Serial Monitor. Έτσι και χρησιμοποιώντας την διαδικασία επανάληψης (loop) της γλώσσας Arduino μπορούμε να στέλνουμε κάθε στιγμή τις διαφορετικές μετρήσεις που διαβάζουμε στα topics τα οποία επιθυμούμε. Έχοντας λοιπόν συνδέσει πρώτα τον κόμβο μας στο δίκτυο NB-IoT της Vodafone, θέτουμε κατά σειρά τις εντολές για να συνδεθεί ο κόμβος με το APN της EMnify και την διεύθυνση του EMQX στο διαδίκτυο για να δίνει η σύνδεση των πιστοποιητικών των οποίων ορίσαμε. Στην συνέχεια αυτό που θα χρειαστεί είναι ορίσουμε την διαδικασία publish του κόμβου να γίνεται με μία διαδικασία loop ανά κάθε λεπτό για να ακολουθεί τις μετρήσεις της θερμοκρασίας καθώς και της υγρασίας. Τέλος για να δείξουμε τις μετρήσεις αυτές στην Node-RED θα χρησιμοποιήσουμε τους κόμβους «gauge» της Node-RED και θα τους παραμετροποιήσουμε για να δείχνουν μετρήσεις από 0 έως 100 για την υγρασία και -50 έως 100 για την θερμοκρασία. Ανατρέχοντας στο dashboard της Node-RED μπορούμε να βλέπουμε τις μετρήσεις της Node-RED γραφικά και σε πραγματικό χρόνο.

```

sendATcommand("AT+CGACT=1", 2000);
sendATcommand("AT+CREG=1", 2000);
sendATcommand("AT+SMCONF=CLIENTID, UNIWA_SIM7000", 2000);
sendATcommand("AT+CGATT=1", 2000);
sendATcommand("AT+CNACT=1,em", 5000);
sendATcommand("AT+SMCONF=URL,195.251.95.14,8883", 2000);
sendATcommand("AT+CSSLCFG=convert,2,ca.pem", 2000);
sendATcommand("AT+CSSLCFG=convert,1,client.pem,client.key", 2000);
sendATcommand("AT+SMSSL=1,ca.pem,client.pem", 2000);
sendATcommand("AT+SMCONN", 5000);
dht.begin();
delay(5000);

```

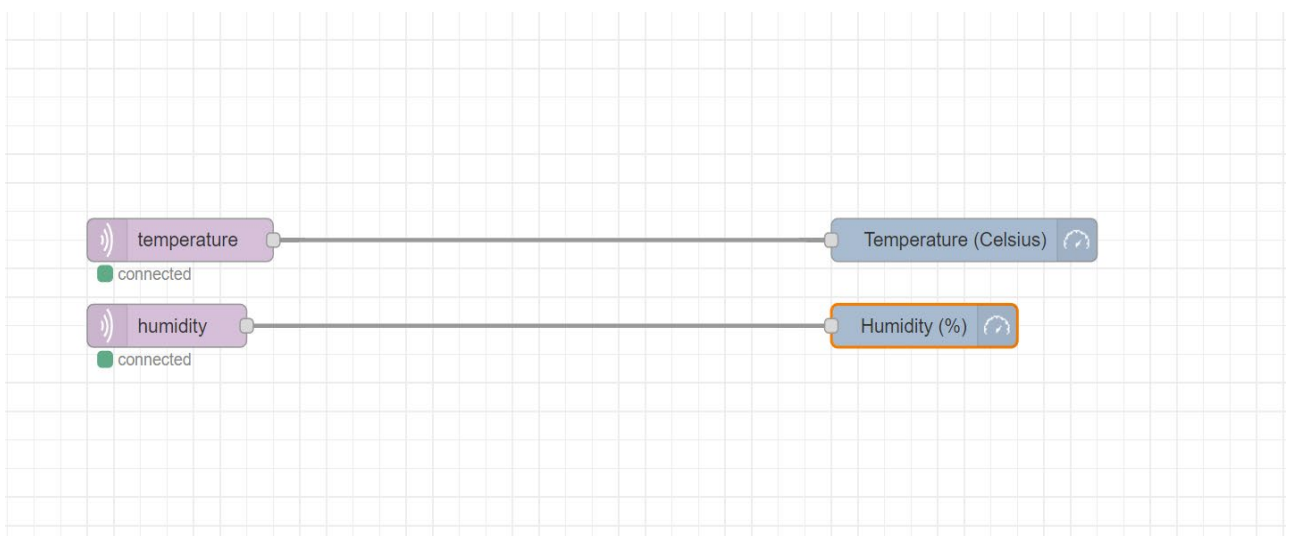
Εικόνα 67: Αυτοματοποιημένες εντολές AT ως μέρος του κώδικα Arduino

```

void loop() {
float temp;
float humi;
sendATcommand("AT+SMPUB=temperature,5,1,1",2000);
sendATcommand1(dht.readTemperature(),2000);
temp = dht.readTemperature();
delay(2000);
sendATcommand("AT+SMPUB=humidity,5,1,1",2000);
sendATcommand1(dht.readHumidity(),2000);
humi = dht.readHumidity();
delay(2000);
delay(60000);
}

```

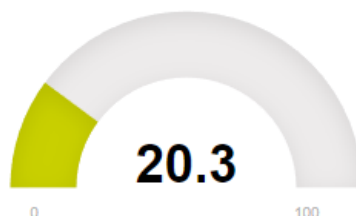
Εικόνα 68: Loop για το publish της θερμοκρασίας και της υγρασίας στα ανάλογα topics.



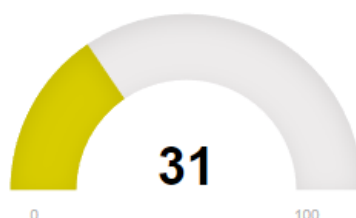
Εικόνα 69: Διάγραμμα Node-RED.

## Environmental Monitoring

Temperature (Celsius)



Humidity (%)



Εικόνα 70: Γραφικές μετρήσεις σε πραγματικό χρόνο.

### 3.7. Βελτιώσεις

Στο επίπεδο αυτό έχουμε υλοποιήσει έναν αυτοματοποιημένο NB-IoT κόμβο, ωστόσο ο κόμβος μας χρειάζεται ακόμα εξωτερική τροφοδοσία και μάλιστα της τάξεως των 9V, κάτι το οποίο δεν συμβαδίζει πλήρως με τα χαρακτηριστικά των LPWAN όπου παρουσιάζουν κόμβους με ελάχιστες απαιτήσεις τροφοδοσίας οι οποίοι είναι δυνατόν να εγκατασταθούν αυτόνομα στον χώρο. Εκτός αυτού, ο κόμβος δεν περιέχει κάποια θήκη προστασίας με ανθεκτικότητα τύπου π.χ. IP67 και δεν μπορούμε να εγγυηθούμε την μακροχρόνια χρήση του σε ένα μη ιδανικό περιβάλλον. Επίσης, το μέγεθος του κόμβου ίσως είναι ακατάλληλο για κάποιες εφαρμογές, π.χ. για την τοποθέτηση του στον σκελετό κάποια ηλεκτρονικής συσκευής.

Βελτιώσεις μπορούν να γίνουν επίσης στον συγχρονισμό του κόμβου σε σχέση με τις PSM και την eDRx λειτουργίες της 3GPP καθώς και τον συγχρονισμό του ή και την επικοινωνία του με άλλους NB-IoT κόμβους μέσω λειτουργιών όπως η λειτουργία D2D και η ανάπτυξη πρωτοκόλλων δρομολόγησης πακέτων. Τέλος, στο πεδίο του server, είναι δυνατόν να υλοποιηθεί βάση δεδομένων η οποία αποθηκεύει τα δεδομένα τα οποία φτάνουν μέσω του κόμβου.

Πραγματοποιήθηκε η μελέτη LPWAN και 5G δικτύων για διαδικασίες έξυπνης πόλης. Μελετήθηκαν οι τεχνολογίες αυτές και αναλύθηκε η χρησιμότητά σε σενάρια έξυπνης πόλης. Αναλύθηκαν οι τεχνολογίες NB-IoT και LoRaWAN και αξιολογήθηκε η χρησιμότητά τους στα εν λόγω σενάρια παρουσιάζοντας το NB-IoT ως την καταλληλότερη τεχνολογία. Μέσω προσομοίωσης δείξαμε ότι σενάρια EWS μέσω NB-IoT και V2V μέσω 5G είναι υλοποιήσιμα, πιθανότατα και άμεσα. Πραγματοποιήθηκε η υλοποίηση ενός χαμηλού κόστους αυτόνομου NB-IoT κόμβου ο οποίος χρησιμοποιεί κρυπτογραφημένη ασφάλεια για να επικοινωνεί δεδομένα σε πραγματικό χρόνο.

Δίκτυα τέτοιου τύπου μπορούν να επηρεάσουν θετικά το επίπεδο ζωής σε μία πόλη αυτοματοποιώντας διαδικασίες οι οποίες σε παλαιότερες εποχές θα χρειαζόντουσαν πολύ χρόνο να επιτευχθούν. Μπορούν να παρέχουν έγκυρη ενημέρωση στους πολίτες και τις αρχές για σενάρια όπως αυτό της έγκυρης προειδοποίησης, εξυπηρετώντας διαδικασίες όπως το έξυπνο parking και η περιβαλλοντική παρακολούθηση. Νέες εφαρμογές όπως το 5G V2V υπόσχονται να βελτιώσουν το κυκλοφοριακό ζήτημα στις οδούς μία πόλης και να εγγυηθούν περαιτέρω ασφάλεια σε αυτές.

Ωστόσο, πρέπει να λάβουμε υπόψιν ότι η ενσωμάτωση τέτοιων δικτύων σε μία πόλη προϋποθέτουν τον χειρισμό τους από μία η και περισσότερες ελεγχόμενες και ηθικές αρχές για να αποφευχθεί η παραποίηση των δεδομένων και η σωστή χρήση και συντήρηση του δικτύου. Ειδικά η ιδέα ότι τα δίκτυα θα ενσωματώνονται μεταξύ τους, περιορίζει τις αρχές που θα τα ελέγχουν και μία αρχή είναι πιο εύκολο να διαφθαρεί. Εκτός αυτού, χρειάζεται ισχυρή ασφάλεια στους κόμβους τόσο σε φυσικό όσο και ψηφιακό επίπεδο για να μην παραβιαστούν ή κλαπούν από επιτήδειους. Χρειάζεται ένα νομικό πλαίσιο το οποίο μπορεί να επιτρέπει ένα δίκτυο αυτόνομων αυτοκινήτων και να ορίζει τις ευθύνες για την μη βέλτιστη χρήση του. Τέλος, πρέπει να υπάρξουν ιατρικές μελέτες που εγγυόνται ότι η καθημερινή αλληλεπίδραση των πολιτών με τόσα ραδιοηλεκτρικά κύματα δεν δημιουργεί σημαντική επιρροή στην υγεία.

- [1] Naik, N. (2018). LPWAN Technologies for IoT Systems: Choice Between Ultra Narrow Band and Spread Spectrum. *2018 IEEE International Systems Engineering Symposium (ISSE)*. doi:10.1109/syseng.2018.8544414
- [2] U. Raza and P. Kulkarni, "Low Power Wide Area Networks: An Overview", Ieeexplore.ieee.org, 2017. [Online]. Available: <https://ieeexplore.ieee.org/document/7815384>
- [3] Gohar, A., & Nencioni, G. (2021). The Role of 5G Technologies in a Smart City: The Case for Intelligent Transportation System. *Sustainability*, 13(9), 5188. doi: 10.3390/su13095188 Logitech C920 USB Web Camera, [https://support.logitech.com/en\\_us/product/hd-pro-webcam-c920/specs](https://support.logitech.com/en_us/product/hd-pro-webcam-c920/specs)
- [4] Guevara, L., & Cheein, F. A. (2020). The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems. *Sustainability*, 12(16), 6469. doi:10.3390/su12166469
- [5] Akyildiz, I., Nie, S., Lin, S., & Chandrasekaran, M. (2016). 5G roadmap: 10 key enabling technologies. *Computer Networks*, 106, 17-48. doi: 10.1016/j.comnet.2016.06.010 RealTerm, <https://sourceforge.net/projects/realterm/>
- [6] Nadeem, L., Azam, M., Amin, Y., Al-Ghamdi, M., Chai, K., Khan, M., & Khan, M. (2021). Integration of D2D, Network Slicing, and MEC in 5G Cellular Networks: Survey and Challenges. *IEEE Access*, 9, 37590-37612. doi: 10.1109/access.2021.3063104 SSD, <https://arxiv.org/abs/1512.023255>
- [7] Internet of Things and Wireless Sensor Network for Smart Cities. (2017). *International Journal Of Computer Science Issues*, 14(5), 50-55. doi: 10.20943/01201705.5055
- [8] M. Ballerini, T. Polonelli, D. Brunelli, M. Magno and L. Benini, "NB-IoT Versus LoRaWAN: An Experimental Evaluation for Industrial Applications," in IEEE Transactions on Industrial Informatics, vol. 16, no. 12, pp. 7802-7811, Dec. 2020, doi: 10.1109/TII.2020.2987423.
- [9] Alper Yegin, Thorsten Kramp, Pierre Dufour, Rohit Gupta, Ramez Soss, Olivier Hersent, Derek Hunt, Nicolas Sornin, 3 - LoRaWAN protocol: specifications, security, and capabilities, LPWAN Technologies for IoT and M2M Applications, Academic Press, 2020, Pages 37-63, ISBN 9780128188804
- [10] A. Lavric and V. Popa, "Internet of Things and LoRa™ Low-Power Wide-Area Networks: A survey," 2017 International Symposium on Signals, Circuits and Systems



(ISSCS), Iasi, 2017, pp. 1-5, doi: 10.1109/ISSCS.2017.8034915.TensorFlow,  
<https://www.tensorflow.org/>

- [11] de Farias Medeiros, D., Villarim, M. R., de Carvalho, F. B. S., & de Souza, C. P. (2020, November 4). Implementation and Analysis of Routing Protocols for LoRa Wireless Mesh Networks. 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON).  
<https://doi.org/10.1109/iemcon51383.2020.9284888>
- [12] Jiang, X., Zhang, H., Barsallo Yi, E. A., Raghunathan, N., Mousoulis, C., Chaterji, S., Peroulis, D., Shakouri, A., & Bagchi, S. (2021). Hybrid Low-Power Wide-Area Mesh Network for IoT Applications. IEEE Internet of Things Journal, 8(2), 901–915.  
<https://doi.org/10.1109/jiot.2020.3009228>
- [13] Lee, H.-C., & Ke, K.-H. (2018). Monitoring of Large-Area IoT Sensors Using a LoRa Wireless Mesh Network System: Design and Evaluation. IEEE Transactions on Instrumentation and Measurement, 67(9), 2177–2187.  
<https://doi.org/10.1109/tim.2018.2814082>
- [14] López Escobar, J. J. L., Gil-Castiñeira, F., & Díaz Redondo, R. P. D. (2020). JMAC Protocol: A Cross-Layer Multi-Hop Protocol for LoRa. Sensors, 20(23), 6893.  
<https://doi.org/10.3390/s20236893>
- [15] Janssen, T., BniLam, N., Aernouts, M., Berkvens, R., & Weyn, M. (2020). LoRa 2.4 GHz Communication Link and Range. Sensors, 20(16), 4366.  
<https://doi.org/10.3390/s20164366> Git, <https://git-scm.com/>
- [16] Mwakwata, C. B., Malik, H., Mahtab Alam, M., Le Moullec, Y., Parand, S., & Mumtaz, S. (2019). Narrowband Internet of Things (NB-IoT): From Physical (PHY) and Media Access Control (MAC) Layers Perspectives. Sensors, 19(11), 2613.  
<https://doi.org/10.3390/s19112613>
- [17] Díaz Zayas, A., Rivas Tocado, F. J., & Rodríguez, P. (2020). Evolution and Testing of NB-IoT Solutions. Applied Sciences, 10(21), 7903.  
<https://doi.org/10.3390/app10217903>
- [18] Sun, R., Talarico, S., Chang, W., Niu, H., & Yang, H. (2019, September). Enabling NB-IoT on Unlicensed Spectrum. 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). <https://doi.org/10.1109/pimrc.2019.8904126>
- [19] Wu, F., Zhang, H., Di, B., Wu, J., & Song, L. (2019, May). Network Controlled D2D Communications: Licensed or Unlicensed Spectrum? ICC 2019 - 2019 IEEE International Conference on Communications (ICC). ICC 2019 - 2019 IEEE International Conference on Communications (ICC).  
<https://doi.org/10.1109/icc.2019.8761477A>.

- [20] Nauman, A., Jamshed, M. A., Ahmad, Y., Ali, R., Zikria, Y. B., & Won Kim, S. (2019, June). An Intelligent Deterministic D2D Communication in Narrow-band Internet of Things. 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC).  
<https://doi.org/10.1109/iwcmc.2019.8766786>
- [21] Althobaiti, O. S., & Dohler, M. (2021). Narrowband-Internet of Things Device-to-Device Simulation: An Open-Sourced Framework. *Sensors*, 21(5), 1824.  
<https://doi.org/10.3390/s21051824>
- [22] O. Liberg et al., "Narrowband Internet of Things 5G Performance," 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 2019, pp. 1-5, doi: 10.1109/VTCFall.2019.8891588.
- [23] S. A. Gbadamosi, G. P. Hancke and A. M. Abu-Mahfouz, "Building Upon NB-IoT Networks: A Roadmap Towards 5G New Radio Networks," in *IEEE Access*, vol. 8, pp. 188641-188672, 2020, doi: 10.1109/ACCESS.2020.3030653.
- [24] Bao, L., Wei, L., Jiang, C., Miao, W., Guo, B., & Li, W. et al. (2018). Coverage Analysis on NB-IoT and LoRa in Power Wireless Private Network. *Procedia Computer Science*, 131, 1032-1038. doi: 10.1016/j.procs.2018.04.252
- [25] S. Persia, C. Carciofi and M. Faccioli, "NB-IoT and LoRA connectivity analysis for M2M/IoT smart grids applications," 2017 AEIT International Annual Conference, Cagliari, 2017, pp. 1-6, doi: 10.23919/AEIT.2017.8240558.
- [26] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue and J. Pr'évotet, "Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp.
- [27] H. Mroue, A. Nasser, S. Hamrioui, B. Parrein, E. Motta-Cruz and G. Rouyer, "MAC layer-based evaluation of IoT technologies: LoRa, SigFox and NB-IoT," 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, 2018, pp. 1-5, doi: 10.1109/MENACOMM.2018.8371016.
- [28] Yocam, E. (2020, October 20). Narrow-band Internet of Things Protocol Standards: Survey of Security and Privacy Control Effectiveness. 2020 International Symposium on Networks, Computers and Communications (ISNCC). 2020 International Symposium on Networks, Computers and Communications (ISNCC).  
<https://doi.org/10.1109/isncc49221.2020.9297222>
- [29] F. L. Coman, K. M. Malarski, M. N. Petersen and S. Ruepp, "Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT," 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766430.

- [30] Overview of IOT Networks - IOT Factory. (2021). Retrieved 14 July 2021, from <https://iotfactory.eu/iot-knowledge-center/overview-of-iot-networks/>
- [31] Evolution of Mobile generation from 1G to 6G – 5G Technology with Matlab. (2021). Retrieved 14 July 2021, from <https://5glearning.org/evolution-of-mobile-generation-from-1g-to-6g/>
- [32] Information and Communications Technology – ICT – Pro Lens Projects L.L.C. (2021). Retrieved 14 July 2021, from <http://prolensprojects.com/services/information-and-communications-technology-ict/>
- [33] Yu, G., Liu, S., & Shangguan, Q. (2021). Optimization and Evaluation of Platooning Car-Following Models in a Connected Vehicle Environment. *Sustainability*, 13(6), 3474. doi: 10.3390/su13063474
- [34] A Primer for LoRa/LoRaWAN. (2021). Retrieved 14 July 2021, from <https://www.leverage.com/blogpost/a-primer-for-loralorawan>
- [35] Cotrim, J., & Kleinschmidt, J. (2020). LoRaWAN Mesh Networks: A Review and Classification of Multihop Communication. *Sensors*, 20(15), 4273. doi: 10.3390/s20154273
- [36] NB-IoT: a sustainable technology for connecting billions of devices - Ericsson Technology Review. (2021). Telefonaktiebolaget LM Ericsson. Retrieved 14 July 2021, from <https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/nb-iot-a-sustainable-technology-for-connecting-billions-of-devices>
- [37] Sinha, R., Wei, Y., & Hwang, S. (2017). A survey on LPWA technology: LoRa and NB-IoT. *ICT Express*, 3(1), 14-21. doi: 10.1016/j.icte.2017.03.004
- [38] [https://www.cadence.com/ko\\_KR/home/tools/system-analysis/rf-microwave-design/awr-design-environment-platform.html](https://www.cadence.com/ko_KR/home/tools/system-analysis/rf-microwave-design/awr-design-environment-platform.html)
- [39] Awr.com. 2021. Simulation Test Bench for NB-IoT Products | AWR Software. <https://www.awr.com/resource-library/simulation-test-bench-nb-iot-products> (Accessed 21 May 2021)
- [40] Nardini, G., Sabella, D., Stea, G., Thakkar, P. and Viridis, A., 2020. Simu5G–An OMNeT++ Library for End-to-End Performance Evaluation of 5G Networks. *IEEE Access*, 8, pp.181176-181191.
- [41] P. A. Lopez et al., "Microscopic Traffic Simulation using SUMO," 2018 21st International Conference on Intelligent Transportation Systems (ITSC), 2018, pp. 2575-2582, doi: 10.1109/ITSC.2018.8569938.
- [42] Mészáros, L., Varga, A. and Kirsche, M., 2019. INET Framework. *Recent Advances in Network Simulation*, pp.55-106.
- [43] Viridis, A., Nardini, G. and Stea, G., 2019. Cellular-Networks Simulation Using SimuLTE. *Recent Advances in Network Simulation*, pp.183-214.

- [44] Nardini, G., Stea, G., Viridis, A. and Sabella, D., 2020. Simu5G: A System-level Simulator for 5G Networks. *Proceedings of the 10th International Conference on Simulation and Modeling Methodologies, Technologies and Applications*.
- [45] G. Nardini, G. Stea, A. Viridis, D. Sabella and P. Thakkar, "Using Simu5G as a Realtime Network Emulator to Test MEC Apps in an End-To-End 5G Testbed," *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, 2020, pp. 1-7, doi: 10.1109/PIMRC48278.2020.9217177.
- [46] Google Earth. 2021. Overview – Google Earth.  
<https://earth.google.com>  
 (Accessed 21 May 2021)
- [47] Meraj Alam (2018); AT Commands; Int J Sci Res Publ 5(5) (ISSN: 2250-3153).  
<http://www.ijsrp.org/research-paper-0515.php?rp=P414086>
- [48] Bender, M. *et al.* (2021) "Open-source MQTT evaluation," *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)* [Preprint]. Available at: <https://doi.org/10.1109/ccnc49032.2021.9369499>.
- [49] Emqx (no date) Emqx/emqx: The most scalable open-source MQTT Broker for IOT, IIoT, and connected vehicles, GitHub. Available at: <https://github.com/emqx/emqx> (Accessed: December 26, 2022).
- [50] (no date) *DFRobot SIM7000\_Arduino\_NB-IoT\_LTE\_GPRS\_Expansion\_Shield\_SKU\_\_DFR0505\_DFR0572*. Available at: [https://wiki.dfrobot.com/SIM7000\\_Arduino\\_NB-IoT\\_LTE\\_GPRS\\_Expansion\\_Shield\\_SKU\\_\\_DFR0505\\_DFR0572](https://wiki.dfrobot.com/SIM7000_Arduino_NB-IoT_LTE_GPRS_Expansion_Shield_SKU__DFR0505_DFR0572) (Accessed: January 2, 2023).
- [51] Rasyad, R.M., Murti, M.A. and Rizki, A.P. (2019) "Design and realization of node MCU module based on Nb-IOT for general Iot Purpose," *2019 IEEE International Conference on Internet of Things and Intelligence System (IoT&IS)* [Preprint]. Available at: <https://doi.org/10.1109/iotais47347.2019.8980450>.
- [52] Khalil-Hani, M., Nambiar, V.P. and Marsono, M.N. (2010) "Hardware acceleration of openssl cryptographic functions for high-performance internet security," *2010 International Conference on Intelligent Systems, Modelling and Simulation* [Preprint]. Available at: <https://doi.org/10.1109/isms.2010.89>.
- [53] *IOT connectivity platform* (no date) *emnify*. Available at: <https://www.emnify.com/> (Accessed: January 8, 2023).
- [54] *QPST tool* (no date) *QPST Tool*. Available at: <https://qpsttool.com/> (Accessed: January 23, 2023).
- [55] Spragins, J. (1996) "TCP/IP illustrated, volume 3: TCP for transactions, HTTP, NNTP and the Unix Domain Protocols," *IEEE Network*, 10(5), p. 5. Available at: <https://doi.org/10.1109/mnet.1996.539855>.

- [56] C. Lesjak *et al.*, "Securing smart maintenance services: Hardware-security and TLS for MQTT," *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, Cambridge, 2015, pp. 1243-1250.
- [57] Bharati Wukkadada; Kirti Wankhede; Ramith Nambiar; Amala Nair, Comparison with HTTP and MQTT In Internet of Things (IoT) ,IEEE, International Conference on Inventive Research in Computing Applications (ICIRCA), 2018, ISBN:978-1-5386-2456-2, p.p 1-4.
- [58] Mishra, B. and Kertesz, A. (2020) "The use of MQTT in M2M and IOT Systems: A survey," *IEEE Access*, 8, pp. 201071–201086. Available at: <https://doi.org/10.1109/access.2020.3035849>.
- [59] Sasaki, Y., Yokotani, T. and Mukai, H. (2018) "Comparison with assured transfer of information mechanisms in Mqtt," *2018 International Japan-Africa Conference on Electronics, Communications and Computations (JAC-ECC)* [Preprint]. Available at: <https://doi.org/10.1109/jec-ecc.2018.8679550>.
- [60] M. Fezari and A. Al Dahoud, "Integrated Development Environment "IDE," 2018, pp. 1–12.
- [61] M. Lekić and G. Gardašević, "IoT sensor integration to Node-RED platform," *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo, 2018, pp. 1-5