



UNIVERSITY OF  
PATRAS  
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ  
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ  
ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΜΣ «ΕΠΙΣΤΗΜΗ & ΤΕΧΝΟΛΟΓΙΑ ΥΠΟΛΟΓΙΣΤΩΝ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εφαρμογές των Τεχνολογιών SDN και NFV σε Κινητά Δίκτυα  
Επικοινωνιών

Της φοιτήτριας: Αναστασίας Α. Κόλλια

Υπεύθυνος καθηγητής: Καθ. Χρήστος Ι. Μπούρας

Τριμελής Επιτροπή: Καθ. Χρήστος Ι. Μπούρας

Καθ. Ιωάννης Γαροφαλάκης

Καθ. Κωνσταντίνος Μπερμπερίδης

Πάτρα, Οκτώβριος 2017

**Πανεπιστήμιο Πατρών, Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών και  
Πληροφορικής**

**Αναστασία Α. Κόλλια**

**© 2017- Με την επιφύλαξη παντός δικαιώματος.**

## Πρόλογος

Αρχικά, βιώθω την ανάγκη να ευχαριστήσω τον υπεύθυνο καθηγητή της διπλωματικής και καθηγητή του Τμήματος Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής της Πολυτεχνικής σχολής του Πανεπιστημίου Πατρών κ. Χρήστο Ι. Μπούρα, για τις θεμελιώδους σημασίας συμβουλές του και την καθοδήγηση, που μου παρείχε σε ολόκληρο το διάστημα εκπόνησης της μεταπτυχιακής διπλωματικής εργασίας, καθώς, επίσης, για τις γνώσεις, που μου μετέδωσε στην επταετή συνολική μου πορεία στο τμήμα Μηχανικών Η/Υ και Πληροφορικής ως προπτυχιακή και μεταπτυχιακή φοιτήτρια, για την ευκαιρία, που μου έδωσε να ασχοληθώ με ένα πραγματικά ενδιαφέρον ζήτημα, αλλά και για τη γενικότερη άψογη συνεργασία. Θα ήθελα να ευχαριστήσω ακόμα και τα υπόλοιπα μέλη της Ερευνητικής Μονάδας 6 για την εύρυθμη συνεργασία, που είχαμε όλα αυτά τα χρόνια.

Ακόμα, επιθυμώ να ευχαριστήσω ιδιαίτερα τα λοιπά μέλη της τριμελούς επιτροπής κρίσης της διπλωματικής μου, δηλαδή τον καθηγητή κ. Γαροφαλάκη και τον καθηγητή κ. Μπερμπερίδη. Οι δύο πιο πάνω διδάσκοντες μου έμαθαν πολλά πράγματα κατά τη διάρκεια της πορείας μου στο τμήμα Μηχανικών Η/Υ και Πληροφορικής, αφού ανελλιπώς παρακολούθησα μαθήματά τους και εν συνεχεία, με υποστήριζαν ιδιαίτερα με τη συμμετοχή τους στην επιτροπή κρίσης της μεταπτυχιακής μου εργασίας για την απονομή του Μεταπτυχιακού Διπλώματος Ειδίκευσης «Επιστήμη και Τεχνολογία Υπολογιστών».

Επιπλέον, ευχαριστώ τον επίκουρο καθηγητή κ. Μακρή, τους αναπληρωτές καθηγητές κ. Χατζηλυγερούδη και κ. Χρηστίδη στους οποίους πραγματοποίησα επικουρικό έργο και συνεργαστήκαμε άψογα κατά τη διάρκεια των μεταπτυχιακών σπουδών. Δεν είναι δυνατό να ξεχάσω τους διδάσκοντες στο τμήμα Μηχανικών Η/Υ και Πληροφορικής, που με ιδιαίτερο ζήλο κατάφεραν να μεταλαμπαδεύσουν πλήθος από τις γνώσεις τους και μεταδώσουν την αγάπη τους για τον τομέα των υπολογιστών σε πολλές γενιές μηχανικών, αλλά και σε εμένα προσωπικά. Τελευταίο, αλλά όχι λιγότερο σημαντικό θα ήθελα να ευχαριστήσω την οικογένεια μου, που με υποστήριζαν ηθικά, πνευματικά, ψυχολογικά και οικονομικά να ολοκληρώσω αυτές τις σπουδές.

*Πάτρα, Οκτώβριος 2017*

*Αναστασία Α. Κόλλια*

## Περίληψη

Στα πλαίσια της εν λόγω διπλωματικής εισάγονται οι βασικές εξελίξεις στον τομέα των δικτύων και ιδίως των κινητών δικτύων επικοινωνίας. Εγείρονται σημαντικά ερωτήματα ως προς ποια είναι η απάντηση στις μεγάλες απαιτήσεις της νέας γενιάς κινητής τηλεπικοινωνίας. Στο Κεφάλαιο 1 εισάγονται τα πιο σημαντικά δεδομένα στον τομέα των κινητών επικοινωνιών, καθώς και τα βασικά ερωτήματα, στα οποία καλείται να δώσει απαντήσεις η παρούσα μεταπτυχιακή διπλωματική εργασία.

Εν συνεχεία, στο Κεφάλαιο 2 εισάγεται η σχετική βιβλιογραφία. Στο κεφάλαιο αυτό περιλαμβάνεται μία επισκόπηση της υπάρχουσας βιβλιογραφίας και επίσης, παρουσιάζονται τα βασικότερα στοιχεία των αναφερόμενων τεχνολογιών Software Defined Networks (SDN) σε κινητά δίκτυα επικοινωνίας, καθώς και της τεχνολογίας Network Function Virtualization (NFV), δηλαδή της εισαγωγής λογισμικού έναντι υλικού για την αντικατάσταση στοιχειωδών δικτυακών λειτουργιών. Παράλληλα καλύπτονται θέματα σχετικά με το SDN σε σταθερά, ενσύρματα, ασύρματα, αδόμητα δίκτυα, καθώς και άλλες σημαντικές πτυχές, όπως το κόστος και η ασφάλεια στα δίκτυα εισάγοντας την καινοτομία.

Στο Κεφάλαιο 3 αναλύεται το θεωρητικό υπόβαθρο, που σχετίζεται άμεσα με το SDN και το NFV. Αναλύονται διεξοδικά οι τεχνολογίες σχετικά με το SDN, το NFV, το Open Network Operating System (ONOS), το Central Office Re-imagined as a Data Center (CORD) και το OpenStack, διότι θεωρούνται τα πιο σημαντικά θεωρητικά στοιχεία σε ότι αναφορά στον τομέα με τον οποίο ασχολείται η παρούσα εργασία. Υπάρχει μία αναλυτική συγκριτική μελέτη της συσχέτισης των δύο τεχνολογιών, καθώς και μία αποτίμηση για το παρόν και το μέλλον τους στις γενιές κινητών τηλεπικοινωνιών.

Η μεθοδολογία των πειραμάτων, που διεξάγονται στη διπλωματική αναλύονται στο Κεφάλαιο 4. Εκεί εξηγούνται το ONOS, καθώς και το Mobile Central Office Re-imagined as a Data Center (MCORD). Εδώ αναλύονται βασικά ζητήματα σε ότι αναφορά στην αρχιτεκτονική του ONOS, ποια είναι η παρούσα κατάσταση σχετικά με την πρόοδο, που έχει σημειωθεί στον τομέα. Αναλύεται ακόμα και η περίπτωση του MCORD και διαφαίνεται ποιες είναι οι κατευθυντήριες οδοί προς αυτή την κατεύθυνση. Επεξηγούνται ακόμα οι σημαντικότερες περιπτώσεις μελέτης, που επιλέχθηκαν, δηλαδή αναλύονται διεξοδικά οι τοπολογίες, οι οποίες θα τοποθετηθούν στον ONOS με βασικό στόχο την εξομοίωση και την πειραματική μελέτη. Εκεί αναλύονται στοιχεία σχετικά με τις επιλογές, που έχουν γίνει για τους σταθμούς βάσης, τα τερματικά, το δίκτυο κλπ. Επίσης, αναλύεται ο POX, που είναι ένας

άλλος βασικός ελεγκτής δικτύου SDN και χρησιμοποιείται για τη σύγκριση με τον ONOS. Τέλος, αναλύεται η διαφοροποίηση, που έχει συντελεστεί σε παραδοσιακές αρχιτεκτονικές με τη χρήση των τεχνολογιών αυτών.

Εν συνεχεία, στο Κεφάλαιο 5, αναλύονται τα βασικά πειράματα, τα οποία πραγματοποιούνται, καθώς και τα αποτελέσματα των σημαντικότερων θεμάτων. Στο σημείο αυτό παρουσιάζονται και σχολιάζονται τα κύρια αποτελέσματα, που προκύπτουν από την πειραματική διαδικασία. Στο παράρτημα υπάρχει ο κώδικας, που χρησιμοποιείται με βασικό στόχο τη διεξαγωγή των πειραμάτων.

Τέλος, σημειώνονται τα πιο σημαντικά αποτελέσματα, τα οποία εξάγονται από την πειραματική διαδικασία, πως αυτά είναι δυνατό να συμβάλουν στο μέλλον της τεχνολογίας και αναλύονται στο Κεφάλαιο 6 καθώς και μελλοντικές κατευθύνσεις, που είναι δυνατό να συμβάλουν στη μελλοντική έρευνα στον τομέα κινητών δικτύων επικοινωνίας, που περιγράφονται στο Κεφάλαιο 7.

*Λέξεις κλειδιά:* 5G, κινητά δίκτυα, MCORD, ONOS, CORD, SDN, NFV, τοπολογίες κινητών δικτύων επικοινωνίας, cloud computing, virtualization, ασύρματα δίκτυα.

## Executive Summary

The demands raised by the next generation of mobile networks are a very controversial issue. In the first chapter, the most important issues concerning 5G are raised. What is more, there is an analysis of the basic questions that will be answered by this thesis in Chapter 1.

In Chapter 2 there is a thorough literature investigation and there is also a presentation of the Software Defined Networks (SDN) of the mobile networks and Network Functions Virtualization (NFV), namely the introduction of software into hardware for replacing hardware with programmable networking functionality. There is also an analysis on matters concerning SDN adaptations in wired, wireless, mobile and adhoc networks. There is also an investigation on the impact SDN and NFV have on other important domains concerning the networking namely the cost reduction and the safety or the better resource allocation.

In Chapter 3 there is an analysis of the theoretical background that is related to the SDN and NFV. The Open Network Operating System (ONOS), the Central Office Re-imagined as a Data Center (CORD) and the OpenStack are thoroughly analyzed and investigated. There is also an analytical comparative review of the combination of the two technologies and the NFV. There's a combinational review of the two technologies and an analysis of the future and present of the two technologies in the mobile networking.

The experimental methodology is explained in Chapter 4. There is an explanation of the Open Network Operating System (ONOS), and the Mobile Central Office Re-imagined as a Data Center (MCORD). Furthermore, there is a presentation of the most important matters and use cases. There are also analyses for the basic experiments realized and the most important results. In the Appendix, there is the code, representing the network topology used for experimentation. POX is also analyzed as it is a very useful SDN controller, which is compared with the ONOS, especially when it comes to educational procedures.

In Chapter 5 there is an analysis of the main results coming from experimenting. Firstly, the results are presented and secondly, they are analyzed. In Chapter 6 the main conclusions are presented and in Chapter 7 there is a presentation of the future activity in the domain for the next years and several suggestions that could be investigated when it comes to SDN, NFV or mobile networking are summarized.

**Keywords:** *5G, mobile networks, MCORD, ONOS, CORD, SDN, NFV, mobile network topologies, cloud computing, virtualization, wireless networks.*

**Δημοσιεύσεις:**

1. Bouras, C., Kokkinos, V., Kollia, A., & Papazois, A. (2015, August). Techno-economic analysis of ultra-dense and DAS deployments in mobile 5G. In *Wireless Communication Systems (ISWCS), 2015 International Symposium on* (pp. 241-245). IEEE. [92]

2. Bouras, C., Kollia, A., & Papazois, A. (2017). Dense Deployments and DAS in 5G: A Techno-Economic Comparison. *Wireless Personal Communications*, 94(3), 1777-1797. [93]
3. Bouras, C., Kollia, A., & Papazois, A. (2016, April). Sensitivity analysis of small cells and DAS techno-economic models in mobile 5G. In *Wireless Communications and Networking Conference (WCNC), 2016 IEEE* (pp. 1-6). IEEE. [94]
4. Bouras, C., Kollia, A., & Papazois, A. (2017). Analyzing Small - cells and Distributed Antenna Systems from Techno - economic Perspective. Retrieved October 2, 2017, from *International Journal of Wireless Networks and Broadband Technologies (IJWNBT)*. [95]
5. Bouras, C., Kollia, A., & Papazois, A. (2017, March). SDN & NFV in 5G: Advancements and challenges. In *Innovations in Clouds, Internet and Networks (ICIN), 2017 20th Conference on* (pp. 107-111). IEEE. [97]
6. Bouras, C., Kollia, A., & Papazois, A. (2017, July). Teaching network security in mobile 5G using ONOS SDN controller. In *Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on* (pp. 465-470). IEEE. [98]
7. Bouras, C., Kollia, A., & Papazois, A. (2017, July). Teaching 5G networks using the ONOS SDN controller. In *Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on* (pp. 312-317). IEEE. [99]
8. Bouras, C., Kollia, A., & Papazois, A. (pending). Exploring SDN & NFV in 5G Using ONOS & POX Controllers. *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)*. [100]

## Περιεχόμενα

Πρόλογος .....	3
Περίληψη .....	4
Executive Summary .....	5
Κατάλογος Σχημάτων & Εικόνων .....	10
Λίστα Πινάκων .....	11
Ακρωνύμια .....	12
1. ΕΙΣΑΓΩΓΗ .....	16
1.1 Συνεισφορά Διπλωματικής .....	17
1.2 Διάρθρωση κεφαλαίων .....	18
1.3 Κινητά Δίκτυα Επικοινωνίας Πέμπτης Γενιάς.....	19
2. ΣΧΕΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ .....	22
2.1 Κινητά Δίκτυα Επικοινωνιών .....	22
2.2 Network Function Virtualization (NFV).....	23
2.3 Software Defined Networking (SDN) σε ενσύρματα δίκτυα.....	23
2.4 Ασφάλεια και κόστος στο Software Defined Networking (SDN) .....	24
2.5 Software Defined Networking (SDN) σε κινητά δίκτυα .....	25
3. ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ .....	27
3.1 Software Defined Networking (SDN).....	27
3.1.1 Πλεονεκτήματα των αρχιτεκτονικών του SDN .....	30
3.1.2 Απαιτήσεις και προκλήσεις σχετικά με το SDN .....	31
3.1.3 Ιστορική επισκόπηση του SDN .....	32
3.2 Network Functions Virtualization (NFV) .....	34
3.2.1 Πλεονεκτήματα του NFV .....	35
3.2.2 Απαιτήσεις και προκλήσεις σχετικά με το NFV .....	36
3.2.3 Ιστορική επισκόπηση του NFV .....	37
3.3 Radio Access Network (RAN).....	37
3.4 Central Office Re-Architected as a Data Center (CORD) .....	40
3.5 OpenStack.....	42
3.6 Ασφάλεια στα δίκτυα SDN.....	44
3.6.1 Προκλήσεις ασφαλείας στα δίκτυα SDN.....	45
3.6.2 Προτεινόμενες Λύσεις για την ασφάλεια στα δίκτυα SDN .....	47
3.7 Σύγκριση- Αποτίμηση Τεχνολογιών.....	51
4. ΜΕΘΟΔΟΛΟΓΙΑ ΠΕΙΡΑΜΑΤΩΝ.....	52
4.1 Mininet.....	53



4.2 Open Network Operating System (ONOS).....	54
4.2.1 Virtual Router (vRouter).....	56
4.2.2 Internet Protocol Radio Access Network (IPRAN) .....	59
4.2.3 Mobile Central Office Re-Imagined as a Data Center (MCORD).....	62
4.2.4 Ασφάλεια στα κινητά δίκτυα 5G με χρήση SDN .....	63
4.2.5 Σύγκριση SDN ελεγκτών (ONOS, POX) για εφαρμογές στην εκπαίδευση .....	67
4.2.6 Τροποποίηση Αρχιτεκτονικής τύπου DAS με χρήση τεχνικών NFV.....	68
4.3 Επεξήγηση Εντολών Τοπολογιών & Εξομοιωτή Δικτύου.....	73
5.ΑΠΟΤΕΛΕΣΜΑΤΑ.....	76
5.1 Virtual Router (vRouter).....	77
5.2 Internet Protocol Radio Access Network (IPRAN) .....	80
5.3 Mobile Central Office Re-Imagined as a Data Center (MCORD).....	85
5.4 Ασφάλεια στα δίκτυα 5G με χρήση SDN .....	89
5.5 Σύγκριση SDN ελεγκτών (ONOS, POX) για εφαρμογές στην εκπαίδευση .....	91
5.6 Τροποποίηση Αρχιτεκτονικής τύπου DAS με χρήση τεχνικών NFV.....	95
6. ΣΥΜΠΕΡΑΣΜΑΤΑ .....	104
7. ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ.....	110
Βιβλιογραφία .....	113
Παράρτημα Α: Τοπολογίες .....	121
Παράρτημα Β: Δημοσιεύσεις.....	131

## Κατάλογος Σχημάτων & Εικόνων

**Εικόνα 3.1:** Διάγραμμα μίας γενικευμένης SDN αρχιτεκτονικής. Περιλαμβάνει τα επίπεδα εφαρμογής, ελέγχου και υποδομής, καθώς και τις διεπαφές μεταξύ τους. Τα southbound και northbound APIs.

**Εικόνα 3.2:** Μία στοιχειώδης RAN αρχιτεκτονική. Φαίνεται η πρόταση για RAN βασισμένο σε Cloud τεχνικές, όπως είναι το SDN και το NFV.

**Εικόνα 3.3:** Ανάλυση πλήρους αρχιτεκτονικής RAN, ειδικά μετά τη χρήση SDN.

**Εικόνα 3.4:** Παρατίθεται η βασικότερη αρχιτεκτονική του OpenStack.

**Εικόνα 3.5:** Τα πιο σημαντικά είδη επιθέσεων, που μπορεί να εμφανιστούν σε κινητά δίκτυα SDN.

**Εικόνα 3.6:** Η πορεία επιθέσεων, που ακολουθούν οι επιτιθέμενοι σε κινητά SDN δίκτυα.

**Εικόνα 3.7:** Η πορεία για τη διασφάλιση των κινητών δικτύων SDN.

**Εικόνα 3.8:** Το σχήμα ασφάλειας των κινητών δικτύων SDN.

**Εικόνα 4.1:** Σχήμα τοπολογίας εικονικού δρομολογητή.

**Εικόνα 4.2:** Σχήμα τοπολογίας κινητής επικοινωνίας.

**Εικόνα 4.3:** Σχήμα τοπολογίας κινητής επικοινωνίας.

**Εικόνα 4.4:** Σχήμα τοπολογίας βασικής CORD αρχιτεκτονικής.

**Εικόνα 4.5:** Σχήμα τοπολογίας IPRAN, που συντελέστηκε η επίθεση.

**Εικόνα 4.6:** Σχήμα της ετερογενούς τοπολογίας, που συντελέστηκε η επίθεση.

**Εικόνα 4.7:** Σχήμα τοπολογίας βασικής DAS αρχιτεκτονικής.

**Εικόνα 4.8:** Σχήμα τοπολογίας virtualized DAS αρχιτεκτονικής.

**Εικόνα 5.1:** Η απόδοση του εικονικού δρομολογητή ως συνάρτηση του χρόνου.

**Εικόνα 5.2:** Η απόδοση της τοπολογίας IPRAN ως συνάρτηση του χρόνου.

**Εικόνα 5.3:** Η απόδοση της τοπολογίας IPRAN για την ετερογενή τοπολογία ως συνάρτηση του χρόνου.

**Εικόνα 5.4:** Μελέτη εφικτότητας κλασικού μοντέλου DAS σχετικά με το εύρος ζώνης.

**Εικόνα 5.5:** Μελέτη εφικτότητας virtualized μοντέλου DAS σχετικά με το εύρος ζώνης.

**Εικόνα 5.6:** Μελέτη εφικτότητας για το κλασικό DAS σχετικά με το σταθμό βάσης.

**Εικόνα 5.7:** Μελέτη εφικτότητας για το virtualized DAS σχετικά με το eNB.

**Εικόνα 5.8:** Μελέτη εφικτότητας για το virtualized DAS σχετικά με το EPC.

**Εικόνα 5.9:** Μελέτη εφικτότητας για το κλασικό DAS σχετικά με τον εξοπλισμό στο σύστημα.

**Εικόνα 5.10:** Μελέτη εφικτότητας για το virtualized DAS σχετικά με τον εξοπλισμό στο σύστημα.

**Εικόνα 5.11:** Μελέτη εφικτότητας για το κλασικό DAS σχετικά με το κόστος υλοποίησης για το σύστημα.

**Εικόνα 5.12:** Μελέτη εφικτότητας για το virtualized DAS σχετικά με το κόστος υλοποίησης για το σύστημα.

**Εικόνα 5.13:** Μελέτη εφικτότητας για το κλασικό DAS σχετικά με το κόστος υλοποίησης της θέσης για το σύστημα.

**Εικόνα 5.14:** Μελέτη εφικτότητας για το virtualized DAS σχετικά με το κόστος υλοποίησης της θέσης για το σύστημα.

**Εικόνα 5.15:** Σύγκριση κόστους κεφαλαίου για τα δύο DAS συστήματα.

**Εικόνα 5.16:** Σύγκριση λειτουργικού κόστους για τα δύο DAS συστήματα.

**Εικόνα 5.17:** Σύγκριση συνολικού κόστους για τα δύο DAS συστήματα.

## Λίστα Πινάκων

**Πίνακας 1:** Χαρακτηριστικά ανά πρότυπο, το οποίο παρουσιάζει ποιες είναι οι βασικότερες απαιτήσεις στο 5G.

**Πίνακας 2:** Τα συστατικά στοιχεία του SDN και η λειτουργικότητα που παρέχουν σε ένα δίκτυο.

**Πίνακας 3:** Χαρακτηριστικά ανά πρότυπο, που παρουσιάζουν οι υφιστάμενες τεχνολογίες.

**Πίνακας 4:** Συστατικά στοιχεία τοπολογίας vRouter.

**Πίνακας 5:** Συστατικά στοιχεία τοπολογίας IPRAN και Heterogeneous.

**Πίνακας 6:** Παράμετροι κοστολόγησης DAS συστημάτων κλασικού και virtualized.

## Ακρωνύμια

**2.5G:** 2,5 (Second and a half generation) γενιά τεχνολογιών κινητής τηλεπικοινωνίας (GPRS)

**2.75G:** 2.75G γενιά τεχνολογιών κινητής τηλεπικοινωνίας (EDGE)

**3G:** Τρίτη γενιά (Third generation) τεχνολογιών κινητής τηλεπικοινωνίας

**3GPP:** 3rd Generation Partnership Project

**4G:** Τέταρτη γενιά (Fourth generation) τεχνολογιών κινητής τηλεπικοινωνίας

**5G:** Πέμπτη γενιά (Fifth generation) τεχνολογιών κινητής τηλεπικοινωνίας

**AaaS:** Anything as a Service

**AP:** Access Point

**BBU:** Base Band Unit

**BS:** Base Station

**BSC:** Base Station Controller

**BW:** Bandwidth

**cBBU:** cellular Base Band Unit

**CDN:** Content Delivery Network

**CDNaaS:** Content Delivery Network as a Service

**CLI:** Command Line Instructions

**CORD:** Central Office Re-imagined as a Data Center

**CPRI:** Common Public Radio Interface

**CSDN:** Cellular Software Defined Network

**DAS:** Distributed Antenna Systems

**DBaaS:** DataBase as a Service

**DDOS:** Distributed Denial of Service

**DNS:** Domain Name Space

**DNSaaS:** Domain Name Space as a Service

**DOS:** Denial of Service

**EDGE:** Enhanced Data Rate for GSM Evolution

**EMP:** Elastic Map Reduce

**EPC:** Evolved Packet Core

**ETSI:** European Telecommunication Standard Institution

**FTTH:** Fiber to the Home

**FW:** Firewall/ FirmWare

**GERAN:** GSM EDGE RAN

**GPON:** Gigabit Passive Optical Network

**GRAN:** GSM RAN

**GSM:** Global System Mobile Communication

**HSS:** Home Subscriber Service

**IaaS:** Internet as a Service

**IoT:** Internet of Things

**IP:** Internet Protocol

**IPRAN:** Internet Protocol Radio Access Network

**LTE:** Long Term Evolution

**MAC:** Media Access Control

**MCORD:** Mobile Central Office Re-imagined as a Data Center

**MeSDN:** Mobile Software Defined Networking

**MIMO:** Multiple Input Multiple Output

**NAT:** Network Address Translation

**NFV:** Network Function Virtualization

**NS:** Network Simulator

**ON:** Open Network

**ONF:** Open Network Foundation

**ONOS:** Open Network Operating System

**OpenRAN:** Open Radio Access Network

**OSS:** Operations Support System

**PCRF:** Policy and Charging Rules Function

**P-GW:** Packet Core Gateway

**PON:** Passive Optical Network

**QoE:** Quality of Experience

**QoS:** Quality of Service

**RAN:** Radio Access Network

**RRH:** Remote Radio Head

**ROADM:** Reconfigurable Optical Add Drop Multiplexer

**SaaS:** Software as a Service

**SDCN:** Software Defined Cellular Network

**SDN:** Software Defined Network

**S-GW:** Serving Gate-way

**SIP:** Session Initiation Protocol

**SLA:** Service Level Agreement

**SSID:** Service Set Identifier

**SSL:** Secure Socket Layer

**SW:** ShortWave

**TCP:** Transport Control Protocol

**TDMA:** Time Division Multiple Access

**TLS:** Transport Layer Security

**TRL:** Technology Readiness Level

**UMTS:** Universal Mobile Telecommunication Systems

**UTRAN:** UMTS RAN

**vBBU:** virtual Base Band Unit

**VM:** Virtual Machine

**VTN:** Virtual Tenant Network

**WAN:** Wide Area Network

**WSDN:** Wireless Software Defined Network

**XaaS:** Anything as a Service

## 1. ΕΙΣΑΓΩΓΗ

Στις μέρες μας, η δικτυακή τεχνολογία διαφοροποιείται σημαντικά βαίνοντας προς το Internet of Things (IoT), εγείρεται ολοένα και περισσότερο η ανάγκη για αποσύνδεση των δικτύων από το υλικό και για την εύρεση νέων περισσότερο αποδοτικών μεθόδων για τη βιώσιμη διαχείριση των φυσικών πόρων, όπως για παράδειγμα το εύρος ζώνης, το φυσικό μέσο και διάφορες άλλες ποσότητες, που σχετίζονται άμεσα με τη διαχείριση πόρων.

Η λογική του cloud computing, δηλαδή τεχνικές υπολογιστικής νέφους, που εισάγουν σε συστήματα εικονικές πηγές και όχι πηγές υλικού, μπορούν να λύσουν σημαντικά προβλήματα σχετικά με τα πιο πάνω ζητήματα και με τις απαιτήσεις, που υπάρχουν από την 5<sup>th</sup> Generation (5G), δηλαδή την 5<sup>η</sup> γενιά δικτύων κινητής επικοινωνίας, που είναι πιο κοντά από ποτέ και επιβάλλει τους δικούς της όρους στο δικτυακό τοπίο. Οι cloud τεχνικές προσφέρουν σημαντικά πλεονεκτήματα, τα οποία είναι χρήσιμα και προσδίδουν νέες δυνατότητες στα δίκτυα. Μερικά από τα πλεονεκτήματα αυτά είναι η σχεδόν απεριόριστη μνήμη, η μεγάλη ταχύτητα επεξεργασίας, ο έλεγχος δεδομένων, η αυξημένη «συνεργατικότητα» μεταξύ ατόμων, αλλά και συσκευών, η ασφάλεια, η εργασία από οποιοδήποτε μέρος, η σημαντική μείωση του κόστους, ιδίως του κόστους κεφαλαίου.

Στην περίπτωση των δικτύων, η λογική του νέφους ενσωματώνεται με συγκεκριμένες βασικές τεχνικές. Η μία τεχνική καλείται Network Function Virtualization (NFV) και συγκεντρώνει όλες τις βασικές ενέργειες, που επιτρέπουν την αντικατάσταση διαφόρων δικτυακών λειτουργιών με λογισμικό. Αναλυτικότερα, εισάγονται διάφορες συναρτήσεις υλοποιημένες με λογισμικό, οι οποίες αντί να χρησιμοποιούν υλικό, που αυτόματα σημαίνει μεγάλο κόστος κεφαλαίου, απαίτηση για φυσική παρουσία τεχνικών στο χώρο, ότι πιθανή καταστροφή κάποιου τμήματος μπορεί να σημαίνει αυτόματα και μη κάλυψη σε μεγάλο μέρος του δικτύου, χρησιμοποιεί κάποιο αντίστοιχο λογισμικό, το οποίο παρακάμπτει όλα αυτά τα ζητήματα και καθιστά τη συντήρηση, πολύ πιο εύκολη, ασφαλή, αξιόπιστη και οικονομική διαδικασία.

Εν συνεχεία, πολύ σημαντική για οποιοδήποτε δίκτυο είναι η εισαγωγή ελέγχου και διαφόρων κανόνων και η διαχείριση των φυσικών πόρων και υποδομών για τη βέλτιστη εξυπηρέτηση χρηστών στο διαδίκτυο και της επίτευξης ποιότητας υπηρεσίας Quality of Service (QoS) και ποιότητα εμπειρίας Quality of Experience (QoE) των διαφόρων χρηστών. Για να πραγματοποιηθεί κάτι τέτοιο απαιτείται μία καθολική οπτική του δικτύου και μία γενικότερη όψη της τοπολογίας, που υπάρχει. Τέτοιες δυνατότητες προσφέρουν οι ελεγκτές



(controllers), οι οποίοι βασίζονται σε λογισμικό και σε τεχνικές σχετικές με αυτό. Τέτοια παραδείγματα είναι το Software Defined Networking (SDN), που παρέχει ελεγκτές, που βασίζονται στο πρωτόκολλο OpenFlow.

## 1.1 Συνεισφορά Διπλωματικής

Η παρούσα διπλωματική πραγματεύεται σύγχρονα θέματα των κινητών δικτύων επικοινωνίας και ενσωματώνει νέες τεχνολογίες στις υπάρχουσες με βασικό στόχο την εξέλιξη και καλύτερη διαχείριση των κινητών επικοινωνιών. Η ιδέα του Cloud, του νέφους δηλαδή είναι μία βασικότερη ιδέα, η οποία πρωταγωνιστεί σε ζητήματα σχετικά με το SDN και το NFV, που ξεφεύγουν από τα στενά όρια της λογικής του υλικού και προωθούν τη χρήση λογισμικού για την πιο εύρυθμη και οικονομικότερη λειτουργία των δικτύων.

Η διπλωματική αυτή απαντά σε βασικά ερωτήματα, που εγείρονται σε σχέση με το συνδυασμό των δύο αυτών τεχνολογιών σε ζητήματα θεωρητικά, επιστημονικής έρευνας, πρακτικά και τεχνικά. Αρχικά, επιλύει ζητήματα, τα οποία σχετίζονται άμεσα με τις απαιτήσεις, που εγείρονται λόγω της έλευσης της πέμπτης γενιάς κινητών επικοινωνιών (5G). Ακόμα, απαντά σε σημαντικά ερωτήματα, που εγείρονται για την ασφάλεια, αξιοπιστία και λειτουργικότητα του SDN. Επιπρόσθετα, καταδεικνύει πώς είναι δυνατό να χρησιμοποιούνται NFVs και το δίκτυο να παραμένει πλήρως λειτουργικό, επεκτάσιμο και αξιόπιστο. Συνοψίζοντας, οι πιο βασικοί στόχοι της παρούσας διπλωματικής είναι οι ακόλουθοι:

- i. Αναλυτική σύνοψη των απαιτήσεων, που σκιαγραφούνται στα κινητά δίκτυα 5G.
- ii. Εκτενής βιβλιογραφική έρευνα στην περιοχή, δηλαδή, πάνω στα ζητήματα των 5G, SDN, NFV και σχετιζόμενων με αυτά τεχνολογιών, μελετών περίπτωσης, συγκριτικών μελετών κλπ.
- iii. Ανάλυση-Επεξήγηση των υποκείμενων τεχνολογιών, κάλυψη σε θεωρία, σχήματα, επεξήγηση, ανάλυση.
- iv. Ανάλυση και επεξήγηση της δομής και της λειτουργικότητας του ONOS και των περιπτώσεων χρήσης αυτού.

- v. Δημιουργία τοπολογιών για την πειραματική αξιολόγηση του ONOS με κύριο σκοπό την απόδειξη της πρακτικής εφαρμογής του ONOS και των βασισμένων σε OpenFlow ελεγκτών, αλλά και της βιωσιμότητας των SDN και NFV.
- vi. Επιλογή πειραματικών παραμέτρων και σεναρίων για τις πειραματικές δοκιμές στο ONOS και σε μελέτες περίπτωσης αυτού και εκτέλεση των προαναφερθέντων.
- vii. Εξαγωγή συμπερασμάτων σχετικά με την εξέλιξη και βιωσιμότητα των συγκεκριμένων τεχνολογιών.
- viii. Πρόταση τεχνολογικών και επιστημονικών μελλοντικών ανοιχτών ζητημάτων για έρευνα για τις υποκείμενες τεχνολογίες.

Επίσης, δημιουργούνται τοπολογίες για τις μελέτες περίπτωσης του ONOS, οι οποίες αναλύονται και εξηγούνται αναλυτικά και προάγουν την αξιολόγηση και ανάλυση της συμπεριφοράς του ONOS, ο οποίος είναι ένας μη εμπορικός ελεγκτής δικτύου και άρα, είναι πολύ σημαντικός για την εξέλιξη της τεχνολογίας για ερευνητικούς, ακαδημαϊκούς, εκπαιδευτικούς και πρακτικούς σκοπούς. Τέλος, συνοψίζονται τα βασικότερα συμπεράσματα, τα οποία προκύπτουν από την αξιολόγηση του ONOS και σκιαγραφούνται οι σημαντικότερες οδοί για τη μελλοντική έρευνα στον τομέα των Κινητών Δικτύων Επικοινωνίας. Βασική συνεισφορά της παρούσας διπλωματικής αποτελούν και οι δημοσιεύσεις, που προέκυψαν από αυτή [97], [98], [99], [100].

## 1.2 Διάρθρωση κεφαλαίων

Στο Κεφάλαιο 2 παρατίθεται η πιο σημαντική σχετική βιβλιογραφία. Τέτοιου είδους βιβλιογραφία συμβάλει στη βαθύτερη κατανόηση της συγκεκριμένης τεχνολογικής πρότασης, καθώς και τις απαιτήσεις, οι οποίες αναμένεται να εμφανιστούν στα επόμενα έτη από την πολλά υποσχόμενη γενιά κινητών τηλεπικοινωνιακών δικτύων. Στο Κεφάλαιο 3 υπάρχει το αντίστοιχο θεωρητικό υπόβαθρο σχετικά με το SDN, το NFV, το ONOS, που είναι ο βασικός ελεγκτής, που θα χρησιμοποιηθεί για την εξομοίωση των τοπολογιών, που επιδιώκεται να δημιουργηθούν. Αναλύεται το Radio Access Network (RAN), αναλύονται βασικά στοιχεία σχετικά με το CORD, αναλύεται το OpenStack. Τέλος, παρατίθεται μία συγκριτική μελέτη σχετικά με τις υφιστάμενες τεχνολογίες.

Στο Κεφάλαιο 4 υπάρχουν αναλυτικά οι πειραματικές διαδικασίες εξηγώντας τις τοπολογίες και για ποιο λόγο αυτές επιλέχθηκαν. Επίσης, διαφαίνεται ποια ζητήματα επιλύουν και ποια ακριβώς δικτυακά μέρη έχουν επιλεγεί σε ποια ποσότητα σχετικά με την κάθε

τοπολογία. Στο Κεφάλαιο 5 σε αντίθεση παρουσιάζονται και αναλύονται διεξοδικά τα βασικότερα μέρη της πειραματικής διαδικασίας.

Στο Κεφάλαιο 6 παρατίθενται, επεξηγούνται και αναλύονται τα βασικότερα συμπεράσματα, που προκύπτουν από την έρευνα, από τη θεωρητική θεμελίωση και από την πειραματική διαδικασία. Στο Κεφάλαιο 7 υπάρχει έντονος προβληματισμός σχετικά με την κατεύθυνση της συγκεκριμένης τεχνολογίας, καθώς και προτάσεις για μελλοντική έρευνα στον τομέα των Κινητών Δικτύων Επικοινωνίας στο εγγύς μέλλον.

### 1.3 Κινητά Δίκτυα Επικοινωνίας Πέμπτης Γενιάς

Η πέμπτη γενιά Δικτύων Κινητής Επικοινωνίας (5G) αναμένεται να πρωταγωνιστήσει το επόμενο διάστημα σε ότι αφορά στην εισαγωγή τεχνολογιών και καινοτομιών στα δίκτυα, καθώς οι εξέχουσες απαιτήσεις αυτής της γενιάς αναμένεται να σκιαγραφούν σημαντικές ανάγκες των τηλεπικοινωνιών και να αποτελέσουν το βασικό έναυσμα για καινοτομία στον τομέα. Βασικότερα ζητήματα, τα οποία έχουν ανακύψει και σχετίζονται με το 5G είναι τα ακόλουθα:

- **Παρεμβολές:** Αυτές οι παρεμβολές μπορεί να προέρχονται από γειτονικές κυψέλες αν πρόκειται για κυψελωτά δίκτυα. Επίσης, υπάρχουν παρεμβολές λόγω του χώρου, για παράδειγμα λόγω γεωμετρίας, λόγω κτηρίων, λόγω ηλεκτρομαγνητικών ακτινοβολιών και σημάτων. Ακόμα, υπάρχει θόρυβος, που δε σχετίζεται άμεσα με το μεταδιδόμενο σήμα, αλλά με άλλα σήματα.
- **Μεγάλη κατανάλωση ενέργειας:** Συχνά, παρατηρείται μεγάλη δυσαρέσκεια σε ορισμένους χρήστες, οι οποίοι θεωρούν ότι στις κινητές συσκευές τους π.χ. κινητά, ταμπλέτες ή laptops κλπ. η διαθέσιμη ενέργεια καταναλώνεται ταχύτατα.
- **Υποχρησιμοποίηση του εύρους ζώνης:** Αυτός είναι και ο βασικός σκοπός, που γίνονται προσπάθειες σε θεωρητικό και πρακτικό επίπεδο με στόχο την αναδιανομή του εύρους ζώνης με βέλτιστο τρόπο.

- Handovers: πρέπει να γίνονται αποδοτικά ούτως ώστε είτε να μην εμφανίζεται το φαινόμενο του ping pong, το οποίο δημιουργεί πρόβλημα στο ότι καταναλώνει μεγάλη ενέργεια στη συσκευή και δεσμεύει πόρους σε 2 γειτονικούς σταθμούς βάσης.
- Ποιότητα σημάτων: Ενδέχεται να είναι χαμηλότερη από την προσδοκώμενη και να δημιουργούνται προβλήματα στις κλήσεις και στη διακίνηση των δεδομένων.
- Μειωμένη χωρητικότητα δικτύου: Τα δίκτυα σήμερα περιλαμβάνουν μεγάλους όγκους δεδομένων.
- Ασφάλεια και ιδιωτικότητα χρηστών: Επίσης, ίσως τα λογισμικά να μην είναι ενημερωμένα. Ακόμα, διάφορα ζητήματα αυθεντικοποίησης και πιστοποίησης χρηστών.

Με στόχο να απαντηθούν αυτά τα προβλήματα, επισημαίνονται οι βασικές απαιτήσεις των 5G δικτύων. Οι πιο σημαντικές από τις οποίες συνοψίζονται παρακάτω:

- Υψηλοί ρυθμοί δεδομένων και μεταγωγής αυτών.
- Χαμηλή καθυστέρηση και χαμηλοί χρόνοι μεταφοράς πακέτων δεδομένων.
- Χαμηλό κόστος κεφαλαίου και λειτουργικό κόστος.
- Εξασφάλιση γρήγορων χρόνων απόκρισης υπηρεσιών.
- Ποικιλία περιπτώσεων χρήσης, όπως ο απομακρυσμένος έλεγχος και η υπολογιστική νέφος.
- Βελτιστοποίηση της κινητικότητας μεταξύ των κυψελών.
- Διάκριση μεταξύ των τηλεπικοινωνιακών επιπέδων.
- Εξασφάλιση των τεχνολογιών πρόσβασης και εκσυγχρονισμός των υλικών πόρων.
- Υποστήριξη επικοινωνίας από τα πάντα στα πάντα.
- Υψηλή χωρητικότητα και χαμηλή καθυστέρηση του φυσικού μέσου με διατήρηση χαμηλού κόστους για την παροχή των υπηρεσιών αυτών.
- Επίσης, το δίκτυο πρέπει να είναι προγραμματιζόμενο.

Τα βασικότερα ζητήματα και απαιτήσεις, που εγείρονται από τη 5G οδηγούν ξεκάθαρα στην υιοθέτηση τεχνικών και τεχνολογιών σχετικών με το νέφος. Το Cloud αναμένεται να συμβάλει σημαντικά σε ζητήματα, όπως τη μετατροπή του δικτύου σε προγραμματιζόμενο, στον εκσυγχρονισμό των υλικών πόρων, στο χαμηλό κόστος δικτύων, στην αποφυγή του υλικού και την παρουσία και εκμετάλλευση εφαρμογών λογισμικού. Είναι ιδιαίτερα σημαντικό να συνοψιστούν τα βασικότερα σημεία στα οποία θεωρείται ότι οι εξεταζόμενες τεχνολογίες ικανοποιούν τις απαιτήσεις για την επόμενη γενιά κινητής επικοινωνίας, δηλαδή το 5G.

**Πίνακας 1: Χαρακτηριστικά ανά πρότυπο, το οποίο παρουσιάζει τις βασικότερες απαιτήσεις στην 5G και πώς καλύπτεται από το αναφερθέν πρότυπο (Συνδυασμός SDN & NFV).**

<b>Απαίτηση 5G και κατεύθυνση</b>	<b>Χωρητικότητα</b>	<b>Υψηλός ρυθμός δεδομένων</b>	<b>Αξιοπιστία</b>	<b>Ενεργειακή Απόδοση</b>	<b>Κινητικότητα</b>	<b>Κάλυψη</b>
<b>Εικονικότητα</b>	✓	✓	✓	✓		
<b>Επεκτασιμότητα</b>	✓				✓	✓
<b>Αποδοτικότητα</b>	✓	✓	✓	✓		✓
<b>Πρότυπα Διεπαφής</b>	✓		✓	✓		✓
<b>Πληροφοριο-κεντρικότητα</b>		✓	✓	✓	✓	
<b>Ευφυΐα</b>	✓		✓	✓	✓	
<b>Ετερογένεια</b>	✓	✓	✓	✓	✓	✓
<b>QoS &amp; QoE</b>	✓	✓	✓	✓	✓	✓
<b>Πρότυπα ελεγκτών</b>	✓	✓	✓	✓	✓	✓
<b>Ανάπτυξη πολιτικών και πρωτοκόλλων</b>	✓	✓	✓	✓	✓	✓
<b>Ευέλικτη διαχείριση κίνησης</b>				✓	✓	✓

<b>Software Defined RAN</b>		✓		✓		✓
-----------------------------	--	---	--	---	--	---

## 2. ΣΧΕΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Στο εν λόγω κεφάλαιο παρατίθεται και αναλύεται η προτεινόμενη βιβλιογραφία. Υπάρχουν ερευνητικές εργασίες δημοσιευμένες σε συνέδρια και περιοδικά, καθώς και μελέτες από σημαντικούς οργανισμούς σχετικούς με τα δίκτυα. Αξιολογήσεις σχετικά με τον ONOS συντελούνται και σε άλλες ερευνητικές εργασίες. Υπάρχει αρκετό υλικό σχετικά με τον ONOS και το CORD [47], [48]. Παρουσιάζονται σενάρια λειτουργίας δύο και τριών ελεγκτών. Επίσης, αναπτύσσονται δύο διαφορετικά είδη πρωτοκόλλων χρησιμοποιώντας κατανεμημένες εκδόσεις, οι οποίες συμβάλουν στην ικανοποίηση πλήθους αναγκών, όπως η επεκτασιμότητα και η αξιοπιστία [66], [67]. Ο έλεγχος του συστήματος όσον αφορά στο OpenFlow είναι δυνατό να πραγματοποιηθεί σε μεγάλη κλίμακα. Αν και ο ONOS παρέχει έναν τρόπο διανομής των εργασιών [68]. Το OFMon ορίζεται ως το μοναδικό σύστημα ελέγχου. Με βασικό στόχο την αξιολόγηση της κεντρικής μονάδας επεξεργασίας, καθώς και της χρήσης, που γίνεται σε αυτή.

### 2.1 Κινητά Δίκτυα Επικοινωνιών

Οι πιθανές απαιτήσεις ενός κινητού δικτύου της πέμπτης γενιάς κινητής επικοινωνίας, καθώς και διάφορα πιθανά σενάρια λειτουργίας αναλύονται στο [1]. Εισάγονται σημαντικές τεχνικές, που επιτρέπουν γρηγορότερες επικοινωνίες. Παρουσιάζεται ένας πιθανός σχεδιασμός δικτύου, υπάρχουν διάφορες προτάσεις για εναλλακτικές τεχνολογίες, όπως πληροφορίας, διάφορες τεχνικές και συγκεκριμένες προτάσεις τεχνολογίας.

Ενδεικτικά, η μελέτη [5] αναλύει μία λογική τεχνικών και παρουσιάζει μία συνολική αρχιτεκτονική για δίκτυα τέταρτης γενιάς. Επίσης, υπάρχουν αναλύσεις σχετικά με το RAN και την εισαγωγή των συστατικών του δικτύου, την ποιότητα υπηρεσίας [6]. Αναλύονται και διαχωρίζονται τα βασικά συστατικά στοιχεία μίας αρχιτεκτονικής τέταρτης γενιάς [7].

Υπάρχει μεγάλο πλήθος εργασιών, που ασχολούνται εξειδικευμένα με το RAN. Το RAN χωρίζεται σε διάφορα τμήματα, όπως ο SDN ελεγκτής, το πρωτόκολλο ανοιχτού φάσματος. Αναλύεται η στρατηγική ελέγχου [42]. Υπάρχουν διάφορες χρήσεις και περιπτώσεις χρήσης [43]. Το Netshare συμβάλει στην καλύτερη διαχείριση των φυσικών πόρων και στην επαναχρησιμοποίηση οντοτήτων [45]. Τέλος, η Fujitsu έχει εισάγει μία αντίστοιχη αρχιτεκτονική για παρόχους και για χρήστες κινητών υπηρεσιών [46].

## 2.2 Network Function Virtualization (NFV)

Όσον αφορά στην τεχνολογία του NFV υπάρχουν αρκετές μελέτες, όπως η [2], που αφορά στον συμπληρωματικό ρόλο, που παρουσιάζουν οι τεχνολογίες SDN και NFV. Υπάρχουν δύο συγκεκριμένες προτάσεις, χρησιμοποιώντας ως SDN σύστημα το TOSCA και ως NFV το NETCONF. Η μελέτη [3] παρουσιάζει τα πιο σημαντικά κίνητρα να χρησιμοποιεί κανείς NFV, αποδεικνύει την πιθανότητα συνύπαρξης των εικονικών και μη εικονικών δικτυακών δομών στο ίδιο κινητό δίκτυο. Εν συνεχεία, το ETSI στην ιστοσελίδα του [5], περιλαμβάνει πολλές διαφορετικές ιδέες, αναλύσεις, προσεγγίσεις, μελέτες περίπτωσης σχετικά με τη συγκεκριμένη τεχνολογία. Ο Open Network Foundation (ONF) επίσης, έχει μελετήσει εις βάθος το εν λόγω ζήτημα. Οι ασύρματες επικοινωνίες αναλύονται στο [9]. Υπάρχουν περιληπτικά οι πιο κύριες κατευθύνσεις στον τομέα. Βασικά πλεονεκτήματα είναι ο κεντρικός έλεγχος και το υψηλό επίπεδο καινοτομίας.

## 2.3 Software Defined Networking (SDN) σε ενσύρματα δίκτυα

Το ενσύρματο SDN αναλύεται εις βάθος σε πολλές μελέτες. Αρχικά, υπάρχουν λεπτομερείς έρευνες σχετικά με τα προγραμματιζόμενα δίκτυα [10]. Υπάρχει μία ενδελεχής έρευνα της υλοποίησης του SDN σε ενσύρματα, ασύρματα και κινητά δίκτυα [11]. Μοντέλο για την ανάπτυξη του SDN, σημαντικοί ορισμοί μειονεκτήματα, πλεονεκτήματα, προκλήσεις περιλαμβάνονται στο [12]. Επίσης, υπάρχει βασική περιγραφή της υποδομής και του ελέγχου στο OpenFlow πρωτόκολλο. Εκτός από το πρωτόκολλο στο [13] αναλύονται σημαντικές πτυχές, που αναμένεται να οδηγήσουν στην πρακτική υλοποίηση του SDN.

Οι πιο σημαντικές ενέργειες, που πρέπει να πραγματοποιηθούν με στόχο να μεταβούν τα δίκτυα στην εποχή του SDN αναλύονται στο [14]. Η ανάλυση όλων των στοιχείων της SDN τεχνολογίας, όπως η θεωρία, η ιστορία, οι ορισμοί, οι λειτουργίες, τα προβλήματα που αυτό

λύνει, οι διάφορες εφαρμογές, οι καταλληλότερες γλώσσες προγραμματισμού και μελλοντικές επιδιώξεις στον τομέα αναλύονται στο [15]. Στο [16] αναλύεται μία βασική αρχιτεκτονική με βασικό χαρακτηριστικό το διαχωρισμό του τμήματος ελέγχου και τμήματος δεδομένων. Στην εργασία [17] υπάρχουν τα οφέλη από την υιοθέτηση του SDN, οι σημαντικότερες απαιτήσεις σε αξιοπιστία και υψηλή αποδοτικότητα.

## 2.4 Ασφάλεια και κόστος στο Software Defined Networking (SDN)

Υπάρχουν ακόμα μελέτες, που πραγματεύονται σημαντικά ζητήματα, όπως η ασφάλεια στο SDN. Είναι σημαντικό να αναλυθεί πώς επιτυγχάνεται μεγαλύτερη ασφάλεια στο SDN [19]. Αναλύονται διεξοδικά οι τεχνικές, σύμφωνα με τις οποίες είναι δυνατόν να αποφευχθεί μία αρκετά γνωστή επίθεση των υπολογιστών, όπως για παράδειγμα, είναι η άρνηση υπηρεσιών DOS. Όσον αφορά στα κινητά δίκτυα υπάρχει, επίσης, ανάγκη επίλυσης ζητημάτων ασφαλείας, που σχετίζονται πάλι με τις επιθέσεις τύπου DOS ή με επιθέσεις τύπου Distributed DOS (DDOS). Επίσης, αναλύεται το spoofing και πώς μπορεί να αποφευχθεί. Υπάρχει μία περίληψη σχετικά με τα ζητήματα ασφαλείας, που είναι δυνατό να ανακύψουν και σχετίζονται με τις παρούσες τεχνολογικές προτάσεις. [20].

Το DaMask-D είναι το βασικό σύστημα ασφαλείας [79] και [81]. Το μοντέλο, που ακολουθείται έχει έναν χρόνο δημιουργίας, που είναι γραμμική συνάρτηση σε σύγκριση με τα δεδομένα του συνόλου δεδομένων, που παρατίθεται από το σύστημα. Οι αρχές και οι πρακτικές για την ασφάλεια στο SDN παρουσιάστηκαν από τον ONF [76].

Το υβριδικό σύννεφο παραμένει η ιδανικότερη λύση για δικτύωση νέφους, εφόσον, επιτρέπει να κρύβεται η βασική υποδομή, ενώ παρέχονται διάφορες δημόσιες υπηρεσίες [74]. Όταν συμβαίνει μία επίθεση από botnet ή κάποιου χρήστη, είναι σημαντικό να λαμβάνονται σημαντικά ζητήματα υπόψη, ώστε να προλαμβάνεται σχετικά γρήγορα και να αποτρέπεται συνολικά η κατάρρευση του δικτύου [82]. Ο καταιγισμός DDOS επιθέσεων μπορεί να αποτραπεί αν συντελεστούν ορισμένες ενέργειες προστασίας [82].

Οι ελεγκτές δικτύου μπορούν να ενημερώνουν και να διαγράφουν ροές πληροφορίας αντιδρώντας σε απάντηση σε πακέτα επιτιθέμενα ή να προλάβουν δημιουργώντας προ-αποφασισμένους κανόνες [75]. Σήμερα, ολοένα αυξάνεται το πλήθος των επιθέσεων στα δίκτυα [73]. Με σκοπό την αποτροπή τους εισάγεται η λογική των αυστηρών και ελαστικών timeouts. Η στατιστική πληροφορία, που εξάγεται από το δίκτυο είναι δυνατό να συμβάλει ενεργά στο να παρακολουθούνται ανωμαλίες στο δίκτυο και τη δικτυακή κυκλοφορία.



Μερικά από τα σημαντικότερα μειονεκτήματα του SDN σχετικά με την ασφάλεια είναι: οι ευάλωτοι ελεγκτές, κίνδυνοι σχετικοί με ανοιχτά προγραμματιζόμενες διεπαφές, πολλά σημεία επιθέσεων λόγω των διαφόρων στρωμάτων του SDN και της επικοινωνίας μεταξύ αυτών, τα οποία πρέπει να ξεπεραστούν με στόχο την ευρεία υιοθέτηση της τεχνολογίας [77]. Σημαντικό ζήτημα είναι ότι περνάει κάποιος χρόνος μέχρι να βρεθεί η επίθεση και να ξεκινήσουν να πραγματοποιούνται ενέργειες για την αποτροπή της κυκλοφορίας [72]. Μέσα στις βασικότερες τεχνικές για την αποτροπή των DDOS επιθέσεων μπορεί να σημειωθούν και οι κανόνες για τις ροές, που είναι σημαντικοί για την αποτροπή «κακής» κυκλοφορίας [78].

Μετά την υιοθέτηση του παιχνιδιού Stackelberg ενός βασικού ζητήματος της θεωρίας παιγνίων υλοποιούνται διάφορες στρατηγικές για τη διαχείριση του διαθέσιμου εύρους ζώνης, καθώς και για τη διαχείριση του εύρους ζώνης και του υπολογισμού κόστους. Εγείρεται ακόμα η ιδέα της διάσπασης των στρατηγικών κόστους. Οι τηλεπικοινωνιακοί πάροχοι κερδίζουν περισσότερα οφέλη όταν υιοθετούν SDN λύσεις [21]. Επίσης, αναλύονται οι τιμές, που είναι δυνατό να εισαχθούν, καθώς και οι πιο σημαντικές συναλλαγές στο σύστημα [22]. Στην εργασία [23] αναλύονται τα ζητήματα, που σχετίζονται με τα Service Level Agreement (SLA) και πως οι ελεγκτές δικτύου στο SDN δημιουργούν διαφορετικές ροές δεδομένων, ούτως ώστε να τις διαχωρίζουν και να περιγράφονται οι αντίστοιχες παροχές στα υπογεγραμμένα SLAs.

Με στόχο την εκτίμηση του κόστους κεφαλαίου, λειτουργικού και του συνολικού κόστους, εισάγονται μοντέλα οικονομικά και αρχιτεκτονικά βασισμένα στο SDN και το NFV και τις αρχιτεκτονικές νέφους στο 5G [86]. Το κόστος κεφαλαίου είναι δυνατό να μειωθεί περισσότερο από 68%, το λειτουργικό κόστος μειώνεται περισσότερο από 63% και το συνολικό κόστος ελαττώνεται 69% σε σχέση με τα παραδοσιακά σενάρια.

## 2.5 Software Defined Networking (SDN) σε κινητά δίκτυα

Εξέχουσας σημασίας είναι η μελέτη των κινητών δικτύων SDN. Παρατίθενται οι βασικές απαιτήσεις των κινητών δικτύων πέμπτης γενιάς και οι βασικές κατευθυντήριες οδοί, που ορίζουν οτιδήποτε αναφορά στο μέλλον των κινητών επικοινωνιών [24]. Το SDN in Generalized Mobile Network Architecture (SIGMONA) παρουσιάζεται στο [25]. Μία διαφορετική προσέγγιση σημειώνεται σε ότι αναφορά στην κρυπτογράφηση των δεδομένων με το Secure Socket Layer (SSL) ή Transport Layer Security (TLS). Τα κύρια προβλήματα, που επιλύονται συνοψίζονται στο [26].

Ακόμα, υπάρχουν εργασίες, όπως οι [27], που περιλαμβάνουν βασικές αναλύσεις για τα πιο στοιχειώδη θέματα σχετικά με το SDN κινητής επικοινωνίας. Αναλύεται τι είναι το Mobile SDN (meSDN), δηλαδή η κινητή έκδοση του SDN [28]. Περιλαμβάνονται διάφορες σημαντικές προκλήσεις, που εγείρονται λόγω του συνδυασμού των αδόμητων δικτύων με το SDN [29]. Αναλύονται τα βασικά σημεία των κινητών δικτύων Internet Protocol (IP) και πως είναι δυνατό να συμβάλει το SDN στο να αποστέλλονται όλα τα πακέτα με βάση το μικρότερο μονοπάτι [30].

Αναλύονται οι απαιτήσεις των κινητών δικτύων 5<sup>ης</sup> γενιάς, καθώς και περιγράφονται τα βασικά σημεία των Radio Access Networks (RAN) και Evolved Packet Core (EPC) [31]. Στη μελέτη [32] εισάγονται ζητήματα σχετικά με το ότι τα δίκτυα είναι προγραμματιζόμενα και περιλαμβάνουν πολύ μεγάλα επίπεδα αφαίρεσης. Οι πολιτικές σχετικά με την επεκτασιμότητα και την ευελιξία, τον απομακρυσμένο έλεγχο των κινητών σταθμών βάσης, οι πολιτικές προσβασιμότητας και ποιότητας υπηρεσίας αναλύονται διεξοδικά στο [33]. Μία αρχιτεκτονική SDN περιγράφεται στο [34]. Συνοψίζονται οι πιο σημαντικές λειτουργίες σχετικά με τα επίπεδα ελέγχου και δεδομένων, τη βελτιστοποίηση του δικτύου και σχετικά με καινοτόμες εφαρμογές.

Εγείρονται ζητήματα, που άπτονται της αλλαγής των SDN με σκοπό την κάλυψη ασύρματων αναγκών και διαχωρίζονται οι ελεγκτές δικτύου σε δύο κατηγορίες ανάλογα με την πολιτική βελτιστοποίησης, που ακολουθούν [35]. Οι πιο βασικές ενέργειες των μηχανικών σε ότι αναφορά στην αύξηση του διαθέσιμου εύρους ζώνης, στην ανάπτυξη MIMO τεχνικών, καθώς και στη συλλογή στοιχείων από την κατάσταση του δικτύου αναλύονται στο [36]. Μηχανισμοί, που επιτυγχάνουν το διαμοιρασμό της δικτυακής υποδομής, την εικονική χρήση των βασικών εξυπηρετητών και πολιτικές δυναμικής διαχείρισης της ενέργειας εισάγονται στο [37]. Το Blueprint εισάγει το NOX ελεγκτή με βασικό στόχο να πραγματοποιηθούν πειράματα και εξομοιώσεις για τη χρήση του SDN σε ασύρματα δίκτυα επικοινωνίας. Επίσης, σημειώνονται πειράματα για την απώλεια πακέτων και τα handovers [38]. Οι βασικές απαιτήσεις και τα βασικά σενάρια σχετικά με το SDN αναλύονται στην [39]. Τα small cells μαζί με σημαντικές προκλήσεις της πέμπτης γενιάς κινητής επικοινωνίας περιγράφονται και σχετίζονται με τη διαχείριση των παρεμβολών, την ασφάλεια, την υψηλή πολυπλοκότητα, λόγω του αυξημένου πλήθους handovers και στις δυσκολίες, που εμφανίζονται στην αντιμετώπιση αυτών των δυσκολιών [40].

### 3. ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

Στο εν λόγω κεφάλαιο θα αναλυθούν διεξοδικά οι βασικές τεχνολογίες, που πραγματεύεται η παρούσα διπλωματική. Ο συνδυασμός των δύο τεχνολογικών προτάσεων, δηλαδή του SDN και του NFV αποτελεί πολλά υποσχόμενη λύση για τα μελλοντικά δίκτυα επικοινωνιών. Η μετάβαση από το υλικό στο λογισμικό προσδίδει πολλά σημαντικά και θεμελιώδη πλεονεκτήματα, όπως είναι η ευκολότερη διαχείριση των προβλημάτων και των κακών κείμενων στο δίκτυο, όπως η γρηγορότερη ανάπτυξη νέων χαρακτηριστικών, π.χ. η εισαγωγή νέας λειτουργικότητας. Επίσης, το να υπάρχουν «εικονικές» συσκευές ή συσκευές με πολύ λίγη ευφυΐα στις οποίες προσθέτοντας την κατάλληλη προγραμματιζόμενη λογική να επιτυγχάνεται να εκτελούνται σημαντικές διεργασίες καθώς και να υπάρχει καθολική όψη του δικτύου είναι ιδιαίτερα σημαντικό.

Τα CORD και OpenStack είναι εξέχουσας σημασίας και μεταφέρουν το νέφος ή cloud και τα πλεονεκτήματα, που αυτό προσδίδει στο επίπεδο του διαδικτύου. Είναι ευρέως γνωστό ότι το νέφος παρέχει πολλά πλεονεκτήματα σε ότι αφορά στην αποθήκευση πληροφοριών, ειδικά σε πληροφορία μεγάλου όγκου. Γίνεται αντιληπτό ότι ιδανικά η αξιοποίηση αυτού του χαρακτηριστικού θα ήταν δυνατό να οδηγήσει σε εκμετάλλευση των στατιστικών ενός δικτύου με αποτέλεσμα την καλύτερη διαχείριση και αναβάθμιση του δικτύου σε σημαντικά επίπεδα. Υπάρχουν προβλήματα παρεμβολών μεταξύ των συσκευών, αλλά και με τον αέρα, με τα κτήρια και άλλα φυσικά ή τεχνητά εμπόδια, που είναι δυνατό να εμφανίζονται. Ακόμα, στα περισσότερα κυψελωτά δίκτυα εμφανίζεται το σημαντικό θέμα της διακυβελικής παρεμβολής, που σημαίνει την παρεμβολή, που εμφανίζεται από την ταυτόχρονη εκπομπή γειτονικών κυψελών.

#### 3.1 Software Defined Networking (SDN)

Η τεχνολογία του Software Defined Networking (SDN) είναι μία σημαντική προσέγγιση, που επιτρέπει στους διαχειριστές του δικτύου να διαχειριστούν όλες τις πιθανές υπηρεσίες και λειτουργικότητες με κάποια επίπεδα αφαίρεσης και πολύ χαμηλά επίπεδα λειτουργικότητας. Η βασική ανάγκη για χρήση και δημιουργία SDN είναι ότι οι παραδοσιακές αρχιτεκτονικές είναι περιορισμένες και δεν παρέχουν τη δυναμική, επεκτάσιμη, υπολογιστική και αποθηκευτική δομή, που παρέχουν οι σύγχρονες μέθοδοι, όπως είναι τα κέντρα δεδομένων. Αυτό συμβαίνει με το διαχωρισμό μεταξύ του ελεγκτή (control plane) σε σχέση με το επίπεδο, που προωθεί την κίνηση στον επιλεγμένο προορισμό (data plane).

Οι ελεγκτές SDN βασίζονται στο πρωτόκολλο OpenFlow για απομακρυσμένη επικοινωνία με τα στοιχεία, που υπάρχουν στο επίπεδο δικτύου με βασικό στόχο να αποφασιστεί το μονοπάτι, που θα ακολουθηθεί από τα πακέτα του δικτύου μεταξύ των μεταγωγέων δικτύου. Οι μεταγωγείς δικτύου είναι απλοϊκές συσκευές, χωρίς ιδιαίτερη ευφυΐα και αποτελούν συσκευές στο 2<sup>ο</sup> δικτυακό επίπεδο. Τα SDN παρέχουν αρχιτεκτονικές δυναμικές, αποδοτικές από άποψη κόστους και εύκολα προσαρμοζόμενες. Επίσης, είναι προγραμματιζόμενες και οι λειτουργίες προώθησης τους είναι αυθαίρετες από εφαρμογές και υπηρεσίες δικτύου.

Το SDN μπορεί να επεκταθεί σε πολλά είδη δικτύων μεταξύ των οποίων τα ενσύρματα, ασύρματα, κινητά και αδόμητα δίκτυα. Στα κινητά δίκτυα, ενσωματώνονται διάφορες λειτουργίες σχετικές με την κίνηση, καθώς και τη διαχείριση των σταθμών βάσης. Σε αδόμητα δίκτυα, εκτός από την προφανή λειτουργικότητα του ασύρματου δικτύου, δεν είναι πολύ ενδιαφέρον ή σημαντικό να επεξεργάζεται κανείς πληροφορίες σχετικά με την κινητικότητα, αφού συνήθως δεν σημειώνεται κίνηση και η θέση ενός αισθητήρα σε ένα αδόμητο δίκτυο είναι σχετικά σταθερή. Βασικό στοιχείο σε αυτή την περίπτωση είναι η συλλογή δεδομένων σε κάποια καταβόθρα, η οποία γίνεται με πολύ πιο εύκολο τρόπο, ειδικά αν αναλογιστεί κανείς το ζήτημα ότι η προώθηση, ο έλεγχος και έπειτα, η διαχείριση της πληροφορίας είναι δυνατό να διαχειρίζονται από σύστημα λογισμικού με βάση το SDN.

Η βασική δομή, που περιλαμβάνει κάθε SDN δίκτυο χωρίζεται σε τρία βασικά μέρη. Το πρώτο μέρος αποτελεί το επίπεδο υποδομής, το δεύτερο το επίπεδο ελέγχου και το τρίτο το επίπεδο εφαρμογών. Το επίπεδο υποδομής (infrastructure layer) περιλαμβάνει ουσιαστικά ό,τι υλικό υπάρχει στο δίκτυο. Αυτό συνήθως περιορίζεται σε κάποια απλά switches. Βασικός στόχος είναι η αποδέσμευση από το υλικό. Συνεπώς, αυτά τα switches είναι whitebox, δηλαδή δεν πραγματοποιούν κάποια εξειδικευμένη λειτουργία σε υλικό. Είναι περισσότερο βασισμένα σε λογισμικό. Κάτι τέτοιο σημαίνει ότι απαιτείται η χρήση NFV, δηλαδή της εξομοίωσης δικτυακών λειτουργιών με βασικό στόχο να λυθεί το βασικό πρόβλημα, που προκύπτει και να εισαχθεί σε αυτά τα «κουτιά» λογική προγραμματισμού με απώτερο σκοπό να εκτελούν εξειδικευμένες λειτουργίες. Το επίπεδο υποδομής επικοινωνεί με βάση το OpenFlow πρωτόκολλο με το επίπεδο ελέγχου. Το OpenFlow πρωτόκολλο ή κάθε άλλο πιθανό πρωτόκολλο, που επιτρέπει την επικοινωνία μεταξύ της υποδομής και του ελέγχου καλείται και Southbound API.

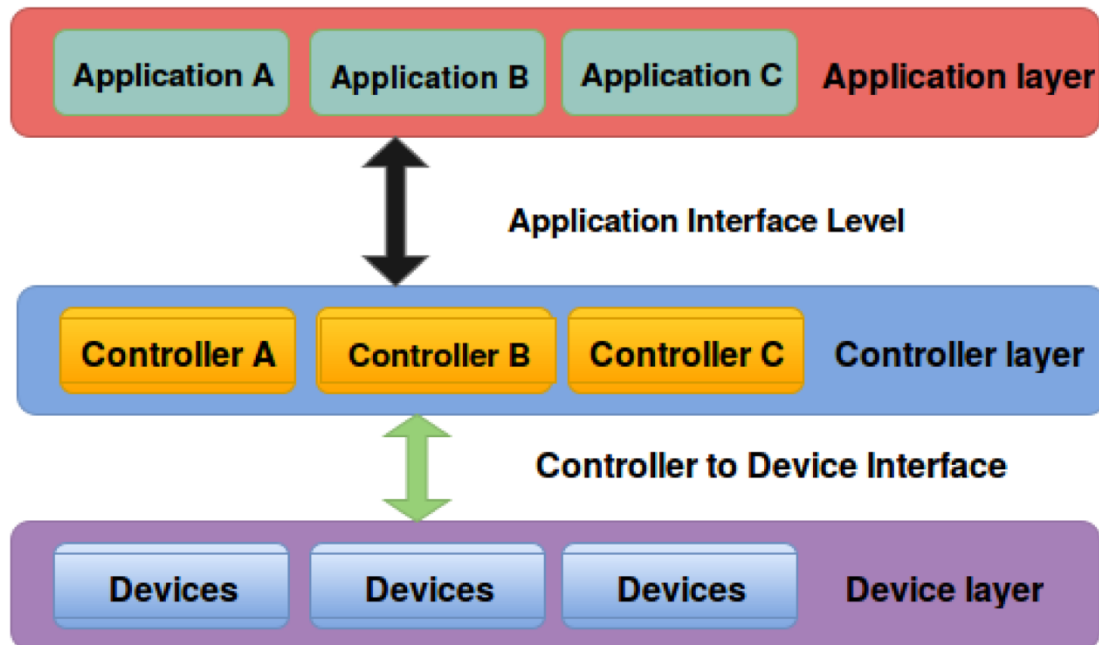
Το επίπεδο ελέγχου (control layer) είναι ουσιαστικά ο εγκέφαλος του δικτύου και παρέχει μία κεντροκοποιημένη οπτική στο εν λόγω δίκτυο. Είναι δυνατό να υπαγορεύει τι πρέπει να κάνουν ουσιαστικά οι συσκευές στο επίπεδο υποδομής, ελέγχει τη δρομολόγηση της κίνησης και την κίνηση του δικτύου. Ουσιαστικά, είναι το πιο σημαντικό κομμάτι, το οποίο υπάρχει σε κάθε δίκτυο και σε κάθε τύπο δικτύου. Είναι δυνατό να αναπτυχθούν πολιτικές σύμφωνα με τις οποίες δεδομένα, τα οποία προκύπτουν από τη λειτουργία του ελεγκτή να είναι δυνατό να αξιοποιηθούν καταλλήλως και να προκύψουν στοιχεία, τα οποία είναι σημαντικά, όπως στατιστική απεικόνιση και κατάλληλη αξιοποίηση των δικτυακών ροών σχετικά με ορισμένες παραμέτρους.

Το επίπεδο εφαρμογών (application layer) συνδέεται με το επίπεδο ελέγχου δια μέσου Northbound APIs. Σε αυτό το επίπεδο είναι σημαντικό να χρησιμοποιείται λογική, που υπάρχει πάνω από αυτό το επίπεδο με βασικό σκοπό να λειτουργούν εφαρμογές σχετικές με επιχειρηματικούς σκοπούς. Είναι δυνατό να βοηθήσει τους διαχειριστές δικτύου να παρακολουθήσουν την κίνηση, αλλά και να ενορχηστρώσουν παρεχόμενες υπηρεσίες.

**Πίνακας 2: Τα συστατικά στοιχεία του SDN και η λειτουργικότητα, η οποία παρέχουν σε ένα δίκτυο.**

Συστατικό στοιχείο δικτύου	Λειτουργικότητα
Επίπεδο Εφαρμογών	Περιλαμβάνει κάθε πιθανή εφαρμογή, που παρέχεται.
Επίπεδο ελέγχου	Συστάδα ελεγκτών δικτύου, που πραγματοποιούν τον δικτυακό έλεγχο.
Τμήμα Δεδομένων	Περιλαμβάνει λειτουργικότητα, που αναφέρεται στα επίπεδα (4-7) του μοντέλου ISO/OSI.
Northbound Διεπαφή	Επιτρέπει την επικοινωνία μεταξύ του επιπέδου ελέγχου και εφαρμογών.
Southbound Διεπαφή	Επιτρέπει την επικοινωνία μεταξύ του επιπέδου ελέγχου και δεδομένων.
Υλικό	Μεταγωγείς, τείχη προστασίας, πιθανώς εικονικά υλοποιημένα.

Μία πιθανή αρχιτεκτονική, που θα μπορούσε να έχει δημιουργηθεί με βάση ένα SDN σύστημα παρατίθεται στην εικόνα 3.1:



Εικόνα 3.1: Διάγραμμα μίας γενικευμένης SDN αρχιτεκτονικής. Περιλαμβάνει τα επίπεδα εφαρμογής, ελέγχου και υποδομής, καθώς και τις διεπαφές μεταξύ τους. Τα southbound και northbound APIs.

### 3.1.1 Πλεονεκτήματα των αρχιτεκτονικών του SDN

Οι SDN αρχιτεκτονικές παρουσιάζουν συγκριτικά πλεονεκτήματα συγκριτικά με τις υπάρχουσες παραδοσιακές αρχιτεκτονικές, αφού είναι:

- Προγραμματιζόμενες άμεσα: Το SDN επιτρέπει στους διαχειριστές δικτύου να διαχειριστούν ή ακόμα και να βελτιστοποιήσουν το δίκτυο πολύ γρήγορα μέσω δυναμικών και αυτόματων SDN προγραμμάτων, τα οποία μπορεί να γράψουν, διότι τα προγράμματα, που εκτελούνται δεν εξαρτώνται από υλικό.
- Ευέλικτες: Ο διαχωρισμός ανάμεσα στον έλεγχο και στην προώθηση των δεδομένων παρέχει τη δυνατότητα στους διαχειριστές δικτύου να διαχειρίζονται τη κίνηση δυναμικά, ώστε να είναι δυνατό να αλλάξει και να ανατεθεί στις ανάγκες, που δημιουργούνται.
- Δημιουργούν ένα κεντρικά διαχειρίσιμο δίκτυο: Η ευφυΐα του δικτύου βρίσκεται σε ελεγκτές SDN βασιζόμενους σε λογισμικό, οι οποίοι διατηρούν μία καθολική οπτική του δικτύου.

- Βασίζονται σε ανοιχτά λογισμικά και είναι ουδέτερα σε σχέση με αντίστοιχα εμπορικά προγράμματα: Όταν υλοποιηθούν μέσω ανοιχτών πρωτοτύπων είναι δυνατό να απλοποιηθεί ο σχεδιασμός και η λειτουργία, διότι οι οδηγίες, ειδικά σε σχέση με τους παραδοσιακούς, εμπορικούς ελεγκτές.
- Χαμηλού κόστους: Η ελάττωση υλικού σηματοδοτεί τη μείωση κόστους κεφαλαίου. Άλλωστε τα SDN δίκτυα αποτελούνται από μεταγωγείς-κουτιά χωρίς μεγάλη λογική μέσα τους και κατ' επέκταση ιδιαίτερα χαμηλού κόστους. Τα κόστη λειτουργίας μειώνονται αν δεν υπάρχει υλικό, τα κόστη για την καταναλισκόμενη ενέργεια και συντήρηση ελαττώνονται, αφού εμπίπτουν σε κόστη, που σχετίζονται μόνο με τη συντήρηση του λογισμικού.
- Επιτρέπουν την καινοτομία: Όπως γίνεται ευρέως αντιληπτό, οι ενημερώσεις του λογισμικού είναι δυνατό να γίνονται σταδιακά με σχετικά χαμηλό κόστος. Εφόσον, οι περισσότερες εφαρμογές και λειτουργικότητές τους είναι υλοποιημένες σε λογισμικό μία αλλαγή δεν αυξάνει ιδιαίτερα το κόστος.
- Εύκολα επεκτάσιμες: Το ότι υπάρχουν πολλοί μεταγωγείς χαμηλού κόστους και μπορεί να προστεθούν περισσότεροι είναι ιδιαίτερα σημαντικό και σηματοδοτεί ότι απλά με τη διασύνδεση του στο επίπεδο του ελεγκτή είναι δυνατό να εξακολουθήσει να λειτουργεί ομαλά το δίκτυο.

### 3.1.2 Απαιτήσεις και προκλήσεις σχετικά με το SDN

Εκτός από τα συγκριτικά πλεονεκτήματα, που σαφέστατα εμφανίζει το SDN υπάρχει ένα μεγάλο πλήθος προκλήσεων και απαιτήσεων, που πρέπει να ξεπεραστούν με βασικό στόχο την ευρεία υιοθέτηση της συγκεκριμένης τεχνολογικής πρότασης. Οι πιο σημαντικές συνοψίζονται παρακάτω:

- Απαιτείται προτυποποίηση των διεπαφών, που σχετίζονται με τον έλεγχο και τα δεδομένα. Είναι σημαντικό να αναπτυχθεί πρότυπο, που να περιγράφει πως πρέπει να δομούνται οι διεπαφές και να θέτει ακριβείς προδιαγραφές.
- Είναι απαραίτητο να υπάρχει προστασία σε ό,τι αναφορά τις εμπορικές εκδόσεις του SDN.
- Χρειάζονται μέτρα για να αποφεύγεται η μείωση της απόδοσης.

- Πρέπει να δημιουργηθούν πολιτικές ελέγχου των δεδομένων, ώστε να μπορούν να αξιοποιηθούν καταλλήλως αν χρειάζεται σε συγκεκριμένο χώρο ή χρόνο κάποια τροποποίηση ή δυναμική διαχείριση του δικτύου.
- Χρειάζεται να εξασφαλιστεί η αδιάκοπη συνδεσιμότητα και η ταχεία ανάκτηση σε περίπτωση σημαντικού προβλήματος.
- Είναι απαραίτητη η δημιουργία πολιτικών ασφαλείας σχετικά με τα κινητά δίκτυα.
- Είναι ιδιαίτερα σημαντικό να επιτυγχάνεται η υποστήριξη ετερογενών τεχνολογιών και συσκευών.
- Είναι υψίστης σημασίας αν ο ελεγκτής μπορεί να περιλαμβάνει μηνύματα, τα οποία να ειδοποιούν για υψηλή πτώση της απόδοσης, δηλαδή αν τα επίπεδα απώλειας πακέτων είναι ασυνήθιστα υψηλά.
- Επίσης, πρέπει να αναπτυχθούν τα πρότυπα διαχωρισμού των δικτυακών ροών δεδομένων.
- Να αναπτυχθούν εμπορικές υπηρεσίες για την εξασφάλιση κερδών από το SDN.
- Καλλιεργείται η αντίληψη για την εμπιστοσύνη στο λογισμικό, εφόσον θα μετατραπούν οι περισσότερες συσκευές υλικού σε εφαρμογές λογισμικού.
- Το υλικό πρέπει να αντικατασταθεί από το αντίστοιχο πιο απλό υλικό το οποίο θα υπάρχει στα SDN δίκτυα.
- Χρειάζεται να προωθηθεί η είσοδος του SDN στην αγορά και να σημειώνονται λιγότεροι κίνδυνοι υλοποίησης.

### 3.1.3 Ιστορική επισκόπηση του SDN

Η απαρχή του SDN σημειώθηκε αμέσως μετά την έκδοση της Java, που είναι μία γλώσσα αντικειμενοστραφούς προγραμματισμού, που εκδόθηκε από τη Sun το 1995. Το πρώτο SDN πρότζεκτ σημειώθηκε από την AT&T και λέγεται «GeoPlex». Το εν λόγω πρότζεκτ εισάγει την ιδέα ότι οι δικτυακές εφαρμογές (APIs) και ο δυναμικός χαρακτήρας της Java προσφέρονται για τη μετάβαση από τα συμβατικά δίκτυα σε αυτά, που ασχολούνται με τη διασύνδεση του επιπέδου του λειτουργικού συστήματος με το επίπεδο των εφαρμογών. Τελικά, το συγκεκριμένο πρότζεκτ οδήγησε σε μία πλατφόρμα, η οποία ήταν δυνατό να



διαχειρίζεται το δίκτυο και διάφορες εφαρμογές πραγματικού χρόνου. Δεν ήταν λειτουργικό σύστημα και ούτε μπορούσε εύκολα να γίνει ανταγωνιστική πρόταση συγκριτικά με τα κλασικά λειτουργικά συστήματα. Βασικό του χαρακτηριστικό είναι μία διεπαφή χρήσης ενός ή περισσότερων λειτουργικών συστημάτων, που τρέχουν σε υπολογιστές, οι οποίοι απλά συνδέονται στο διαδίκτυο. Κύρια λειτουργικότητά του ήταν ότι περιλάμβανε περιγραφή σε χάρτη για όλες τις δραστηριότητες, που σημειώνονταν στο διαδίκτυο.

Εν συνεχεία, το συγκεκριμένο πρότυπο δεν ικανοποιούσε την εταιρεία, η οποία σταδιακά στράφηκε στο Operations Support System (OSS), το οποίο προσέδιδε νέες υπηρεσίες και παρείχε νέα λειτουργικότητα στους υπάρχοντες μεταγωγείς. Όμως, η υπάρχουσα δομή του «GeoPlex» δεν ήταν δυνατό να προσδίδει αυτές τις τροποποιήσεις. Συνεπώς, το ζήτημα των λειτουργικών συστημάτων αποτελούσε τροχοπέδη στα πρώιμα στάδια του SDN.

Το WebSprocket δημιουργήθηκε και χρηματοδοτήθηκε ως νεοφυής επιχείρηση το 1998 από τη Sun Microsystems και τη Javasoft. Η συγκεκριμένη προσπάθεια περιλάμβανε ένα νέο λειτουργικό σύστημα και ένα μοντέλο με μία δομή, που έτρεχε σε πραγματικό χρόνο. Μέσω αυτής της προσέγγισης, καθώς και των διαφόρων εφαρμογών, που είναι δυνατό να γραφτούν με βάση τη Java, το WebSprocket κληρονομούσε κέλυφος, δίκτυο και κλάσεις συσκευής. Αργότερα, τροποποιήθηκε με έναν ειδικό μεταγλωττιστή δικτύου. Η πλατφόρμα επέτρεπε να δημιουργούνται διάφορα στιγμιότυπα από δικτυακές στοιβάδες, διεπαφές, πρωτόκολλα ως πολλαπλά νήματα.

Το 2000 άρχισαν να σημειώνονται σημαντικές προσπάθειες όσον αφορά στη δημιουργία του πρώτου εμπορικού μεταγωγέα βασισμένο σε λογισμικό. Άλλες σημαντικές καινοτομίες της περιόδου είναι η επέκταση σε περιορισμένες όμως εκδόσεις άλλων πρωτοκόλλων και υπηρεσιών, όπως για παράδειγμα τα Transmission Control Protocol (TCP) και User Datagram Protocol (UDP). Την ίδια εποχή αναγνωρίστηκε και η ανάγκη για προγραμματιζόμενα δίκτυα, ενώ αναγνωρίστηκε πως αυτά θα αποτελούν τη μεγάλη εξέλιξη στον τομέα του Διαδικτύου. Το επόμενο, που κυκλοφόρησε το 2000 γνωστό ως «Supranet» αποτελεί ουσιαστικά προπομπό του γνωστού Internet of Things (IoT). Ταυτόχρονα τον Οκτώβριο του 2000 το Gartner Group επέλεξε το «WebSprocket» ως την κορυφαία αναδυόμενη τεχνολογική πρόταση στον κόσμο.

Το 2001 η Ericson μαζί με το «WebSprocket» κατοχύρωσαν την άδεια να δημιουργήσουν τον πρώτο εμπορικό μεταγωγέα λογισμικού. Η μεγάλη εξέλιξη και γρήγορη δημιουργία της στοιβάδας ελέγχου κλήσεων κατέστησε το Supranet τη βασική τεχνολογία για

την επικοινωνία και διανομή δικτυακών υπηρεσιών. Το πρώτο πείραμα SDN πραγματοποιήθηκε στο Οχάιο των Ηνωμένων Πολιτειών και αποτελούσε μία μελέτη περίπτωσης του Internet 2 πρωτοκόλλου.

Υπήρξε μία σχετική κάμψη στον τομέα μέχρι το 2003, που ανακαλύφθηκε η εφαρμογή Content Delivery Control Network και κατοχυρώθηκε με ειδική πατέντα. Έπειτα, άρχισαν να ενσωματώνονται τέτοιου είδους τεχνικές σε διάφορα συστήματα με σκοπό τον έλεγχο διαφόρων δικτυακών στοιχείων, όπως για παράδειγμα εξυπηρετητές περιεχομένου, δρομολογητές, μεταγωγείς, πύλες με βασικό στόχο την προσπάθεια προστασίας από υποκλοπές και κλοπές περιεχομένου, ή από την ανεπιθύμητη παρεμβολή και εισροή στο σύστημα από χρήστες μη εξουσιοδοτημένους κυρίως από ομότιμους χρήστες. Μία άλλη εφαρμογή, που χρησιμοποιούταν ως το 2007 ήταν η μεταφορά περιεχομένου για υπηρεσίες με πληρωμή. Το SDN, όπως είναι σήμερα γνωστό άρχισε να εισάγεται το 2007. Προσπάθειες σημειώθηκαν στο Berkeley και στο Stanford. Ο ONF είναι ένας οργανισμός, ο οποίος ιδρύθηκε το 2011 με βασικό στόχο να προωθήσει το SDN και να προτυποποιήσει το OpenFlow πρωτόκολλο.

### 3.2 Network Functions Virtualization (NFV)

Η τεχνική του NFV είναι πολύ σημαντική για τα ασύρματα δίκτυα. Είναι δυνατό διάφορες δικτυακές λειτουργίες να πραγματοποιούνται σε υλικό γενικού σκοπού, όπως για παράδειγμα οι απλοί μεταγωγείς δικτύου, οι οποίοι μετά από την εισαγωγή NFV λειτουργούν ως δρομολογητές, δηλαδή ανωτέρου επιπέδου συσκευές. Ένα άλλο παράδειγμα είναι ότι θα μπορούσαν να αντικατασταθούν τα τείχη προστασίας (firewalls) ή ακόμα και άλλες συσκευές. Οι συσκευές αυτές πλέον φιλοξενούνται σε εικονικές μηχανές (Virtual Machines VMs). Μία σημαντική εφαρμογή είναι η εφαρμογή του NFV σε λειτουργίες όπως η Network Address Translation (NAT) και Domain Name Services (DNS), που αποτελούν πρωτόκολλα αντιστοίχισης IP διευθύνσεων σε ονόματα διευθύνσεων στο διαδίκτυο [48].

Οι λειτουργικότητες αυτές δίνουν τη δυνατότητα να μην απαιτείται εξειδικευμένο υλικό για κάθε λειτουργία με σκοπό να δομηθεί μία αλυσίδα υπηρεσιών. Το λογισμικό μπορεί να ενσωματώνει τη λειτουργία ή τη χωρητικότητα του εξυπηρετητή. Κάτι τέτοιο σημαίνει την μείωση του κόστους κεφαλαίου, αλλά και του λειτουργικού κόστους. Ακόμα, μπορεί για παράδειγμα να αποδοθεί και εικονικό εύρος ζώνης σε κάποιο τμήμα του απατώντας με έναν πιο ευέλικτο τρόπο στις ανάγκες, που εγείρονται στο δίκτυο. Συνεπώς, γίνεται κατανοητό ότι

είναι μία τεχνολογία σχεδιασμένη να απομονώνει και να διανέμει δικτυακούς πόρους και δικτυακά συστατικά με σκοπό την δημιουργία μία πλήρως εικονικής υποδομής.

Το NFV είναι διαφορετικό από το SDN, αλλά είναι συμπληρωματικό με αυτό. Είναι σημαντικό να συνδυάζονται και να προσδίδουν ουσιαστικά σε μία αρχιτεκτονική τα βασικά τους πλεονεκτήματα. Μία σημαντική δυνατότητα, που παρέχεται από το NFV είναι ότι είναι δυνατό να προκύψουν σημαντικά οικονομικά οφέλη για νέες υπηρεσίες, οι οποίες δημοσιεύονται σε λιγότερο χρόνο.

### 3.2.1 Πλεονεκτήματα του NFV

Το NFV προσδίδει σημαντικά πλεονεκτήματα, εισάγει νέες τεχνικές αντιμετώπισης ζητημάτων περισσότερο λογισμικό-κεντρικές, μειώνει το μεγάλο κόστος το οποίο εισάγεται για την εξασφάλιση του συγκεκριμένου δικτυακού εξοπλισμού. Από την άλλη μεριά, είναι δυνατό να απλοποιηθούν διάφορες διαδικασίες, αφού το λογισμικό είναι πιο εύκολα «διαχειρίσιμο» σε θέματα βλαβών και η ανάκαμψη ενός συστήματος είναι πιο γρήγορη [62], [63], [64], [65]. Συνοπτικά τα πιο βασικά οφέλη, που παρουσιάζει το NFV είναι:

- Μείωση του κόστους κεφαλαίου. Καθίσταται σαφές ότι μειώνονται οι επιχειρηματικοί κίνδυνοι, που μπορούν να προκύψουν από την επένδυση και τη συντήρηση σε υλικό.
- Μείωση του λειτουργικού κόστους. Βασικό είναι ότι αρχικά μειώνεται η ενέργεια λόγω του λιγότερου ρεύματος, που καταναλώνεται από τις συσκευές, αλλά και από την ψύξη, που απαιτείται για πληθώρα συσκευών σε έναν χώρο.
- Μείωση του χώρου. Ένα άλλο πρακτικό ζήτημα, αλλά εξίσου βασικό είναι η μείωση του χώρου της υποδομής. Συχνά, είναι σημαντικό το γεγονός ότι απαιτείται πολύς χώρος για την υποδομή, που σημαίνει εξοικονόμηση χώρου και εξοικονόμηση χρήματος.
- Γρηγορότερη κυκλοφορία στην αγορά. Είναι σημαντικό ότι εμφανίζονται γρηγορότερα νέες υπηρεσίες ή μετεξελίξεις των ήδη υπαρχουσών υπηρεσιών. Αυτό συμβαίνει ιδίως, διότι παρουσιάζονται διάφορες ευκαιρίες για επένδυση.
- Ευελιξία. Η ευελιξία γίνεται αμέσως κατανοητή λόγω του λογισμικού, αλλά και λόγω της ευκολίας μετακίνησης ή τοποθέτησης λειτουργικού τμήματος σε συγκεκριμένο σημείο.

- Επεκτασιμότητα. Η επεκτασιμότητα είναι ένα βασικό πλεονέκτημα, διότι μπορούν να τοποθετηθούν περισσότερες λειτουργικότητες σε περισσότερα σημεία.

Για αυτές και για ακόμα περισσότερες σημαντικές συμβολές του NFV στη νέα τεχνολογική πραγματικότητα αναμένεται ότι θα ενσωματωθεί όχι μόνο δίνοντας τα σημαντικά πλεονεκτήματα στο SDN [62], [63], [64], [65]. Τέλος, είναι σημαντικό να τονιστεί ότι είναι δυνατό να συνυπάρχουν οι εικονικές με μη εικονικές υπηρεσίες.

### 3.2.2 Απαιτήσεις και προκλήσεις σχετικά με το NFV

Η ευρεία υιοθέτηση της τεχνολογίας, που σχετίζεται με το NFV απαιτεί να ληφθούν συγκεκριμένα μέτρα, ώστε να επιλυθούν οι σημαντικότερες προκλήσεις, που σχετίζονται με τη συγκεκριμένη τεχνολογία. Η απάντηση και επίλυση των προβλημάτων αναμένεται να οδηγήσει στην υιοθέτηση και συνεργασία του NFV όχι μόνο με SDN, αλλά και με διάφορες άλλες σημαντικές τεχνολογίες [62], [63], [64], [65].

Αρχικά, είναι σημαντικό να υπάρχει αένας έλεγχος και να λαμβάνονται υπόψη ορισμένες σημαντικές όψεις. Μόλις, για κάποιο λόγο φαίνεται ότι το δίκτυο συγχρωτίζεται σημαντικά, θα πρέπει να εισάγονται επιπρόσθετες πηγές, που να παρέχουν τη δυνατότητα να επιλύεται το εν λόγω πρόβλημα. Είναι υψίστης σημασίας να αναπτυχθούν τεχνικές αξιοποίησης της πληροφορίας, που προκύπτει λόγω των εικονικών δεδομένων και η εύρεση αποδοτικού τρόπου αξιοποίησης του μεγάλου όγκου δεδομένων. Όσον αφορά στη δημιουργία πολιτικών επέκτασης δικτύου απαιτείται να σημειωθούν και να πραγματοποιηθούν ενέργειες σχετικές με το ζήτημα αυτό.

Είναι σημαντικό να επιτυγχάνεται μεγάλη αξιοπιστία των δικτύων. Αυτό είναι δυνατό να συμβεί από τη μεγάλη πολυπλοκότητα των συσκευών και τεχνολογιών, που θα εμφανίζονται στο 5G. Πρέπει να σημειωθούν εικονικά τερματικά, τα οποία όμως να εξασφαλίζεται ότι είναι εξίσου αξιόπιστα με τα αντίστοιχα συμβατικά. Είναι σημαντικό να εξασφαλιστούν όποια κενά ασφαλείας ειδικά, όσα προκύπτουν με γνώμονα τη χρήση του ίδιου φυσικού μέσου. Ένα θεμελιώδες ζήτημα προκύπτει με βάση την επεκτασιμότητα. Απαιτείται να είναι εύκολο να επεκταθούν οι συσκευές σε εικονικές, τα δίκτυα και οι υποδομές. Επίσης, είναι σημαντικό να επιταχυνθεί η υλοποίηση εφαρμογών βασιζόμενων σε λογισμικό χωρίς να παρουσιάζονται τα ίδια υψηλά κόστη, τα οποία προκύπτουν όταν χρησιμοποιείται υλικό.

Τελευταίο, αλλά όχι λιγότερο σημαντικό είναι το να μειωθεί το κόστος. Επίσης, πρέπει να ελαττωθούν τα σημαντικά λειτουργικά κόστη, υπάρχει μικρός κύκλος ζωής των εργαλείων και άρα απαιτούνται νέα, που επιβαρύνουν το κόστος της συνολικής υποδομής σε τακτά χρονικά διαστήματα.

### 3.2.3 Ιστορική επισκόπηση του NFV

Η βασική ιδέα προέκυψε από παρόχους υπηρεσίας, οι οποίοι κατέβαλαν προσπάθεια να επιταχύνουν τη διαδικασία της υλοποίησης νέων υπηρεσιών με βασικό στόχο να υποστηριχθεί το εισόδημα, καθώς και με αντικειμενικό στόχο την ανάπτυξη. Το υλικό εισάγει περιορισμούς. Με βασικό στόχο την επιτάχυνση της καινοτομίας δημιουργήθηκε ο ETSI. Ο συγκεκριμένος οργανισμός κατέβαλε σημαντικές προσπάθειες στην προτυποποίηση και εξέλιξη της συγκεκριμένης τεχνολογίας. Σκιαγραφήθηκαν οι απαιτήσεις για βασικές δικτυακές λειτουργικότητες, όπως για παράδειγμα είναι το NFV MANO. Επίσης, είναι σημαντικό, διότι λειτουργεί σε συνεργατικά προγράμματα, όπως το OPNFV.

Τον Οκτώβριο του 2012 μία συγκεκριμένη ομάδα πραγματοποίησε και εξέδωσε το NFV. Από τότε υπάρχουν περισσότερες καινοτομίες και πρόοδοι, όπως είναι για παράδειγμα η υλοποίηση, καθώς και διάφορες περιπτώσεις χρήσης, οι οποίες σχετίζονται για τους πωλητές και τους τηλεπικοινωνιακούς παρόχους.

## 3.3 Radio Access Network (RAN)

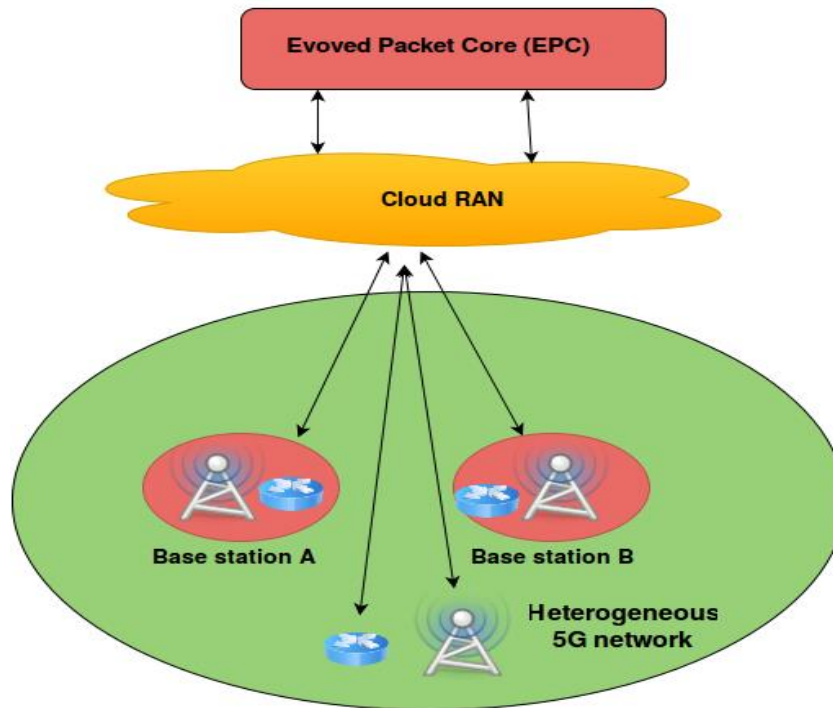
Το Radio Access Network είναι τμήμα ενός τηλεπικοινωνιακού συστήματος. Είναι δυνατό να υπάρχει μεταξύ μίας συσκευής, όπως ένα κινητό τηλέφωνο, ή υπολογιστή ή οποιαδήποτε άλλη συσκευή εκ του μακρόθεν ελεγχόμενη. Εξαρτάται βέβαια από το πρότυπο, το κινητό τηλέφωνο και άλλες ασύρματες συσκευές διαφέρουν σημαντικά ως εξοπλισμός χρήστη, εξοπλισμός τερματικού, κινητός σταθμός βάσης κλπ. Η λειτουργικότητα του RAN παρέχεται από ένα τσιπάκι πυριτίου [46]. Υπάρχουν πολλά είδη RAN δικτύων, τα οποία είναι τα εξής:

- GSM RAN (GRAN): το οποίο είναι το Global System Mobile Communication (GSM) RAN, το οποίο είναι τα δίκτυα δεύτερης γενιάς.

- GSM EDGE RAN (GERAN), το οποίο είναι σχεδόν το ίδιο με το GRAN με τη διαφορά ότι υπάρχουν διάφορα πακέτα με Enhanced Data for GSM Evolution (EDGE) υπηρεσίες είναι δίκτυα περισσότερο εξελιγμένα από τα αρχικά δίκτυα 2<sup>ης</sup> γενιάς, εντούτοις, όμως, δεν είναι τόσο ικανοποιητικά όσο αυτά της 3<sup>ης</sup> γενιάς.
- UMTS RAN (UTRAN): πρόκειται για ένα UMTS RAN, δηλαδή δίκτυα 3<sup>ης</sup> γενιάς κινητής τηλεπικοινωνίας.
- E-UTRAN, που είναι LTE RAN σχετίζεται με τα δίκτυα 4<sup>ης</sup> γενιάς κινητής τηλεπικοινωνίας.

Επίσης, είναι πιθανό μία συσκευή να είναι συνδεδεμένη σε περισσότερες τεχνολογίες, χωρίς προβλήματα. Οι περισσότερες νέες τεχνολογίες είναι προς τα πίσω συμβατές (backwards compatibility). Τα ζητήματα προκύπτουν σε άλλους τύπους επικοινωνίας, όπως είναι τα πολυμεσικά δεδομένα ή η συνδεσιμότητα στο διαδίκτυο, που σε πρώιμες μορφές δεν είναι διαθέσιμες ή τα επίπεδα των δικτυακών δεδομένων είναι χαμηλά και δεν μπορούν να καλύψουν τη συνδεσιμότητα. Είναι δυνατό να αναπτυχτούν τεχνικές ενσωμάτωσης της λειτουργικότητας των SDN και NFV στο RAN. Τα σημαντικότερα ζητήματα, που αναμένεται να επιλυθούν είναι τα εξής:

- Αξιοποίηση δικτυακών πόρων
- Handovers
- Αξιοποίηση εύρους ζώνης κάθε κυψέλης για κυψελωτά δίκτυα
- Εξοικονόμηση ενέργειας.
- Διαχείριση του δικτύου.
- Επεκτασιμότητα και ευελιξία



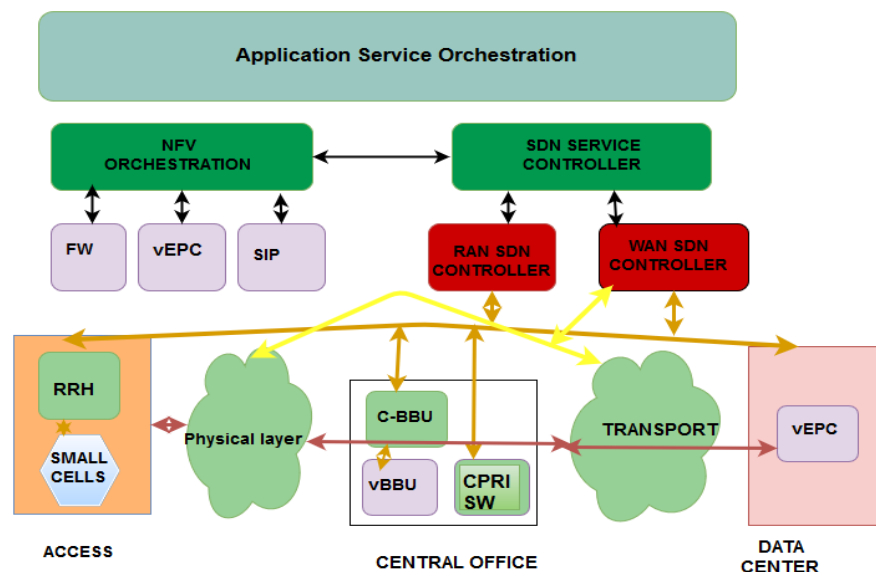
Εικόνα 3.2: Μία στοιχειώδης RAN αρχιτεκτονική. Φαίνεται η πρόταση για RAN βασιζόμενο σε Cloud τεχνικές, όπως είναι το SDN και το NFV.

Το RAN αποτελείται από πολλά μικρότερα συστατικά στοιχεία, τα οποία το συνθέτουν και συντελούν στην αναπόσπαστη λειτουργία του. Αυτά τα συστατικά συνοψίζονται παρακάτω:

- **Firmware (FW)** είναι το τμήμα λογισμικού, που υποδεικνύει τρόπους, σύμφωνα με τους οποίους το υλικό επικοινωνεί με τις συσκευές. Υπάρχει σύνολο εντολών το οποίο προκύπτει και σηματοδοτεί το συγκεκριμένο ζήτημα.
- **Orchestration** είναι το τμήμα, που ουσιαστικά ενορχηστρώνει το NFV. Το NFV είναι σημαντικό και εισάγει τη δικτυακή λειτουργικότητα.
- **Session Initiation Protocol (SIP)** αποτελεί πρωτόκολλο επικοινωνίας δικτύων υπολογιστών και έχει εφαρμογή μέσω διαδικτύου ή μέσω ενός τοπικού δικτύου.
- **Controller** είναι ο ελεγκτής δικτύου. Υπάρχουν πολλά είδη ελεγκτών δικτύου, οι οποίοι εμφανίζονται στο δίκτυο. Επίσης, μπορεί να υπάρχουν ελεγκτές υλικού, ελεγκτές λογισμικού κλπ.

- **Remote Radio Head (RRH)** αποτελείται από έναν αποδέκτη και αποστολέα, που συνδέεται με τον πίνακα ελέγχου του παρόχου δια μέσου ηλεκτρικής ή ασύρματης υποδομής.
- **Cellular Base Band Unit (cBBU)** είναι το διαθέσιμο εύρος ζώνης και περιγράφει πως αυτό είναι δυνατό να διανεμηθεί. Αυτό μπορεί να είναι εικονικό ή να εισαχθεί σε αυτό εικονική λογική διαχείρισης και τότε είναι virtual BBU (vBBU).
- **Shortwave SW** είναι συσκευές, που επιτελούν μετάδοση σε ζώνες μικρού κύματος, όπως οι ζώνες από 1.6 μέχρι 30 MHz.
- **Common Public Radio Interface (CPRI)** αποτελεί επιτυχή είσοδο στη συνεργασία με τη βιομηχανική ανάπτυξη.

Τα πιο πολλά από αυτά τα συστατικά είναι δυνατόν να ενσωματώνουν cloud τεχνικές με αποτέλεσμα να αντικαθίστανται από αντίστοιχες εφαρμογές λογισμικού. Το RAN επικοινωνεί με το EPC, το οποίο εξίσου μπορεί να είναι εικονικό (virtual) και άρα να εξοικονομούνται πολλές σημαντικές ενέργειες, υποδομές, κόστος κλπ.



Εικόνα 3.3: Ανάλυση πλήρους αρχιτεκτονικής RAN, ειδικά μετά τη χρήση SDN.

### 3.4 Central Office Re-Architected as a Data Center (CORD)

Το CORD έχει κύριο στόχο να φέρει τα πλεονεκτήματα ενός κέντρου δεδομένων και τις ευκολίες, που παρέχονται από τα σύννεφα στους παρόχους τηλεπικοινωνιακών υπηρεσιών. Τα μητροπολιτικά δίκτυα σχεδιάζονται βασιζόμενα σε τρεις συγκεκριμένες προσεγγίσεις [46],



[47], [48], [49]. Τα πάντα σαν υπηρεσία γνωστό και ως Everything as a Service (EaaS) περιλαμβάνουν περισσότερες υπηρεσίες μερικές από τις οποίες είναι οι ακόλουθες:

- Πρόσβαση ως Υπηρεσία- Access as a Service (AaaS), το οποίο περιλαμβάνει την πρόσβαση σε άλλες υπηρεσίες.
- Υπηρεσία ως συνδρομητή- Subscriber as a Service (SaaS), το οποίο περιλαμβάνει διάφορες υπηρεσίες, που είναι δυνατό να παρέχονται σε έναν συνδρομητή.
- Το διαδίκτυο ως υπηρεσία ή Internet as a Service (IaaS), στο οποίο το σύννεφο παρέχει δυνατότητες δικτύωσης.
- Η διανομή περιεχομένου του διαδικτύου ως υπηρεσία CDNaaS.

Η πιο σημαντική του λειτουργία είναι ότι παρέχει τη δυνατότητα επέκτασης σε εικονικές υπηρεσίες. Επίσης, παρέχει οπτική ίνα ως υπηρεσία, κυρίως ως το σπίτι Fiber-To-The-Home (FTTH), το οποίο βασίζεται στο Λογισμικό ως Υπηρεσία Software as a Service (SaaS). Αποτελεί ένα συνδυασμό των τεχνολογιών νέφους, SDN και NFV. Η αρχιτεκτονική του CORD αποτελείται από διάφορα στοιχεία τα πιο βασικά από τα οποία παρατίθενται ακολούθως:

- Υπάρχουν διάφοροι εξυπηρετητές, που καλύπτουν τις ανάγκες, που ανακύπτουν.
- Παρέχουν μηχανισμούς αποθήκευσης.
- Παρέχουν ψηφιακές εισόδους και εξόδους.
- Παρέχουν Switches 48 θυρών, τα οποία είναι Whitebox Switces.
- Παρέχει πυρήνες ROADMs.
- Πρόσβαση σε Gigabit Ethernet Passive Optical Network (GPON).
- Ίνα, που δομείται σε μία δεντρική μορφή τριών επιπέδων (Πυρήνα, συσσωμάτωση, tore switches).
- Υπάρχουν μεγάλοι εξυπηρετητές, που για να εξυπηρετήσουν μεγάλες υποδομές, δομούνται σε TORE.
- Τα φύλλα των switches συνδέονται σε όλες τις ράχες του δικτύου.

Η μεγάλη σημασία του CORD είναι ότι παρέχει υπηρεσίες από άκρο σε άκρο για SDN-NFV. Επίσης, είναι δυνατό να συμβάλει δυναμικά στη μείωση του κόστους είτε του λειτουργικού κόστους, λόγω του χαμηλότερου κόστους συντήρησης λογισμικού στο νέφος. Επίσης, μειώνεται το κόστος κεφαλαίου, το οποίο σχετίζεται με τη μείωση του υλικού και της μικρότερης επένδυσης σε αυτό. Λόγω του σύννεφου είναι δυνατό οι νέες υπηρεσίες, που

παρέχονται να έρχονται στην αγορά ακόμα πιο γρήγορα. Προστίθεται τέλος υπεραξίας στις υπηρεσίες, που σχετίζονται με το νέφος και άρα εμφανίζονται νέες λειτουργικότητες. Τα βασικά τμήματα ενός CORD συστήματος παρατίθενται παρακάτω:

- Υλικό
- ONOS- ελεγκτής δικτύου
- Διαχείριση εικονικών υπηρεσιών (XOS, Openstack)
- Εικονικές συναρτήσεις και λειτουργίες του δικτύου. Εικονική πρόσβαση σε PON.
- Ανοιχτό φύλλο στη σπονδυλική στήλη της οπτικής ίνας.

Για να οδεύσει κανείς στη μαζική μετάβαση προς το CORD απαιτείται η μετάβαση σε εικονικές έναντι σε συσκευές υλικού. Επίσης, στην μετατροπή των συναρτήσεων και των δικτυακών λειτουργιών σε εικονικές. Τέλος, είναι πολύ σημαντικό να μπορέσει το υλικό, που υπάρχει σήμερα πρέπει να μεταλλαχτεί σε λογισμικό [46], [47], [48], [49].

### 3.5 OpenStack

Μία τεχνολογία εφάμιλλη αυτής του CORD είναι η τεχνολογία OpenStack. Το OpenStack αποτελεί ένα λειτουργικό σύστημα σύννεφου, το οποίο είναι δυνατό να ελέγχει σημαντικό τμήμα υπολογιστικών πόρων, όπως μεγάλου όγκου υπολογισμούς, διαχείριση του αποθηκευτικού χώρου και δικτυακές πηγές μέσω ενός κέντρου δεδομένων. Όλα αυτά διαχειρίζονται μέσω δικτύου και μέσω μίας ειδικά διαμορφωμένης πλατφόρμας. Το γεγονός προσφέρει στο διαχειριστή διαδικτύου πλήρεις δυνατότητες ελέγχου, καθώς και την κατάλληλη αξιοποίηση όλων των πόρων μέσα σε μία διεπαφή [71].

Το OpenStack διατίθεται δωρεάν. Παρέχει μία πλατφόρμα για υπολογιστική μέσω σύννεφου και υλοποιείται ως υποδομή σε μία υπηρεσία (Infrastructure As A Service-IaaS). Η πλατφόρμα λογισμικού αποτελείται από διασυνδεδεμένα συστατικά στοιχεία, που ελέγχουν τις υποδομές υλικού επεξεργασίας, αποθήκευσης και δικτύωσης μέσω ενός κέντρου δεδομένων. Οι χρήστες είτε επιτυγχάνουν τον έλεγχο μέσω μίας πλατφόρμας διαδικτύου, μέσω εργαλείων γραμμής εντολών ή μέσω μίας εφαρμογής.

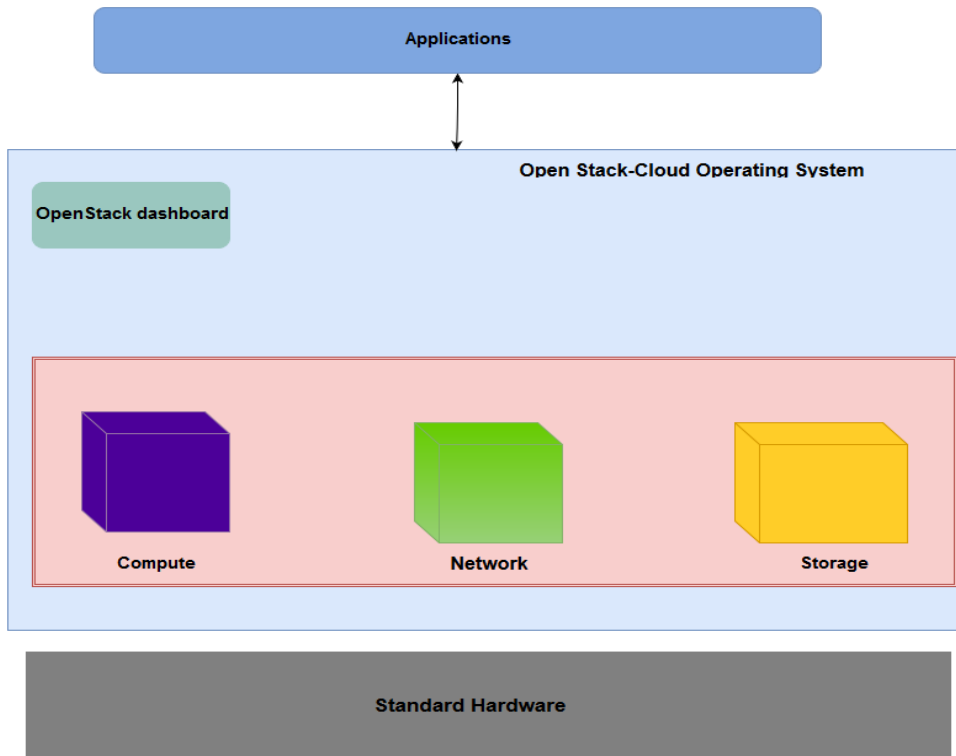
Υπάρχουν πολλά συστατικά στοιχεία από τα οποία αποτελείται το OpenStack. Τα πιο σημαντικά από τα οποία παρατίθενται ακολούθως, μαζί με τον τομέα στον οποίο αυτά εμφανίζονται:

- **Nova**, που καλύπτει τον τομέα των υπολογισμών και είναι IaaS.

- **Neutron**, που σχετίζεται με τη δικτύωση και διαχειρίζεται το δίκτυο και τις διευθύνσεις IP. Παλιότερα ήταν γνωστό και ως **Quantum**.
- **Cinder**, που σχετίζεται με την αποθήκευση μπλοκ πληροφορίας.
- **Keystone**, που σχετίζεται με την ταυτοποίηση και την αυθεντικοποίηση των χρηστών σε ένα οποιοδήποτε σύστημα.
- **Glance**, που σχετίζεται με τις εικόνες και παρέχει με την ανακάλυψη, την εγγραφή και διάφορες άλλες υπηρεσίες.
- **Swift**, που σχετίζεται με την αποθήκευση αντικειμένων και είναι ένα αρκετά εύκολα επεκτάσιμο σύστημα.
- **Horizon**, που σχετίζεται με την πλατφόρμα των διαχειριστών και παρέχει γραφική διεπαφή και πρόσβαση στις ιδεατές πηγές.
- **Heat**, που σχετίζεται με τη διαχείριση των υπηρεσιών στο σύννεφο.
- **Mistral**, που καλύπτει την γραμμή εργασιών, εφόσον ο χρήστης έχει ήδη γράψει ένα πρόγραμμα σε μία γλώσσα γραμμής εργασιών.
- **Ceilometer**, καλύπτει τα συστήματα χρέωσης, που συμβάλουν στην παροχή διαφοροποιημένων υπηρεσιών και εξειδικευμένες πολιτικές χρέωσης.
- **Trove**, που παρέχει Βάση Δεδομένων ως Υπηρεσία (DataBase-as-a-Service-DaaS) παρέχοντας συσχετιστική και μη συσχετιστική μηχανή αναζήτησης.
- **Sahara**, είναι ένα βασικό εργαλείο, που παρέχει συστοιχίες από Hadoop, και βασική του χρήση είναι η γνωστή Elastic Map Reduce (EMR) τεχνική **IroniC**, είναι το πρότζεκτ, που καλύπτει και την υπηρεσία πραγματικού υλικού εκτός από τις εικονικές πηγές,
- **Zaqar**, επιτρέπει τα μηνύματα μίας υπηρεσίας με πολλούς Web-developers, που επιδιώκουν να επικοινωνούν γραπτά.
- **Manila**, είναι το σύστημα, το οποίο καλύπτει το διαμοιραζόμενο σύστημα αρχείων και παρέχει μία ανοιχτή εφαρμογή.
- **Designate**, παρέχει το Domain Name Space (DNS) ως υπηρεσία (DNS-as-a-Service-DNSaaS).
- **Searchlight** παρέχει υψηλές δυνατότητες αναζήτησης.

- **Barbican** είναι μία εφαρμογή σχεδιασμένη για ασφαλή αποθήκευση, σχεδιασμό και διαχείριση.

Το σύστημα OpenStack παρατίθεται στην εικόνα 3.4. Σε αυτό περιγράφονται οι διάφορες υπηρεσίες, που παρέχονται από το OpenStack. Αυτό παρέχει τον υπολογισμό, τη δικτύωση και την αποθήκευση. Το εν λόγω λειτουργικό σύστημα βασίζεται σε υλικό πραγματικό ή εικονικό και υποστηρίζει πολλές εφαρμογές.



Εικόνα 3.4: Παρατίθεται η βασικότερη αρχιτεκτονική του OpenStack.

### 3.6 Ασφάλεια στα δίκτυα SDN

Η ραγδαία ανάπτυξη της τεχνολογίας οδηγεί σταδιακά στην υιοθέτηση νεών τεχνικών και ιδεών στα δίκτυα νέας γενιάς. Η ενσωμάτωση των SDN στα ήδη επισφαλή κινητά δίκτυα επικοινωνίας δυσχεραίνει τη δυσπιστία των ρυθμιστικών παραγόντων στη νέα τεχνολογία. Η αντικατάσταση πολλών συσκευών δικτύου με εικονικές μηχανές και λογισμικό, επίσης, εγείρει σημαντικά ζητήματα σχετικά με την διασφάλιση της ασφάλειας και της εύρυθμης λειτουργίας του δικτύου. Συνεπώς, διαφαίνεται υψίστης σημασίας οι δύο νέες ιδέες και προσεγγίσεις, που αναμένεται να κυριαρχήσουν στα δίκτυα επόμενης γενιάς να προσδίδουν στον τελικό χρήστη, αλλά και στον πάροχο, που θα τις υιοθετήσει ίδια ή και περισσότερη ασφάλεια συγκριτικά με

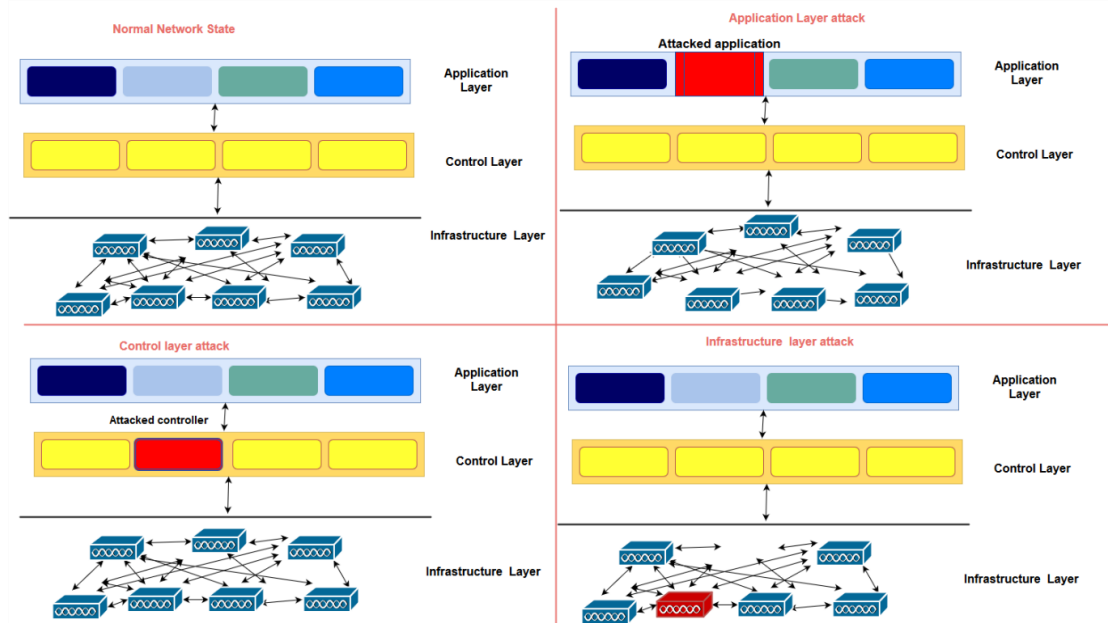
τις συμβατικές και παραδοσιακές τεχνολογίες. Η κεντρική φύση του SDN, που βασίζεται στο επίπεδο ελέγχου, το οποίο περιλαμβάνει συνολικά όλη την ευφυία του δικτύου, καθώς πραγματοποιεί τις πιο σημαντικές διαδικασίες, έρχεται σε πλήρη αντίθεση με τις αντιλήψεις, που επικρατούσαν τα προηγούμενα έτη και τάσσονταν ξεκάθαρα υπέρ των κατακεκομμένων συστημάτων, που περιλαμβάνουν πολλά διαφορετικά επίπεδα ελέγχου ή τις διεργασίες, που αποθηκεύονται σε πολλά ενδεχομένως και απομακρυσμένα μεταξύ τους μέρη.

### 3.6.1 Προκλήσεις ασφαλείας στα δίκτυα SDN

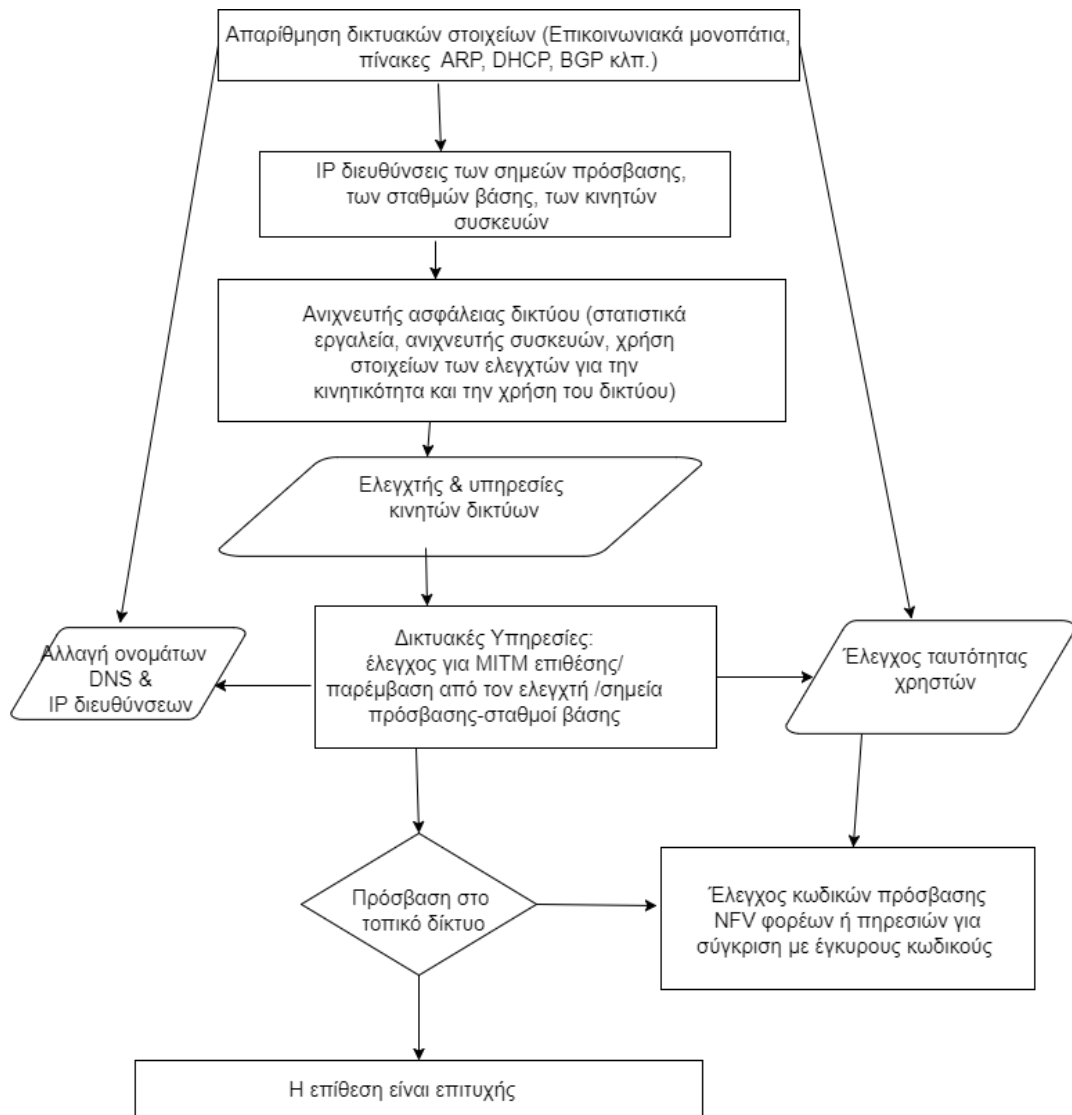
Το SDN περιλαμβάνει σημαντικά πλεονεκτήματα, εντούτοις εμφανίζει μεγάλα ποσοστά δυσπιστίας από άτομα και επιχειρήσεις, που επισημαίνουν τις πιο σημαντικές προκλήσεις, που αποτελούν τροχοπέδη. Αναλυτικά οι πιο σοβαρές απειλές, που παρατηρούνται συνοψίζονται παρακάτω:

- **Eavesdropping:** Η παρακολούθηση του δικτύου ή κάποιων συσκευών αυτού από κακόβουλες συσκευές. Αυτό το είδος επίθεσης είναι γνωστό ως eavesdropping.
- **Identity spoofing:** στην περίπτωση αυτή ένας χρήστης ή ένας υπολογιστής μπορεί να μιμηθεί μία άλλη συσκευή του δικτύου, όπως για παράδειγμα τους μεταγωγείς και έτσι να εισβάλει σε ένα τμήμα του δικτύου, στο οποίο δεν μπορεί να εισβάλει.
- **Κωδικός πρόσβασης:** Οι περισσότεροι ελεγκτές δικτύου περιλαμβάνουν ένα σύστημα αυθεντικοποίησης για κάθε υπεύθυνο.
- **MITM:** Είναι η επίθεση σύμφωνα με την οποία παρεμβάλλεται κάποιος χρήστης στη μεταξύ δύο συσκευών επικοινωνία, με αποτέλεσμα αυτή να μην είναι ανεμπόδιστη.
- **Sniffer:** Στο SDN ένας δικτυακός αναλυτής πρωτοκόλλου είναι ένα εργαλείο παρακολούθησης του δικτύου και είναι δυνατό να γίνει θύμα των επιτιθέμενων στο δίκτυο.
- **Εφαρμογές:** Υπάρχουν εφαρμογές δημόσιου και ιδιωτικού χαρακτήρα. Οι δημόσιες εφαρμογές μπορούν να υποστούν επίθεση.
- **DOS & DDOS:** Είναι ο βασικότερος τύπος επίθεσης, μιας και μπορεί να θέσει μέρος ή ολόκληρο το δίκτυο εκτός λειτουργίας.
  - στέλνουν πακέτα αδιάκοπα.
  - Ο ελεγκτής ή οι δρομολογητές δεν έχουν πλέον πίνακα δρομολόγησης ή ο πίνακας δρομολόγησης τους δε λειτουργεί.

- Τίθεται ο ελεγκτής εκτός λειτουργίας.
- **Προστασία προσωπικών Δεδομένων:** Οι περισσότερες κινητές συσκευές δεν έχουν κωδικούς πρόσβασης ενεργοποιημένους. Τα τηλεπικοινωνιακά κανάλια είναι μη ασφαλή για τα δεδομένα.
- **Προστασία του λογισμικού:** Το λογισμικό των συσκευών πρέπει να ενημερώνεται τακτικά, να διατηρείται η νεότερη έκδοση και να μην περιλαμβάνει ρυθμίσεις, που δεν παρέχονται από υπεύθυνα πηγή.



Εικόνα 3.5: Τα πιο σημαντικά είδη επιθέσεων, που μπορεί να εμφανιστούν σε κινητά δίκτυα SDN.



**Εικόνα 3.6: Η πορεία επιθέσεων, που ακολουθούν οι επιτιθέμενοι σε κινητά SDN δίκτυα.**

### 3.6.2 Προτεινόμενες Λύσεις για την ασφάλεια στα δίκτυα SDN

Η εξασφάλιση της ποιότητας και ασφάλειας τέτοιων τύπων δικτύων έχει όχι μόνο οφέλη για τη βιωσιμότητα των συστημάτων, αλλά και οικονομικές συσχετίσεις. Αναλυτικά ο ONF έχει σκιαγραφήσει πώς πρέπει να είναι ένα ασφαλές σχήμα αρχιτεκτονικό στο [76] και αναφέρει πως πρέπει να:

- Καθορίζονται οι εξαρτήσεις ασφαλείας και τα όρια εμπιστοσύνης σε ένα κινητό δίκτυο.
- Εξασφαλίζεται η ταυτότητα των σταθμών βάσης και των access points.
- Δομούνται ισχυρές πολιτικές ασφαλείας βασισόμενες σε ανοιχτά πρότυπα.

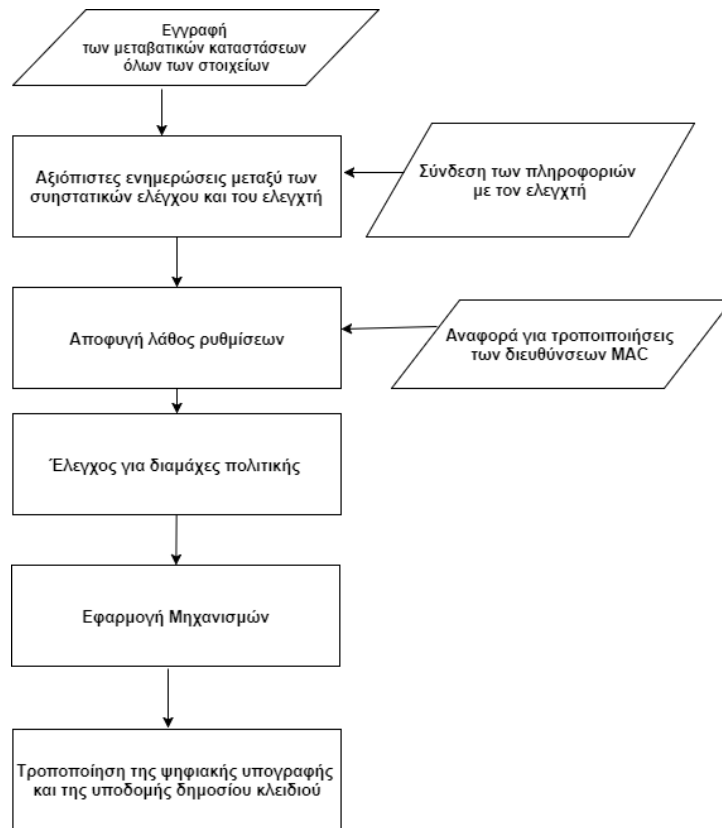
- Προστατεύονται όλα τα SDN επίπεδα: εφαρμογών, υποδομής, ελέγχου και οι διασυνδέσεις μεταξύ τους.
- Προστατεύονται τα λειτουργικά δεδομένα μεταξύ των ελεγκτών και των access points.
- Αρχικοποιείται ο σχεδιασμός συστημάτων με πρότυπα ασφάλειας.
- Παρέχεται ανιχνευσιμότητα και αναγνωρισιμότητα άγνωστων συσκευών.
- Αναλύονται οι ακριβείς ιδιότητες των διαχειρίσιμων ελέγχων ασφάλειας.

Οι βασικότερες λύσεις, που συνοψίζονται σε κινητά δίκτυα SDN, που βρίσκονται σε λειτουργία είναι οι ακόλουθες:

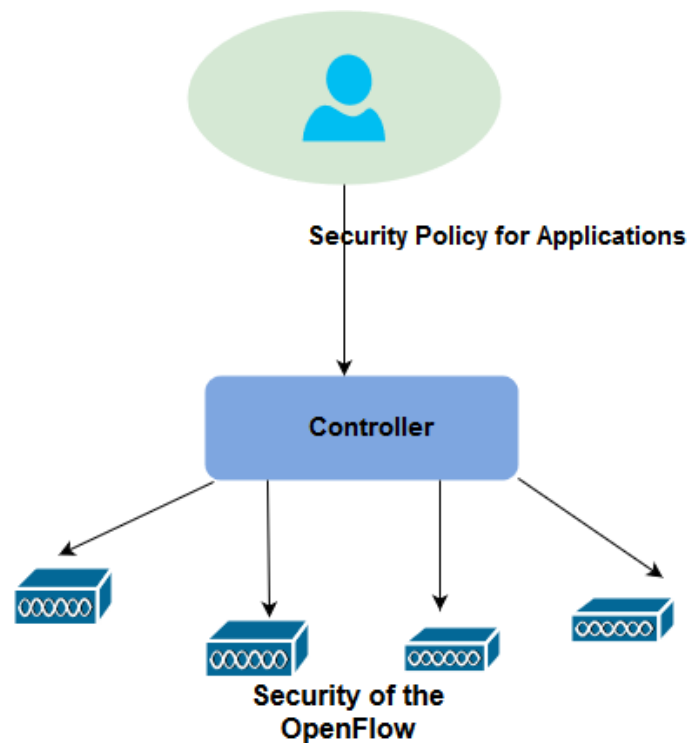
- **Γενικές κατευθύνσεις ασφάλειας:** Η πρόληψη είναι μία καλή ιδέα. Δηλαδή, οι αρχιτεκτονικές πρέπει να δομούνται σύμφωνα με το παραπάνω πρότυπο. Η ασφάλεια πρέπει να λαμβάνεται εκ των προτέρων υπόψη
- **Δημιουργία αντιγράφων ασφαλείας:** Συστήνεται να υπάρχουν συχνά αντίγραφα ασφαλείας για τον ελεγκτή.
- **Τείχη προστασίας:** Τα τείχη προστασίας πλέον δομούνται βάση εικονικών δομών της NFV τεχνολογίας, συνεπώς, βασίζονται σε λογισμικό και περιλαμβάνουν σημαντικά πλεονεκτήματα του λογισμικού.
- **Επιλογή διαχειριστικών κωδικών πρόσβασης:** Οι κωδικοί πρόσβασης πρέπει να είναι περίπλοκοι και να μην είναι δυνατό να «μαντεύονται» από κάποιον εισβολέα. Μία πιθανή λύση είναι να εισαχθούν πολλαπλά επίπεδα πιστοποίησης ενός χρήστη, που επιδιώκει να συνδεθεί στην επιφάνεια του ελεγκτή.
- **Ενημέρωση συστημάτων:** Τα συστήματα λογισμικού χρειάζεται να ενημερώνονται τακτικά για να συμβαδίζουν με τις νεότερες εκδόσεις..
- **Προστασία διευθύνσεων MAC:** Οι διευθύνσεις δεν πρέπει να είναι ορατές από άλλους χρήστες ή ιδιαίτερα σε εικονικές συσκευές ίσως είναι σημαντικό να μεταβάλλονται για να μην ανιχνεύονται.
- **Παρακολούθηση πακέτων για να αποφεύγονται επιθέσεις κατά των ελεγκτών:** Η τεχνολογία SDN επιτρέπει να υπάρχουν ένα ή περισσότερα στιγμιότυπα ελεγκτών δικτύων στο σύστημα.
- **Δημιουργία σχεδίου ασφαλείας:** Είναι σημαντικό να υπάρχει σχετικό πρότυπο ασφαλείας, που να ικανοποιείται από όλους τους σχεδιαστές, χρήστες, παρόχους κλπ.



- **Αυστηρές στρατηγικές πιστοποίησης:** Οι αυστηρότερες στρατηγικές πιστοποίησης πρέπει να επιβληθούν σε ολόκληρο το δίκτυο, ούτως ώστε να εξαλείφονται οι επιθέσεις.
- **Απομακρυσμένη απενεργοποίηση χαμένων/κλεμμένων συσκευών:** Στις μέρες μας οποιαδήποτε κινητή συσκευή αποτελεί κερκόπορτα για κάθε χρήστη, καθώς ενσωματώνει τη δραστηριότητά του σε πολλά διαφορετικά δικτυακά συστήματα και εφαρμογές, όπως κοινωνικά δίκτυα, τραπεζικές συναλλαγές κλπ.
- **Τεχνικές ελέγχου:** Οι τεχνικές ελέγχου είναι ένας αποτελεσματικός τρόπος για έλεγχο αν ένα διαφορετικό μέλος εμπλέκεται στην επικοινωνία.
- **Τερματικό:** Ειδική φροντίδα πρέπει να λαμβάνεται υπόψη μεταξύ των μεταγωγέων, των σταθμών βάσης, των access points και των συνδεδεμένων συσκευών.
- **Λίστες:** Είναι σημαντικό να δημιουργηθούν λευκές και μαύρες λίστες, που να περιλαμβάνουν συσκευές, που μπορεί να έχουν πρόσβαση και άλλες που δεν πρέπει να έχουν.
- **Κρυπτογράφηση:** Η κρυπτογράφηση είναι σημαντική όχι μόνο για επικοινωνίες δύο μερών και πιστοποίηση της επικοινωνίας μεταξύ δύο χρηστών, αλλά μπορεί να είναι και ένα εργαλείο για αποθήκευση δεδομένων σε συσκευή ή σε εξωτερικό μέσο.



Εικόνα 3.7: Η πορεία για τη διασφάλιση των κινητών δικτύων SDN.



Εικόνα 3.8: Το σχήμα ασφάλειας των κινητών δικτύων SDN.

### 3.7 Σύγκριση- Αποτίμηση Τεχνολογιών

Οι δύο βασικές τεχνολογίες το SDN και το NFV παρουσιάζουν σημαντικές ομοιότητες και σημαντικές διαφορές και είναι συμπληρωματικές. Έχουν σημαντικότερα πλεονεκτήματα, τα οποία μπορούν να προσδώσουν σημαντικές βελτιώσεις στις σύγχρονες τηλεπικοινωνίες. Το SDN υλοποιήθηκε με βασικό στόχο το διαχωρισμό του ελέγχου από τη μεταγωγή δεδομένων. Επίσης, αποτελεί μία σημαντική μέθοδο για τον έλεγχο και τον προγραμματισμό των δικτύων. Το NFV αποτελεί μία αφαίρεση των δικτυακών λειτουργιών από τις συσκευές υλικού. Τα επίπεδα αφαίρεσης δεν έχουν ακόμα προτυποποιηθεί. Είναι εύκολο να χρησιμοποιηθούν διάφορες μέθοδοι αφαίρεσης και λογικής.

Ένα άλλο βασικό θέμα είναι η διαχείριση της κίνησης, ενόσω το SDN παρέχει τον ελεγκτή, ο οποίος εκτελεί βασικές λειτουργίες και είναι δυνατό να κατανέμει καλύτερα τις επικοινωνίες, καθώς και τους τρόπους με τους οποίους γίνεται η επικοινωνία, καθώς και τα μικρότερα επικοινωνιακά μονοπάτια κλπ. Επίσης, οι ενέργειες εικονικότητας του δικτύου συμβάλουν προς αυτή την κατεύθυνση. Ακόμα, οι ίδιες τεχνικές σε συνδυασμό με τα SDN και NFV είναι δυνατό να δημιουργήσουν συστήματα χρέωσης. Λόγω της βελτιστοποίησης της κίνησης στο δίκτυο είναι δυνατό και τα handovers να γίνονται με αποδοτικό τρόπο και μόνο όταν χρειάζεται επιλέγοντας κατάλληλη πολιτική.

Όσον αφορά στη διαφορετικότητα των δικτυακών πηγών είναι σημαντικό ότι οι πηγές αυτές είναι δυνατό να υποστηρίζονται σε περισσότερους τύπους δικτύων. Υποστηρίζουν ακόμα διάφορες λύσεις ετερογενείς ή και ομογενείς. Ακόμα, τα περισσότερα λογισμικά, που σχετίζονται και με τεχνολογίες είναι ανοιχτά. Μπορεί κανείς να αναπτύξει μία δική του έκδοση εμπορική. Οι ελεγκτές SDN βρίσκονται στο κέντρο δεδομένων, ενώ τα NFVs βρίσκονται στα δίκτυα παρόχων υπηρεσιών. Και οι δύο είναι τεχνολογίες είναι εφαρμόσιμες και είναι σε υψηλά επίπεδα τεχνολογικής ετοιμότητας Technology Readiness Level (TRL).

**Πίνακας 3: Χαρακτηριστικά ανά πρότυπο, το οποίο παρουσιάζει τα χαρακτηριστικά, που παρουσιάζουν οι υφιστάμενες τεχνολογίες.**

Χαρακτηριστικά ανά Πρότυπο	MeSD N	CSD N	WSD N	NetShare	SoftRA N	OpenRA N	MCOR D
NFV αφαίρεση	✓	✓	✓	✓			✓
Ετερογένεια	✓		✓		✓	✓	✓

<b>Εικονικότητα</b>	✓	✓	✓	✓	✓	✓	✓
<b>Επεκτασιμότητα</b>	✓	✓	✓	✓	✓	✓	✓
<b>Αξιοπιστία</b>				✓			✓
<b>Υλοποίηση</b>				✓			✓
<b>Αξιολόγηση-Πειράματα</b>		✓		✓	✓	✓	✓
<b>Εφαρμογή</b>	✓	✓	✓	✓	✓	✓	✓
<b>Ανοιχτό λογισμικό</b>	✓	✓	✓		✓	✓	✓
<b>TRL</b>	6	4	4	6	6	6	7
<b>Δικτυακό Τμήμα</b>	EPC & RAN	EPC & RAN	EPC & RAN	RAN	RAN	RAN	EPC & RAN

#### 4. ΜΕΘΟΔΟΛΟΓΙΑ ΠΕΙΡΑΜΑΤΩΝ

Στην παρούσα διπλωματική βασικός στόχος είναι η αξιολόγηση των νέων τεχνολογιών και διαφόρων εφαρμογών, που πιθανόν προκύπτουν από αυτές. Ο συνδυασμός των SDN και NFV συμβάλει στην κατάστρωση ειδικών τοπολογιών, οι οποίες αναδεικνύουν τις δυνατότητες ενός ελεγκτή δικτύου με το όνομα ONOS, που βασίζεται σε λογισμικό ανοιχτού κώδικα και είναι πολύ σημαντικός για την εξέλιξη και αξιοποίηση των δικτυακών εφαρμογών και καινοτομιών στα σύγχρονα δίκτυα.

Αρχικά, είναι σημαντικό να εξεταστεί ο ONOS, ο οποίος είναι ελεγκτής δικτύου και οι θεμελιώδεις δυνατότητες, που αυτός παρέχει. Για να εισαχθεί μία τοπολογία στον ONOS πρέπει να γραφτεί και να εξομοιωθεί μέσω του Mininet, το οποίο είναι γνωστός εξομοιωτής δικτύου. Είναι, επίσης, σημαντικό να αναλυθούν οι μελέτες περίπτωσης, που υπάρχουν και είναι δυνατό να χρησιμοποιηθούν στον ONOS, όπως για παράδειγμα η virtual Router (vRouter), η IPRAN και η MCORD. Ακόμα, παρουσιάζονται θέματα ασφάλειας και οι εφαρμογές του εν λόγω ελεγκτή σε αυτές τις προκλήσεις, αλλά και γενικότερα η απόκριση των καινοτομιών αυτών στις προκλήσεις, που προκύπτουν. Παράλληλα, συνοψίζονται οι νέες ανάγκες και τι πρέπει να ληφθεί υπόψιν μετά την ενσωμάτωση των SDN και NFV. Ο

συγκεκριμένος ελεγκτής συγκρίνεται με τον ελεγκτή POX, ο οποίος είναι ένας άλλος ελεγκτής δικτύου, επίσης υποστηρίζει SDN και επικοινωνεί με τους μεταγωγείς μέσω του OpenFlow πρωτοκόλλου. Είναι ένας σημαντικός ελεγκτής δικτύων με ευρεία εφαρμογή σε εκπαιδευτικές εφαρμογές. Είναι κι αυτός ανοιχτού κώδικα και ως αποτέλεσμα καθένας μπορεί να έχει πρόσβαση σε αυτόν. Είναι ακόμα υψίστης σημασίας να γίνει κατανοητό πώς επικοινωνούν οι τοπολογίες, που δομούνται με τον ελεγκτή και με τα λοιπά δικτυακά στοιχεία. Ακόμα, παρουσιάζονται τα βασικά στοιχεία της κάθε τοπολογίας, καθώς και οι σημαντικότερες επιλογές, που έγιναν στις παραμέτρους και στις τοπολογίες και εξηγούνται αναλυτικά, ώστε να γίνουν πιο κατανοητά τα αποτελέσματα, που προκύπτουν.

Επίσης, παρουσιάζεται μία τροποποίηση ενός υπάρχοντος τεχνο-οικονομικού μοντέλου μετά την ενσωμάτωση των νέων αυτών προτάσεων και ιδίως του DAS πάνω στα πιο ακριβά του τμήματα, όπως για παράδειγμα στη δέσμευση του εύρους ζώνης, στις κεραίες του και στους σταθμούς βάσης, μειώνοντας τα κόστη κεφαλαίου για την υιοθέτηση των τεχνολογιών αυτών, αλλά και ενσωματώνοντας τα προφανή πλεονεκτήματα της εικονικής τεχνολογίας, που παρουσιάστηκαν προηγουμένως.

Για να τρέξουν τα πιο πάνω λογισμικά, απαιτείται η χρήση λειτουργικού συστήματος Linux. Είναι, επίσης, ένα αρκετά διαδεδομένο λειτουργικό σύστημα, που βασίζεται σε ανοιχτό κώδικα και έχει μία πολύ ενεργή κοινότητα χρηστών, που το υποστηρίζει. Το συγκεκριμένο λογισμικό είναι δυνατό να εγκατασταθεί σε υπολογιστή ως κύριο λειτουργικό σύστημα. Από την άλλη μεριά, είναι δυνατό να δημιουργηθεί μία εικονική μηχανή –Virtual Machine (VM) σε λειτουργικό τύπου Windows για παράδειγμα. Στην παρούσα διπλωματική χρησιμοποιήθηκε λειτουργικό σύστημα Windows 10, πάνω στο οποίο χτίστηκε εικονική μηχανή τύπου Linux 14.04 LTS μέσω του Oracle VM, αλλά και λειτουργικό σύστημα Linux 14.04 εγκατεστημένο σε υπολογιστή αυτόνομα.

## 4.1 Mininet

Το Mininet είναι γνωστός δικτυακός εξομοιωτής, που συμβάλει στην παραγωγή εικονικών τοπολογιών τοπικά σε έναν υπολογιστή με βασικό στόχο να εξομοιωθούν τοπολογίες. Η έκδοση του Mininet, που χρησιμοποιείται στα εν λόγω πειράματα λέγεται Mininet-wifi. Είναι μία έκδοση του γνωστού εξομοιωτή δικτύων, που υποστηρίζει την εξομοίωση όχι μόνο των ασύρματων δικτυακών τοπολογιών, αλλά και τη δημιουργία άλλων τοπολογιών ενσύρματων δικτύων.

Το σημαντικό χαρακτηριστικό, που περιλαμβάνεται σε αυτή την έκδοση είναι η δυνατότητα εισαγωγής κινητικότητας στο ασύρματο δίκτυο. Είναι δυνατό να εισαχθεί σε αυτό λογική, η οποία σχετίζεται με τις περιπτώσεις των κινητών και κυψελωτών δικτύων. Για παράδειγμα, θα μπορούσαν να υπάρχουν κινητές συσκευές, οι οποίες να μετακινούνται σε ένα δίκτυο, να γίνονται διάφορα handovers και να ελέγχεται η αποδοτικότητα του δικτύου σε κάθε μία από αυτές τις περιπτώσεις. Γίνεται εύκολα κατανοητό ότι θα μπορούσε να εισαγάγει πολύτιμες εκπαιδευτικές εφαρμογές και εξομοιώσεις, οι οποίες ως τώρα δημιουργούνταν και ελέγχονταν από άλλους εξομοιωτές δικτύων, όπως για παράδειγμα, οι network simulators (ns). Είναι σημαντικό να σημειωθεί ότι είναι λογισμικό ανοιχτού κώδικα, δηλαδή δεν απαιτείται κάποιο κόστος για τη χρήση, εγκατάσταση ή τη συντήρησή του ή για πρόσθετες δυνατότητες.

Το Mininet-wifi προσδίδει λειτουργικότητα ασύρματου δικτύου. Μπορεί να υπάρξουν δικτυακά μέρη, όπως access points (AP), σταθμοί βάσης- base stations (BS), εισαγωγή ασύρματων πρωτοκόλλων, ιδέες για κινητικότητα και για handovers δικτύων. Μπορεί να συνδυαστεί με τη χρήση 802.11 πρωτοκόλλου. Το Mininet είναι πιθανό να εγκατασταθεί σε μία εικονική μηχανή. Μετά από εκτέλεση διαφόρων πειραμάτων και εντολών στο Mininet εξάγονται σημαντικά στοιχεία και συμπεράσματα για κάθε δίκτυο. Επίσης, το Mininet παρέχει τη δυνατότητα να υπάρχουν γραφικές απεικονίσεις. Είναι ζωτικής σημασίας να περιγραφεί αναλυτικά η χρήση για κάθε μία από τις χρησιμοποιούμενες εντολές. Αυτό θα πραγματοποιηθεί αναλυτικά παρακάτω στο αντίστοιχο κεφάλαιο.

Τέλος, συνδυάζεται ιδανικά και με τους δύο ελεγκτές (ONOS, POX) και είναι δυνατό αλληλοεπιδρώντας με τον έναν ή με τον άλλον ελεγκτή να ελέγχεται σε κάθε στιγμή η κατάσταση του δικτύου και να γίνεται μία προσπάθεια να υποστηρίζεται η όλη εξομοίωση συνολικά.

## 4.2 Open Network Operating System (ONOS)

Ο πιο σημαντικός ίσως από τους ελεγκτές δικτύου ανοιχτού κώδικα είναι ο ONOS. Αυτός ο δικτυακός ελεγκτής έχει ως βασικό στόχο να δημιουργήσει ένα λειτουργικό σύστημα SDN για παρόχους υπηρεσιών τηλεφωνίας και επικοινωνιών. Τα πιο σημαντικά του πλεονεκτήματα συνοψίζονται στα ακόλουθα: επεκτασιμότητα, υψηλή απόδοση και υψηλή διαθεσιμότητα. Ο ONOS κυκλοφόρησε στις 5 Δεκεμβρίου του 2014 από το ON.Lab. Τον Οκτώβριο του 2015 το Linux Foundation ένταξε τον ONOS στα συνεργατικά του πρότζεκτ.

Σαν τεχνολογία ο ONOS είναι σχεδιασμένος σε JAVA και παρέχει SDN εφαρμογές πλατφόρμας μαζί με έναν Apache Karaf. Το σύστημα λειτουργεί ως μία συστάδα (cluster) κόμβων, οι οποίοι είναι πανομοιότυποι όσον αφορά σε θέματα βλαβών και δε δημιουργούν διακοπές στη λειτουργία τους. Ο ONOS ελέγχει τη λειτουργία του δικτύου. Όπως σε κάθε SDN ελεγκτή, είναι δυνατό να δημιουργηθούν περισσότερα του ενός στιγμιότυπα του ελεγκτή και έτσι να διασφαλίζεται η απρόσκοπτη λειτουργία του δικτύου και του επιπέδου ελέγχου σε κάποια περίπτωση επίθεσης.

Από τεχνικής άποψης ο ONOS βασίζεται σε γνωστά/υπαρκτά πρωτόκολλα, εντούτοις δεν είναι άρρηκτα συνδεδεμένη η λειτουργία του με αυτά. Τα πιο σημαντικά στοιχεία, τα οποία εισάγει είναι τα υψηλά επίπεδα αφαίρεσης, τα μοντέλα. Αυτά τα μοντέλα επεκτείνονται και από εφαρμογές κατά τη διάρκεια εκτέλεσης. Για να αποτραπεί να συνδεθούν τα συστήματα με συγκεκριμένες ρυθμίσεις ή με κάποιο συγκεκριμένο πρωτόκολλο ελέγχου, οποιοδήποτε συγκεκριμένο λογισμικό ελέγχου πρέπει να έρχεται σε άμεση επαφή με τις βιβλιοθήκες και το υλικό και να δεσμεύει συγκεκριμένες λογικές και πρότυπα, ώστε να απομονώνεται σε ένα δικό του επίπεδο το οποίο καλείται πάροχος ή οδηγός (provider ή driver). Επίσης, κάθε λογισμικό σε άμεση επαφή με δια-συσταδικά επικοινωνιακά πρωτόκολλα απομονώνεται σκόπιμα σε ένα δικό του επίπεδο γνωστό ως αποθήκη ή store.

Συνολικά, η πλατφόρμα παρέχει εφαρμογές και μελέτες περίπτωσης υψηλού επιπέδου αφαίρεσης. Μέσω της πλατφόρμας είναι δυνατό το σύστημα να «μαθαίνει» για την κατάσταση του δικτύου και άρα, μπορεί να ελέγχει τις ροές και συνολικά τη δικτυακή κίνηση. Εισάγεται ακόμα, μία αφαίρεση για το γράφημα του δικτύου παρέχοντας πληροφορία σχετικά με τη δομή και την τοπολογία του. Ο στόχος των ροών είναι να δομούνται σε μία αφαίρεση συσκευοκεντρική και να επιτρέπεται στις εφαρμογές να έχουν άμεση ροή ή κίνηση μέσω μίας συγκεκριμένης συσκευής, χωρίς να είναι ανάγκη να γίνεται γνωστός ο πίνακας αγωγών (pipeline table). Αυτές οι τεχνολογικές ιδιαιτερότητες παρέχουν μία ελευθερία στη δημιουργία και τη διαχείριση της αντίστοιχης συσκευής.

Ο ONOS περιλαμβάνει σημαντικά πλεονεκτήματα, αυτός είναι και ο βασικός λόγος για τον οποίον αξιοποιείται για πειραματικές διαδικασίες. Τα πιο σημαντικά από τα οποία είναι:

- Άμεσα προγραμματιζόμενος, ειδικά χωρίς την εγκατάσταση υλικού.
- Μειωμένο κόστος κεφαλαίου, λειτουργικό κόστος κλπ.

- Κεντρική διαχείριση δικτύων, λόγω των SDN ελεγκτών.
- Επίπεδα αφαίρεσης για δεδομένα, έλεγχο και συσκευές.
- Αποδοτικές τροποποιήσεις (πρότυπα, στάνταρντ, πρωτόκολλα, εφαρμογές ελέγχου και διεπαφών.
- Αποδοτική διαχείριση φυσικών πόρων.
- Επεκτασιμότητα, που παρέχεται από το SDN και το NFV.
- Ευκολότερη συντήρηση.
- Επεκτάσιμα και εύκολα διαχειρίσιμα συστατικά στοιχεία.
- Συνεκτικές αρχιτεκτονικές.
- Αφαίρεση επιπέδων δεδομένων και ελέγχου.
- Εύκολη προσθήκη εξυπηρετητών.
- Κατανεμημένος πυρήνας.

Σήμερα, περιλαμβάνει περισσότερες από 9 εκδόσεις και πολλές μελέτες περίπτωσης και χρήσης. Έχει μία πολύ ζωντανή κοινότητα, που αναπτύσσει νέες δυνατότητες και έχει δημιουργήσει σημαντικές εφαρμογές του, όπως για παράδειγμα μία πολύ πλούσια διεπαφή, που διευκολύνει σημαντικά το χρήστη και του δίνει ένα πολύ πιο φιλικό περιβάλλον να πειραματιστεί και να πραγματοποιήσει ενέργειες. Μία από τις τρέχουσες δράσεις σχετικά με τον ελεγκτή είναι οι δράσεις, που πραγματοποιούνται ως προς την τοπικότητά του με μετάφραση σε πολλές γλώσσες εκτός από τα αγγλικά, με σκοπό αυτές οι γλώσσες να εμφανίζονται στη διεπαφή του και να κάνουν το περιεχόμενό του πιο εύκολα κατανοητό.

#### 4.2.1 Virtual Router (vRouter)

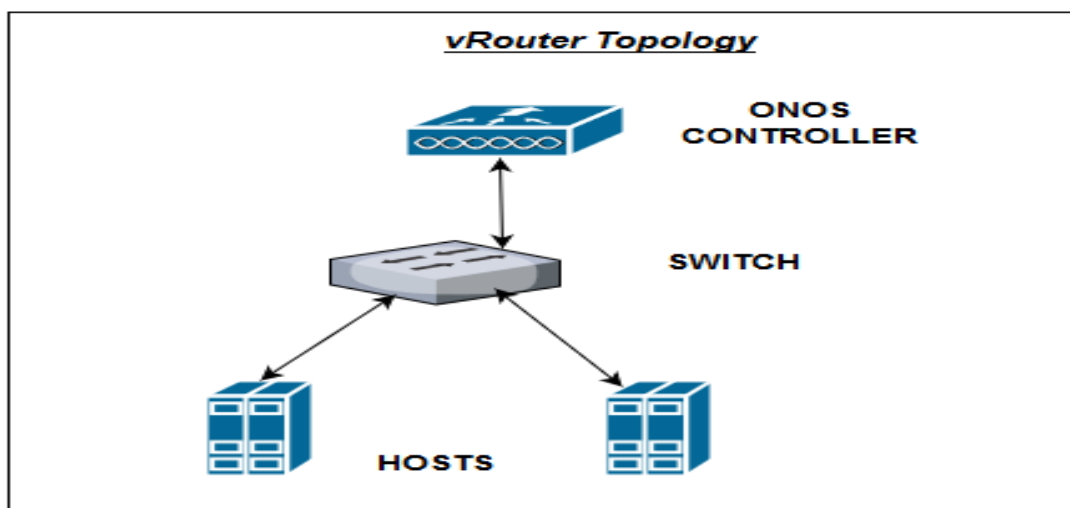
Μία βασική μελέτη περίπτωσης του ONOS είναι η δημιουργία ενός εικονικού δρομολογητή. Οι δρομολογητές είναι συσκευές στο 3<sup>ο</sup> επίπεδο του μοντέλου αναφοράς ISO/OSI, δηλαδή είναι συσκευές δικτύου. Η δρομολόγηση είναι μία πολύπλοκη διαδικασία. Συνεπώς, οι δρομολογητές ήταν ως σήμερα συσκευές υλικού, οι οποίες είχαν περίπλοκα κυκλώματα, αφού είχαν να πραγματοποιήσουν μία πολύ δύσκολη δουλειά. Αρχικά, διάφοροι αλγόριθμοι δρομολόγησης ενσωματώνονται και δρομολογούν τα πακέτα σύμφωνα με διάφορα πολύπλοκα κριτήρια. Το κόστος τους είναι σχετικά υψηλό και παράλληλα καταναλώνουν



ρεύμα. Έτσι, εγείρεται η ανάγκη για δημιουργία συσκευών λιγότερο πολύπλοκων, που θα καταναλώνουν λιγότερο ρεύμα και θα διαθέτουν σημαντικές ευκολίες και πλεονεκτήματα καλύπτοντας τα προβλήματα, που εμφανίζουν οι σημερινές.

Η συγκεκριμένη περίπτωση δημιουργεί έναν «εικονικό» δρομολογητή, ο οποίος ουσιαστικά είναι ένας μεταγωγέας, δηλαδή μία συσκευή χαμηλότερου επιπέδου, αφού οι μεταγωγείς ανήκουν στο 2<sup>ο</sup> επίπεδο του μοντέλου αναφοράς ISO/OSI, δηλαδή το επίπεδο διασύνδεσης δεδομένων. Οι συσκευές αυτές αποτελούν μία λύση, πολύ πιο οικονομική, η οποία δεν περιλαμβάνει λογική και ευφυΐα και είναι πολύ λιγότερο «έξυπνη». Δεν έχει πολύπλοκο υλικό, το οποίο μπορεί να εκτελεί πολύπλοκες διαδικασίες. Εντούτοις, εισάγοντας σε αυτήν λογικές προγραμματιζόμενων δικτυακών συναρτήσεων είναι δυνατό να προσφέρονται σημαντικές δυνατότητες και να παρέχεται μία πολύ σημαντική εναλλακτική πρόταση. Από την άλλη, η διασύνδεση με τον ελεγκτή σε αυτού του τύπου τα δίκτυα, εξασφαλίζει ότι όλη τη σκληρή δουλειά στην τοπολογία την πραγματοποιεί ο ONOS. Ένας ελεγκτής λειτουργεί ως η κύρια πηγή ανταλλαγής πληροφοριών στο δίκτυο.

Υπάρχει αντίστοιχη περίπτωση χρήσης του ONOS. Για την ενεργοποίηση της εφαρμογής απαιτείται ένας μεταγωγέας, ένα στιγμιότυπο του ONOS και το Quagga, για την επικοινωνία με άλλους δρομολογητές. Στη συγκεκριμένη τοπολογία τοποθετούνται 2 υπολογιστές και 1 μεταγωγέας, ο οποίος δρα ως δρομολογητής. Θα μπορούσαν να τοποθετηθούν αντίστοιχα πολύ περισσότερα στοιχεία και να δώσουν πολύ μεγαλύτερες τοπολογίες, κάτι το οποίο όμως, δεν έχει ιδιαίτερο νόημα, εφόσον, στόχος είναι να δειχτεί κατά πόσο βοηθά στον έλεγχο και αναλαμβάνει δράση ο ελεγκτής καθιστώντας απλές συσκευές σημαντικά στοιχεία με δυνατότητες δρομολόγησης. Στο παρακάτω σχήμα εμφανίζονται σημαντικά στοιχεία σχετικά με την τοπολογία του εικονικού δρομολογητή.



**Εικόνα 4.1: Σχήμα τοπολογίας εικονικού δρομολογητή.**

Στην εικόνα 4.1 φαίνεται το σχήμα της τοπολογίας, που διαμορφώνεται για το εν λόγω παράδειγμα. Ο μεταγωγέας αποτελεί έναν εικονικό δρομολογητή, ο οποίος είναι σε θέση να δρομολογεί πακέτα κατόπιν των εντολών του ελεγκτή δικτύου. Οι SDN ελεγκτές είναι πολύ ισχυροί και αποτελούν την ευφυία του δικτύου. Στον Πίνακα 4 αναλύονται διεξοδικά οι παράμετροι, που επιλέγονται για το μεταγωγέα και τους υπολογιστές, που συμμετέχουν στην τοπολογία. Είναι προφανές, ότι θα μπορούσαν να σημειωθούν διάφορες τιμές για τις MAC και IP διευθύνσεις μέσα στο δίκτυο, χωρίς να επηρεάζει αυτό το σύνολο των πειραμάτων. Για λόγους, όμως παρουσίασης συνοψίζονται και παρουσιάζονται. Ο ελεγκτής καθ' όλη τη διάρκεια των πειραμάτων ελέγχει τα συνδεδεμένα αντικείμενα και στη διεπαφή του περιλαμβάνονται όλες οι αλληλεπιδράσεις μεταξύ των στοιχείων στο δίκτυο.

Για να αποδειχθεί αυτό πραγματοποιούνται πειράματα με βάση τις πιο θεμελιώδεις εντολές, που περιλαμβάνει ο ελεγκτής ONOS, με βάση την τοπολογία με στόχο να αναδειχθεί ότι σε κάθε βήμα υπάρχει πλήρης έλεγχος και πλήρης ανάλυση της λειτουργίας του δικτύου. Παρατηρείται πως σε αυτήν την κατεύθυνση συμβάλουν ιδιαίτερα οι εντολές του, όπως οι: summary, flows, devices κ.α., που εξηγούνται αναλυτικά πιο κάτω.

**Πίνακας 4: Συστατικά στοιχεία τοπολογίας vRouter**

<u>Συστατικό</u>	<u>MAC</u>	<u>IP</u>
<b>Μεταγωγέας 1 (Switch 1)</b>	00:00:00:00:00:01	10.0.0.1/24
<b>Υπολογιστής 1</b>	00:00:00:00:00:03	10.0.2.2/24
<b>Υπολογιστής 2</b>	00:00:00:00:00:04	10.0.2.3/24

#### 4.2.2 Internet Protocol Radio Access Network (IPRAN)

Η IPRAN περίπτωση είναι μία περίπτωση χρήσης του ελεγκτή ONOS για κινητά δίκτυα επικοινωνίας. Συγκεκριμένα, στην περίπτωση αυτή, μπορεί να εισαχθούν τοπολογίες ασύρματων ή και κινητών δικτύων και να δημιουργηθούν ιδανικές συνθήκες για να πειραματιστεί κανείς με διάφορα σημαντικά ζητήματα, όπως για παράδειγμα με τη δημιουργία σταθμών βάσης, με τη δημιουργία των ασύρματων στοιχείων της τοπολογίας με ρύθμιση αυτών. Ακόμα, είναι δυνατό να πειραματιστεί κανείς με την κινητικότητα και να ελέγχονται τα handovers και άλλα σημαντικά στοιχεία, που επηρεάζουν σε μεγάλο βαθμό της απόδοση του δικτύου.

Όσον αφορά στην IPRAN ασύρματη περίπτωση τοπολογίας είναι δυνατό να δημιουργηθούν δύο διαφορετικά σενάρια. Η μία τοπολογία έχει μόνο ασύρματα και κινητά στοιχεία και ονομάστηκε IPRAN, ενώ η άλλη έχει κινητά, ασύρματα και σταθερά στοιχεία δικτύων και καλείται ετερογενής, λόγω του γεγονότος ότι παράλληλα εξετάζονται στοιχεία σχετικά με κινητά δίκτυα και ενσύρματα δίκτυα. Και στις δύο τοπολογίες υπάρχουν διάφορα στοιχεία, τα οποία συνδέονται με τον ONOS. Στην πρώτη περίπτωση υπάρχει σημείο πρόσβασης access point και σταθμοί βάσης base stations. Στη δεύτερη περίπτωση προστίθενται και μεταγωγείς και απλοί υπολογιστές.

Αρχικά, η IPRAN περιλαμβάνει ένα σημείο πρόσβασης, 2 σταθμούς βάσης και έναν ελεγκτή δικτύου ONOS, ο οποίος συνδέεται με αυτά και μπορεί να τα ελέγξει και να τα διαχειριστεί. Όσον αφορά σε αυτό υπάρχουν διάφορα συστατικά στοιχεία, τα οποία αναλυτικά παρατίθενται ακολούθως στον Πίνακα 5. Όσον αφορά, στο σημείο πρόσβασης περιέχονται συστατικά, λειτουργία, κανάλι, θέση. Έτσι, ρυθμίζονται τα στοιχεία του δικτύου. Παρατηρείται ότι τα στοιχεία θα μπορούσαν να έχουν ρυθμιστεί με διαφορετικό τρόπο, αλλά για λόγους παρουσίασης επιλέχθηκαν αυτές οι παράμετροι.

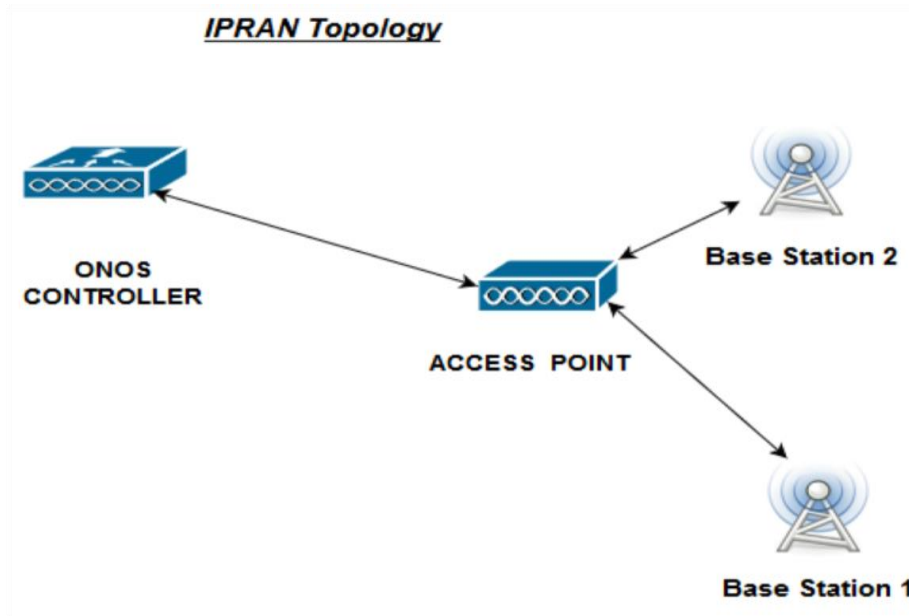
Ακόμα, υπάρχουν για τους σταθμούς βάσης τα στοιχεία MAC και τις IP διευθύνσεις, καθώς και οι θέσεις τους στο δίκτυο στο πεδίο Θέση. Ακόμα, υπάρχουν 4 υπολογιστές, για τους οποίους παρατίθενται οι MAC και IP διευθύνσεις τους. Στο πρώτο σενάριο συμμετέχουν οι Σταθμοί βάσης 1 και 2, καθώς και το σημείο πρόσβασης. Ενώ, στη δεύτερη περίπτωση όλα τα παραπάνω, καθώς και οι υπολογιστές.

Υπάρχει αντίστοιχη περίπτωση με το όνομα IPRAN στις περιπτώσεις χρήσης του ONOS. Μπορεί να δημιουργηθούν αρκετές τοπολογίες μεγάλης έκτασης, ή ακόμα και να εισαχθεί κινητικότητα σε αυτές με στόχο να γίνονται διάφορα πειράματα. Εδώ, δημιουργείται

ένα απλό σχήμα τοπολογίας με βασικό στόχο την ανάδειξη της επιτυχίας του ελεγκτή ONOS να πραγματοποιεί έλεγχο και ενέργειες κεντρικά ελέγχοντας όλο το δίκτυο. Άλλωστε, οι αδυναμίες, που εμφανίζουν τα κινητά δίκτυα αποτελούν μόνες τους εφαλτήριο για νέες ερευνητικές ενέργειες και δράσεις, που θα βελτιώσουν σημαντικά την όλη κατάσταση των κινητών δικτύων επικοινωνίας.

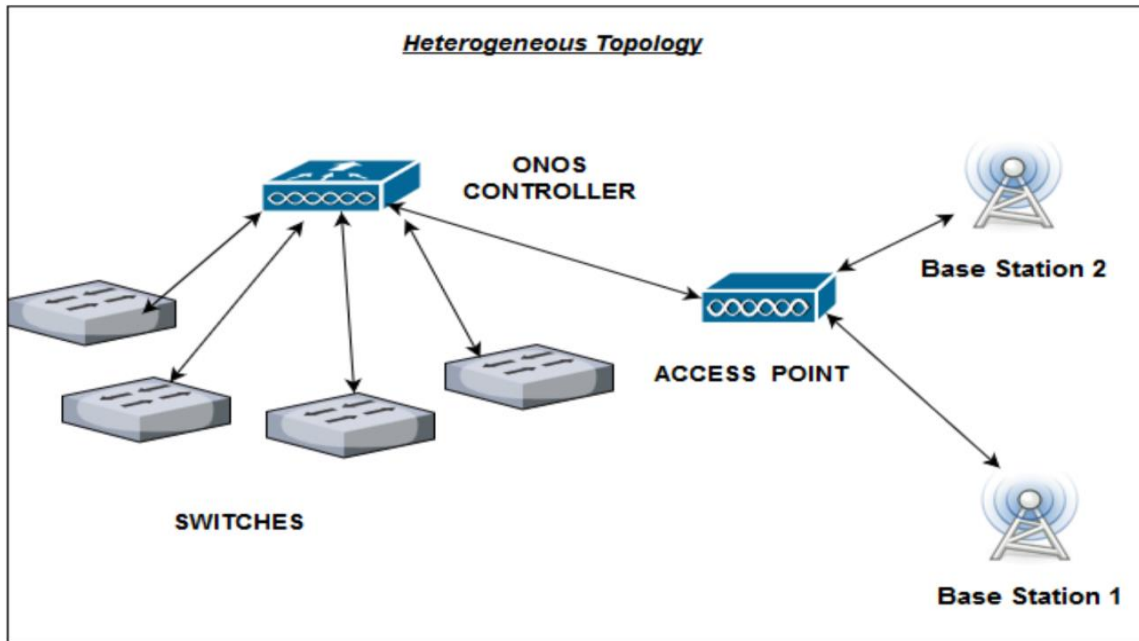
**Πίνακας 5: Συστατικά στοιχεία τοπολογίας IP-RAN και Heterogeneous**

<u>Συστατικό</u>	<u>Λειτουργία</u>	<u>Κανάλι</u>	<u>Θέση</u>
Σημείο Πρόσβασης (Access Point)	g	1	10.30.0
<u>Συστατικό</u>	<u>MAC</u>	<u>IP</u>	<u>Θέση</u>
Σταθμός Βάσης 1 (Base Station 1)	00:00:00:00:00:01	10.0.0.1/8	10.20.1
Σταθμός Βάσης 2 (Base Station 2)	00:00:00:00:00:02	10.0.0.2/8	50.20.1
Υπολογιστής 1	00:00:00:00:00:03	10.0.1.1/24	
Υπολογιστής 2	00:00:00:00:00:04	10.0.2.1/24	
Υπολογιστής 3	00:00:00:00:00:05	10.0.3.1/24	
Υπολογιστής 4	00:00:00:00:00:06	10.0.4.1/24	



Εικόνα 4.2: Σχήμα τοπολογίας κινητού δικτύου επικοινωνίας.

Όσον αφορά στην ετερογενή τοπολογία ενσωματώνονται τα πιο πάνω στοιχεία, τα οποία είναι συστατικά των ασύρματων δικτύων, καθώς και οι μεταγωγείς, οι οποίοι υπάρχουν και είναι 4 το πλήθος και περιλαμβάνονται κι αυτοί στη συγκεκριμένη τοπολογία. Τα πιο πάνω στοιχεία περιγράφονται στον Πίνακα 5. Στις εικόνες 4.2 και 4.3 αναπαρίστανται οι τοπολογίες, που δημιουργούνται. Φαίνονται όλα τα στοιχεία. Είναι σημαντικό να σημειωθεί πως και στην περίπτωση αυτή, ο πιο σημαντικός παράγοντας είναι οι μεταγωγείς, οι σταθμοί βάσης και οι υπολογιστές, που αλληλοεπιδρούν και αποστέλλουν πακέτα εκατέρωθεν. Από την άλλη μεριά, όμως και στην προκειμένη περίπτωση όλη η ευφυΐα και όλες οι δραστηριότητες στο δίκτυο ελέγχονται από τον ελεγκτή, ο οποίος είναι εκείνος, που καθορίζει την κίνηση και την απόκριση των συσκευών. Παράλληλα, χάρη στη πλούσια διεπαφή του έχει κάθε στιγμή όψη του δικτύου. Κάτι που αποδεικνύεται με την χρήση των βασικών εντολών του, όπως για παράδειγμα flow, summary, devices κλπ.



Εικόνα 4.3: Σχήμα τοπολογίας ετερογενούς δικτύου επικοινωνίας.

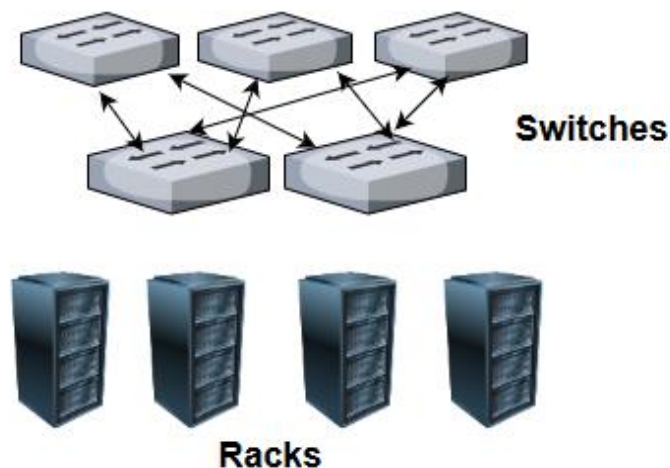
#### 4.2.3 Mobile Central Office Re-Imagined as a Data Center (MCORD)

Τα CORD και MCORD είναι πολύ σημαντικά για τα σημερινά δίκτυα, όχι μόνο σαν τεχνολογικές προσεγγίσεις, αλλά γιατί παρέχουν πολύ σημαντικά εργαλεία για την εξοικονόμηση κόστους. Η ενσωμάτωση SDN, NFV και τεχνικών νέφους στο δίκτυο σηματοδοτεί μία νέα εποχή και αποτελεί ένα πολύ σημαντικό εφαλτήριο για τις νέες τεχνολογίες στον τομέα, αλλά εισάγει συνάμα μία πολύ διαφορετική προσέγγιση στη μέχρι σήμερα γνωστή πραγματικότητα.

Για τη δημιουργία του MCORD χρησιμοποιείται η αντίστοιχη περίπτωση του ONOS. Αυτό συμβαίνει με μία μέθοδο γνωστή ως CORD-In-A-Box ή με ένα απλό σκριπτ. Αυτές οι μέθοδοι αναλύονται αρκετά μέσα από την ενεργή κοινότητα, που υπάρχει για το CORD και υποστηρίζεται πλήρως διαδικτυακά στο OpenCORD.org. Ο χρήστης δύναται να δημιουργήσει πολλαπλά στιγμιότυπα από εικονικές μηχανές χωρίς τη χρήση υλικού. Χρησιμοποιούνται πολλά λογισμικά μεταξύ των οποίων: OpenStack, XOS, ONOS, volt, VSG, vRouter και εικονικό δίκτυο τύπου Virtual Tenant Network (VTN). Απαιτείται ένας λογαριασμός CloudLab με σκοπό να υπάρχει σύνδεση σε εικονικό εξυπηρετητή και να δημιουργούνται μεταγωγείς απομακρυσμένα και να χρησιμοποιούνται μαζί με τα άλλα στοιχεία για την εξομίωση.

Μετά την εγκατάσταση και την ύπαρξη ενός CloudLab. Υπάρχει περιβάλλον πειραμάτων. Στη ListView υπάρχουν ssh εντολές, που βοηθούν να συνδεθούν οι εξυπηρετητές. Αυτό προσδίδει διάφορες σημαντικές δυνατότητες, όπως τον καθαρισμό του περιβάλλοντος και την προετοιμασία του για τον πειραματισμό. Υπάρχουν εικονικές BBU και P-GW περιπτώσεις. Υπάρχει δυνατότητα πλοήγησης σε VTN και έτσι είναι δυνατό να δημιουργούνται εύκολα ροές δεδομένων, καθώς και διαφορετικά δικτυακά slices. Στην εικόνα 4.4 παρατίθεται μία ποιοτική ανάλυση μίας αρχιτεκτονικής τύπου CORD.

Σημαντικό εργαλείο αποτελεί το ότι σε αυτή την περίπτωση χρήσης υπάρχει μία πολύ πλούσια διεπαφή, η οποία προσθέτει σημαντικά στοιχεία στη συγκεκριμένη περίπτωση, ενώ από την άλλη μεριά, διευκολύνει σημαντικά την όψη και την κατανόηση τους. Σημειώνοντας, οι δύσκολες έννοιες και οι σημαντικές εφαρμογές, που μπορεί να βρει η τεχνολογία, ιδίως, αφού η δημιουργία μίας νέας υπηρεσίας μέσω της διεπαφής αποτελεί μία απλή διαδικασία, όπως θα αναδειχθεί παρακάτω.



Εικόνα 4.4: Σχήμα τοπολογίας βασικής CORD αρχιτεκτονικής.

#### 4.2.4 Ασφάλεια στα κινητά δίκτυα 5G με χρήση SDN

Με χρήση των τοπολογιών στο 4.2.2, δηλαδή των κινητών τοπολογιών, πραγματοποιούνται κάποια επιπλέον πειράματα, τα οποία καταδεικνύουν την ασφάλεια των κινητών δικτύων σε σχέση με το SDN. Σήμερα, ολοένα και περισσότερο αμφισβητείται η ασφάλεια των δικτύων SDN, καθώς νέα προβλήματα έχουν προκύψει και απαιτούν νέες πιο προοδευτικές λύσεις. Ακόμα, οι τεχνικές νέφους έχουν κι αυτές τα δικά τους κενά ασφαλείας παρά τα όσα πλεονεκτήματα συσσωρεύουν και αποτελούν πολύ σημαντικό εργαλείο για τα

σημερινά και μελλοντικά δίκτυα. Ένα βασικό ερώτημα, που τίθεται είναι αφού όλη η ευφυία είναι εμφωλευμένη στον ελεγκτή, τότε αν βγει εκτός λειτουργίας αυτός τι θα γίνει;

Αρχικά, κάθε δικτυακός ελεγκτής με την έννοια του SDN μπορεί να μην είναι ένας μόνο ελεγκτής, αλλά να αποτελείται από περισσότερους ελεγκτές δημιουργώντας συνολικά μία συστάδα. Έτσι, μπορεί να ανταποκριθεί κάποιος από τους άλλους ελεγκτές αν βγει ένας από αυτούς εκτός λειτουργίας. Εν συνεχεία, είναι δυνατό να λειτουργούν περισσότερα του ενός στιγμιότυπα ελεγκτή και να σημειώνεται άμεση αντικατάσταση με το υγιές στιγμιότυπο σε περίπτωση κατάρρευσης.

Ο ONOS συγκεκριμένα περιλαμβάνει και αντίστοιχη ασφαλή λειτουργία, δηλαδή, είναι δυνατό να εισέρχεται σε ασφαλή λειτουργία ή να μην εισέρχεται σε αυτή. Η ασφαλής λειτουργία είναι μία ακόμα δυνατότητα, που παρέχει ο συγκεκριμένος δικτυακός ελεγκτής. Η δυνατότητα αυτή είναι τρέχον πρότζεκτ και άρα, ενδεχομένως νέες δυνατότητες, που να εξασφαλίζουν την ασφάλεια πολύ πιο δυναμικά σε ένα δίκτυο και στο επίπεδο ελέγχου αυτού να ενσωματωθούν αργότερα. Καθώς νέες μελέτες έρχονται στο φως συνάμα νέες απειλές δημοσιοποιούνται. Αυτό από μόνο του αποτελεί κίνητρο για μία εκ των προτέρων αποδοτικότερη σχεδίαση.

Στην πρώτη περίπτωση, που υπάρχει ένα access point και δύο σταθμοί βάσης, οι σταθμοί συνδέονται με το access point, το οποίο επικοινωνεί με τον ONOS. Αυτός ελέγχει συνολικά την τοπολογία κι είναι σε θέση να ανταποκρίνεται στις αλλαγές του δικτύου, να παρακολουθεί τα εκτεινόμενα και να δρομολογεί τα πακέτα.

Στους δύο σταθμούς βάσης δημιουργείται ένα πρόβλημα. Ο 2<sup>ος</sup> σταθμός βάσης πλημμυρίζεται από κίνηση, προερχόμενη από τον 1<sup>ο</sup> σταθμό, ο οποίος έχει πέσει θύμα επίθεσης. Για να γίνει αυτό χρησιμοποιούνται οι δύο παρακάτω εντολές:

- **sta1 ping -s &**
- **sta1 ping -c 10.000.000.000 sta2**

Το γεγονός αυτό ουσιαστικά καταδεικνύει πώς ένας χρήστης, μπορεί να επιτεθεί σε ένα στοιχείο της τοπολογίας. Αν για παράδειγμα, το στοιχείο θύμα έχει πολύ γρήγορη κίνηση, τότε είναι δυνατό στέλνοντας απαγορευτικό πλήθος πακέτων να δεσμεύσει την κίνηση επ άπειρων μην επιτρέποντας παράλληλα την επικοινωνία με τις άλλες συσκευές ή μεταξύ των άλλων συσκευών. Αξιοποιώντας την ασφαλή και μη ασφαλή λειτουργία του ONOS, τα ίδια ακριβώς πειράματα πραγματοποιούνται στην περίπτωση, που η ασφαλής λειτουργία του ONOS είναι



ενεργή και όταν δεν είναι ενεργή. Με σκοπό να προκύψει η σύγκριση δεν πραγματοποιείται καμία επιπρόσθετη αλλαγή για να καταδειχτεί αν και κατά πόσο επηρεάζει η ασφαλής αυτή λειτουργία επηρεάζει τη συμπεριφορά του ελεγκτή, καθώς και την επίθεση στο δίκτυο.

Επίσης, με την ίδια λογική πραγματοποιούνται τα πειράματα στην ετερογενή τοπολογία. Εκεί, υπάρχουν 2 σταθμοί βάσης, 1 σημείο πρόσβασης, 4 μεταγωγείς και 4 υπολογιστές συνδεδεμένοι στο κάθε μεταγωγέα. Στην περίπτωση αυτή, όλα τα επί μέρους δικτυακά στοιχεία επικοινωνούν με τον ελεγκτή, ο οποίος είναι ο δικτυακός εγκέφαλος και ελέγχει τα πάντα. Στους απλούς μεταγωγείς τοποθετείται προγραμματιζόμενη λογική και με τον τρόπο αυτό είναι δυνατό να πραγματοποιούν και διαδικασίες δρομολόγησης, που είναι μία πολύπλοκη διαδικασία, ενώ στην πραγματικότητα το υλικό τους δεν είναι τόσο αναβαθμισμένο. Αναλυτικά, ο μεταγωγέας είναι 2<sup>ο</sup> ISO/OSI επιπέδου συσκευή σε αντίθεση ο δρομολογητής είναι 3<sup>ο</sup> επιπέδου. Στην περίπτωση αυτή ένας μεταγωγός, που δυνητικά μπορεί να χρησιμοποιηθεί ως δρομολογητής γίνεται θύμα επίθεσης, με αποτέλεσμα να «αποπροσανατολίζονται τα πακέτα», να χαλάνε οι πίνακες ARP γεμίζοντας σκουπίδια είτε να σταματά εντελώς η δρομολόγηση πακέτων από και προς τον ελεγκτή.

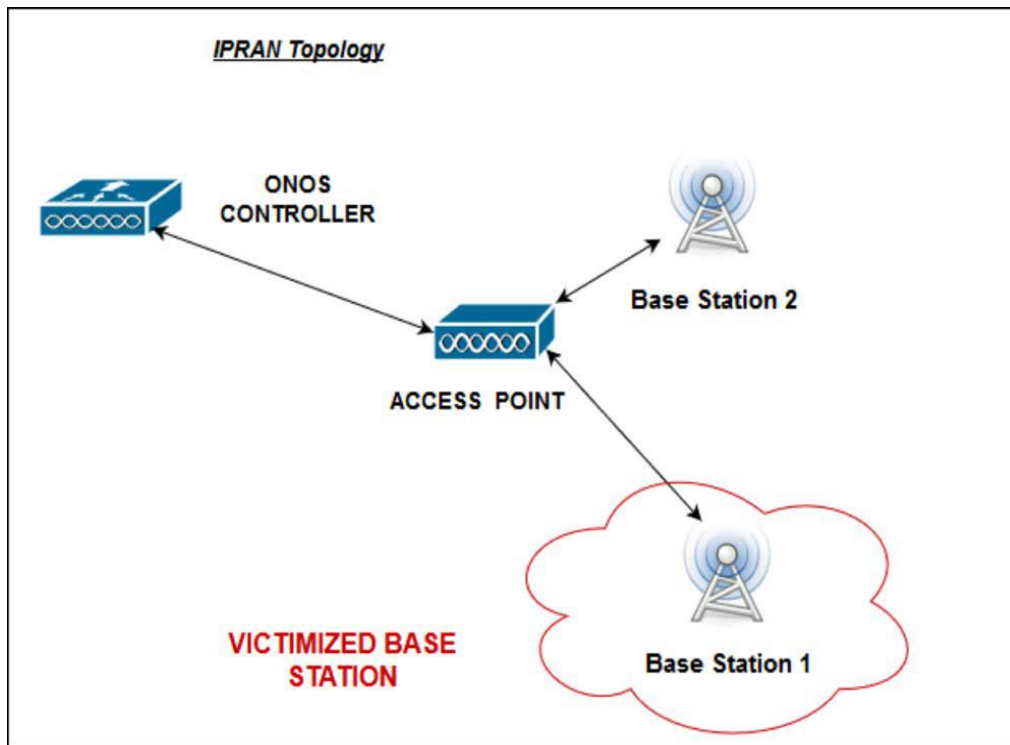
Στη συγκεκριμένη περίπτωση, θα πραγματοποιηθεί επίθεση στον 3<sup>ο</sup> μεταγωγέα, ο οποίος παγιδεύεται από την κακόβουλη επίθεση, η οποία γίνεται χρησιμοποιώντας τις πιο κάτω εντολές:

- **xterm s3**
- **tcpdump -i any**

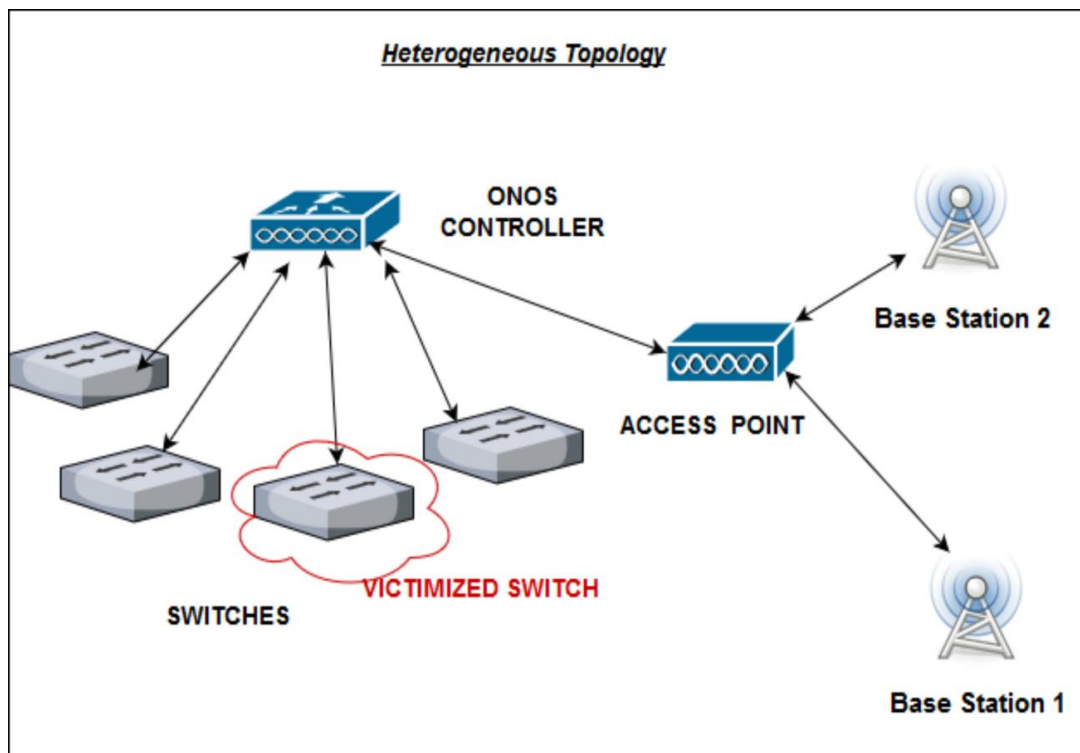
Τέλος, για να ενεργοποιηθεί η ασφαλής λειτουργία του ONOS, πρέπει να χρησιμοποιηθούν οι εντολές, που παρατίθενται ακολούθως:

- Ενεργοποιηθεί η ασφαλής έκδοση του karaf: **onos-setup-karaf secure**
- Ενεργοποιηθεί το ONOS Tarball: **onos-package -s -t.**

Ύστερα, γίνεται επανεκκίνηση του ελεγκτή και τα ίδια ακριβώς πειράματα εκτελούνται και με τη χρήση της ασφαλούς αυτής λειτουργίας. Στις εικόνες 4.5 και 4.6 παρατίθενται αντίστοιχα οι τοπολογίες, πώς διαμορφώνονται μετά τις επιθέσεις, καθώς και ποια είναι τα βασικά στοιχεία, τα οποία δέχονται την κάθε επίθεση.



**Εικόνα 4.5:** Σχήμα τοπολογίας IPRAN, που συντελέστηκε η επίθεση.



**Εικόνα 4.6:** Σχήμα της ετερογενούς τοπολογίας, που συντελέστηκε η επίθεση.

#### 4.2.5 Σύγκριση SDN ελεγκτών (ONOS, POX) για εφαρμογές στην εκπαίδευση

Σήμερα, κρίνεται ολοένα και περισσότερο επιτακτική η ανάγκη να ενσωματώνονται στην εκπαίδευση νέες τεχνικές σχετικές με τα δίκτυα SDN και με τις τεχνικές virtualization στο δίκτυο. Μέχρι τώρα, σε λίγα πανεπιστήμια έχουν ενσωματωθεί μαθήματα των σύγχρονων δικτύων και των καινοτόμων τεχνολογιών. Οι τεχνικές αυτές αποτελούν συχνά δυσνόητα θέματα και δυσνόητες έννοιες, που δεν είναι εύκολο να επεξηγηθούν θεωρητικά και ενδεχομένως πρακτικά παραδείγματα να ήταν πιο εύκολο να αποδώσουν τα πιο βασικά σημεία της κάθε τεχνολογικής πρότασης σε αντίθεση με τις παραδοσιακές μεθόδους εκμάθησης των δικτύων και των μεθόδων χρήσης εικονικών μηχανών έναντι υλικού.

Ο πιο κοινός ελεγκτής λογισμικού, που χρησιμοποιείται σε περιπτώσεις εκπαίδευσης σε ακαδημαϊκό επίπεδο είναι ο POX. Ο POX είναι επίσης ένας ελεγκτής, που επικοινωνεί με τους μεταγωγείς βάση OpenFlow. Ο POX είναι υλοποιημένος σε γλώσσα Python, σε αντίθεση με τον ONOS, που είναι σε Java και δέχεται ως είσοδο τοπολογίες γραμμένες σε Python, οι οποίες εκκινούν από το Mininet και εμφανίζουν διάφορα στοιχεία για το δίκτυο και για την τοπολογία, που εξετάζεται.

Για να είναι περισσότερο ενιαία η σύγκριση των δύο δικτυακών ελεγκτών είναι σημαντικό να εξεταστούν οι ίδιες τοπολογίες για να παρατηρηθεί σε ποια σημεία ομοιάζουν και σε ποια σημεία διαφέρουν. Είναι ακόμα σημαντικό να παρατηρηθεί ποιος είναι πιο ευνοϊκός σχετικά με την εκπαιδευτική διαδικασία, αλλά και σε ποιες εφαρμογές θα είναι καλύτερος ο καθένας και για ποιο λόγο.

Ο POX εγκαθίσταται πολύ εύκολα χρησιμοποιώντας μόνο 2 ουσιαστικά εντολές για την αποθήκευσή των αρχείων του τοπικά και μία για την εκτέλεση του αντίστοιχου script για να εγκατασταθεί ο POX. Αναλυτικά, παρατίθενται και επεξηγούνται οι εντολές παρακάτω:

- **sudo apt-get install git:** είναι απαραίτητο να είναι εγκατεστημένο το Git, το οποίο αποτελεί ένα σύστημα ελέγχου των εκδόσεων του λογισμικού, που υπάρχει σε έναν υπολογιστή.
- **git clone <http://github.com/noxrepo/pox>:** με την εντολή αυτή αντιγράφονται και αποθηκεύονται τα περιεχόμενα αρχεία, που δομούν τον POX από τον αντίστοιχο ιστότοπο, που βρίσκονται.
- **cd pox:** έπειτα, τοπικά στο σύστημα με την εντολή cd γίνεται αλλαγή του φακέλου και αλλάζει ο φάκελος ως POX.
- **./pox.py:** Τρέχει το script, που εγκαθιστά τον POX.

Για τον παραπάνω σκοπό, οι τοπολογίες, που χρησιμοποιήθηκαν στο 4.2.1, 4.2.2 στον ONOS controller ενσωματώνονται και στον POX. Καταγράφονται τα αποτελέσματα του POX, συγκρίνονται με αυτά του ONOS και παρατηρείται η σημαντική τους διαφοροποίηση. Παρατηρείται ότι για να γίνουν πειράματα π.χ. για τα CORD και MCORD, πρέπει να δομηθούν αντίστοιχες περιπτώσεις και να δημιουργηθούν, ώστε να γίνουν πειράματα στον POX. Αυτό θα δημιουργούσε αυτόματα μεγάλο φόρτο εργασίας είτε στο φοιτητή είτε στο διδάσκοντα, ενώ από την άλλη μεριά θα εστιάσει κανείς σε θέματα της υλοποίησης του MCORD, ενώ ίσως είναι πιο σημαντικό να εγκύψει κανείς στη λειτουργία και τις εφαρμογές του. Έτσι, στον POX μπορεί να γίνουν μόνο τα αντίστοιχα με τις τοπολογίες πειράματα. Από την άλλη μεριά, στον POX δεν υπάρχει γνωστή περίπτωση ασφαλούς λειτουργίας και άρα είναι πιο πολύπλοκο να διασφαλιστεί η ασφάλεια του SDN δικτύου.

Για την εκκίνηση των τοπολογιών στον POX χρησιμοποιούνται οι παρακάτω εντολές:

- **sudo mn --topo vrouter.py --controller remote**
- **sudo mn --topo IPRAN.py --controller remote**
- **sudo mn --topo heterogeneous.py --controller remote**

#### 4.2.6 Τροποποίηση Αρχιτεκτονικής τύπου DAS με χρήση τεχνικών NFV

Σε παλαιότερες ερευνητικές ενέργειες [92], [95] και [96] είχαν περιγραφεί μοντέλα αρχιτεκτονικής και μαθηματικά μοντέλα σχετικά με τις τεχνικές και οικονομικές πλευρές των τεχνολογιών. Ακόμα, είχαν γίνει πειράματα, που έδειχναν τα πιο σημαντικά κόστη, καθώς και καταδείκνυαν την εφαρμογή των επί μέρους τεχνολογιών DAS και small cells σύμφωνα με το μέγεθος της υποδομής, που επιδιωκόταν να καλυφθεί.

Εν συνεχεία, στα [93], [94], είχε πραγματοποιηθεί έρευνα και μελέτη εφικτότητας σχετικά με ένα παραδοσιακό σύστημα Distributed Antenna System (DAS), το οποίο είχε συγκριθεί με τεχνικές Ultra-Density και πιο συγκεκριμένα με τα small cells και είχε βρεθεί ότι για να αποτελέσει τεχνολογία, που μπορεί να χρησιμοποιηθεί για τις γενιές 5G και εξής, θα πρέπει να μειωθούν σημαντικά πολλά είδη κόστους αυτών. Για το σκοπό αυτό, η μελέτη εφικτότητας ανέδειξε ποια ήταν τα κύρια κόστη και ποια ήταν πιο σημαντικό να μειωθούν αν όχι να ελαχιστοποιηθούν με στόχο να μειωθεί ραγδαία το κόστος κεφαλαίου, το λειτουργικό κόστος και το συνολικό κόστος της συγκεκριμένης τεχνολογίας.

Εφαρμόζοντας τεχνικές virtualization δικτύων είναι δυνατό να προκύψουν σημαντικά οφέλη από άποψη κόστους και τεχνολογίας. Οι τεχνικές αυτές αντικαθιστούν το υλικό με άλλο,

το οποίο είναι πολύ πιο απλοϊκό με αποτέλεσμα, εισάγοντας σε αυτό λογικές προγραμματισμού, να μπορεί να πραγματοποιεί πολύ πιο δύσκολες και απαιτητικές εργασίες. Ακόμα, γίνεται εμφανές ότι είναι πολύ πιο εύκολο να συντηρηθεί λογισμικό και γενικά, μπορεί να προκύψουν και άλλα σημαντικά οικονομικά οφέλη, αφού απλούστερες συσκευές καταναλώνουν λιγότερο ρεύμα, χρειάζονται λιγότερη συντήρηση, λιγότερο προσωπικό για συντήρηση και χαμηλότερο κόστος για τη λειτουργία τους κλπ. Εν τούτοις, εμφανίζονται και σημαντικά ερωτήματα, όπως με ποιον τρόπο θα είναι συμβατές οι νέες με τις παλαιότερες τεχνολογίες, αν θα είναι διαθέσιμες οι υπηρεσίες σε περίπτωση βλάβης ή επίθεσης στο λογισμικό, που τρέχουν, κ.α.

Στο συγκεκριμένο κεφάλαιο θα παρουσιαστεί μία προτεινόμενη αρχιτεκτονική, που μεταβάλλει την αρχιτεκτονική, που είχε προταθεί σε προηγούμενες ερευνητικές δράσεις [92], [93], [94], [95], [96] με σκοπό να μειωθούν τα κόστη. Για το σκοπό αυτό θα ενσωματωθούν τεχνικές virtualization στα εξής τμήματα:

- Εύρος ζώνης
- Κεραίες
- Σταθμοί Βάσης

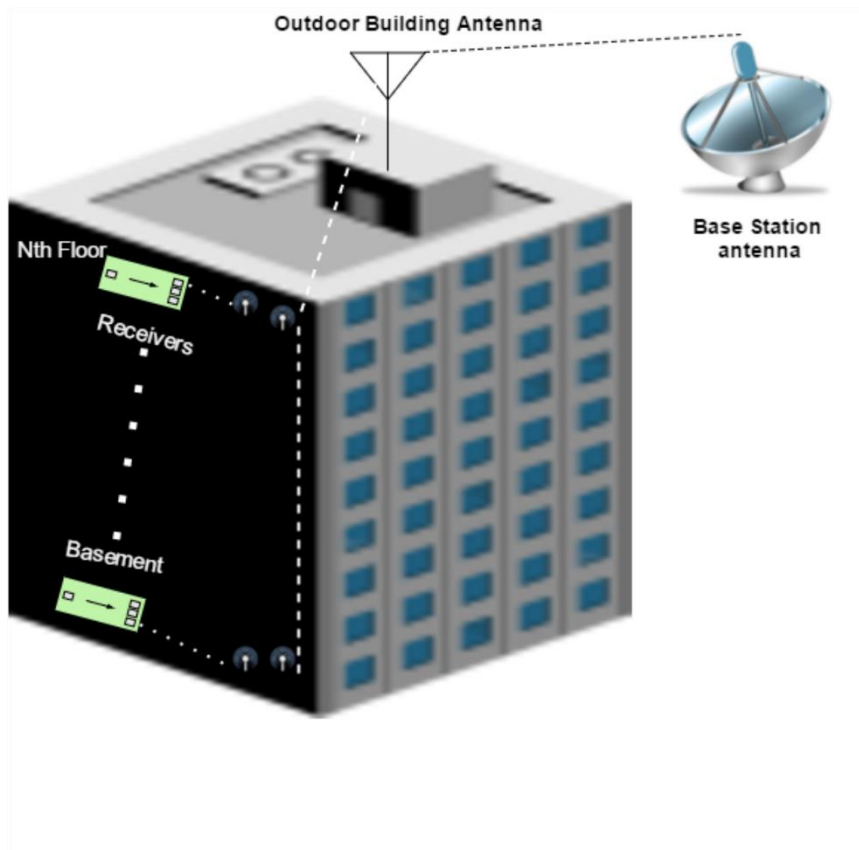
Μπορούν να χρησιμοποιηθούν τεχνικές virtualization στο εύρος ζώνης, αυτό αμέσως αυξάνει το διαθέσιμο εύρος ζώνης, με αποτέλεσμα να μειώνεται το κόστος, αφού λιγότερο εύρος ζώνης μπορεί να καλύψει την ίδια περιοχή. Το κόστος για τις κεραίες μειώνεται, αφού μπορεί να αντικατασταθεί με πιο απλές συσκευές με προγραμματιζόμενη λογική και να αποτελεί μια πιο οικονομικά βιώσιμη λύση. Το ίδιο και οι σταθμοί βάσης. Άλλα κόστη μειώνονται παράλληλα. Τα κόστη αυτά σχετίζονται άμεσα με τη τοποθέτηση, την εξοικονόμηση ενέργειας, τη λειτουργία και διαχείριση, τα διάφορα κόστη κλπ.

Το πιο απλό υλικό συμβάλει στο να καταναλώνεται λιγότερη ενέργεια, να καταλαμβάνεται λιγότερος χώρος από τις συσκευές και να σπαταλούνται λιγότερα χρήματα συνολικά. Αυτές οι τροποποιήσεις στο υλικό, μπορούν αν εφαρμοστούν πάνω στο οικονομικό μοντέλο, που είχε υλοποιηθεί στις προηγούμενες αυτές ερευνητικές δραστηριότητες να προκύψουν τα νέα κόστη. Αυτό είναι εφικτό, επειδή είχε περιγραφεί μαθηματικά και άρα απαιτείται μόνο τροποποίηση των τιμών των παραμέτρων με προσαρμογή τους στο 2017, καθώς και στα πιθανά σενάρια λόγω της εισαγωγής virtualization στα συστατικά των δικτύων. Έπειτα, θα συγκριθούν τα παλιά με τα νέα αποτελέσματα και θα φανεί ξεκάθαρα η υπεροχή του εν λόγω μοντέλου σε σχέση με το παραδοσιακό.

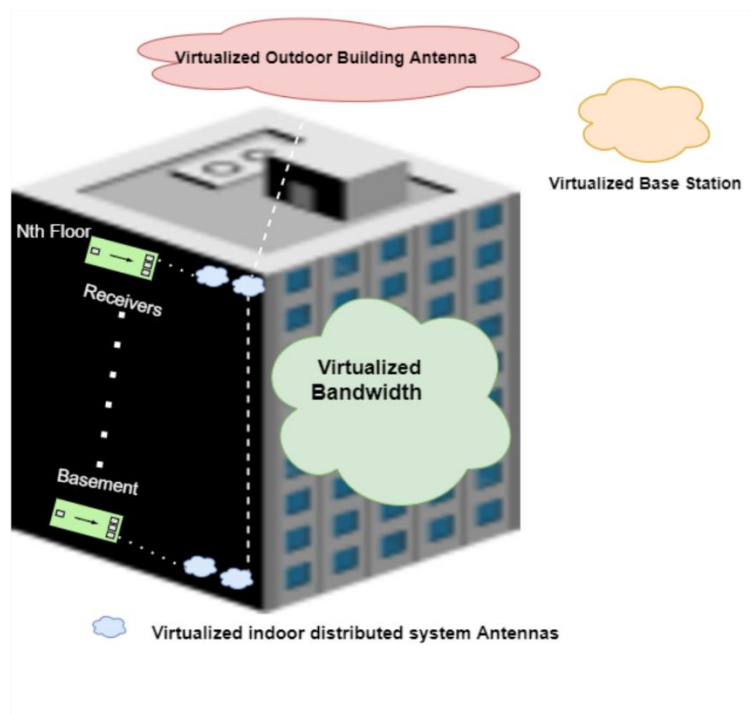
Σε μία βασική DAS αρχιτεκτονική υπάρχουν δύο υποσυστήματα. Υπάρχουν οι σταθμοί βάσης και το καταναμημένο σύστημα. Το καταναμημένο σύστημα περιλαμβάνει ένα πλήθος κόμβων κεραίας ανάλογα με το μέγεθος του κτηρίου, που επιδιώκεται να καλυφτεί. Το σύνηθες είναι να υπάρχουν 2 κεραίες σε κάθε όροφο, αλλά μπορεί να υπάρχουν και περισσότερες αν αυτό καθίσταται αναγκαίο. Ακόμα, μπορεί να υπάρχουν κι άλλες συσκευές επανάληψης για τα σήματα κλπ. Όλες οι κεραίες επικοινωνούν με μία κεντρική κεραία στην κορυφή του κτηρίου και αυτή με τη σειρά της με το κέντρο εκπομπής. Αν χρειάζεται υλικό καλωδίωσης αυτό μπορεί να είναι χαλκός ή και οπτική ίνα. Ο σταθμός βάσης είναι όμοιος με έναν σταθμό βάσης μακρο-κυβελών. Οι συγκεκριμένες αρχιτεκτονικές είχαν παρουσιαστεί πολύ αναλυτικά στα: [92], [93], [94], [95] οπότε εδώ παρατίθεται μία σύνοψη αυτών. Το μοντέλο κόστους αναλύθηκε διεξοδικά και στην προπτυχιακή διπλωματική [95]. Σε αυτή την προσέγγιση παρατίθενται αποτελέσματα για καθένα από τα επί μέρους κόστη (κεφαλαίου, λειτουργικό, συνολικό) σε σύγκριση με τον αριθμό των κεραιών στο σύστημα με στόχο να συγκριθούν με παλιότερες πειραματικές δραστηριότητες και να φανεί η συμβολή του προτεινόμενου μοντέλου στην τεχνολογία.

Στις εικόνες 4.7 και 4.8 παρατίθενται η βασική αρχιτεκτονική, καθώς και το νέο σενάριο μετά την υιοθέτηση των καινοτόμων τεχνικών των εικονικών δικτύων. Παρατηρείται ότι ενώ στην πρώτη περίπτωση υπάρχει μεγάλη υποδομή σε υλικό, στην δεύτερη περίπτωση αυτό αντικαθίσταται από πολύ πιο απλοϊκές μεθόδους καταλήγοντας παράλληλα σε μία πιο ευνοϊκή αρχιτεκτονική, που περιέχει συσκευές με προγραμματιζόμενη λογική εντός τους και αποτελεί μία σημαντική λύση για μείωση των αποδεδειγμένα ακριβών στοιχείων, που υπήρχαν παλιά με οικονομικά αποδοτικότερα.

Επίσης, αναμένεται ότι οι λύσεις αυτές θα προσδώσουν παράλληλα κι άλλα πιο σημαντικά οφέλη, αφού το απλούστερο υλικό σημαίνει και πιο χαμηλού κόστους συντήρηση, χαμηλότερη κατανάλωση ενέργειας, μικρότερο χώρο δεσμευμένο από τα συγκεκριμένα στοιχεία του δικτύου και άλλες δυνατές ευκολίες, όπως για παράδειγμα λιγότερα κόστη στήριξης, θέσης, λιγότερο προσωπικό κλπ. Έτσι, είναι σημαντικό να αναπτυχθεί μία μελέτη εφικτότητας ελέγχοντας όλες τις παραμέτρους, που επηρεάζονται έμμεσα ή άμεσα μετά από την υιοθέτηση των νέων τεχνικών.



Εικόνα 4.7: Σχήμα τοπολογίας βασικής DAS αρχιτεκτονικής.



Εικόνα 4.8: Σχήμα τοπολογίας virtualized DAS αρχιτεκτονικής.

Ενώ, έχει περιγραφεί το μοντέλο της αρχιτεκτονικής και του κόστους για το εν λόγω σύστημα, εν τούτοις, δεν έχουν αναλυθεί οι παράμετροι, που πρόκειται να επιλεγούν για το τροποποιημένο virtualized DAS. Στο [94] πραγματοποιήθηκε εκτενής έρευνα σχετικά με τις τιμές, που θα προκύψουν για κάθε κόστος στο μέλλον. Η 5G είναι μία μελλοντική τεχνολογική γενιά και ως αποτέλεσμα είναι πιθανό μέχρι το 2020, που αυτή αναμένεται, να προκύψουν νέα στοιχεία και νέα τιμολογιακή πολιτική για όλα αυτά. Μάλιστα, στις [93] και [94] είχαν ελεγχθεί σενάρια, στα οποία το κόστος αυξανόταν ή μειωνόταν έως και 50%.

Από την άλλη μεριά, σήμερα είναι γνωστές οι τιμές για όλα τα μεγέθη, που συμμετέχουν στη διαμόρφωση του κόστους. Σύμφωνα με την υπάρχουσα βιβλιογραφία οι virtualized τεχνικές αναμένεται να μειώσουν το κόστος από 40-80% σε σχέση με τις τιμές, που ισχύουν σήμερα. Με βάση αυτό το σενάριο, δημιουργήθηκε νέα κοστολόγηση για τις παραμέτρους, οι οποίες πρέπει να τοποθετηθούν στο μοντέλο για να υπολογιστούν τα αντίστοιχα νέα κόστη. Με σκοπό να πραγματοποιηθεί μελέτη εφικτότητας και να φανούν τα νέα κόστη αναλυτικά και η επίδρασή τους στο μοντέλο δημιουργούνται διαστήματα τιμών, τα οποία αποτελούν τις προβλεπόμενες μελλοντικές τιμές για όλα συστατικά στοιχεία του κόστους, όπως για παράδειγμα για τα κόστη των σταθμών βάσης EPC, eNB, του κόστους για τον εξοπλισμό του DAS, σχετικά με το κόστος της θέσης του συστήματος, το κόστος λειτουργίας, το κόστος καλωδίωσης, το κόστος για το εύρος ζώνης, την κατανάλωση ενέργειας και τα κόστη υλοποίησης.

Όπως φαίνεται στον Πίνακα 6, υπάρχουν οι τιμές για το παραδοσιακό και το εικονικό μοντέλο. Ακόμα, είναι προφανές ότι σε πολλά από τα είδη κόστους το εικονικό μοντέλο έχει πολύ χαμηλότερες χρεώσεις.

**Πίνακας 6: Παράμετροι κοστολόγησης DAS συστημάτων κλασικού και virtualized.**

Παράμετρος	Περιγραφή	Παραδοσιακό μοντέλο	Virtualized μοντέλο
$C_{eNB}$	Κόστος για τον κόμβο eNB	[500, 1500] €	[200 ,600] €
$C_{EPC}$	Κόστος για έναν κόμβο EPC	[55 ,165] €	[22, 66]
$N$	Πλήθος DAS σταθμών βάσης	1	1
$r$	Περιοδικό επιτόκιο	[2,20]%	[2,20]%
$C_{eq}$	Κόστος εξοπλισμού DAS	[5950 , 17850] €	[2380, 7140] €
$d$	Αριθμός κατανεμημένων συστημάτων	[2 ,200] κεραιές	[2, 200] κεραιές



<b>C<sub>st</sub></b>	Κόστος θέσης συστήματος	[1550 ,4650] €	[620, 1860] €
<b>C<sub>run</sub></b>	Κόστος λειτουργίας	[446,25 , 1338,75] €	[178,5 , 535,5] €
<b>C<sub>bh</sub></b>	Κόστος οπτικής ίνας	[2400, 7200] €	[2400, 7200] €
<b>BW</b>	Κόστος για τη διασύνδεση σχετικά με το εύρος ζώνης	[5, 15] Gbps	[5, 15] Gbps
<b>f<sub>BW</sub></b>	Εύρος ζώνης σε €/ Gbps	[585 , 1755]	[234, 702]
<b>C<sub>pw</sub></b>	Κόστος κατανάλωσης ενέργειας	[78,84 ,236,54] €	[31,54 , 94,61] €
<b>C<sub>inc</sub></b>	Κόστος υλοποίησης	[1400, 4200] €	[560, 1680] €

### 4.3 Επεξήγηση Εντολών Τοπολογιών & Εξομοιωτή Δικτύου

Είναι σημαντικό να εξηγηθούν οι εντολές, οι οποίες περιλαμβάνονται και να επεξηγηθεί βήμα-βήμα η χρήση τους σε κάθε περίπτωση. Για τη δημιουργία της κάθε τοπολογίας απαιτείται η χρήση της γλώσσας Python. Με τη χρήση της Python και την εισαγωγή των δημιουργούμενων τοπολογιών στον ελεγκτή δικτύου ONOS διαφαίνεται ο τρόπος με τον οποίον μία απλή τοπολογία αλληλοεπιδρά με τον ελεγκτή δικτύου, καθώς και πόσο σημαντικός ελεγκτής είναι ο ONOS και πόσες πολλές δυνατότητες προσδίδει για πειραματισμό και εξοικείωση με δίκτυα μεγάλης ή μικρότερης κλίμακας. Για την εξομοίωση χρησιμοποιείται ο γνωστός εξομοιωτής δικτύου Mininet και Mininet-Wifi για τις ασύρματες και κινητές περιπτώσεις. Ακόμα, χρησιμοποιείται η έκδοση του ONOS Falcon, η οποία περιλαμβάνει επεκτάσεις για δυνατότητες σχετικές και με το CORD.

Διάφορες βιβλιοθήκες του Mininet είναι σημαντικές και χρήσιμες να εισαχθούν ούτως ώστε να λειτουργήσει η τοπολογία. Εισάγεται η «**TOPO**», η οποία είναι μία κλάση, η οποία περιλαμβάνει σημαντικά στοιχεία για κάθε τοπολογία, όπως για παράδειγμα προσθήκη συστατικών στοιχείων στην τοπολογία. Ακόμα, εισάγεται η «**MININET**», που περιλαμβάνει στοιχεία για τον εξομοιωτή δικτύων. Η Command Line Instruction (CLI) «**CLI**» είναι κλάση, που δημιουργεί τη διεπαφή χρήστη για τη γραμμή εντολών και είναι υπεύθυνη για τις σχετικές αυτές ενέργειες. Οι κλάσεις «**SETLOGLEVEL**», «**INFO**» και «**DEBUG**» περιλαμβάνουν στοιχεία σχετικά με την αποσφαλμάτωση και με τα αρχεία καταγραφής. Επίσης, η κλάση «**REMOTE CONTROLLER**» περιλαμβάνει αρχεία, που σχετίζονται με ελεγκτή δικτύου,

που βρίσκεται απομακρυσμένα. Υπάρχουν διάφορες βασικές μέθοδοι, που χρησιμοποιούνται καθολικά, όπως για παράδειγμα:

- **addSwitch:** προσθέτει ένα μεταγωγέα στην τοπολογία και επιστρέφει το όνομά του. Μπορεί να δεχτεί διάφορες παραμέτρους σχετικές με τη διεύθυνση IP, με τη MAC διεύθυνση του, με το όνομά του κλπ.
- **addHost:** προσθέτει έναν υπολογιστή στην τοπολογία και επιστρέφει το όνομα του. Μπορεί να δεχτεί διάφορες παραμέτρους σχετικές με τη διεύθυνση IP, με τη MAC διεύθυνση του, με το όνομά του κλπ.
- **addLink:** προσθέτει έναν σύνδεσμο δύο κατευθύνσεων στην τοπολογία. Ορίζει δύο στοιχεία μεταξύ των οποίων υπάρχει ο συγκεκριμένος σύνδεσμος. Για παράδειγμα, σύνδεσμος μεταξύ δύο μεταγωγέων, ενός μεταγωγέα και ενός υπολογιστή, ενός ελεγκτή κι ενός δρομολογητή και ούτω καθεξής.
- **addBaseStation(name, ssid, mode, channel, position range):** Προσθέτει σημείο πρόσβασης (Access Point-AP) με παραμέτρους, που δίνονται ως ορίσματα. Πιο συγκεκριμένα ορίζεται το όνομα του σταθμού, το Service Set Identifier (SSID), ο τρόπος λειτουργίας του, το κανάλι λειτουργίας, η θέση μέσα στην τοπολογία, καθώς και η περιοχή, η οποία δύναται να καλύψει.
- **addStation(name, mac, ip, position):** Προσθέτει σταθμό βάσης με συγκεκριμένο όνομα, διεύθυνση Media Access Control (MAC), σε συγκεκριμένη Internet Protocol (IP) διεύθυνση και προστίθεται σε συγκεκριμένο χώρο της τοπολογίας.
- **Mininet:** είναι η βασική κλάση, που χρησιμοποιείται για τη δημιουργία και διαχείριση του δικτύου.
- **Mininet (topo=topo, controller=RemoteController):** Δηλώνεται η τοπολογία και ο ελεγκτής δικτύου, ο οποίος είναι απομακρυσμένος, δηλαδή ο ONOS ή ο POX ανάλογα το αντίστοιχο πείραμα. Ο κάθε ελεγκτής υπάρχει και προσπελαύνεται από συγκεκριμένη διεύθυνση.
- **start:** Μέθοδος, που εκκινεί την τοπολογία του δικτύου.
- **stop:** Μέθοδος, που τερματίζει την τοπολογία του δικτύου.
- **CLI:** Μέθοδος, που περιλαμβάνει τη γραμμή εντολών, όπου μπορεί να γραφτούν διάφορες εντολές και στοιχεία σχετικά με το δίκτυο.
- **net.plotGraph(max\_x, max\_y):** Δημιουργεί γραφικές απεικονίσεις των τοπολογιών του δικτύου. Επίσης, καθορίζει το μέγεθος της προκύπτουσας γραφικής απεικόνισης.

- **pingAll:** ελέγχει τη συνδεσιμότητα του δικτύου βάζοντας κάθε κόμβο να στείλει πακέτα δεδομένων σε κάποιον άλλον κόμβο δοκιμαστικά με σκοπό να φανεί αν όλα βαίνουν καλά στην τοπολογία.
- **quaggaConfFile:** εισάγεται σε ένα αρχείο, το οποίο είναι απαραίτητο για το Quagga. Το quagga είναι ο τρόπος με τον οποίον υλοποιείται το πρωτόκολλο Border Gateway Protocol (BGP) στον ONOS.
- **zebraConfFile:** περιλαμβάνει πληροφορία σημαντική για τη ρύθμιση παραμέτρων στο Quagga.
- **terminate:** η μέθοδος αυτή ορίζεται και τερματίζει τα διάφορα παραδείγματα, που σημειώνονται και δημιουργούνται κατά τη διάρκεια εκτέλεσης του προγράμματος.
- **build:** η μέθοδος αυτή ορίζεται και περιλαμβάνει τη δημιουργία διαφόρων σημαντικών παραγόντων για την τοπολογία. Για παράδειγμα, δημιουργούνται μεταγωγείς, δρομολογητές, διάφοροι σύνδεσμοι μεταξύ τους κλπ.
- **zebraConf = '%s/zebra.conf' % CONFIG\_DIR:** προσδίδει συγκεκριμένες λειτουργικότητες, λόγω του αρχείου zebra, το οποίο ρυθμίζει παραμέτρους του Quagga.
- **root = net.addHost( 'root', inNamespace=False, ip='10.10.10.2/24'):** Σύνδεση με το BGP, ώστε να αλληλεπιδρά με το ONOS σε συγκεκριμένη διεύθυνση.
- **for i in range (start\_value, end\_value ):** εντολές τέτοιου τύπου δίνουν μία δομή επανάληψης από μία αρχική τιμή έως μία τελική τιμή. Κλασική δομή επανάληψης for, η οποία υπάρχει σε διάφορες γλώσσες προγραμματισμού.
- **eth0 = {'mac': '00:00:00:00:0%s:01' % i, 'ipAddrs' : ['10.0.%s.1/24' % i] }:** εντολές τέτοιου τύπου χρησιμοποιούνται για να ρυθμιστούν παράμετροι των hosts, δηλαδή υπολογιστών, που συμμετέχουν στο δίκτυο και σχετίζονται με διεύθυνση IP και διεύθυνση MAC, που αυτοί επιδιώκεται να περιλαμβάνουν.
- **bgpIntfs = {'bgp-eth0' : bgpEth0, 'bgp-eth1' : bgpEth1}:** καθορίζει πώς το BGP μέσω του Quagga θα αλληλεπιδρά με το ONOS στην τοπολογία.

Υπάρχουν δύο βασικοί τρόποι να εισαχθούν οι συγκεκριμένες ρυθμίσεις στην τοπολογία. Αρχικά, είναι δυνατό να εισαχθούν αρχεία .json, τα οποία περιλαμβάνουν στοιχεία για τις διευθύνσεις MAC, IP κλπ. σε συγκεκριμένο φάκελο των αρχείων του ONOS τα οποία, όμως καλούνται μέσα από την τοπολογία. Από την άλλη μεριά, μπορεί να γίνει η ρύθμιση αυτή δια μέσου του αρχείου της τοπολογίας με εντολές, όπως αυτές, που παρουσιάστηκαν παραπάνω.

Η **app activate org.onosproject.vrouter** εντολή στον ONOS εκκινεί την εφαρμογή του εικονικού δρομολογητή (vRouter). Υπάρχουν ακόμα, ορισμένες εντολές, οι οποίες εκτελούνται στον ONOS και προσδίδουν σημαντικά αποτελέσματα. Οι πιο σημαντικές από τις οποίες είναι:

- **summary:** Δίνει περίληψη των βασικότερων συστατικών, που ελέγχει ο ελεγκτής δικτύου. Για παράδειγμα, πόσες συσκευές υπάρχουν εκεί, πόσοι μεταγωγείς είναι συνδεδεμένοι, πόσοι σταθμοί βάσης, πόσα access points κλπ.
- **devices:** Αναδεικνύει όλες τις συσκευές, που υπάρχουν στην τοπολογία αναλυτικά και τις παρουσιάζει μέσα στη διεπαφή του ONOS.
- **Flows:** Δίνει όλες τις ροές δεδομένων σε μία τοπολογία. Είναι δυνατό να παρατηρηθούν οι πιο σημαντικές εξ' αυτών και να διαχειρίζονται ανάλογα από τον ελεγκτή.
- **Net:** Αναδεικνύει την κατάσταση του δικτύου, πόσες συσκευές έχει αυτό, πως αυτές αλληλοεπιδρούν, καθώς και πώς γίνεται η επικοινωνία μεταξύ τους.

## 5.ΑΠΟΤΕΛΕΣΜΑΤΑ

Κρίνεται υψίστης σημασίας να παρατεθούν τα βασικότερα αποτελέσματα της πειραματικής ανάλυσης σχετικά με τον ONOS και τις μελέτες περίπτωσης. Αυτό το γεγονός θα αποδώσει τα βασικότερα συμπεράσματα- αποτελέσματα σχετικά με το SDN και τη σημασία των εφαρμογών αυτού σε ό,τι αναφορά στην εξέλιξη των δικτύων και της ζητούμενης εφαρμογής λογισμικού σε αυτά. Οι πειραματικές διαδικασίες αναμένεται να αναδείξουν το ρόλο των τεχνολογιών και κατά πόσο είναι σημαντικές και βιώσιμες λύσεις, ειδικά λόγω της αναμενόμενης εμφάνισης της 5G γενιάς κινητής επικοινωνίας.

Αναλύονται τα πειράματα, που εκτελέστηκαν στον ελεγκτή δικτύου ONOS και στον POX. Πραγματοποιήθηκαν διάφορα πειράματα σχετικά με τις μελέτες περίπτωσης εικονικού δρομολογητή, καθώς και στις περιπτώσεις των ασύρματων δικτύων. Εν συνεχεία, εκτελέστηκαν πειράματα σχετικά με την ασφάλεια, που μπορεί να βελτιωθεί σημαντικά αν υιοθετηθεί μία αρχιτεκτονική με τον συγκεκριμένο δικτυακό ελεγκτή. Ακόμα, σημειώθηκαν πειράματα σχετικά με την απόδοση των συστημάτων και ελέγχθηκε αν και κατά πόσο η υιοθέτηση μίας SDN προσέγγισης είναι δυνατό να επηρεάσει αρνητικά τα ενσύρματα και κινητά δίκτυα και να προσδώσει χαμηλότερες ταχύτητες μετάδοσης των πακέτων. Ακόμα,

δομήθηκε ένα σενάριο μίας τοπολογίας απαλλαγμένης από υλικό και ενσωματώνοντας σε αυτή λογισμικό ωθώντας παράλληλα σε νέες ιδέες και νέες αρχιτεκτονικές.

Εκτός από την εκτέλεση εντολών στο Mininet και στο Mininet-wifi, καθώς και στη διεπαφή του ONOS ελεγκτή, παρατίθενται και οι γραφικές απεικονίσεις των παραστάσεων, που δημιουργήθηκαν απεικονίζοντας τη σχέση του διαθέσιμου εύρους ζώνης και του ρυθμού μετάδοσης των δεδομένων σε ένα συγκεκριμένο χρονικό παράθυρο 15 δευτερολέπτων (0-15s). Το σημαντικό είναι ότι απεικονίζονται όλες οι ενέργειες και οι αλλαγές στο δίκτυο του ελεγκτή.

Με βάση αυτά τα αποτελέσματα, τα οποία παρατίθενται ακολούθως, εξάγονται τα βασικότερα συμπεράσματα σχετικά με την εισαγωγή εικονικών συσκευών στα δίκτυα. Επίσης, υπάρχουν εφαρμογές στα κινητά δίκτυα. Ακόμα, συνοψίζονται εφαρμογές των δικτύων αυτών με τη χρήση των τεχνολογιών SDN και NFV. Συγκρίνονται οι POX και ONOS δικτυακοί ελεγκτές και οι εφαρμογές αυτών στον ακαδημαϊκό χώρο και στα εργαστήρια δικτύων για να αναδειχθεί η συμβολή τους στην εξοικείωση των φοιτητών με τέτοιου είδους καινοτομίες. Ενώ, παρακάτω παρατίθενται αναλυτικά όλα τα πειράματα.

## 5.1 Virtual Router (vRouter)

Διεξήχθησαν πολλά πειράματα σχετικά με την περίπτωση χρήσης του SDN εικονικού δρομολογητή. Αναλυτικά, θα παρατεθούν τα βασικότερα βήματα, τα οποία ακολουθήθηκαν κατά την πειραματική διαδικασία σχετικά με τη συγκεκριμένη δημιουργούμενη τοπολογία. Ο ONOS είναι ένας ελεγκτής δικτύου, που περιλαμβάνει σημαντικές εντολές, οι οποίες έχουν δομηθεί ώστε να μπορούν ανά πάσα στιγμή να δίνουν στον ελεγκτή τη δυνατότητα να έχει τον έλεγχο του δικτύου και να «παρακολουθεί» συνολικά την κατάσταση και πως αυτή εξελίσσεται.

Τα βήματα, που πραγματοποιήθηκαν κατά την πειραματική διαδικασία είχαν ως κύριο σκοπό να αναδείξουν τη λειτουργία του μεταγωγέα ως δρομολογητή, πιθανά πειράματα για την επεξήγηση ενός εικονικού δρομολογητή σε ένα εργαστήριο δικτύων. Βασίζονται στον ONOS και τις εντολές, που περιλαμβάνει και αναλύονται παρακάτω:

- Με την εκκίνηση της διεπαφής του ONOS εκτελείται η εντολή «summary» πριν ξεκινήσει η τοπολογία στο δίκτυο. Η μόνη συσκευή, που εμφανίζεται είναι ο ελεγκτής δικτύου (ONOS). Δεν παρατίθεται κανένα άλλο στοιχείο. Το δίκτυο είναι κενό και έτοιμο να εισαχθεί η επιδιωκόμενη τοπολογία.

- Μετά την εισαγωγή της τοπολογίας μέσα στο δίκτυο και την εκτέλεση της εντολής «summary» υπάρχει μία επιπρόσθετη συσκευή, δηλαδή ο μεταγωγέας (switch). Αυτό είναι φυσιολογικό, καθώς ο ελεγκτής του δικτύου επικοινωνεί άμεσα με το μεταγωγέα, ο οποίος δρα ως δρομολογητής. Ακόμα, δεν έχει υπάρξει κάποια αλληλεπίδραση με το υπόλοιπο δίκτυο και ως αποτέλεσμα δεν είναι δυνατό να εμφανίζονται άλλες συσκευές κλπ.
- Μετά από εκτελέσεις της εντολής «ring», δηλαδή μετά από ελέγχους για τη συνδεσιμότητα μεταξύ των συσκευών των διαφόρων στοιχείων της τοπολογίας, στον ONOS υπάρχουν 2 διαφορετικοί υπολογιστές και διάφορες ροές δεδομένων, που ανταλλάζουν πακέτα. Τα πειράματα, που πραγματοποιούνται είναι αναλυτικά: «h1 ring h2», «h2 ring h1». Όλοι οι υπολογιστές είναι πλέον συνδεδεμένοι. Τα ring συνδέουν τους υπολογιστές μεταξύ τους και είναι υπεύθυνα για την ανταλλαγή πακέτων. Μετά τα πειράματα αυτά και οι δύο συσκευές εμφανίζονται στη διεπαφή του ελεγκτή και μπορεί να διαχειριστεί πιθανές σχετικές ενέργειες, όπως για παράδειγμα, αν είναι εφικτό να σταματήσει κάποιες ροές ή να σταματήσει ο ελεγκτής τη συνδεσιμότητα με κάποιον από τους υπολογιστές, το μεταγωγέα κλπ.
- Η εκτέλεση της εντολής «devices» εκ νέου εκτός από τον ελεγκτή περιλαμβάνει το μεταγωγέα, καθώς και τους υπολογιστές. Η εντολή αυτή δείχνει όλες τις συνδεδεμένες συσκευές στο δίκτυο.
- Τα πακέτα ανταλλάσσονται με 0% απώλειες σε μικρό χρονικό διάστημα, κάτι το οποίο φαίνεται εκτελώντας την εντολή «flows», δηλαδή τις ροές δεδομένων, που ανταλλάσσονται στην τοπολογία. Εκεί περιλαμβάνονται όλες οι ροές, που υπάρχουν στο δίκτυο και αναδεικνύονται μέσω της διεπαφής του ONOS.
- Με την εκτέλεση της εντολής «net» παρατηρείται η συνολική κατάσταση του δικτύου και διαφαίνεται η λειτουργία του μεταγωγέα ως δρομολογητή. Εκεί παρατηρούνται τα πιο σημαντικά στοιχεία του δικτύου, δηλαδή οι υπολογιστές, ο μεταγωγέας, ο ελεγκτής, οι ροές κλπ. Αποτυπώνει μία περίληψη της κατάστασης του δικτύου.

Στον POX δε μπορούν να εκτελεστούν τέτοιες εντολές. Το Mininet περιλαμβάνει και αναδεικνύει τις αλλαγές, που γίνονται στον POX. Ο POX περιλαμβάνει μία στοιχειώδη διεπαφή, που δείχνει στοιχεία για τη συνδεσιμότητα του στην τοπολογία και το δίκτυο και δεν είναι δυνατό μέσω αυτού να προκύψει διαχείριση της τοπολογίας. [100]

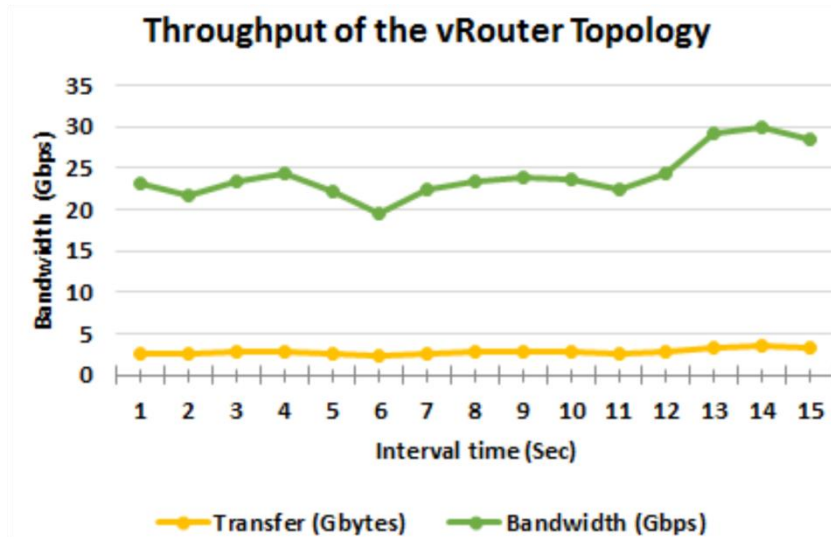
Τρέχοντας την ίδια τοπολογία στον POX και εκτελώντας πειράματα ring ανάμεσα στους υπολογιστές παρατηρείται πως οι υπολογιστές διασυνδέονται μεταξύ τους και σε αυτή την περίπτωση δια μέσου του SDN ελεγκτή και μπορούν να αλληλοεπιδρούν σημαντικά λόγω

των ισχυρών και ευφυών αυτών ελεγκτών. Από την άλλη μεριά, όμως, δεν παρατηρείται καμία τέτοια σημαντική και πλούσια διεπαφή, η οποία να αναδεικνύει κάθε φορά τα πιο σημαντικά από τα στοιχεία, που υπάρχουν στην τοπολογία με αποτέλεσμα, κάθε φορά, να πρέπει να ανατρέχει κανείς στο τερματικό και να παρατηρεί το δίκτυο. Ο POX έχει κάποιες δικές του πληροφορίες, που αναφέρουν στοιχεία για τη σύνδεσή του στο δίκτυο. Εντούτοις, δεν περιλαμβάνει το μεγάλο σετ εντολών του ONOS και ως αποτέλεσμα πρέπει κανείς να δημιουργήσει τις δικές του εφαρμογές και να τις τρέξει. Από την άλλη μεριά όμως, είναι σχετικά εύκολος στη χρήση του στην περίπτωση των ενσύρματων και εικονικών δικτύων και μπορεί πολύ εύκολα να συντελέσει στη διδασκαλία των δικτύων σε κάποιο εργαστήριο, κυρίως σε θέματα, που άπτονται της τοπολογίας και λιγότερο σε θέματα, που άπτονται της συνολικότερης εικόνας και των διασυνδεδεμένων συσκευών στο δίκτυο.

Συνολικά, η πειραματική διαδικασία καταδεικνύει ότι η υλοποίηση εικονικού δρομολογητή είναι δυνατή αν σε αυτόν ενταχθούν λογικές προγραμματισμού και τροποποιηθεί η συμπεριφορά του ώστε να συμπεριφέρεται σα δρομολογητής. Ακόμα, είναι δυνατό να εισαχθούν στην τοπολογία πλήθος συσκευών και υπολογιστών, οι οποίες ελέγχονται από τον ελεγκτή δικτύου. Όλες οι συσκευές είναι συνδεδεμένες μεταξύ τους, διότι είναι δυνατό να ανταλλάζουν μηνύματα κάτι το οποίο διαφαίνεται και στον ελεγκτή. Ακόμα, η απώλεια πακέτων είναι πολύ χαμηλή και κατ' επέκταση μπορεί να επιτευχθούν υψηλοί ρυθμοί μετάδοσης. Κάθε αλλαγή, που συντελείται στο δίκτυο διαφαίνεται επίσης και στον ελεγκτή του δικτύου. [99]

Το TCP είναι το βασικό πρωτόκολλο 4<sup>ου</sup> επιπέδου ISO/OSI. Το συγκεκριμένο πρωτόκολλο μεταδίδει πληροφορία. Εκτός αυτού, είναι ένα ιδιαίτερα αξιόπιστο πρωτόκολλο, αφού πριν από τη μετάδοση υπάρχουν μηνύματα acknowledge, δηλαδή, αναγνώρισης για την εγκαθίδρυση σύνδεσης μεταξύ των δύο συνδεδεμένων μερών. Έπειτα, αποστέλλονται τα δεδομένα. Στο τέλος, αποστέλλονται μηνύματα τερματισμού. Μετά από πειράματα απόδοσης, παρατίθενται οι ροές δεδομένων ως απόδοση προς χρόνο. Το δίκτυο είναι αποδοτικό. Στο χρονικό διάστημα 0-15sec από την αρχή του πειράματος 42.2Gbytes μεταφέρονται συνολικά και το διαθέσιμο εύρος ζώνης κατά μέσο όρο είναι στα 24.1 Gbps.

Στην εικόνα 5.1 παρατίθεται η απόδοση του δρομολογητή ως συνάρτηση του χρόνου. Η γραφική αυτή απεικόνιση δείχνει τη μεταφορά σε Gbytes, καθώς και το εύρος ζώνης σε GBps. Αυτά τα πειράματα, προκύπτουν από το mininet με τη χρήση xterm για τα συστατικά του δικτύου. Εν τούτοις, για λόγους απεικόνισης, η γραφική παράσταση μεταφέρθηκε στο excel, διότι θεωρείται ότι προέκυψε ποιο ξεκάθαρη απεικόνιση με το συγκεκριμένο εργαλείο.



Εικόνα 5.1: Η απόδοση του εικονικού δρομολογητή ως συνάρτηση του χρόνου.

## 5.2 Internet Protocol Radio Access Network (IPRAN)

Διεξήχθησαν πολλαπλά πειράματα σχετικά με την περίπτωση χρήσης του ONOS IPRAN σε κινητό δίκτυο SDN. Αναλυτικά, θα παρατεθούν τα βασικότερα βήματα, τα οποία ακολουθήθηκαν κατά την πειραματική διαδικασία σχετικά με τη συγκεκριμένη δημιουργούμενη τοπολογία. Τα βήματα αυτά έχουν ως στόχο να αναδείξουν πως το ONOS ανταποκρίνεται στις νέες συνθήκες και ιδίως στα κινητά δίκτυα και πως είναι δυνατό να διατηρεί τον έλεγχο του δικτύου ακόμα και σε κινητές τοπολογίες. [99]

Στην πρώτη τοπολογία περιλαμβάνεται ένα σημείο πρόσβασης και δύο σταθμοί βάσης. Τα βήματα, που πραγματοποιήθηκαν αναλύονται παρακάτω:

- Με την εκκίνηση της διεπαφής του ONOS εκτελείται η εντολή «summary» πριν εκκινηθεί η τοπολογία. Η μόνη συσκευή, που εμφανίζεται είναι ο ελεγκτής δικτύου (ONOS). Κάτι, που κρίνεται ως φυσιολογικό μιας και δεν έχουν εισαχθεί άλλες εντολές και κατά συνέπεια, δεν είναι δυνατό
- Μετά την εισαγωγή της τοπολογίας μέσα στο δίκτυο και την εκτέλεση της εντολής «summary» υπάρχει μία επιπρόσθετη συσκευή, δηλαδή το σημείο πρόσβασης (access point). Αυτό είναι φυσιολογικό, αφού αυτή είναι η βασική συσκευή, που αλληλοεπιδρά με τον ελεγκτή και αποτελεί το σημείο επικοινωνίας του δικτύου και του ελεγκτή.
- Μετά από εκτελέσεις της εντολής «ping», δηλαδή μετά από ελέγχους για τη συνδεσιμότητα μεταξύ των συσκευών των διαφόρων στοιχείων της τοπολογίας, στον



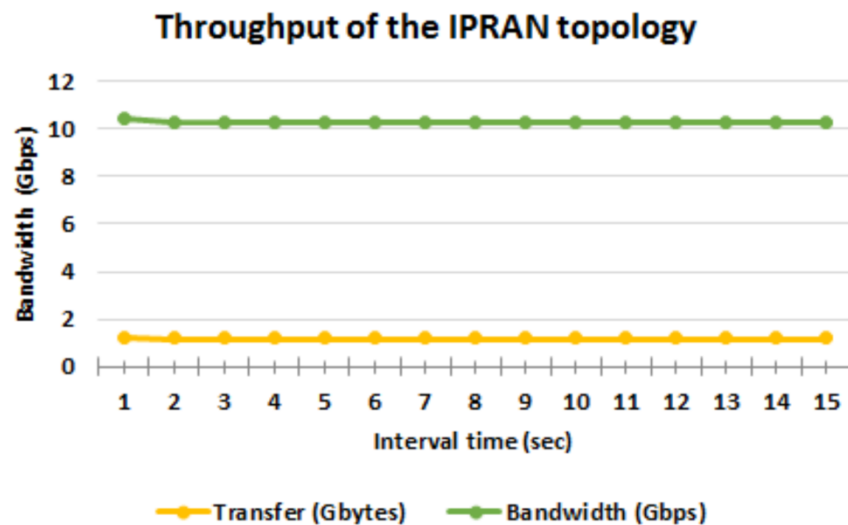
ONOS υπάρχουν 2 διαφορετικοί σταθμοί βάσης και διάφορες ροές δεδομένων, που ανταλλάζουν πακέτα. Τα πειράματα, που πραγματοποιούνται είναι αναλυτικά: «bs<sub>1</sub> ring bs<sub>2</sub>», «bs<sub>2</sub> ring bs<sub>1</sub>». Όλοι οι σταθμοί βάσης είναι πλέον συνδεδεμένοι. Το δίκτυο φαίνεται συνδεδεμένο και τα πακέτα ανταλλάσσονται με εύρυθμο τρόπο.

- Η εκτέλεση της εντολής «devices» εκ νέου εκτός από τον ελεγκτή περιλαμβάνει το access point, καθώς και τους σταθμούς βάσης. Κάτι το οποίο αποτελεί ένα πολύ σημαντικό κριτήριο για το ότι ο ελεγκτής έχει κάθε φορά τον έλεγχο του δικτύου συνολικά. Στη διεπαφή του ONOS απεικονίζονται όλες οι συνδεδεμένες συσκευές και με χρήση των εντολών, που υπάρχουν στον ONOS, μπορεί να σταματήσει κανείς ή να εκκινήσει τις συσκευές κλπ.
- Τα πακέτα ανταλλάσσονται με 0% απώλειες σε μικρό χρονικό διάστημα, κάτι το οποίο φαίνεται εκτελώντας την εντολή «flows», δηλαδή οι ροές δεδομένων, που ανταλλάσσονται στην τοπολογία. Με αυτή την εντολή γίνεται εμφανές το σύνολο των ροών και ως αποτέλεσμα μπορεί να σταματήσει κανείς κάποια ροή μέσα από τη διεπαφή του ελεγκτή αν θέλει.
- Με την εκτέλεση της εντολής «net» παρατηρείται η συνολική κατάσταση του δικτύου και διαφαίνεται η λειτουργία των συσκευών. Κάτι τέτοιο είναι πολύ σημαντικό και αποτελεί την κυριότερη πηγή ελέγχου στο δίκτυο. Με τον τρόπο αυτό υπάρχει η δυνατότητα να ανακοπεί η κίνηση στο δίκτυο αν και εφόσον, παρατηρηθεί κάτι μη ομαλό και η κίνηση φαίνεται να μη διεξάγεται φυσιολογικά.

Στην εικόνα 5.2 παρατίθεται η απόδοση της τοπολογίας IPRAN. Διαφαίνεται πως η απόδοση στο δίκτυο διατηρείται σε υψηλά επίπεδα σε όλη τη διάρκεια των πειραμάτων σε όλο το παράθυρο των 15 δευτερολέπτων. Από την άλλη μεριά, παρατηρείται χαμηλότερη απόδοση σε σχέση με το ενσύρματο δίκτυο, κάτι που είναι πολύ πιο φυσιολογικό, διότι τα κινητά δίκτυα αντιμετωπίζουν το ζήτημα των παρεμβολών, το οποίο αποτελεί και το σημαντικότερο πρόβλημα των δικτύων τέτοιου τύπου και την πιο σημαντική ερώτηση στον τομέα των επικοινωνιών μέχρι στιγμής. Επίσης, η γραφική απεικόνιση επιλέχθηκε να γίνει σε ms excel, διότι θεωρήθηκε ότι η εφαρμογή αυτή δίνει καλύτερα αποτελέσματα γραφικής απεικόνισης συγκριτικά με τα δικτυακά εργαλεία. [99]

Όσον αφορά στον POX, η συγκεκριμένη τοπολογία μπορεί να εκτελεστεί και να έχει σημαντικά αποτελέσματα. Εκεί, εμφανίζονται στοιχεία για τη συνδεσιμότητα του ελεγκτή στο δίκτυο, ενώ όλοι οι χειρισμοί πρέπει να γίνουν δια μέσου του τερματικού στο mininet-wifi. Κάτι τέτοιο συμβαίνει επειδή αυτός ο ελεγκτής δεν περιλαμβάνει πλούσια γραφική διεπαφή

και πλήθος εντολών. Από την άλλη μεριά, όμως αν βασικός στόχος είναι η ρύθμιση παραμέτρων και η δημιουργία τοπολογιών στο δίκτυο, τότε ίσως προσδίδει σημαντικά εκπαιδευτικά οφέλη. [100]



Εικόνα 5.2: Η απόδοση της τοπολογίας IPRAN ως συνάρτηση του χρόνου.

Εν συνεχεία, όσον αφορά στα πειράματα για την ετερογενή περίπτωση, δημιουργείται μία τοπολογία, που περιλαμβάνει 2 σταθμούς βάσης, 1 σημείο πρόσβασης, 4 μεταγωγείς, και 4 υπολογιστές ανά μεταγωγέα. Αυτό άμεσα προϋποθέτει ότι υπάρχουν και ενσύρματα και ασύρματα στοιχεία και πως όλα αυτά είναι σε θέση να αλληλοεπιδράσουν μεταξύ τους και με τον ελεγκτή. [99], [100]

Στη συγκεκριμένη περίπτωση εισάγεται μία επιπρόσθετη τοπολογία για ετερογενή δίκτυα. Τα περισσότερα δίκτυα είναι σήμερα συνδυασμοί των ασύρματων και ενσύρματων δικτύων. Αυτός είναι ο λόγος, που θεωρήθηκε βασικό να παρουσιαστεί και μία τοπολογία, η οποία περιλαμβάνει και κινητά και ενσύρματα στοιχεία. Τα βήματα, που πραγματοποιήθηκαν στην περίπτωση αυτή, έχουν ως κύριο στόχο να αναδείξουν το ρόλο των ελεγκτών και σε αυτή τη κατάσταση και αναλύονται παρακάτω:

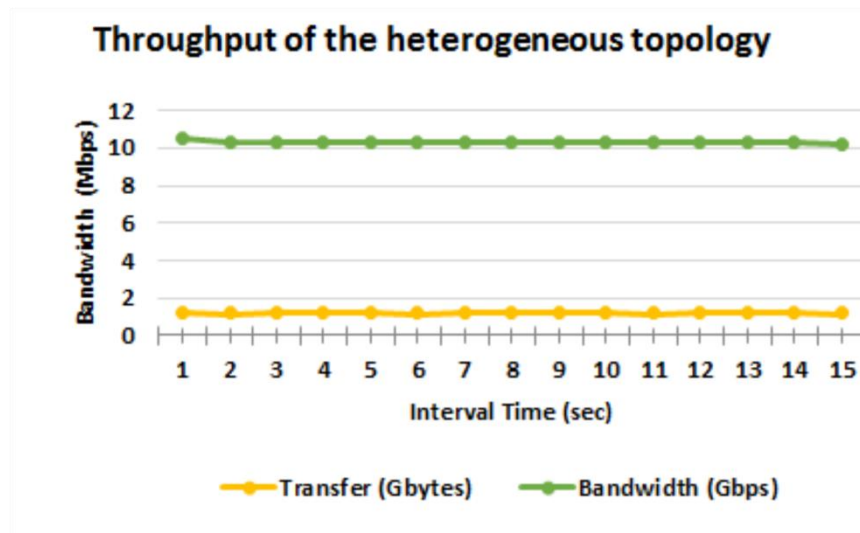
- Με την εκκίνηση της διεπαφής του ONOS εκτελείται η εντολή «summary» πριν να ξεκινήσει η τοπολογία στο δίκτυο. Η μόνη συσκευή, που εμφανίζεται είναι ο ελεγκτής δικτύου (ONOS). Αυτό είναι φυσιολογικό αφού η βασική συσκευή, που επικοινωνεί ο ελεγκτής με το δίκτυο είναι αυτή. Επίσης, δεν έχει σημειωθεί κάποια άλλη αλληλεπίδραση με κάποιο στοιχείο του δικτύου για να φαίνεται κάτι διαφορετικό.
- Μετά την εισαγωγή της τοπολογίας μέσα στο δίκτυο και την εκτέλεση της εντολής «summary» υπάρχει μία επιπρόσθετη συσκευή, δηλαδή το σημείο πρόσβασης (access

point) και ο μεταγωγέας. Εφόσον, εισήχθη η τοπολογία στο δίκτυο παρατηρούνται οι συσκευές, που άμεσα αλληλοεπιδρούν με το δικτυακό ελεγκτή. Έτσι, είναι δυνατό να παρατηρείται η δραστηριότητα του δικτύου.

- Μετά από εκτελέσεις της εντολής «ring», δηλαδή μετά από ελέγχους για τη συνδεσιμότητα μεταξύ των συσκευών των διαφόρων στοιχείων της τοπολογίας, στον ONOS υπάρχουν 2 διαφορετικοί σταθμοί βάσης και διάφορες ροές δεδομένων, που ανταλλάζουν πακέτα. Τα πειράματα, που πραγματοποιούνται είναι αναλυτικά: «bs<sub>1</sub> ring bs<sub>2</sub>», «bs<sub>2</sub> ring bs<sub>1</sub>», «h<sub>1</sub> ring h<sub>2</sub>», «h<sub>2</sub> ring h<sub>1</sub>», «h<sub>2</sub> ring h<sub>3</sub>», «h<sub>3</sub> ring h<sub>2</sub>», », «h<sub>3</sub> ring h<sub>4</sub>», «h<sub>4</sub> ring h<sub>3</sub>. Όλοι οι υπολογιστές και τα λοιπά στοιχεία, που εμφανίζονται στην τοπολογία είναι πλέον συνδεδεμένα και έχουν ανταλλάξει πακέτα.
- Η εκτέλεση της εντολής «devices» εκ νέου εκτός από τον ελεγκτή περιλαμβάνει το access point, τους σταθμούς βάσης, το μεταγωγέα και τους υπολογιστές. Αυτό είναι φυσιολογικό, εφόσον έχει ήδη παρατηρηθεί δράση στο δίκτυο εμφανίζονται στην τοπολογία και αποτελούν τα στοιχεία αυτής.
- Τα πακέτα ανταλλάσσονται με 0% απώλειες σε μικρό χρονικό διάστημα, κάτι το οποίο φαίνεται εκτελώντας την εντολή «flows», δηλαδή οι ροές δεδομένων, που ανταλλάσσονται στην τοπολογία. Εκεί περιλαμβάνονται όλες οι δυνατές ροές. Έτσι, αν παρατηρηθεί κάτι περίεργο ή ασυνήθιστο, όπως για παράδειγμα αν μία τοπολογία μονοπωλεί τους πόρους του δικτύου είναι δυνατό να διακοπεί η ροή αυτή και να σταματήσει διαφυλάσσοντας το δίκτυο να μην καταστεί αχρησιμοποίητο, ή να μην πέσει σε κάποια περίπτωση επίθεσης, όπως για παράδειγμα DOS ή DDOS.
- Με την εκτέλεση της εντολής «net» παρατηρείται η συνολική κατάσταση του δικτύου και διαφαίνεται η λειτουργία των συσκευών. Είναι μία πολύ σημαντική εντολή για τη διαχείριση και τον έλεγχο της λειτουργίας του δικτύου. Το δίκτυο, μπορεί να ελέγχεται από αυτή την εντολή, η οποία καταγράφει αναλυτικά πόσες και ποιες συσκευές υπάρχουν στο δίκτυο, πώς αυτές διασυνδέονται κλπ.

Λόγω της πειραματικής διαδικασίας είναι δυνατό να εισαχθούν στην τοπολογία πλήθος συσκευών, οι οποίες ελέγχονται από τον ελεγκτή δικτύου ONOS. Όλες οι συσκευές είναι συνδεδεμένες μεταξύ τους, διότι είναι δυνατό να ανταλλάζουν μηνύματα μεταξύ τους κάτι το οποίο διαφαίνεται και στον ελεγκτή. Ακόμα, η απώλεια πακέτων είναι πολύ χαμηλή και κατ' επέκταση μπορεί να επιτευχθούν υψηλοί ρυθμοί μετάδοσης. Κάθε αλλαγή, που συντελείται στο δίκτυο διαφαίνεται επίσης και στον ελεγκτή του δικτύου ONOS. Στην περίπτωση αυτή χρησιμοποιείται το Mininet-wifi, διότι η IPRAN είναι μία μελέτη περίπτωσης κινητών

επικοινωνιών. Έτσι, εισάγονται στοιχεία, όπως οι σταθμοί βάσης και τα σημεία πρόσβασης. Με βάση αυτή τη λογική είναι δυνατό να εισαχθεί και κινητικότητα στο δίκτυο και να υπάρχουν συσκευές, που μετακινούνται από τον έναν σταθμό στον άλλον και έτσι να μελετηθούν και άλλα στοιχεία, όπως για παράδειγμα, τα handovers και οι παρεμβολές. [99], [100].



Εικόνα 5.3: Η απόδοση της τοπολογίας IP-RAN για την ετερογενή τοπολογία ως συνάρτηση του χρόνου.

Στον POX δε μπορούν να εκτελεστούν τέτοιες εντολές. Το Mininet περιλαμβάνει και αναδεικνύει τις αλλαγές, που γίνονται στον POX. Ο POX περιλαμβάνει μία στοιχειώδη διεπαφή, που δείχνει στοιχεία για τη συνδεσιμότητα του στην τοπολογία και το δίκτυο και δεν είναι δυνατό μέσω αυτού να προκύψει διαχείριση της τοπολογίας. Ο POX εκτελεί κανονικά την κάθε τοπολογία και αποτελεί μία πολύ σημαντική προέκταση για ακαδημαϊκούς σκοπούς. Από την άλλη μεριά, η δημιουργία συγκεκριμένων υπηρεσιών ή εφαρμογών μπορεί να αποτελέσει πολύ περίπλοκη διαδικασία στον POX και να χρειάζεται η εξειδίκευση και η αφιέρωση πολύ χρόνο για να δημιουργηθεί κάτι πιο σύνθετο, κάτι που σα λογική μπορεί να διαφέρει από τα εργαστήρια δικτύων και να αποτελέσει μεγάλο φόρτο. [100]

Το TCP είναι το βασικό πρωτόκολλο 4<sup>ου</sup> επιπέδου ISO/OSI. Το συγκεκριμένο πρωτόκολλο μεταδίδει πληροφορία. Εκτός αυτού, είναι ένα ιδιαίτερα αξιόπιστο πρωτόκολλο, αφού πριν από τη μετάδοση υπάρχουν μηνύματα acknowledge, δηλαδή, αναγνώρισης για την εγκαθίδρυση σύνδεσης μεταξύ των δύο συνδεόμενων μερών. Έπειτα, αποστέλλονται τα δεδομένα. Στο τέλος, αποστέλλονται μηνύματα τερματισμού. Μετά από πειράματα απόδοσης, παρατίθενται οι ροές δεδομένων ως απόδοση προς χρόνο. Το δίκτυο είναι αποδοτικό. Στο

χρονικό διάστημα 0-15sec από την αρχή του πειράματος 19.2Mbytes μεταφέρονται συνολικά και το διαθέσιμο εύρος ζώνης κατά μέσο όρο είναι στα 10.3 Mbps. Στην εικόνα 5.3 φαίνεται η απόδοση της συγκεκριμένης τοπολογίας. Ενώ, φαίνεται να είναι σε σταθερά επίπεδα, εν τούτοις είναι πολύ χαμηλότερα από εκείνα της ενσύρματης περίπτωσης, κάτι που είναι πολύ πιο φυσιολογικό. Η απόδοση στα ασύρματα δίκτυα είναι παραδοσιακά πολλές φορές χαμηλότερη, ειδικά λόγω των παρεμβολών, που σημειώνονται.

### 5.3 Mobile Central Office Re-Imagined as a Data Center (MCORD)

Η μελέτη περίπτωσης MCORD είναι αρκετά σημαντική. Οι τεχνολογίες SDN και NFV σε συνδυασμό με τις cloud τεχνικές έχουν προσδώσει πολύ διαφορετικά χαρακτηριστικά στο συγκεκριμένο επίτευγμα και αποτελούν μία πολύ σημαντική προσέγγιση όσον αφορά στην απόδοσή του, στην οικονομικότερη προσέγγιση και σε διάφορες μεθόδους, που εξασφαλίζουν πολύ σημαντικά πλεονεκτήματα για τη διαχείριση των δεδομένων και για τα κινητά δίκτυα. Η σημασία του CORD και MCORD καταδεικνύεται από τα πειράματα, τα οποία πραγματοποιήθηκαν και τα αποτελέσματα, τα οποία ελήφθησαν. Αναλυτικά, γίνονται τα πιο κάτω πειράματα, για να διαπιστωθούν οι δυνατότητες, που προσφέρει αυτή η τεχνολογία γενικότερα, αλλά και ειδικότερα στην εκπαιδευτική διαδικασία.

Αρχικά, για την πειραματική διαδικασία επιλέγονται οι παράμετροι, οι οποίες χρησιμοποιούνται και έχουν επεξηγηθεί από το ON.LAB αναλυτικότερα. Υπάρχει μία πολύ μεγάλη διαθέσιμη κοινότητα, που ασχολείται μόνο με το SDN CORD και παρουσιάζει και περιλαμβάνει τα πολύ σημαντικά πλεονεκτήματα. Αυτά παρουσιάζονται αναλυτικά. Η MCORD ξεκίνησε ως μία μελέτη περίπτωσης του ONOS ελεγκτή, σήμερα όμως, έχει μία δικιά της πολύ ενεργή κοινότητα χρηστών και εθελοντών, που ασχολούνται.

Παρατηρώντας προσεχτικά, υπάρχει μία μεγάλη ποικιλία δυνατοτήτων και εφαρμογών, που μπορεί να προκύψουν. Πολλά πειράματα, αλλά και εμπορικά πολλές υπηρεσίες μπορεί να δομηθούν με τον τρόπο αυτό. Πιο συγκεκριμένα, μπορούν να συμπεριληφθούν πολλές υπηρεσίες: RAN, Edge, εικονικό EPC. Είναι σημαντικό ότι αυτές οι υπηρεσίες είναι εύκολα διαχειρίσιμες και μπορούν να δημιουργούνται πολύ εύκολα. Εν συνεχεία, έχουν πολύ σημαντικά οφέλη, αφού περιλαμβάνουν διάφορες υπό-περιπτώσεις.

Κάθε μία από τις υπηρεσίες περιλαμβάνει και άλλα στοιχεία, όπως για παράδειγμα:

- Το RAN περιλαμβάνει εικονικό δίκτυο σύνδεσης επιχειρήσεων Business Connection Network (vBCN), εικονικό BBU και το συμβατικό BBU. Αρχικά, το vBCN μπορεί να

συμβάλει ενεργά ακόμα και σε εμπορικές εφαρμογές. Μπορεί να αξιοποιηθεί από εταιρείες με σκοπό την κάλυψη των δικών τους εικονικών δικτύων και να προκύψουν από αυτό σημαντικά οφέλη άμεσα για μία επιχείρηση, που δεν θα χρειάζεται ενσύρματη υποδομή και πολύπλοκες ακριβές συσκευές, για να πραγματοποιήσει τη σύνδεση όλων των χρηστών της. Από την άλλη μεριά, μπορεί να προκύψουν κι έμμεσα οφέλη, αν ένας πάροχος στηρίζει την παροχή εικονικών δικτύων σε άλλες επιχειρήσεις, πάνω σε αυτή την υπηρεσία. Το ότι υπάρχει εικονικό και συμβατικό BBU αποτελεί επίσης ένα πολύ σημαντικό στοιχείο. Από τη μία πλευρά, σήμερα ολοένα και περισσότερο σημειώνεται η ανάγκη να στρέφεται κανείς στο λογισμικό και να αποφεύγονται ειδικά κόστη και έξοδα για το εύρος ζώνης ή να επαναχρησιμοποιούνται πόροι για λόγους οικονομίας από την άλλη πλευρά, όμως υπάρχει και η ανάγκη να είναι συμβατές οι νέες τεχνολογίες, εφαρμογές και υπηρεσίες με τις παλιότερες, οπότε είναι εξαιρετικά σημαντικό το ότι μπορεί και υποστηρίζεται αντίστοιχα και το συμβατικό μέρος.

- Το Edge περιλαμβάνει τείχος προστασίας, κρυφή μνήμη και βελτιστοποίηση video. Το τείχος προστασίας είναι πολύ σημαντικό καθότι βοηθά σημαντικά στην παροχή ασφάλειας. Με τις σημερινές τεχνολογίες γίνεται ολοένα και πιο επιτακτική η ανάγκη για υψηλότερα επίπεδα ασφάλειας. Σε ένα τείχος προστασίας είναι δυνατό να ενσωματωθούν κανόνες, οι οποίοι να επιτρέπουν ή να απαγορεύουν κάποιες συγκεκριμένες συμπεριφορές, π.χ. ανεξέλεγκτη κίνηση κλπ. αποτρέποντας έτσι να βγει εκτός λειτουργίας το δίκτυο. Η κρυφή μνήμη είναι σημαντική για την πιο αποδοτική κυκλοφορία στο διαδίκτυο. Πληροφορία αποθηκευμένη στην κρυφή μνήμη γίνεται πιο γρήγορα διαθέσιμη αν ζητηθεί. Μία εξίσου σημαντική εφαρμογή είναι η βελτιστοποίηση video. Το video αποτελεί σημαντικό παράγοντα πολυμέσων και κατά συνέπεια, συχνά απαιτούνται κινήσεις και ενέργειες για τη βελτιστοποίηση του.
- Το εικονικό EPC περιλαμβάνει το v-PGW και MME. Μία άλλη σημαντική προσπάθεια, που σημειώνεται είναι η εικονική οπτική του EPC. Είναι μία προτεινόμενη τακτική στα δίκτυα SDN να γίνονται προσπάθειες να αντικαθίστανται με εικονικά κάποια μέρη του δικτύου. Με τον τρόπο αυτό μειώνεται το κόστος, μειώνεται η συντήρηση και μειώνονται διάφορα προβλήματα. Επίσης, οι νέες αρχιτεκτονικές γίνονται πιο ενιαίες μίας και σήμερα ολοένα και περισσότερο γίνεται επιτακτική η ανάγκη μεταφοράς των δικτύων σε λογισμικό έναντι του υλικού. Και οι δύο αυτές ενότητες είναι πολύ σημαντικές. Η v-PGW σχετίζεται με τα δεδομένα στο δίκτυο, κάτι που είναι ιδιαίτερα σημαντικό και η ορθή διαχείρισή τους απασχολεί πολύ τον

επιστημονικό κόσμο σήμερα. Ενώ, το MME είναι πολύ σημαντικό για τη διαχείριση της κίνησης στο δίκτυο και περιλαμβάνει πληροφορία σχετικά με τη διαχείριση της κίνησης και την εκκίνηση και περάτωση διαδικασιών.

Αυτές οι υπηρεσίες βρίσκονται εντός μίας πλατφόρμας παρόχου υπηρεσιών. Υπάρχουν διάφορες κατηγορίες υπηρεσιών. Οι περισσότερες συσκευές και τα περισσότερα δικτυακά μέρη τρέχουν σε εικονικές μηχανές. Μπορούν να δημιουργηθούν πολλά στιγμιότυπα εικονικών μηχανών χρησιμοποιώντας τη δεδομένη πλατφόρμα. Οι συγκεκριμένοι πάροχοι είναι δυνατόν να αποκτήσουν κέρδη δημιουργώντας νέες υπηρεσίες και νέες ευκαιρίες κέρδους. Ακόμα, μεγάλες υπηρεσίες, όπως εταιρείες αποθήκευσης μεγάλου όγκου δεδομένων είναι δυνατό να έχουν τη δυνατότητα να αξιοποιούν αυτές τις τεχνολογίες και να διαχειρίζονται καλύτερα τη σχετική πληροφορία. Είναι σημαντικό ότι σε αυτές τις μεθόδους, ο μεγάλος όγκος των δεδομένων μπορεί να αξιοποιείται καλύτερα και να διατίθεται πιο ορθά η πληροφορία.

Ακόμα, πολλές ακόμα δικτυακές εφαρμογές μπορούν να ελέγχονται από μακριά. Η κρυφή μνήμη και το τείχος προστασίας συμπεριλαμβάνονται στις υπηρεσίες του Edge, οι οποίες είναι δυνατό να ενεργοποιηθούν-απενεργοποιηθούν για τους χρήστες. Η αξιοποίηση αυτών των τεχνικών μπορεί να καθορίσει κατηγορίες χρηστών, στους οποίους να παρέχονται διαφοροποιημένες υπηρεσίες. Από τη μία πλευρά, μπορεί κάποιοι χρήστες, που έχουν πληρώσει, για παράδειγμα, να απολαμβάνουν αυτές τις υποδομές, ενώ από την άλλη μεριά, να είναι δυνατό να περιορίζονται κάποιοι χρήστες σε λιγότερες υπηρεσίες.

Ένα ακόμα βασικό πλεονέκτημα, που παρέχεται από το MCORD είναι η βελτιστοποίηση video. Οι ροές video απαιτούν υψηλές δικτυακές υποδομές και πόρους. Οι ροές video σήμερα αποτελούν τα δεδομένα, που καταλαμβάνουν και καταναλώνουν τα περισσότερα δεδομένα στο διαδίκτυο. Για παράδειγμα, υπάρχουν ζωντανές μεταδόσεις από πολλά κοινωνικά δίκτυα. Επίσης, είναι γνωστό ότι πολλοί χρήστες επιθυμούν και παρακολουθούν ταινίες, σειρές, αγώνες ποδοσφαίρου κλπ. ζωντανά ακόμα και από κινητές συσκευές.

Υπάρχουν άλλου είδους εφαρμογές, στις οποίες το πιο βασικό ζήτημα είναι η απόκριση σε πραγματικό χρόνο. Συνεπώς, σε αυτές τις εφαρμογές, μπορεί να μην είναι ιδιαίτερα μεγάλο το πλήθος των δεδομένων, που ανταλλάσσονται, εντούτοις είναι επιτακτική η ανάγκη να κυκλοφορήσουν γρήγορα και να αποκρίνονται ταχύτατα σε αλλαγές. Κρίνεται λοιπόν σκόπιμο να μελετηθεί-ερευνηθεί αν και κατά πόσο μπορεί να υπάρξει μία σχετική ομαδοποίηση-διαφοροποίηση ροών χωρίζοντας τις ροές video από τις ροές, που απαιτούν απόκριση σε πραγματικό χρόνο.

Άλλες θεμελιώδεις δυνατότητες του MCORD είναι ότι παρέχεται ένα περιβάλλον βελτιστοποίησης κυψελών. Είναι δυνατό να βελτιωθεί η μετάδοση πληροφορίας μεταξύ κυψελών. Πολλά σενάρια όσον αφορά στο τεμαχισμό των ροών του δικτύου μπορούν να δοκιμαστούν και να ελεγχτούν με βάση τη συγκεκριμένη υπηρεσία.

Επιπρόσθετο πλεονέκτημα είναι ότι όλα τα παραπάνω τρέχουν σε εικονικές μηχανές χρησιμοποιώντας τεχνικές NFV, με το να αποφεύγεται η επένδυση σε υλικό, που είναι πολύ πιο επιχειρηματικά «επικίνδυνη» διαδικασία, καθώς ενέχει ρίσκο, αφού συχνά η τεχνολογία προωθείται σημαντικά και το υλικό γίνεται σύντομα παρωχημένο. Για παράδειγμα, τα HSS, MME, P-GW και πολλά ακόμα τρέχουν σε εικονικές μηχανές. Έτσι, είναι δυνατό να δημιουργηθούν πολλά στιγμιότυπα μηχανημάτων σε εικονικά μηχανήματα. Όλες οι συσκευές συνδέονται και αποσυνδέονται εύκολα. Επίσης, το διαθέσιμο εύρος ζώνης μπορεί να αξιοποιείται δυναμικά και να διαχειρίζεται καλύτερα.

Όλες οι ενέργειες σχετικά με τις υπηρεσίες, τη σύνδεση και αποσύνδεση συσκευών από το δίκτυο κλπ. είναι εμφανείς και στην πλατφόρμα. Με την παρούσα τεχνική υπάρχει άμεση είσοδος στους χρονο-προγραμματιστές στην άνοδο και στην κάθοδο δεδομένων. Ακόμα, όλη η κυκλοφορία, οι συσκευές κλπ. εκτός από την πλατφόρμα είναι εμφανή και στο terminal. Παρόλα αυτά η πλατφόρμα είναι μία πολύ εύχρηστη μέθοδος απεικόνισης και διαχείρισης του δικτύου και των όσων έχουν συμβεί σε αυτό.

Η συγκεκριμένη μελέτη περίπτωσης παρέχεται μόνο από τον ελεγκτή ONOS. Ο POX δεν περιλαμβάνει κάποια αντίστοιχη μελέτη περίπτωσης. Με αποτέλεσμα, για να πραγματοποιηθούν σχετικά πειράματα με σκοπό να πραγματοποιηθεί έλεγχος των δυνατοτήτων του MCORD και για την εφαρμογή των τεχνικών του SDN και NFV σε αντίστοιχα είδη κινητών δικτύων, θα πρέπει να δημιουργηθεί αντίστοιχη εφαρμογή στον POX και να πραγματοποιηθούν αντίστοιχα πειράματα. Είναι προφανές ότι σε μία τέτοια περίπτωση, πολύτιμος χρόνος, ο οποίος θα μπορούσε να αποδίδεται σε άλλες εφαρμογές, για παράδειγμα στη δημιουργία σεναρίων για ροές στα δίκτυα πέμπτης γενιάς κινητής επικοινωνίας θα είχε σπαταληθεί με βασικό στόχο να δημιουργηθεί η αντίστοιχη εφαρμογή στον POX. Ακόμα, ο ONOS έχει μία πλούσια διεπαφή και συνεπώς, δεν είναι γνωστό αν θα μπορούσαν να φαίνονται τόσες λεπτομέρειες, όπως αυτές που εμφανίζονται στη διεπαφή του MCORD.

Ακόμα όσον αφορά στην εκπαιδευτική διαδικασία, αν στόχος είναι η εκμάθηση δημιουργίας του MCORD, τότε ο POX, που υποστηρίζει τη δημιουργία νέων εφαρμογών είναι μία πολύ σημαντική λύση, η οποία μπορεί να αποτελέσει πολύ σημαντικό εφαλτήριο για εμβάθυνση σε θέματα κώδικα και εφαρμογών. Από την άλλη μεριά, αν στόχος είναι η διερεύνηση των δυνατοτήτων και των σημαντικότερων παραγόντων σχετικά με το CORD,



θεωρητικά σημεία του MCORD, η ανάλυση της συμπεριφοράς των εικονικών τμημάτων του δικτύου και άλλες σημαντικές εφαρμογές, όπως για παράδειγμα η απεικόνιση, εξέταση και ρύθμιση διαφόρων παραγόντων, τότε η συγκεκριμένη λύση μπορεί να συντελέσει σημαντικά ως εργαλείο χρήσης σε εργαστήρια δικτύων για την ανάδειξη αυτών των τεχνικών και ζητημάτων.

Σε κάθε περίπτωση παρατηρείται ότι ο συνδυασμός των τεχνολογιών SDN και NFV αποτελεί μία πολύ δυναμική εναλλακτική ακόμα και σε περιπτώσεις, όπως είναι αυτές οι σχετικές με το CORD και συμβάλει σημαντικά στον εκσυγχρονισμό και σε μία νέα οπτική των δικτύων, που οι τεχνικές νέφους κατέχουν πολύ πιο ενεργό και σημαντικό ρόλο. Ενώ, διαφαίνεται πως το πλήθος των εφαρμογών, που υποστηρίζουν δεν έχει αναδείξει ξεκάθαρα το μελλοντικό τους ρόλο, αφού μπορούν να συμπληρώνουν κενά, που θα δημιουργηθούν μελλοντικά.

#### 5.4 Ασφάλεια στα δίκτυα 5G με χρήση SDN

Με σκοπό να φανεί ο ρόλος της ασφάλειας και της λειτουργίας του ελεγκτή σε ασφαλές mode, διενεργούνται σε αυτόν διάφορα πειράματα. Στα πειράματα αυτά φαίνεται η απόκριση του ελεγκτή στο δίκτυο μετά την επίθεση σε δύο περιπτώσεις, δηλαδή στην περίπτωση, που ασφαλίζεται ο ελεγκτής και στην αντίθετη περίπτωση. Έτσι, γίνεται σημαντικό να καταγραφούν τα σημαντικότερα αποτελέσματα.

- Αρχικά, ξεκινά ο ONOS και η τοπολογία και εκτελείται η εντολή summary με στόχο να φανούν οι συσκευές, που υπάρχουν συνδεδεμένες στο δίκτυο σε πρώτο βαθμό. Μετά την επίθεση δεν φαίνονται ούτε οι συσκευές ούτε τα πακέτα λόγω της πλημμυρίδας, που υπάρχει στον ελεγκτή. Αυτό σημαίνει πως πλέον ο ελεγκτής έχει «προσβληθεί» κατά κάποιον τρόπο από το φαινόμενο αυτό και δεν μπορεί να διατηρήσει τον έλεγχο, ούτε να επιβάλει την ευφύια του στο δίκτυο. Αυτό είναι ένα πολύ αρνητικό φαινόμενο, αφού σημαίνει πως το δίκτυο είναι ευάλωτο σε επιθέσεις και μπορεί να τεθούν εκτός λειτουργίας για παράδειγμα όλες οι συστάδες των ελεγκτών αν για παράδειγμα υπάρξει επίθεση σε διάφορους κόμβους, που επικοινωνούν με τους επί μέρους ελεγκτές.

Μετά την ενεργοποίηση της ασφαλούς λειτουργίας του ONOS, είναι ορατές οι συσκευές με τον τρόπο, που ήταν προηγουμένως. Στον ONOS σημειώνεται επίθεση, υπάρχει διάχυτο το

πρόβλημα, εφόσον, οι πόροι του συστήματος είναι δεσμευμένοι από αυτή την πρακτικά αέναη δημιουργία κίνησης στο δίκτυο. Πιο συγκεκριμένα και αναλυτικά:

Για την IP-RAN τοπολογία, μετά την ενεργοποίηση της ασφαλούς λειτουργίας:

- Εκτελώντας την εντολή «summary» παρατηρείται ο ελεγκτής του δικτύου και οι λοιπές συσκευές, δηλαδή οι σταθμοί βάσης και το access point.
- Με την εντολή «flows» παρατηρούνται όλες οι ροές, που υπάρχουν και ελέγχονται διεξοδικά οι ανταλλαγές των πακέτων.
- Ακόμα με την εντολή «devices» φαίνονται όλες οι συσκευές, που είναι συνδεδεμένες στο δίκτυο, δηλαδή οι σταθμοί βάσης και το σημείο πρόσβασης.
- Τέλος, με την εντολή «network» φαίνονται όλα τα στοιχεία του δικτύου και οι ροές των δεδομένων και κατά συνέπεια, είναι δυνατό αν και εφόσον, παρατηρηθεί κάτι παράξενο, όπως για παράδειγμα, η μονοπώληση του δικτύου από κάποια συγκεκριμένη συσκευή να διακοπεί η συγκεκριμένη ροή αποτρέποντας κατάρρευση του δικτύου.

Για την ετερογενή τοπολογία, μετά την ενεργοποίηση της ασφαλούς λειτουργίας:

- Εκτελώντας την εντολή «summary» παρατηρείται ο ελεγκτής του δικτύου και οι λοιπές συσκευές, δηλαδή οι σταθμοί βάσης, το access point, οι 4 μεταγωγείς και οι 4 υπολογιστές. Αυτό είναι φυσιολογικό, εφόσον, η ασφαλής λειτουργία είχε ενεργοποιηθεί, ο ελεγκτής ήταν σε θέση να παρακολουθεί τα δεδομένα και να καταγράφει τις συσκευές και τη συμπεριφορά τους.
- Με την εντολή «flows» παρατηρούνται όλες οι ροές, που υπάρχουν και ελέγχονται διεξοδικά οι ανταλλαγές των πακέτων, ανάμεσα στους υπολογιστές, τους σταθμούς βάσης, το σημείο πρόσβασης και τους μεταγωγείς.
- Ακόμα με την εντολή «devices» φαίνονται όλες οι συσκευές, που είναι συνδεδεμένες στο δίκτυο, δηλαδή οι μεταγωγείς, οι υπολογιστές, οι σταθμοί βάσης και το σημείο πρόσβασης.
- Τέλος, με την εντολή «network» φαίνονται όλα τα στοιχεία του δικτύου και οι ροές των δεδομένων και κατά συνέπεια, είναι δυνατό αν και εφόσον, παρατηρηθεί κάτι παράξενο, όπως για παράδειγμα, η μονοπώληση του δικτύου από κάποια συγκεκριμένη συσκευή να διακοπεί η συγκεκριμένη ροή αποτρέποντας κατάρρευση του δικτύου.

Αυτό συμβαίνει και στις δύο τοπολογίες. Στην πρώτη περίπτωση, ο ελεγκτής, μπορεί να σταματήσει τη ροή οποιαδήποτε στιγμή. Για παράδειγμα, θα μπορούσε να θεωρείται

κριτήριο επίθεσης, αν η αποστολή πακέτων ξεπερνά ένα συγκεκριμένο όριο είτε προκαθορισμένου χρόνου είτε πακέτων. Έτσι, θα μπορούσαν να δημιουργηθούν ορισμένοι βασικοί κανόνες, τους οποίους να εφαρμόζει ο ελεγκτής και να κόβει πιθανά ύποπτη κίνηση, για παράδειγμα, θα μπορούσε να δημιουργεί μία λίστα κακών διευθύνσεων είτε IP είτε MAC και να είναι κατά κάποιον τρόπο «επιφυλακτικός» σε αυτές, δηλαδή έτοιμος να διακόψει τη σύνδεση αν προβούν σε κάποια μη επιτρεπτή ενέργεια.

Η δημιουργία μαύρης λίστας (blacklist) δε θα αφήνει ορισμένες συσκευές να προβαίνουν σε ενέργειες. Ένα άλλο παράδειγμα, θα μπορούσε να είναι η αξιοποίηση των στατιστικών στοιχείων ανάλογα με τη μέρα και την ώρα, αν για παράδειγμα είναι δυνατό Δευτέρα και πρωί να σημειωθεί τεράστια κίνηση από οικιακό δίκτυο, οι στατιστικές από προηγούμενες μέρες θα ανακόπτουν κάποια τέτοια επίθεση. Αυτό ίσως συμβάλει ενεργά όχι μόνο στην προφύλαξη των δικτύων και την a priori ασφαλή δημιουργία του, αλλά και την καταλληλότερη διαχείριση των πόρων. Ακόμα, η αξιοποίηση στατιστικών δεδομένων μπορεί να συμβάλει σε αυτό. Αυτά τα δεδομένα μπορούν να αποθηκεύονται σε cloud και να μην καταλαμβάνουν φυσικούς πόρους, αποτελώντας έτσι μία ευνοϊκή εναλλακτική για το δίκτυο.

Στη δεύτερη τοπολογία, υπάρχει μία διαφορά, επειδή πρόκειται για μία περίπτωση, που το πρόβλημα προκαλείται σε δρομολογητή είναι δυνατό να μεταβληθεί σημαντικά ο πίνακας δρομολόγησης και να μην επιτρέπει στις δρομολογήσεις να γίνονται πραγματικά. Κάτι που σημαίνει ότι πρέπει να βρεθούν τρόποι, όπου ακόμα και η εξωτερική παρακολούθηση κάποιας συσκευής από κάποιο κακόβουλο λογισμικό, άτομο ή δίκτυο να αποτρέπεται από τον ελεγκτή και να μην εξακολουθεί στο δίκτυο. Ή ακόμα και να μην επιτρέπεται η αλλαγή των πινάκων δρομολόγησης.

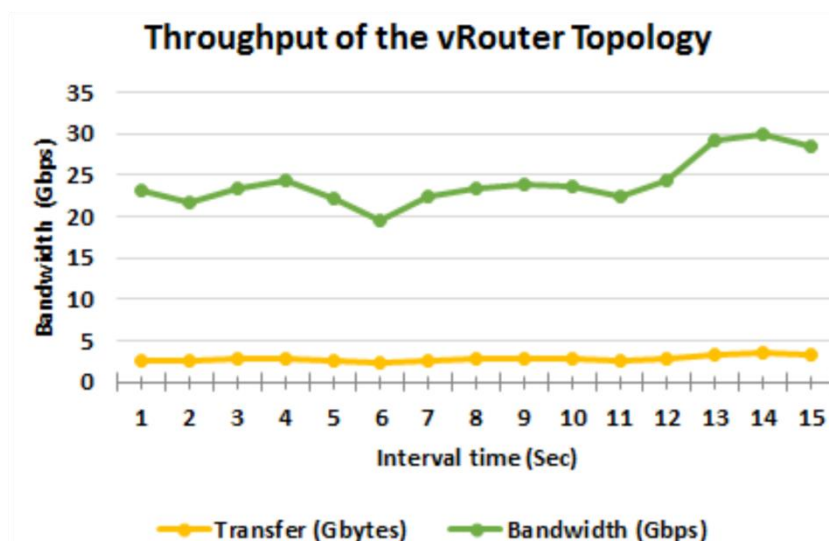
## 5.5 Σύγκριση SDN ελεγκτών (ONOS, POX) για εφαρμογές στην εκπαίδευση

Είναι σημαντικό να συγκριθούν οι δύο αυτοί δικτυακοί ελεγκτές με σκοπό να αναδειχθεί η διαφορά τους, η συσχέτισή τους και οι πιο σημαντικές τους εφαρμογές. Πιο συγκεκριμένα, πραγματοποιούνται τα ίδια πειράματα στους δύο ελεγκτές και σημειώνονται τα βασικότερα αποτελέσματα. Κάθε μία από τις τοπολογίες ξεκινά να εκτελείται ξεχωριστά στον ελεγκτή. Οι vRouter, η IPRAN και η ετερογενής τοπολογία εισέρχεται στον ελεγκτή δικτύου.

Αρχικά, ξεκινάει ο POX και ενσωματώνεται σε αυτόν κάθε τοπολογία χωριστά. Τα αποτελέσματα, που προκύπτουν ομοιάζουν με εκείνα στα 5.1 και 5.2. Παρατηρείται ότι ενώ,

στο Mininet και το Mininet-wifi, που είναι οι εξομοιωτές δικτύου παράγονται τα ίδια ακριβώς αποτελέσματα και προκύπτουν οι ίδιες γραφικές απεικονίσεις και παραστάσεις, ο POX δεν περιλαμβάνει τόσο λεπτομερή διεπαφή σε σχέση με τον ONOS. Εντολές, όπως devices, flows, κλπ., που περιλαμβάνονται στον ONOS, δεν υπάρχουν στον POX, με αποτέλεσμα τα αποτελέσματα στη διεπαφή του να μην είναι τόσο λεπτομερή. Συγκεκριμένα στη vRouter περίπτωση:

- Εκτελώντας πειράματα «ring» για τον έλεγχο της συνδεσιμότητας των συσκευών, παρατηρείται ότι όλες οι συσκευές είναι συνδεδεμένες μεταξύ τους, δηλαδή ο μεταγωγέας επικοινωνεί με τον ελεγκτή, οι υπολογιστές επικοινωνούν μεταξύ τους και με το μεταγωγέα και πακέτα ανταλλάσσονται επιτυχώς.
- Εκτελώντας την εντολή «nodes» παρατίθενται στοιχεία σχετικά με τους κόμβους στο δίκτυο και παρατηρείται ο μεταγωγέας.
- Με τη χρήση iperf πειραμάτων λαμβάνονται πληροφορίες για την απόδοση των συσκευών στο δίκτυο.



Εικόνα 5.1: Η απόδοση του εικονικού δρομολογητή ως συνάρτηση του χρόνου.

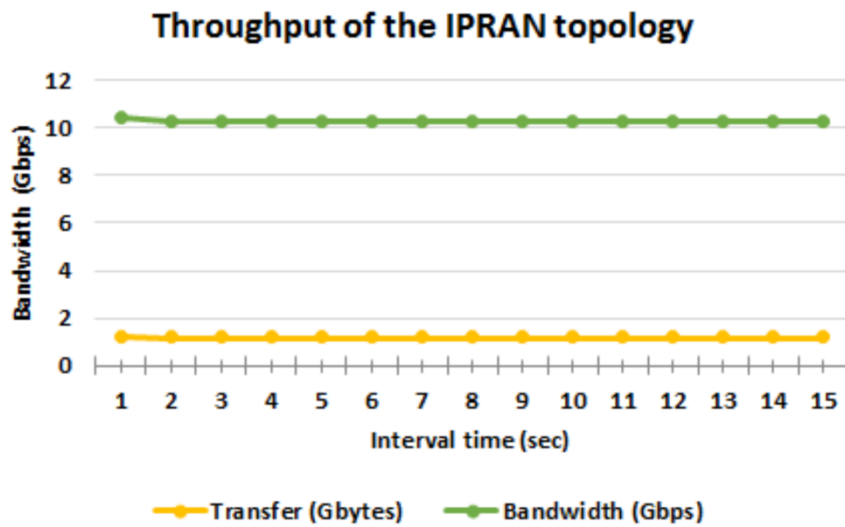
Η γραφική απεικόνιση, που προέκυψε ήταν αντίστοιχη με αυτή, που προέκυψε και στην προηγούμενη περίπτωση (κεφάλαιο 5.1). Επίσης, κρίθηκε αναγκαίο η απεικόνιση να γίνει με χρήση του ms excel εργαλείου για λόγους παρουσίασης, μιας και θεωρείται ότι οι γραφικές παραστάσεις, που προκύπτουν απεικονίζονται καλύτερα με αυτή τη μέθοδο.

Συγκεκριμένα στην IPRAN περίπτωση:

- Εκτελώντας πειράματα «ring» για τον έλεγχο της συνδεσιμότητας των συσκευών, παρατηρείται ότι όλες οι συσκευές είναι συνδεδεμένες μεταξύ τους, δηλαδή το σημείο πρόσβασης επικοινωνεί με τον ελεγκτή, οι σταθμοί βάσης μπορούν να επικοινωνούν

μεταξύ τους και με το σημείο πρόσβασης και διάφορα πακέτα ανταλλάσσονται επιτυχώς.

- Εκτελώντας την εντολή «nodes» παρατίθενται στοιχεία σχετικά με τους κόμβους στο δίκτυο και παρατηρείται το σημείο πρόσβασης.
- Με τη χρήση iperf πειραμάτων λαμβάνονται πληροφορίες για την απόδοση των συσκευών στο δίκτυο.

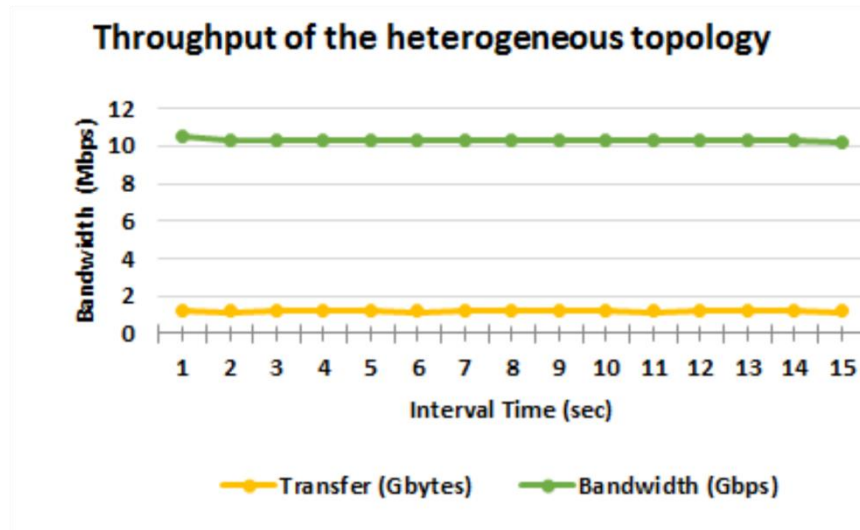


Εικόνα 5.2: Η απόδοση της τοπολογίας IPRAN ως συνάρτηση του χρόνου.

Η γραφική απεικόνιση, που προέκυψε ήταν αντίστοιχη με αυτή, που προέκυψε και στην προηγούμενη περίπτωση (Κεφάλαιο 5.2). Επίσης, κρίθηκε αναγκαίο η απεικόνιση να γίνει με χρήση του ms excel εργαλείου για λόγους παρουσίασης, μιας και θεωρείται ότι οι γραφικές παραστάσεις, που προκύπτουν απεικονίζονται καλύτερα με αυτή τη μέθοδο.

Συγκεκριμένα στην ετερογενή περίπτωση:

- Εκτελώντας πειράματα «ring» για τον έλεγχο της συνδεσιμότητας των συσκευών, παρατηρείται ότι όλες οι συσκευές είναι συνδεδεμένες μεταξύ τους, δηλαδή το σημείο πρόσβασης επικοινωνεί με τον ελεγκτή, οι σταθμοί βάσης μπορούν να επικοινωνούν μεταξύ τους και με το σημείο πρόσβασης, το ίδιο και οι μεταγωγείς και οι υπολογιστές και διάφορα πακέτα ανταλλάσσονται επιτυχώς.
- Εκτελώντας την εντολή «nodes» παρατίθενται στοιχεία σχετικά με τους κόμβους στο δίκτυο και παρατηρείται το σημείο πρόσβασης και ο μεταγωγέας.
- Με τη χρήση iperf πειραμάτων λαμβάνονται πληροφορίες για την απόδοση των συσκευών στο δίκτυο.



Εικόνα 5.3: Η απόδοση της τοπολογίας IPRAN για την ετερογενή τοπολογία ως συνάρτηση του χρόνου.

Η γραφική απεικόνιση, που προέκυψε ήταν αντίστοιχη με αυτή, που προέκυψε και στην προηγούμενη περίπτωση (κεφάλαιο 5.2). Επίσης, κρίθηκε αναγκαίο η απεικόνιση να γίνει με χρήση του ms excel εργαλείου για λόγους παρουσίασης, μιας και θεωρείται ότι οι γραφικές παραστάσεις, που προκύπτουν απεικονίζονται καλύτερα με αυτή τη μέθοδο.

Ο POX περιλαμβάνει διεπαφή και σημειώσεις σχετικές με στοιχεία για τη συνδεσιμότητά του στο δίκτυο και στην τοπολογία. Έτσι, δεν μπορεί κανείς να διαχειριστεί μία τοπολογία εύκολα μέσω της διεπαφής του, αλλά χρειάζεται η επέμβαση στον εξομοιωτή δικτύου Mininet ή Mininet-Wifi αντίστοιχα για να γίνονται τροποποιήσεις στην τοπολογία. Από τον POX, δεν είναι δυνατό να τερματιστεί μία ροή και ούτε να ελεγχθούν οι ροές και να προκύψουν διάφορα άλλα διαγνωστικά μηνύματα χρήσιμα για τη λειτουργία του δικτύου. Δεν περιλαμβάνει αυτές τις εντολές και αυτά τα διαγνωστικά μηνύματα, αλλά ούτε και την πλούσια διεπαφή, που περιλαμβάνει ο ONOS.

Η διεπαφή του ONOS επιτρέπει να ελέγχεται ποιες, πόσες συσκευές είναι συνδεδεμένες όλες τις καταστάσεις των συσκευών, τις ροές, τις μηχανές και πολλά ακόμα, αφού περιλαμβάνει εντολές για το πλήθος πακέτων, που έχουν επεξεργαστεί σε κάθε επεξεργαστή κλπ. Ακόμα, στον ONOS οι vRouter και IPRAN είναι υπάρχουσες μελέτες

περίπτωσης με έτοιμα tutorials, με τα οποία μπορεί κανείς να πειραματιστεί, σε αντίθεση, κάτι τέτοιο δεν υφίσταται στον POX.

Εν συνεχεία, σε ό,τι αναφορά στην 5.3 στον POX για να ελέγξει κανείς πώς είναι δυνατό να εφαρμοστούν τα CORD και MCORD και ποιες επιπρόσθετες δυνατότητες μπορούν να προσφέρουν οι εικονικές μηχανές σε αυτά, θα πρέπει να δημιουργήσει αντίστοιχο κώδικα εφαρμογής τους, αφού στον POX δεν υπάρχουν σαν αντίστοιχη μελέτη περίπτωσης και κατά συνέπεια, πρέπει να δημιουργηθούν από την αρχή με σκοπό να εκτελεστούν και να πραγματοποιηθούν σε αυτό διάφορα πειράματα.

Συνεπώς, γίνεται αντιληπτό ότι ανάλογα με την επιδιωκόμενη εφαρμογή υπάρχουν και αντίστοιχα πλεονεκτήματα/μειονεκτήματα σε κάθε ελεγκτή δικτύου. Από τη μία ο ONOS έχει έτοιμες μελέτες περίπτωσης, έτοιμη διεπαφή, πολλές εντολές και μία κοινότητα, που ασχολείται με όλα αυτά τα θέματα. Από την άλλη μεριά, ο POX είναι καταλληλότερος για να την ανάπτυξη σχετικών εφαρμογών και κατά συνέπεια για την εκμάθηση και τη δημιουργία νέων αντικειμένων. Οπότε σημειώνεται ότι και οι δύο είναι σημαντικοί για εφαρμογές εκπαίδευσης και για εργαστήρια δικτύων.

## 5.6 Τροποποίηση Αρχιτεκτονικής τύπου DAS με χρήση τεχνικών NFV

Μία άλλη σημαντική εφαρμογή των εξεταζόμενων τεχνολογιών είναι η τροποποίηση βασικών αρχιτεκτονικών με χρήση των αναφερθέντων τεχνολογικών προτάσεων. Ένα παράδειγμα είναι να τροποποιηθούν γνωστές αρχιτεκτονικές και δικτυακές τεχνολογίες επιλέγοντας να αντικατασταθούν κάποια τμήματα με εικονικά. Η NFV DAS αρχιτεκτονική οδηγεί στη μείωση του κόστους της συνολικής δομής για το ίδιο σενάριο κόστους. Επιλέχθηκαν οι βασικές παράμετροι του νέου μοντέλου βάση της βιβλιογραφικής υπόθεσης ότι οι τεχνικές αυτές μειώνουν το κόστος από 40-80%. Μέσα σε ένα διάστημα τιμών 40-80% της σημερινής τιμής επιλέχθηκαν τυχαίες τιμές, με βάση τις οποίες, πραγματοποιήθηκαν νέες μελέτες εφικτότητας, παρόμοιες με αυτές, που είχαν συντελεστεί σε παλαιότερες ερευνητικές δράσεις [93], [94].

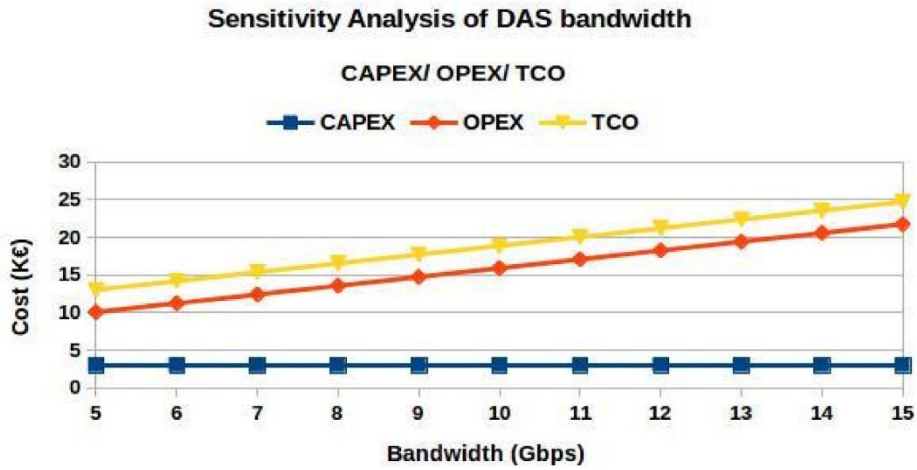
Με σκοπό να αναδειχθούν τα οφέλη από αυτή την προσέγγιση, ακολούθως, παρατίθενται τα αποτελέσματα των μελετών εφικτότητας για το εύρος ζώνης, το σταθμό βάσης, τον εξοπλισμό, την υλοποίηση των συστημάτων, της θέσης κλπ.. Παρατηρείται ότι όλες οι παρακάτω πειραματικές διαδικασίες αναδεικνύουν την υπεροχή του μοντέλου μετά την ενσωμάτωση τεχνικών virtualization στο σύστημα και την αντίστοιχη μείωση του κόστους,

που προκύπτει συγκριτικά με τα γραφήματα, που περιγράφουν την αντίστοιχη μελέτη στα κλασικά δίκτυα. Η ελάττωση αυτή του κόστους προκύπτει συνολικά, όπως για παράδειγμα για τα κόστη κεφαλαίου, για τα κόστη λειτουργίας και για το συνολικό κόστος, όμως προκύπτει κι εξετάζοντας κάθε παράγοντα ξεχωριστά. Γίνεται προφανές, ότι όποια περίπτωση κι αν ελεγχθεί σε σχέση για παράδειγμα με όλες τις προηγούμενες μελέτες [93], [94], καθίσταται σαφές ότι το συγκεκριμένο μοντέλο διατηρεί τα κόστη πολύ χαμηλότερα.

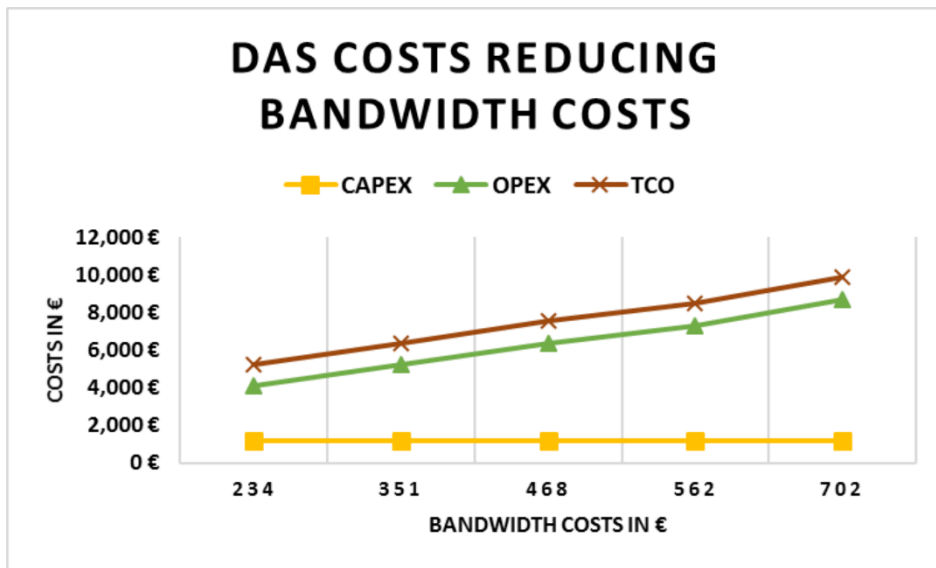
Πιο συγκεκριμένα, παρατηρείται ότι και στα δύο μοντέλα το κόστος για το εύρος ζώνης (εικόνες 5.4-5.5) επιδρά κυρίως στο λειτουργικό και στο συνολικό κόστος. Από την άλλη μεριά, παρατηρείται ότι τα συνολικά κόστη είναι έως και 2.5 φορές χαμηλότερα για καθεμία από τις πιο ακριβές περιπτώσεις. Το εύρος ζώνης επιδρά στο λειτουργικό κόστος, αφού η ενοικίαση του γίνεται συνήθως ετησίως και άρα είναι ένα ποσό, που καλύπτεται σε τακτά χρονικά διαστήματα. Τα κόστη για τους σταθμούς βάσης (εικόνες 5.6-5.8) επιδρούν κυρίως στο κόστος κεφαλαίου, διότι πρέπει να εξασφαλιστεί η υποδομή εξ αρχής για να ολοκληρωθεί η δημιουργία του δικτύου. Είναι σημαντικό ότι μείωση στο κόστος για το σταθμό βάσης σημαίνει και μείωση στο συνολικό κόστος του δικτύου, στο λειτουργικό και στο κόστος κεφαλαίου.

Το κόστος του απαραίτητου υποστηρικτικού εξοπλισμού (εικόνες 5.9-5.10) αυξάνει το λειτουργικό κόστος. Ακόμα, παρατηρείται ότι όλα τα είδη κόστους μειώνονται 2.5 περίπου φορές στο μοντέλο, που υλοποιείται συγκριτικά με το κλασικό μοντέλο. Τα κόστη υλοποίησης (εικόνες 5.11-5.12) έχουν σημαντική επίδραση στο κόστος κεφαλαίου. Αν απλοποιηθεί ο εξοπλισμός, τότε απλοποιούνται και οι απαραίτητες ενέργειες για τη δόμηση του συνολικού συστήματος. Έτσι, παρατηρείται σημαντική μείωση όλων των ειδών κόστους. Σε αντίθεση, η θέση επιδρά στο λειτουργικό κόστος, αφού αν χρειάζεται μετακίνηση, τότε καλύπτεται αυτό το κόστος. Αποτελεί ένα κόστος συντήρησης και διαχείρισης της καλής λειτουργίας του συστήματος. Από την άλλη μεριά, είναι σημαντικό να τονιστεί ότι και σε αυτή την περίπτωση τα συνολικά κόστη μειώνονται 2 έως 2.5 φορές.

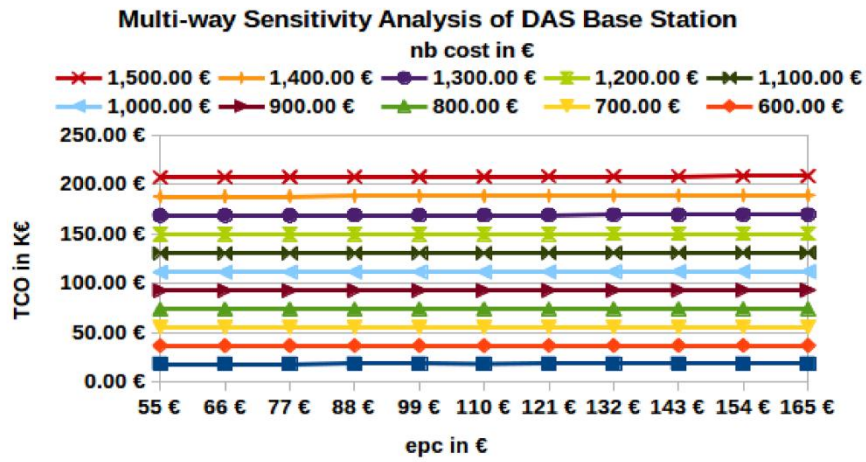




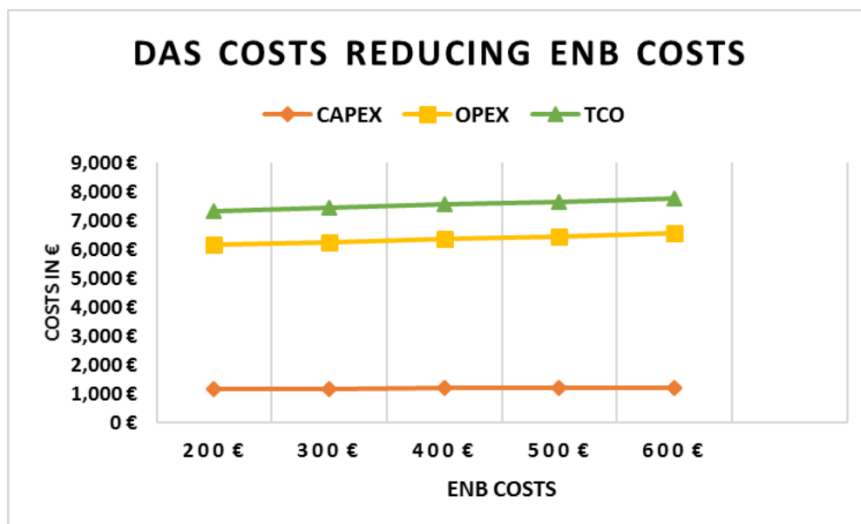
Εικόνα 5.4: Μελέτη εφικτότητας κλασικού μοντέλου DAS σχετικά με το εύρος ζώνης. [93], [94]



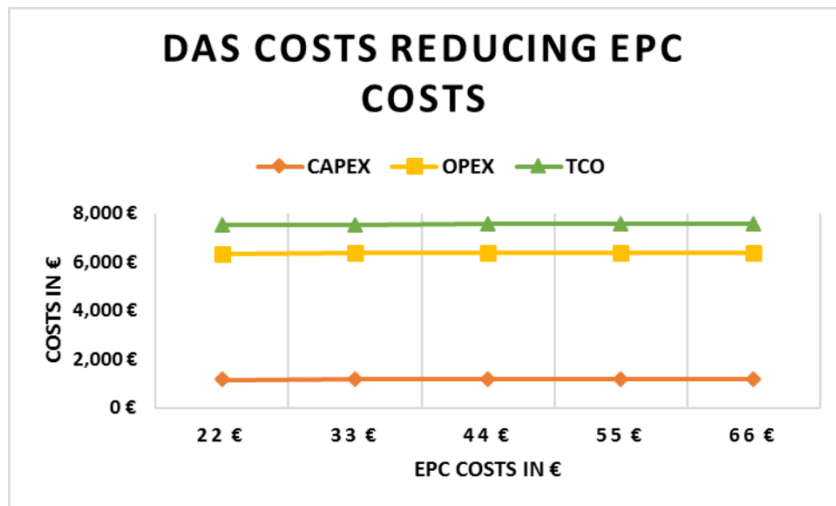
Εικόνα 5.5: Μελέτη εφικτότητας virtualized μοντέλου DAS σχετικά με το εύρος ζώνης.



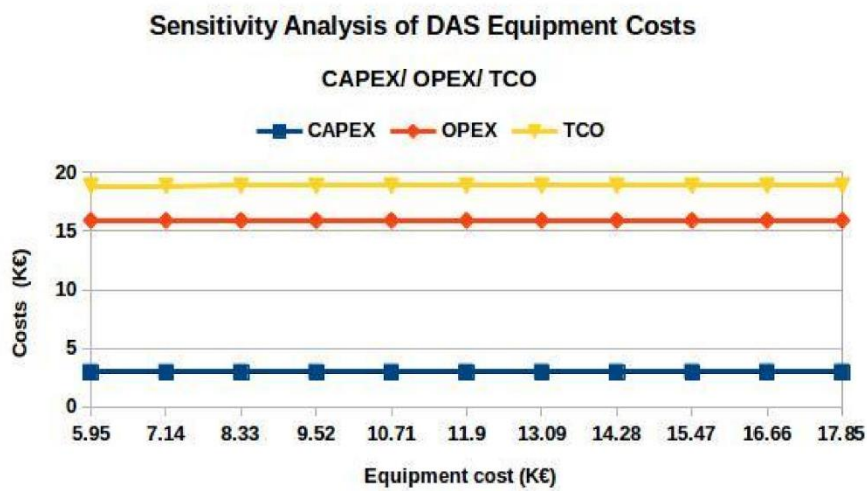
Εικόνα 5.6: Μελέτη εφικτότητας για το κλασικό DAS σχετικά με το σταθμό βάσης. [93], [94]



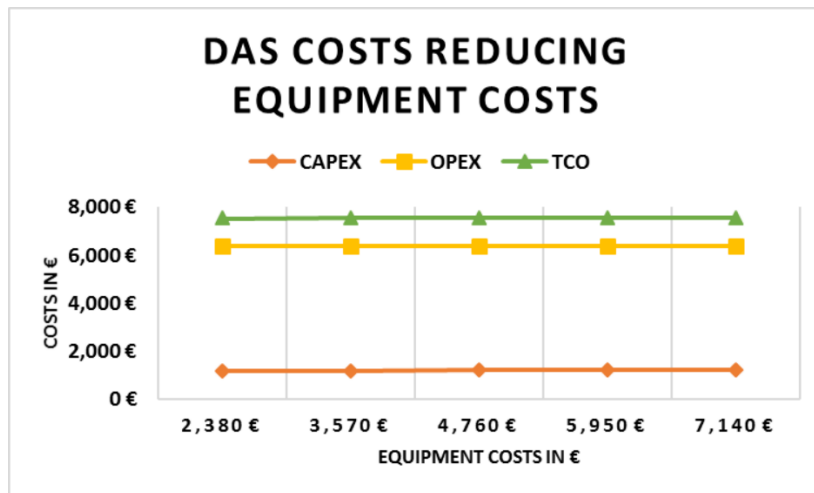
Εικόνα 5.7: Μελέτη εφικτότητας για το virtualized DAS σχετικά με το eNB.



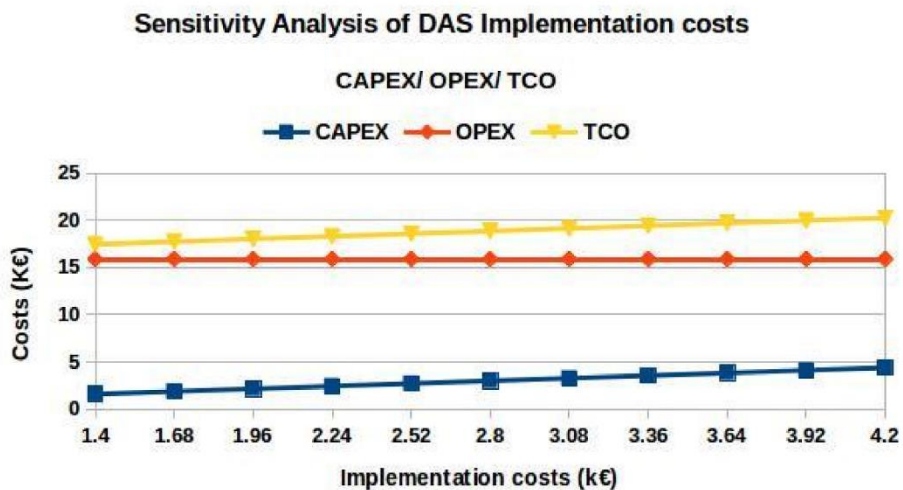
Εικόνα 5.8: Μελέτη εφικτότητας για το virtualized DAS σχετικά με το EPC.



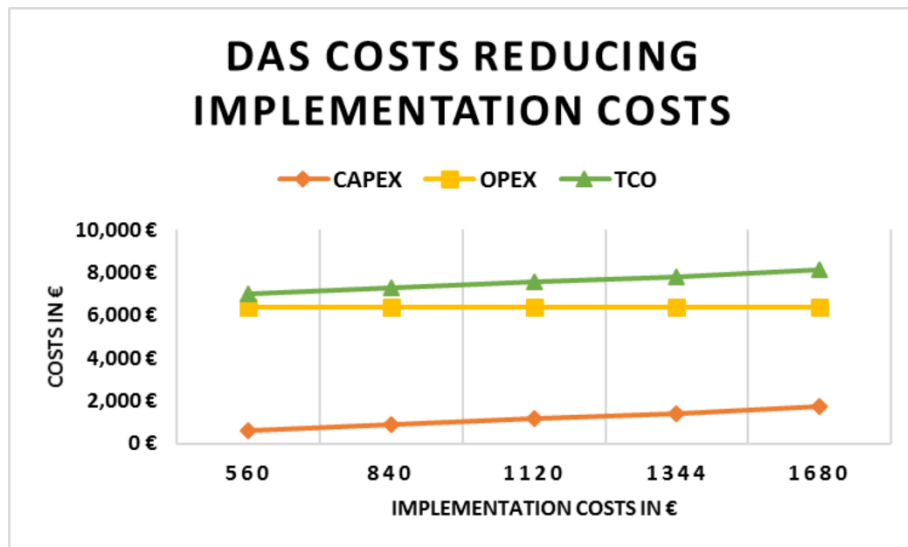
Εικόνα 5.9: Μελέτη εφικτότητας για το κλασικό DAS σχετικά με τον εξοπλισμό στο σύστημα. [93], [94]



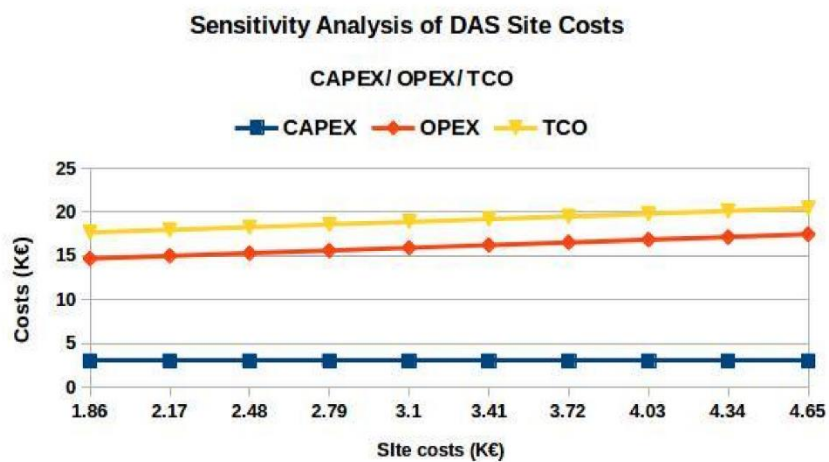
Εικόνα 5.10: Μελέτη εφικτότητας για το virtualized DAS σχετικά με τον εξοπλισμό στο σύστημα.



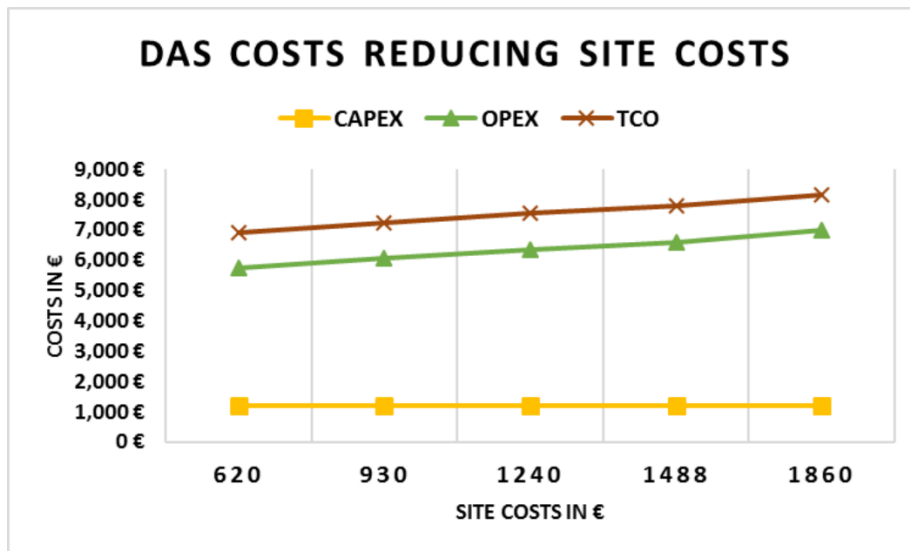
Εικόνα 5.11: Μελέτη εφικτότητας για το κλασικό DAS σχετικά με το κόστος υλοποίησης για το σύστημα. [93], [94]



Εικόνα 5.12: Μελέτη εφικτότητας για το virtualized DAS σχετικά με το κόστος υλοποίησης για το σύστημα.



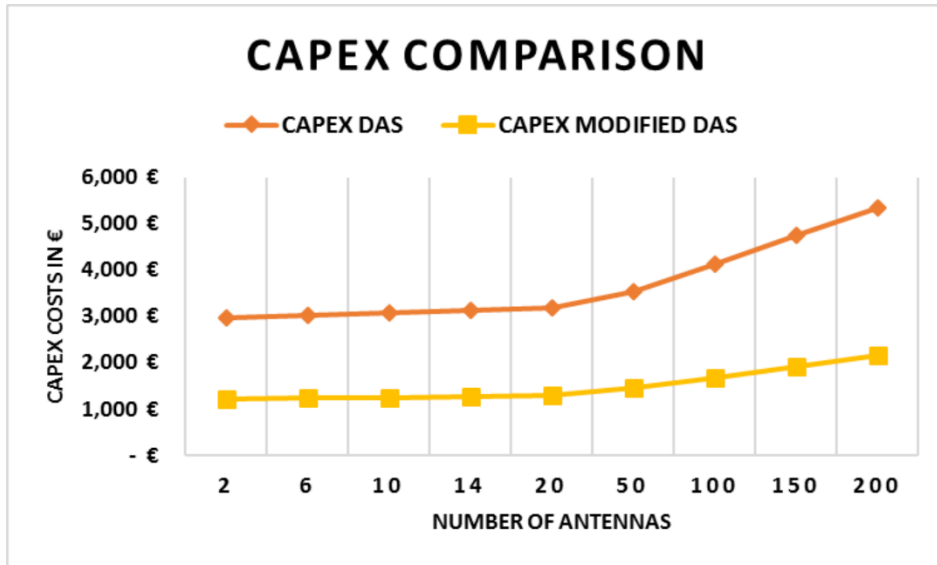
Εικόνα 5.13: Μελέτη εφικτότητας για το κλασικό DAS σχετικά με το κόστος υλοποίησης της θέσης για το σύστημα. [93], [94]



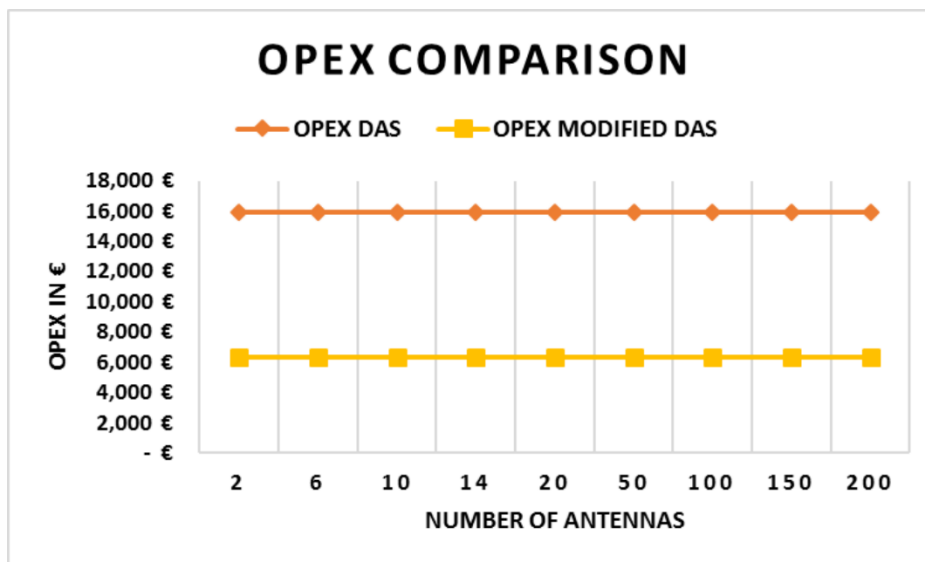
**Εικόνα 5.14: Μελέτη εφικτότητας για το virtualized DAS σχετικά με το κόστος υλοποίησης της θέσης για το σύστημα.**

Στις παρακάτω εικόνες 5.15-5.17 συγκρίνονται αντίστοιχα το κόστος κεφαλαίου, το λειτουργικό κόστος και το συνολικό κόστος για τις δύο αρχιτεκτονικές σε σχέση με το πλήθος κεραιών του συστήματος, αφού αυτό ουσιαστικά καθορίζει και το μέγεθος της συνολικής υποδομής. Σε κάθε μία από τις παρακάτω περιπτώσεις, φαίνεται ότι υπάρχει σημαντική υπεροχή του σεναρίου με τα virtualized συστατικά, αφού όλα τα είδη κόστους μειώνονται σημαντικά και καθιστούν τη δημιουργία, υλοποίηση και εγκατάσταση της δικτυακής υποδομής DAS περισσότερο έτοιμη σχετικά με τις υποδομές για τις επόμενες γενιές κινητών επικοινωνιών. Παρατηρείται εκθετική αύξηση στο κόστος κεφαλαίου με την αύξηση του πλήθους των κεραιών, ενώ το κόστος στο κλασικό DAS είναι 2 ή και 3 φορές μεγαλύτερο από το κόστος κεφαλαίου στο virtualized μοντέλο. Το λειτουργικό κόστος είναι σταθερό με την αύξηση του πλήθους των κεραιών, παρόλα αυτά όμως, το virtualized μοντέλο είναι παραπάνω από 2 φορές πιο οικονομικό από το κλασικό μοντέλο. Το συνολικό κόστος είναι σε σχετικά υψηλά επίπεδα και είναι 3 φορές μικρότερο στο virtualized μοντέλο.

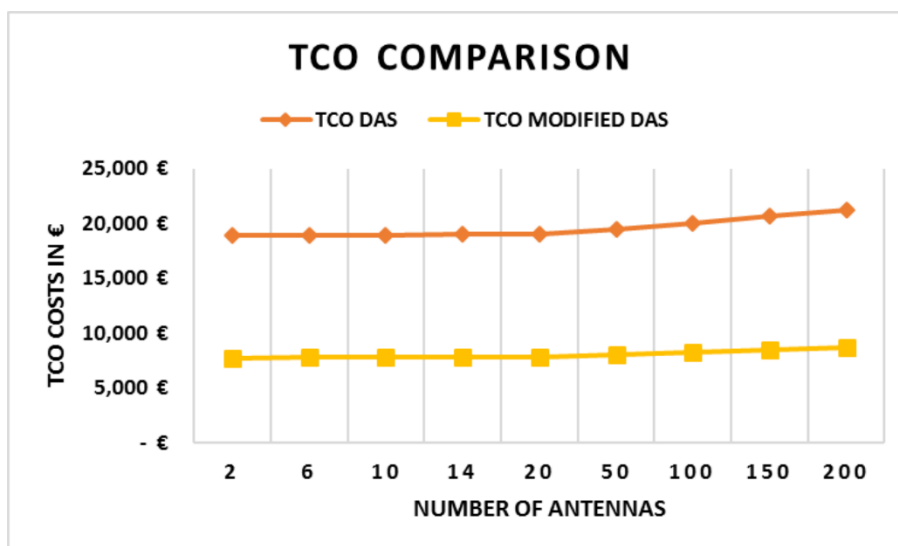
Συνεπώς, γίνεται προφανές ότι η επίδραση της virtualized αρχιτεκτονικής είναι ιδιαίτερα σημαντική σε ότι αφορά στο κόστος και συνεπώς, είναι δυνατό να δημιουργεί πιο ευέλικτες και πιο οικονομικά βιώσιμες δομές ικανές να καλύψουν τις ανάγκες της 5G και να ανταποκριθούν επιτυχώς στις υψηλές οικονομικές προσδοκίες των επιχειρήσεων. Ακόμα, ότι η εισαγωγή της συγκεκριμένης ιδέα στα δίκτυα αποτελεί πολύ δυνατό εργαλείο και είναι εξαιρετικά



Εικόνα 5.15: Σύγκριση κόστους κεφαλαίου για τα δύο DAS συστήματα.



Εικόνα 5.16: Σύγκριση λειτουργικού κόστους για τα δύο DAS συστήματα.



Εικόνα 5.17: Σύγκριση συνολικού κόστους για τα δύο DAS συστήματα.

## 6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Τις περισσότερες φορές η έρευνα και τα πειράματα προσδίδουν νέες ιδέες για ερευνητική δραστηριότητα και δημιουργούν την ανάγκη για νέα πειράματα. Τα SDN και NFV είναι τεχνολογίες με πολλές δυνατότητες και για το λόγο αυτό εγείρουν νέους σπόρους πειραματισμού σε ότι αναφορά στα δίκτυα επόμενης γενιάς, αλλά και σε άλλες εφαρμογές, που μπορεί κανείς να φανταστεί. Από την άλλη μεριά, οι σύγχρονες τεχνολογίες, όπως για παράδειγμα οι IoT και οι M2M επικοινωνίες αναμένεται σε συνδυασμό με τις συγκεκριμένες τεχνολογίες να δημιουργήσουν την βάση για σενάρια επιστημονικής φαντασίας, όπου τα πάντα θα είναι συνδεδεμένα με τα πάντα.

Εντούτοις, κρίνεται κρίσιμο να παρουσιαστούν τα σημαντικότερα συμπεράσματα σχετικά με τα αποτελέσματα της πειραματικής διαδικασίας, που παρουσιάστηκε στην παρούσα διπλωματική. Οι εφαρμογές, οι οποίες εξετάστηκαν στην περίπτωση αυτή μπορεί να μην είναι όλες οι δυνατές, που υπάρχουν όμως, είναι πολύ σημαντικές εφαρμογές για τη λειτουργία των δικτύων, για την εκπαίδευση για τα IPRAN επίπεδα, για τη λειτουργία εικονικών συσκευών, για την τροποποίηση τεχνοοικονομικών μοντέλων.

Αρχικά, ενώ οι τοπολογίες, που δημιουργήθηκαν φαίνονται απλές, εν τούτοις, είναι δυνατό να επεκταθούν για περισσότερα στοιχεία και για μεγαλύτερα δίκτυα. Εν συνεχεία, με τις τεχνικές αυτές είναι δυνατό να εξεταστούν διάφορα θέματα, όπως για παράδειγμα, η κινητικότητα στο δίκτυο, τα handovers, οι παρεμβολές κλπ. Οι απλές αυτές τοπολογίες



ανέδειξαν τις φύσεις των δύο αυτών ελεγκτών και σηματοδότησαν ποια είναι τα βασικότερα πειράματα, που μπορούν να γίνουν. Έπειτα, προέκυψαν αποτελέσματα, τα οποία είναι σημαντικά και αποτελούν εφαλτήριο για τεχνολογική δημιουργία.

Ο ONOS είναι ένας ελεγκτής, που επιτρέπει την εύκολη εισδοχή τοπολογιών και τη διαμόρφωση κατάλληλων ρυθμίσεων στο δίκτυο. Είναι εύκολο να δημιουργηθούν διάφορα στοιχεία της τοπολογίας και να είναι ορατά στον ελεγκτή και αυτός να τα διαχειρίζεται. Ακόμα, πολλαπλά στιγμιότυπα ενός ελεγκτή μπορούν να εισαχθούν στην τοπολογία και να προσδώσουν σημαντικά οφέλη στο δίκτυο. Αρχικά, μειώνεται ο κίνδυνος να αποσυνδεθεί ένα τμήμα του δικτύου λόγω κάποιας βλάβης. Αν ο ελεγκτής αποσυνδεθεί, μπορεί να ανατεθεί η κίνηση σε άλλα στιγμιότυπα ελεγκτών, ώστε να επιδιορθωθούν οι βλάβες και η λειτουργία του δικτύου να παραμένει αδιάκοπη.

Ο ONOS είναι ένας ελεγκτής, που βασίζεται σε ανοιχτό λογισμικό. Το γεγονός αυτό παρέχει τη δυνατότητα να αξιοποιηθούν πολλοί και διαφορετικοί παράγοντες. Αρχικά, είναι δυνατό να λειτουργήσει ευεργετικά στην εκπαίδευση. Το ανοιχτό λογισμικό παρέχει τη δυνατότητα να αξιοποιείται από χρήστες δωρεάν. Δεν εγείρεται η ανάγκη για επιπλέον άδειες εμπορικής χρήσης και άρα, το κόστος, που εξοικονομείται χρησιμοποιείται για χρήματα, που μπορούν να αξιοποιηθούν σε άλλες εφαρμογές. Για παράδειγμα, σε ένα πανεπιστήμιο, μπορεί να εξασφαλιστεί άδεια για εμπορική χρήση ενός εκπαιδευτικού λογισμικού, από την άλλη μεριά, όμως με το να εξοικονομηθούν τα χρήματα καλύπτονται άλλες πηγές για ερευνητικές δραστηριότητες. Το ίδιο και ο ελεγκτής δικτύου POX. Οπότε αποτελούν σημαντικά εργαλεία για εργαστήρια δικτύων.

Σε εργαστήρια και μαθήματα δικτύων μπορούν να μελετηθούν διάφορα θέματα σχετικά με τα πιο χαρακτηριστικά είδη επιθέσεων σε δίκτυα επόμενης γενιάς, να μελετηθούν και να διδαχθούν οι συνδυασμοί των SDN & NFV, να εξηγηθούν έννοιες σχετικές με τα CORD και MCORD, σχετικά με τεχνικές virtualization. Θα μπορούσαν να εξηγηθούν οι επιθέσεις και οι απειλές ασφάλειας δικτύων τύπου SDN, που είναι θεμελιωδώς διαφορετικές έννοιες σε σχέση με τα κλασικά δίκτυα. Ακόμα, θα μπορούσαν να αναλυθούν μηχανισμοί κρυπτογράφησης, δημιουργίας τειχών προστασίας και άλλων μεθόδων διασφάλισης δικτύου. Από την άλλη μεριά, θα μπορούσαν να εξηγηθούν νέα πρωτόκολλα και νέα πρότυπα, που είναι διαθέσιμα σήμερα.

Ακόμα, πρέπει να μελετηθεί εις βάθος η μεγάλη διαφορά των λύσεων στα δίκτυα τέτοιου τύπου σχετικά με τα παραδοσιακά δίκτυα. Για παράδειγμα, είναι σημαντικό να ενσωματώνονται τέτοιες λύσεις εικονικών δικτύων σε διάφορα είδη δικτύων, αλλά και για παράδειγμα να αξιοποιηθούν για άλλους στόχους. Συνάμα, θα μπορούσαν ακόμα να

μελετηθούν μηχανισμοί επιθέσεων και μηχανισμοί αποτροπής αυτών με διαφορετικούς τρόπους βασιζόμενοι σε εργαλεία της ανάλυσης και της στατιστικής απεικόνισης του δικτύου.

Σε σύγκριση με άλλους παρόμοιους ελεγκτές, π.χ. POX, ο ONOS διαφοροποιείται σημαντικά, αφού παρέχει έτοιμες μελέτες περίπτωσης για το κομμάτι των ασύρματων και ενσύρματων δικτύων και για εικονικές μηχανές και καθένας, μπορεί να εστιάσει τη μελέτη αμιγώς στο κομμάτι των SDN δικτύων και πως αυτό μεταβάλλει τα δίκτυα σε σχέση με όσα είναι ήδη γνωστά σήμερα. Στον POX πρέπει να γραφούν εφαρμογές αν επιδιώκεται να εκτελεστούν διάφορα πειράματα. Για παράδειγμα, τα CORD και MCORD είναι πολύ πιο εύκολο να εξεταστούν στον ONOS, αφού παρέχονται ως έτοιμες μελέτες περίπτωσης, και άρα είναι πολύ πιο απλό να γίνουν σχετικά πειράματα σε σχέση με τις ροές δεδομένων και πώς αυτές μπορούν να διαχωριστούν σε κινητά δίκτυα επόμενης γενιάς. Αν όμως, το ζητούμενο σε ένα εργαστήριο δικτύων είναι η δημιουργία εφαρμογών και τοπολογιών, τότε ο POX είναι πιο κατάλληλος, αφού δεν απαιτούνται πολύπλοκες διαδικασίες για την εγκατάστασή του σε αντίθεση με τον ONOS. Σε κάθε περίπτωση είναι και οι δύο σημαντικοί και μπορούν να συμβάλουν ενεργά στην εκπαίδευση των φοιτητών στο συγκεκριμένο τομέα.

Τα πειράματα και οι τοπολογίες, που δομήθηκαν επεξηγούν κινητά δίκτυα, κινητές τοπολογίες. Εμπεριέχουν τη ρύθμιση κινητών συσκευών, κινητών δικτύων και ιδεατών δρομολογητών. Εγείρουν ζητήματα της προγραμματιστικής λογικής σε απλά συστήματα και απλές συσκευές. Συμβάλουν στην κατανόηση των επιπέδων αφαίρεσης ενός δικτύου SDN. Ακόμα, ο ONOS και ο POX είναι εύχρηστοι ελεγκτές για χρήστες Unix συστημάτων. Υπάρχει μία πολύ ζωντανή κοινότητα, ευρύ υλικό και οδηγοί χρήσης σχετικά με το ONOS, που είναι δυνατό και ένας άπειρος χρήστης μελετώντας να πραγματοποιήσει χρήση και αξιοποίηση του ελεγκτή για τους δικούς του στόχους. Έτσι, καθένας, που χρειάζεται έναν ελεγκτή δικτύου μπορεί να πειραματιστεί με το συγκεκριμένο εργαλείο.

Τα CORD και MCORD είναι σημαντικά για πολλούς λόγους εκτός από εφαρμογές σχετικές με δίκτυα. Το MCORD, πιο συγκεκριμένα, μπορεί να συμβάλει ενεργά στην έρευνα σχετικά με τις ροές δεδομένων στα δίκτυα. Είναι αρκετά σημαντικό να υπάρξει ο βέλτιστος αριθμός ροών στο δίκτυο. Είναι γνωστό ότι στο IPv6, δηλαδή το πρωτόκολλο διαδικτύου στην 6<sup>η</sup> έκδοση, η οποία αναμένεται να υιοθετηθεί άμεσα, εφόσον θα απαιτούνται πολύ περισσότερες διευθύνσεις από τις σημερινές διαθέσιμες για κάλυψη όλων των διασυνδεδεμένων δικτυακών συσκευών, διατίθενται 20 δυαδικά ψηφία για τις ροές, το οποίο σημαίνει ότι μπορεί να υποστηρίξει 2<sup>20</sup> διαφορετικές ροές. Πιθανές ροές, που θα μπορούσαν να υπάρξουν είναι:

- Εφαρμογές Content Delivery Network Quality of Experience

- Εφαρμογές βίντεο streaming
- Εφαρμογές εικονικής πραγματικότητας
- IoT και εφαρμογές αυτού, δηλαδή επικοινωνία μεταξύ μηχανών, εφαρμογές τηλειατρικής
- Εφαρμογές δημόσιας ασφάλειας

Από τη μία μεριά, είναι σημαντικό να υπάρχουν διαφοροποιημένες ροές, ώστε να εξασφαλίζεται ότι ανάλογα με τη ζητούμενη εφαρμογή δεσμεύονται οι απαραίτητες πηγές. Για παράδειγμα, είναι γνωστό ότι σε κάποιες εφαρμογές, όπως για παράδειγμα εφαρμογές τραπεζικές είναι απαραίτητο να αποκρίνονται σε πραγματικό χρόνο (real time responsive). Από την άλλη μεριά, οι εφαρμογές βελτιστοποίησης βίντεο, απαιτούν σημαντικό εύρος ζώνης (bandwidth) για να πραγματοποιείται καλύτερη απεικόνιση του βίντεο. Σε εφαρμογές τύπου crowdsource δεν είναι απαραίτητο να λαμβάνονται συνέχεια οι πληροφορίες, αλλά μπορεί να λαμβάνονται όταν το δίκτυο δεν έχει ιδιαίτερο φόρτο. Από την άλλη όμως, το να υπάρξουν διάφορες ροές θα οδηγήσει σε πολλούς διαφορετικούς κανόνες αξιοποίησης των διαθέσιμων πόρων, καθώς και σε διαμελισμό της λογικής δημιουργώντας περιπτώσιακές ροές. Κατά συνέπεια, κρίνεται απαραίτητο να εξεταστεί ο αποδοτικότερος τρόπος να δημιουργηθούν και να προσδιοριστούν οι ροές (flows) στο 5G και πόσες ροές είναι αποδοτικές χωρίς απώλεια της γενικότητας.

Η δυναμική των παρόχων δικτυακών υπηρεσιών είναι δυνατό να αυξηθεί σημαντικά στα επόμενα χρόνια, λόγω της χρήσης SDN και NFV, των διεπαφών, του λογισμικού ανοιχτού κώδικα και της πλατφόρμας. Ακόμα, αναμένεται ότι η τόσο εύκολη δημιουργία υπηρεσιών π.χ. από την πλατφόρμα του MCORD θα προσδώσει μία νέα δυναμική στα πράγματα και μία νέα δυναμική στους παρόχους. Παράλληλα, θα ενισχυθούν σημαντικά τα σενάρια ομαδοποίησης χρηστών οι αμειβόμενες υπηρεσίες, καθώς και τα SLAs. Επίσης, είναι δυνατό να προκύψουν εργαλεία υπολογισμού του κόστους, αφού ίσως με τις τεχνικές νέφους κάτι τέτοιο είναι πολύ πιο εύκολο.

Ακόμα εγείρονται σημαντικότερες προκλήσεις, όπως για παράδειγμα, η ανάγκη απλοϊκού υλικού, που με την προσθήκη λογικών προγραμματισμού στο δίκτυο, θα παρέχει συνθετότερες δυνατότητες σε ένα απλό δίκτυο, όπως για παράδειγμα, στην περίπτωση του εικονικού δρομολογητή. Σημαντικά επακόλουθα της καθολικής θέασης του δικτύου, της υψηλής απόδοσης και της συνύπαρξης της ήδη υπάρχουσας υποδομής με τη νέα, πρέπει να είναι να μην εμφανίζονται σημαντικά προβλήματα και να εξαλείφονται τα ήδη γνωστά δικτυακά εμπόδια.

Οι υπάρχουσες πηγές είναι δυνατό να διανέμονται πιο βελτιωμένα και να αποφεύγεται η «υποχρησιμοποίησή» τους. Επίσης, η αξιοποίηση της στατιστικής και της «παρακολούθησης» του δικτύου από τον ελεγκτή σε πραγματικό χρόνο είναι δυνατό να παρέχει ποιότητα υπηρεσίας και εμπειρίας, εξυπνότερες πόλεις, εξυπνότερα νοσοκομεία, εφαρμογές τηλεματικής σε ζητήματα κοινής ωφέλειας, για σκοπούς εκπαίδευσης και τηλεεκπαίδευσης και επικοινωνία μεταξύ μηχανών. Είναι πιθανό να δημιουργηθούν επιπρόσθετες ροές δεδομένων, όπως για παράδειγμα:

- Τομή διαφόρων υπηρεσιών
- Τομή ροών ανάλογα με χρήστη/συσκευή/τύπο δεδομένων
- Ποιότητα Υπηρεσίας και Ποιότητα Εμπειρίας
- Τομή επιχειρησιακών ροών
- Ροές βάση τοποθεσίας

Στα πλαίσια αυτά, ο έλεγχος των ροών και η δημιουργία τους καθίσταται ευκολότερη λόγω της διαχείρισης ελέγχου ροών μέσω του MCORD, λόγω της δυνατότητας ευελιξίας και λόγω των αναλύσεων, που μπορεί να προκύψουν λόγω του ελέγχου των προγραμματιζόμενων διεπαφών.

Όλα τα προηγούμενα πιθανά σενάρια μπορούν να υιοθετηθούν με χρήση του MCORD. Για παράδειγμα, το MCORD παρέχει εύκολη προσθήκη υπηρεσιών στην πλατφόρμα, που το ελέγχει. Από την άλλη μεριά, πολλές δυνατότητες παρέχονται στους παρόχους υπηρεσιών. Με την υιοθέτηση αυτής της τεχνικής αναμένεται να παρέχονται και στο χρήστη μακροπρόθεσμα σημαντικά οφέλη, όπως για παράδειγμα, καλύτερη απόδοση δικτύου και επίτευξη υψηλότερης κάλυψης για όλους τους χρήστες στο δίκτυο. Ενδεχομένως, να μειωθεί και το κόστος των παροχών υπηρεσιών.

Επιπρόσθετα, είναι πιθανό να δημιουργηθούν διαφορετικοί ελεγκτές και υπηρεσίες. Το βασικό πλεονέκτημα της διάθεσης λογισμικού ανοιχτού κώδικα συνίσταται στο ότι είναι δυνατό να δημιουργηθούν με βάση το παρεχόμενο λογισμικό, όπως για παράδειγμα με βάση τον εν λόγω ελεγκτή δικτύου διαφοροποιημένοι ελεγκτές, αφού κάθε ενδιαφερόμενος μπορεί να εισάγει επιπρόσθετα ζητήματα, διεπαφές και εφαρμογές επεκτείνοντας τον ήδη υπάρχοντα ελεγκτή σε μία δική του έκδοση ακόμα και εμπορική. Αυτό είναι σημαντικό, καθώς «σώζει» χρόνο και χρήμα. Ο χρόνος εξοικονομείται, διότι δεν απαιτείται η δημιουργία της βάσης του ελεγκτή, αλλά οι προστιθέμενες ανάγκες κάθε παρόχου, επιχείρησης κλπ.

Παρέχονται, ακόμα, τα βασικά πλεονεκτήματα του λογισμικού, αφού πρόκειται για ελεγκτή, που βασίζεται σε λογισμικό, είναι λογικό, ότι αποφεύγονται τα ζητήματα, που εγείρονται σχετικά με το υλικό. Τέτοια παραδείγματα είναι η επεκτασιμότητα, η αξιοπιστία, η

μείωση του κόστους, η ευελιξία, ο ευκολότερος έλεγχος ασφαλείας κλπ. Οι συσκευές είναι κυρίως βασισμένες σε λογισμικό, τα μηχανήματα, που περιλαμβάνονται είναι κυρίως εικονικές μηχανές και αυτός είναι ο λόγος για τον οποίο εξοικονομείται ενέργεια και πολλές εφαρμογές αναμένεται να γίνονται πιο γρήγορα. Για πολλές επιχειρήσεις το επενδυτικό ρίσκο είναι μικρότερο, αφού το να «εγκλωβιστούν» χρήματα σε υλικό είναι πολύ επικίνδυνο ειδικά σε εποχές οικονομικής κρίσης, όπως σήμερα, που ενέχονται σημαντικοί κίνδυνοι για κάθε επιχείρηση και οι επενδύσεις αντιμετωπίζονται με αυξημένη δυσπιστία. Οι εικονικές μηχανές και γενικότερα η αξιοποίηση του λογισμικού έναντι του υλικού είναι πιο βιώσιμη τεχνική για οποιαδήποτε επιχείρηση.

Η πιο καθολική όψη του δικτύου, που παρέχεται από τον ελεγκτή μπορεί να οδηγήσει σε καλύτερη διάθεση και διαχείριση των πόρων στο δίκτυο. Μπορεί να δημιουργήσει νέες σημαντικές υπηρεσίες, μπορεί να συμβάλει καθοριστικά στη δημιουργία βελτιωμένων πρωτοκόλλων ή αλγορίθμων για τη δρομολόγηση πακέτων, αφού είναι πιθανό η ευρεία όψη του δικτύου να οδηγήσει σε παρατηρήσεις, ιδιαίτερα χρήσιμες για την κίνηση και τις ανάγκες των χρηστών στο δίκτυο.

Η χρήση μεθόδων virtualization σε διάφορα στοιχεία ενός δικτύου, όπως για παράδειγμα στην περίπτωση της DAS αρχιτεκτονικής, μπορούν να συμβάλουν ενεργά στη μείωση του κόστους κεφαλαίου, του λειτουργικού κόστους και του συνολικού κόστους πολλές φορές. Αυτό συμβαίνει, διότι αλλάζουν οι υποδομές και γίνονται πιο απλές και βασίζονται περισσότερο σε λογισμικό. Κάτι τέτοιο, μπορεί να εξοικονομήσει πολλά χρήματα, ιδίως στο κομμάτι της συντήρησης, αλλά φυσικά και στο τμήμα της υλοποίησης. Αναλυτικά, οι πιο απλές συσκευές, όχι μόνο έχουν λιγότερα έξοδα, αλλά και η συντήρησή τους είναι πιο εύκολη, αφού μπορεί να απαιτείται μία απλή ενημέρωση του λογισμικού ή νέες εκδόσεις κατάλληλα ρυθμισμένες για τη συγκεκριμένη εφαρμογή. Ακόμα, το να μειωθεί σημαντικά η πολυπλοκότητα των συσκευών οδηγεί σε μείωση του χώρου των εγκαταστάσεων, μείωση της υποδομής, ελάττωση του καταναλισκόμενου ρεύματος και μείωση της αντίστοιχης δαπάνης. Το συγκεκριμένο γεγονός εκτός ότι εξοικονομεί χρήματα αποτελεί και έναυσμα για πράσινη καινοτομία και επιχειρηματικότητα.

Τελικά, παρατηρείται ότι οι συγκεκριμένες τεχνολογίες αποτελούν πηγή έμπνευσης και θα αποτελέσουν σημαντικό κομμάτι της έρευνας στο μέλλον, αφού αναμένεται να φανεί πως αυτές οι τεχνολογίες πρόκειται να προωθήσουν τα δίκτυα, σε ποιες κατευθύνσεις θα τα οδηγήσουν, με ποιες άλλες γνωστές δομές μπορούν να συνδυαστούν, τι άλλα σημαντικά οφέλη πρόκειται να προσφέρουν. Ακόμα, είναι εμφανές ότι επειδή είναι στην απαρχή τους, κατ' επέκταση στο μέλλον μπορεί να βρεθεί πλήθος ακόμα εφαρμογών αυτών των τεχνολογιών,

που σήμερα μπορεί να είναι όχι μόνο αδιανόητο, αλλά και εξαιρετικά απίστευτο ότι η τεχνολογία βαίνει προς την κατεύθυνση αυτή. Έτσι, θεωρείται ότι οι επιστήμονες και οι μηχανικοί στον τομέα των τηλεπικοινωνιών, της δικτύωσης και της πληροφορικής γενικότερα, θα αξιοποιήσουν πολλές από τις τεχνικές σε τομείς ζωτικής σημασίας.

## 7. ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

Πέραν των σημαντικότητας αποτελεσμάτων– συμπερασμάτων, τα οποία προκύπτουν με την πειραματική διαδικασία εγείρονται νέες ερευνητικές προκλήσεις και ερωτήσεις σχετικά με τις νέες τεχνολογίες SDN, NFV, CORD, MCORD, ONOS, καθώς και με τις απαιτήσεις, που εισάγονται από την 5G τεχνολογία. Οι δεδομένες τεχνολογίες κρίνονται ως σημαντικότερες σε ό,τι αναφορά στην είσοδό τους σε διάφορες εφαρμογές σχετικές με τα δίκτυα και στην επέκταση των υπάρχοντων δικτύων για την απόκριση αυτών στις μελλοντικές απαιτήσεις.

Σα μελλοντική έρευνα, μπορεί να σημειωθεί η εξερεύνηση πιθανών άλλων εφαρμογών των εν λόγω τεχνολογιών σε άλλα ζητήματα. Είναι σημαντικό να εξασφαλιστεί η ασφάλεια και να βρεθούν μέθοδοι να επιτυγχάνεται αυτή σε δίκτυα τύπου SDN τόσο στην ασύρματη όσο και στην ασύρματη περίπτωση. Ακόμα, είναι υψίστης σημασίας να δημιουργηθούν συγκεκριμένα πρότυπα, που να εξασφαλίζουν την ασφαλή λειτουργία των δικτύων σε κάθε επίπεδο, όπως για παράδειγμα από και προς το επίπεδο ελέγχου από και προς το επίπεδο εφαρμογών και από και προς το επίπεδο υποδομής.

Ακόμα, είναι βασικό να βρεθούν μέθοδοι, που να μειώνουν σημαντικά τα κόστη για τους παρόχους, τους χρήστες και για την κοινότητα των τηλεπικοινωνιών γενικότερα. Άλλωστε, σήμερα τόσο οι χρήστες όσο και οι πάροχοι έχουν γίνει ιδιαίτερα απαιτητικοί σχετικά με το να απολαμβάνουν και να παρέχουν οικονομικές και αποδοτικές υπηρεσίες αντιστοίχως. Οπότε είναι σημαντικό να ερευνηθούν τρόποι είτε να μειώνονται τα κόστη, όπως για παράδειγμα ενσωματώνοντας καινοτομίες σε παραδοσιακές μεθόδους μειώνοντας έτσι τη υλική υποδομή και κατ' επέκταση τα κόστη συντήρησης.

Επιπρόσθετα, σήμερα γίνεται ολοένα και περισσότερο λόγος για την αειφόρα και την πράσινη ανάπτυξη, οπότε δεδομένου ότι μεγάλο μέρος των εκπομπών ή της κατανάλωσης ρεύματος μπορεί να προκύπτει και λόγω των τηλεπικοινωνιών διαφαίνεται ως πρωταρχική ανάγκη η ερευνητική κίνηση και προς την κατεύθυνση αυτή. Θα ήταν πολύ ενδιαφέρον αν συνδυαζόταν η ενσωμάτωση ανανεώσιμων πηγών ενέργειας σε σταθμούς βάσης, κινητά δίκτυα, όπως π.χ. με ηλιακά πάνελ, με ανεμογεννήτριες κλπ.

Είναι, επίσης, υψίστης σημασίας να μελετηθούν δυνατές τροποποιήσεις των γνωστών πρωτοκόλλων, όπως τα: ARP, BGP, UDP, TCP, SSL, TLS, IP κλπ., ώστε να ανταποκρίνονται στις ανάγκες ασφάλειας των μελλοντικών δικτύων 5G. Πρέπει ακόμα, να ληφθούν υπόψη οι αδυναμίες του πρωτοκόλλου OpenFlow και να δημιουργηθούν κατάλληλες εκδόσεις αυτού, που να αντιμετωπίζουν τα κενά ασφάλειας σε κάθε επίπεδο. Είναι σημαντικό να βρεθούν όλες οι κερκόπορτες, που μπορεί να οδηγήσουν σε μη φυσιολογική λειτουργία, ή ακόμα και να θέσουν ολόκληρο το δίκτυο εκτός λειτουργίας. Νέοι κρυπτογραφικοί μηχανισμοί πρέπει να εισαχθούν στα συστήματα, οι οποίοι να είναι δυνατό να παρέχουν σημαντικές διεξόδους ή εναλλακτικά σχέδια αν το δίκτυο πέσει θύμα επιθέσεων.

Πρέπει να δημιουργηθούν κατάλληλα πρότυπα, που να επιβάλουν πολιτικές, οι οποίες να είναι σε θέση να αποκλείουν πιθανόν ύποπτους χρήστες, να αποτρέπουν περιπτώσεις hacking και κατάρριψης ιστοσελίδων κλπ. ή ακόμα και να συμβάλουν στην αποτροπή υποκλοπής πληροφορίας από πιθανούς στόχους, που περιλαμβάνουν μεγάλα ποσά εμπιστευτικών πληροφοριών.

Ακόμα, επειδή τα πιο πολλά αντικείμενα στο νέο δίκτυο αποτελούνται από λογισμικό, πρέπει να υπάρχουν μηχανισμοί πιστοποίησης της ποιότητας του λογισμικού στο συγκεκριμένο τομέα, καθώς και της ασφάλειας αυτού. Οπότε, είναι σημαντικό ως μελλοντική έρευνα να προταθούν τέτοιοι μηχανισμοί, οι οποίοι να είναι δυνατό να εκτελούν αυτούς τους ελέγχους και να πιστοποιούν ουσιαστικά την ποιότητα του λογισμικού και συνάμα τη διατήρησή αυτού σε πλήρως λειτουργική κατάσταση.

Επιπρόσθετα, είναι σημαντικό να μελετηθεί πώς είναι δυνατό να γίνονται οι λύσεις αυτές εφαλτήριο για την έρευνα και την εκπαίδευση. Ακόμα, η εκπαιδευτική τεχνολογία στον τομέα των δικτύων και επικοινωνιών είναι δυνατό να προαχθεί μέσω των εφαρμογών του ONOS. Συνεπώς, είναι δυνατό να σημειωθούν τεχνικές, οι οποίες να μπορούν να παρέχουν σημαντικά οφέλη σε σχέση με την ακαδημαϊκή και πανεπιστημιακή εκπαίδευση στο θέμα. Είναι σημαντικό να σημειωθούν μέθοδοι να ενσωματωθεί η εξήγηση των SDN & NFV στα σύγχρονα προγράμματα σπουδών. Επίσης, είναι σημαντικό να συγκριθούν όλοι οι διαθέσιμοι δικτυακοί ελεγκτές και να αναδειχθεί ποιος είναι ο πιο κατάλληλος για εκπαιδευτικές εφαρμογές.

Επιπλέον, είναι κρίσιμο να αναπτυχθούν επιπλέον υπηρεσίες, οι οποίες να αποδώσουν οικονομικά οφέλη στους παρόχους και ποιότητα εμπειρίας και υπηρεσίας στον απλό χρήστη. Για παράδειγμα, η στροφή στο λογισμικό είναι δυνατό να ωθήσει στη δημιουργία συστήματος χρέωσης πολύ χαμηλότερου κόστους, πολύ πιο εύκολα διαχειρίσιμο από τον πάροχο, που να επιδιώκει να αποδίδει νέες κλάσεις σε διαφορετικούς πελάτες. Επίσης, είναι βασικό να

αξιοποιηθούν οι τεχνικές αυτές με σκοπό τη βελτίωση της ποιότητας βίντεο και η καλύτερη κάλυψη παρόμοιων εφαρμογών, όπως για παράδειγμα του livestreaming, καθώς και η κάλυψη τηλεδιασκέψεων από κινητές συσκευές αποδοτικά και σε καλή ποιότητα εικόνας και ήχου.

Εν συνεχεία, είναι σημαντικό να προτυποποιηθεί μία αρχιτεκτονική-πρότυπο σχετικά με τα SDN και NFV στον εν λόγω τομέα των κινητών δικτύων. Ακόμα, το συγκεκριμένο πρότυπο πρέπει να καθιστά σαφές πως πραγματοποιείται η ασφάλεια στα συγκεκριμένα δίκτυα και με ποιους τρόπους εξασφαλίζεται η βελτιστοποίηση των δικτύων. Σε αυτά τα πλαίσια είναι σημαντικό να προταθούν μηχανισμοί ασφαλείας και ανάνηψης του δικτύου σε περίπτωση ολικής απώλειας ή βλάβης αυτού. Όσον αφορά στο πρωτόκολλο OpenFlow είναι σημαντικό να αξιοποιηθούν τεχνικές, που προάγουν την ασφάλεια μεταξύ του ελεγκτή και των μεταγωγών, που υπάρχουν.

Ο ONOS είναι σημαντικό να συγκριθεί με άλλους γνωστούς ελεγκτές εκτός του POX και να χρησιμοποιηθεί σε παραδείγματα πραγματικού χρόνου ή πραγματικών δικτύων με απώτερο σκοπό να αναδειχθεί η σημασία του και η αξιοπιστία του και σε αυτές τις εφαρμογές. Επίσης, θα είναι ιδιαίτερα ενδιαφέρον να αναδειχθεί πως θα γίνει ο ONOS από ανοιχτού κώδικα εμπορικής φύσεως αν αποφασίσει κάποια εταιρεία να αναπτύξει βασιζόμενη σε αυτή το δικό της σύστημα ελεγκτή και τη δική της προσέγγιση ως προς τη διεπαφή κλπ.

Ακόμα, μπορεί να μελετηθούν και άλλα αρχιτεκτονικά μοντέλα και πρότυπα. Επιπλέον, είναι σημαντικό να δημιουργηθούν σημαντικές ιδέες για το πως μπορεί να μειωθεί το κόστος με βάση αυτές τις τεχνικές. Είναι σημαντικό να βρεθούν νέες πιθανές εφαρμογές, όπως είναι για παράδειγμα η virtualization ή ακόμα να εξερευνηθεί αν και κατά πόσο είναι δυνατό να ενσωματωθεί σε άλλα δίκτυα, με αποτέλεσμα να αποδίδονται σημαντικά οφέλη και να είναι δυνατό να δίνεται μία νέα όψη σε παραδοσιακές τεχνολογίες, ώστε να αξιοποιούνται με έναν διαφορετικό τρόπο.

Τέλος, καθίσταται σαφές ότι ο συγκεκριμένος συνδυασμός τεχνολογιών είναι τόσο πολυδιάστατος και τόσο ευεργετικός για τα σύγχρονα δίκτυα από πολλές απόψεις και ως αποτέλεσμα, δεν μπορεί να είναι γνωστό από τώρα ποια ή ποιες πρόκειται να αποτελέσουν οι μελλοντικές σκέψεις και βλέψεις του τομέα. Σίγουρο είναι ότι θα υπάρξει μεγάλο ενδιαφέρον σχετικά με τις παραπάνω προσεγγίσεις.



## Βιβλιογραφία

1. Orange, J. S. B., Armada, A. G., Evans, B., Galis, A., & Karl, H. (2015). White Paper for Research Beyond 5G. Accessed, 23, 2016.
2. Chappell, C. (2015). Deploying virtual network functions: The complementary roles of TOSCA and NETCONF/YANG. Heavy Reading, Cisco, Alcatel-Lucent, New York, NY, USA, Tech. White Paper.
3. ETSI, GSNFV. "Network Functions Virtualisation (NFV); Use Cases." V1 1 (2013): 2013-10.
4. <http://www.etsi.org/technologies-clusters/technologies/nfv/nfv-poc> (12/2016)
5. Beming, P., Frid, L., Hall, G., Malm, P., Noren, T., Olsson, M., & Rune, G. (2007). LTE-SAE architecture and performance. Ericsson Review, 3, 98-104.
6. Alcatel Lucent, "The LTE Network Architecture: A Comprehensive Tutorial," Strategic Whitepaper, 2009.
7. Sesia, S., Toufik, I., & Baker, M. (2015). LTE-the UMTS long term evolution. John Wiley.
8. ONF. OpenFlow enabled SDN and NFV. ONF. Requirements Analysis for Transport OpenFlow/SDN. 2014.
9. OpenFlow-Enabled Mobile and Wireless Networks.ONF. September 2013.
10. Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials, 16(3), 1617-1634.
11. Xia, W., Wen, Y., Foh, C. H., Niyato, D., & Xie, H. (2015). A survey on software-defined networking. IEEE Communications Surveys & Tutorials, 17(1), 27-51.
12. Lav Gupta. SDN: Development, Adoption and Research Trends. December 2013.
13. Schneider, F., Egawa, T., Schaller, S., Hayano, S. I., Schöller, M., & Zdarsky, F. (2014). Standardizations of sdn and its practical implementation. NEC Technical Journal, Special Issue on SDN and Its Impact on Advanced ICT Systems, 8(2).
14. Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., ... & Rao, N. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. IEEE Communications Magazine, 51(7), 36-43.

15. Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1), 14-76.
16. Arlimatti, S., Hassan S., Habbal A. and Arif S. SOFTWARE DEFINED NETWORKING AND OPENFLOW: A CRITICAL REVIEW. *ARNP Journal of Engineering and Applied Sciences*. February 2015. 10(3).
17. Jammal, M., Singh, T., Shami, A., Asal, R., & Li, Y. (2014). Software defined networking: State of the art and research challenges. *Computer Networks*, 72, 74-98.
18. Ali, S. T., Sivaraman, V., Radford, A., & Jha, S. (2015). A survey of securing networks using software defined networking. *IEEE transactions on reliability*, 64(3), 1086-1097.
19. G. Garg and R. Garg "Review on architecture and security issues in SDN", *International Journal of Innovative Research in Computer and Communication Engineering*" Vol. 2, Issue 11, pp. 6519-6524, November 2014.
20. Liyanage, M., Ahmed, I., Ylianttila, M., Santos, J. L., Kantola, R., Perez, O. L., ... & Jimenez, C. (2015, September). Security for future software defined mobile networks. In *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on* (pp. 256-264). IEEE.
21. Eghbali, H., & Wong, V. W. (2015, June). Bandwidth allocation and pricing for SDN-enabled home networks. In *2015 IEEE International Conference on Communications (ICC)* (pp. 5342-5347). IEEE.
22. Wang, B., Bin, Z., Yao, M., & Wang, W. (2015). Virtual Tenant Network Research based on Price Mechanism in SDN Architecture.
23. Artuso, M., Caba, C. M., Christiansen, H. L., & Soler, J. (2016). Towards Flexible SDN-based Management for Cloud-based Mobile Networks. In *IEEE/IFIP Network Operations and Management Symposium*.
24. Chen, T., Matinmikko, M., Chen, X., Zhou, X., & Ahokangas, P. (2015). Software defined mobile networks: concept, survey, and research directions. *IEEE Communications Magazine*, 53(11), 126-133.
25. <https://www.celticplus.eu/sigmona-sdn-concept-in-generalized-mobile-network-architectures/> (12/2016)
26. Anderson, T., Bosch, P., & Duminuco, A. (2016). Bandwidth Control and Regulation in Mobile Networks via SDN/NFV-Based Platforms.

27. Yang, M., Li, Y., Jin, D., Zeng, L., Wu, X., & Vasilakos, A. V. (2015). Software-defined and virtualized future mobile and wireless networks: A survey. *Mobile Networks and Applications*, 20(1), 4-18.
28. Lee, J., Uddin, M., Tourrilhes, J., Sen, S., Banerjee, S., Arndt, M., ... & Nadeem, T. (2014, June). meSDN: mobile extension of SDN. In *Proceedings of the fifth international workshop on Mobile cloud computing & services* (pp. 7-14). ACM.
29. Ku, I., Lu, Y., & Gerla, M. (2014, August). Software-defined mobile cloud: Architecture, services and use cases. In *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 1-6). IEEE.
30. Pupatwibul, P., Banjar, A., Sabbagh, A. A., & Braun, R. (2013, October). Developing an application based on OpenFlow to enhance mobile IP networks. In *Local Computer Networks Workshops (LCN Workshops), 2013 IEEE 38th Conference on* (pp. 936-940). IEEE.
31. Li, Y. (2015). Future Cellular Network Architecture. *The Future of Wireless Networks: Architectures, Protocols, and Services*, 21, 1.
32. Kabir, M. H. (2014). A Novel Architecture for SDN-based Cellular Network. *International Journal of Wireless & Mobile Networks*, 6(6), 71.
33. Li, L. E., Mao, Z. M., & Rexford, J. (2012, October). Toward software-defined cellular networks. In *2012 European Workshop on Software Defined Networking* (pp. 7-12). IEEE.
34. Bradai, A., Singh, K., Ahmed, T., & Rasheed, T. (2015). Cellular software defined networking: a framework. *IEEE Communications Magazine*, 53(6), 36-43.
35. Ali-Ahmad, H., Cicconetti, C., De la Oliva, A., Mancuso, V., Sama, M. R., Seite, P., & Shanmugalingam, S. (2013, November). An SDN-based network architecture for extremely dense wireless networks. In *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for* (pp. 1-7). IEEE.
36. Riggio, R., Gomez, K. M., Rasheed, T., Schulz-Zander, J., Kuklinski, S., & Marina, M. K. (2014, November). Programming software-defined wireless networks. In *10th International Conference on Network and Service Management (CNSM) and Workshop* (pp. 118-126). IEEE.
37. Bernardos, C. J., De La Oliva, A., Serrano, P., Banchs, A., Contreras, L. M., Jin, H., & Zúñiga, J. C. (2014). An architecture for software defined wireless networking. *IEEE Wireless Communications*, 21(3), 52-61.

38. Yap, K. K., Sherwood, R., Kobayashi, M., Huang, T. Y., Chan, M., Handigol, N., ... & Parulkar, G. (2010, September). Blueprint for introducing innovation into wireless mobile networks. In Proceedings of the second ACM SIGCOMM workshop on Virtualized infrastructure systems and architectures (pp. 25-32). ACM.
39. Marc Mendonca, Katia Obraczka, Thierry Turetli. The Case for Software-Defined Networking in Heterogeneous Networked Environments. Paolo Costa and Wenjun Hu and Vyas Sekar. CoNEXT Student '12 Proceedings of the 2012 ACM conference on CoNEXT student workshop, Dec 2012, Nice, France. ACM New York, NY, USA, pp.59-60, 2012.
40. Duan, X., & Wang, X. (2015). Authentication handover and privacy protection in 5G hetnets using software-defined networking. IEEE Communications Magazine, 53(4), 28-35.
41. Dely, P., Kessler, A., & Bayer, N. (2011, July). Openflow for wireless mesh networks. In Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on (pp. 1-6). IEEE.
42. Yang, M., Li, Y., Jin, D., Su, L., Ma, S., & Zeng, L. (2013, August). OpenRAN: a software-defined ran architecture via virtualization. In ACM SIGCOMM computer communication review (Vol. 43, No. 4, pp. 549-550). ACM.
43. Bansal, M., Mehlman, J., Katti, S., & Levis, P. (2012, August). Openradio: a programmable wireless dataplane. In Proceedings of the first workshop on Hot topics in software defined networks (pp. 109-114). ACM.
44. Gudipati, A., Perry, D., Li, L. E., & Katti, S. (2013, August). SoftRAN: Software defined radio access network. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 25-30). ACM.
45. Mahindra, R., Khojastepour, M. A., Zhang, H., & Rangarajan, S. (2013, October). Radio access network sharing in cellular networks. In 2013 21st IEEE International Conference on Network Protocols (ICNP) (pp. 1-10). IEEE.
46. <http://www.fujitsu.com/downloads/TEL/fnc/whitepapers/CloudRANwp.pdf> (12/2016)
47. <http://onosproject.org/wp-content/uploads/2015/06/Technical-Whitepaper-CORD.pdf> (12/2016)
48. <http://xosproject.org/wp-content/uploads/2015/04/CORD-meets-NFV.pdf>
49. <http://sdn.ieee.org/newsletter/march-2016/rethinking-the-mobile-edge-network-with-cord-mobile-cord> (12/2016)

50. <http://www.prnewswire.com/news-releases/onos-mobile-cord-m-cord-platform-brings-sdn-nfv-and-cloud-principles-to-mobility--significant-progress-toward-realizing-5g-solutions-300223727.html> (12/2016)
51. <https://www.sdxcentral.com/event/radisys-att-m-cord-nfv-5g-demofriday/> (12/2016)
52. <https://virtualizationreview.com/articles/2015/06/18/cord-demo.aspx> (12/2016)
53. <https://www.celticplus.eu/sigmona-sdn-concept-in-generalized-mobile-network-architectures/>
54. <http://sdn.ieee.org/newsletter/march-2016/rethinking-the-mobile-edge-network-with-cord-mobile-cord>
55. <http://www.prnewswire.com/news-releases/onos-mobile-cord-m-cord-platform-brings-sdn-nfv-and-cloud-principles-to-mobility--significant-progress-toward-realizing-5g-solutions-300223727.html>
56. <https://www.sdxcentral.com/event/radisys-att-m-cord-nfv-5g-demofriday/>
57. <http://xos.wpengine.com/wp-content/uploads/2015/06/Whitepaper-CORD-fabric-demo.pdf>
58. <http://sdn.ieee.org/newsletter/january-2016/rethinking-metro-networks>
59. [http://onosproject.org/wp-content/uploads/2015/06/PoC\\_CORD.pdf](http://onosproject.org/wp-content/uploads/2015/06/PoC_CORD.pdf)
60. <http://onrc.stanford.edu/protected%20files/PDF/ONRC-CORD-Larry.pdf>
61. <https://www.opennetworking.org/images/stories/downloads/showcase/2015-6/CORD-Slides-ONS-ONF-June-11.pdf>
62. <https://www.sdxcentral.com/nfv/definitions/whats-network-functions-virtualization-nfv/>
63. <http://searchsdn.techtarget.com/definition/network-functions-virtualization-NFV>
64. <http://www.advaoptical.com/en/products/technology/what-is-nfv.aspx>
65. <https://www.sdxcentral.com/nfv/definitions/whats-network-functions-virtualization-nfv/>
66. Berde, P., Gerola, M., Hart, J., Higuchi, Y., Kobayashi, M., Koide, T., ... & Parulkar, G. (2014, August). ONOS: towards an open, distributed SDN OS. In Proceedings of the third workshop on Hot topics in software defined networking (pp. 1-6). ACM.
67. Muqaddas, A. S., Bianco, A., Giaccone, P., & Maier, G. (2016). Inter-controller Traffic in ONOS Clusters for SDN Networks. IEEE ICC, Kuala Lumpur, Malaysia, May.

68. Kim, W., Li, J., Hong, J. W. K., & Suh, Y. J. (2016, June). OFMon: OpenFlow monitoring system in ONOS controllers. In 2016 IEEE NetSoft Conference and Workshops (NetSoft) (pp. 397-402). IEEE.
69. Fontes, R. R., Afzal, S., Brito, S. H., Santos, M. A., & Rothenberg, C. E. (2015, November). Mininet-WiFi: Emulating software-defined wireless networks. In Network and Service Management (CNSM), 2015 11th International Conference on (pp. 384-389). IEEE.
70. <http://www.brianlinkletter.com/Mininet-wifi-software-defined-network-emulator-supports-wifi-networks/>
71. <https://www.openstack.org/software/>
72. T. Chin, X. Mountroudou, X. Li, and K. Xiong. Selective packet inspection to detect dos flooding using software defined networking (sdn). In 2015 IEEE 35th International Conference on Distributed Computing Systems Workshops, pages 95–99. IEEE, 2015.
73. J. Francois, L. Dolberg, O. Festor, and T. Engel. Network security through software defined networking: A survey. In Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications, IPTComm '14, pages 6:1–6:8, New York, NY, USA, 2014. ACM.
74. B. JAMES. Security and privacy challenges in cloud computing, environments.
75. R. Jin and B. Wang. Malware detection for mobile devices using software-defined networking. In Proceedings of the 2013 Second GENI Research and Educational Experiment Workshop, GREE '13, pages 81– 88, Washington, DC, USA, 2013. IEEE Computer Society.
76. OPEN NETWORKING FOUNDATION. Principles and practices for securing software-defined networks. Technical report, OPEN NETWORKING FOUNDATION (ONF), January 2015.
77. Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran. Security in software-defined networking: Threats and countermeasures. Mobile Networks and Applications, pages 1–13.
78. M. Vizvary and J. Vykopal. Future of ddos attacks mitigation in software defined networks. In IFIP International Conference on Autonomous Infrastructure, Management and Security, pages 123–127. Springer, 2014.
79. B. Wang, Y. Zheng, W. Lou, and Y. T. Hou. Ddos attack protection in the era of cloud computing and software-defined networking. In 2014 IEEE 22nd International Conference on Network Protocols, pages 624– 629, Oct 2014.

80. Q. Yan and F. R. Yu. Distributed denial of service attacks in software defined networking with cloud computing. *IEEE Communications Magazine*, 53(4):52–59, April 2015.
81. Q. Yan, F. R. Yu, Q. Gong, and J. Li. Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys Tutorials*, 18(1):602–622, Firstquarter 2016.
82. S. T. Zargar, J. Joshi, and D. Tipper. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE Communications Surveys Tutorials*, 15(4):2046–2069, Fourth 2013.
83. [https://www.google.gr/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwjUwfyuweLRAhUBthoKHYhfDvMQjxwIAw&url=http%3A%2F%2Fwww.zte.com.cn%2Fen%2Fmagazine%2Fztetechnologies%2F2015%2Fno2%2Farticles%2F201503%2Ft20150324\\_432513.html&psig=AFQjCNFSrigAk4PaK\\_bqfBI9dW9fnx2jvw&ust=1485612832410415](https://www.google.gr/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwjUwfyuweLRAhUBthoKHYhfDvMQjxwIAw&url=http%3A%2F%2Fwww.zte.com.cn%2Fen%2Fmagazine%2Fztetechnologies%2F2015%2Fno2%2Farticles%2F201503%2Ft20150324_432513.html&psig=AFQjCNFSrigAk4PaK_bqfBI9dW9fnx2jvw&ust=1485612832410415) (27/1/2016).
84. <http://thenewstack.io/sdn-series-part-eight-comparison-of-open-source-sdn-controllers/> (1/2017).
85. [http://rtomaszewski.blogspot.gr/2014\\_04\\_01\\_archive.html](http://rtomaszewski.blogspot.gr/2014_04_01_archive.html) (1/2017).
86. Bouras, C., Ntarzanos, P., & Papazois, A. (2016, October). Cost modeling for SDN/NFV based mobile 5G networks. In *Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), 2016 8th International Congress on* (pp. 56-61).
87. IEEE. S. Cosgrove. Teaching software defined networking: It’s not just coding. In *2016 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, pages 139–144, Dec 2016.
88. T. Chin, X. Mountroudou, X. Li, and K. Xiong. Selective packet inspection to detect dos flooding using software defined networking (sdn). In *2015 IEEE 35th International Conference on Distributed Computing Systems Workshops*, pages 95–99. IEEE, 2015.
89. J. Su´arez-Varela and P. Barlet-Ros. Reinventing netflow for openflow software-defined networks. *arXiv preprint arXiv:1702.06803*, 2017.
90. Y. Taniguchi, H. Tsutsumi, N. Iguchi, and K. Watanabe. Design and evaluation of a proxy-based monitoring system for openflow networks. *The Scientific World Journal*, 2016, 2016.
91. M. D. Moreira, N. C. Fern, H. E. Carvalho, L. Henrique, G. Ferraz, R. S. Couto, I. M. Moraes, M. Elias, M. Campista, L. H. M. Costa, et al. Packet forwarding using openflow.

92. Bouras, C., Kokkinos, V., Kollia, A., & Papazois, A. (2015, August). Techno-economic analysis of ultra-dense and DAS deployments in mobile 5G. In *Wireless Communication Systems (ISWCS), 2015 International Symposium on* (pp. 241-245). IEEE.
93. Bouras, C., Kollia, A., & Papazois, A. (2017). Dense Deployments and DAS in 5G: A Techno-Economic Comparison. *Wireless Personal Communications*, 94(3), 1777-1797.
94. Bouras, C., Kollia, A., & Papazois, A. (2016, April). Sensitivity analysis of small cells and DAS techno-economic models in mobile 5G. In *Wireless Communications and Networking Conference (WCNC), 2016 IEEE* (pp. 1-6). IEEE.
95. Bouras, C., Kollia, A., & Papazois, A. (2017). Analyzing Small - cells and Distributed Antenna Systems from Techno - economic Perspective. Retrieved October 2, 2017, from International Journal of Wireless Networks and Broadband Technologies (IJWNBT)
96. [http://ru6.cti.gr/ru6/system/files/bouras\\_site/ergasies/diplwmatikes/Kollia\\_diplomatiki.pdf?language=el](http://ru6.cti.gr/ru6/system/files/bouras_site/ergasies/diplwmatikes/Kollia_diplomatiki.pdf?language=el)
97. Bouras, C., Kollia, A., & Papazois, A. (2017, March). SDN & NFV in 5G: Advancements and challenges. In *Innovations in Clouds, Internet and Networks (ICIN), 2017 20th Conference on* (pp. 107-111). IEEE.
98. Bouras, C., Kollia, A., & Papazois, A. (2017, July). Teaching network security in mobile 5G using ONOS SDN controller. In *Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on* (pp. 465-470). IEEE.
99. Bouras, C., Kollia, A., & Papazois, A. (2017, July). Teaching 5G networks using the ONOS SDN controller. In *Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on* (pp. 312-317). IEEE.
100. Bouras, C., Kollia, A., & Papazois, A. (pending). Exploring SDN & NFV in 5G Using ONOS & POX Controllers. *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)*.



## Παράρτημα Α: Τοπολογίες

Στο παράρτημα παρατίθεται αντίστοιχα ο κώδικας για καθεμία από τις περιπτώσεις, που μελετήθηκαν και εξηγήθηκαν στην πειραματική διαδικασία. Σε κάθε ένα από τα παρακάτω υπάρχει αντίστοιχα επεξήγηση κάποιων βασικών στοιχείων κώδικα στην αγγλική γλώσσα. Αναλυτικά:

Το αρχείο `vRouter.py` παρατίθεται ακολούθως και περιλαμβάνει τον κώδικα για τη δημιουργία του εικονικού δρομολογητή, πραγματοποιείται επικοινωνία με το BGP πρωτόκολλο υπάρχουν τα κυριότερα στοιχεία της τοπολογίας, όπως PC και μεταγωγείς, εκκινείται το δίκτυο.

### *vRouter.py:*

Η συγκεκριμένη τοπολογία αναφέρεται σε δίκτυο με μεταγωγείς και τερματικά. Για να εκτελεστεί επιτυχώς απαιτείται μηχανήμα, το οποίο έχει εγκατεστημένο mininet, καθώς και τον αντίστοιχο χρησιμοποιούμενο ελεγκτή δικτύου. Η αντίστοιχη υλοποίηση παρατίθεται πιο κάτω. Η εντολή, που χρησιμοποιήθηκε για να τρέξει αυτή η τοπολογία είναι:

```
Sudo mn - -custom ~/mininet/custom/vrouter.py - - topo my topo - -controller remote
```

```
#!/usr/bin/python
```

```
# the main goal of this python script is to create a vrouter
```

```
#a vrouter is a commodity switch that does nothing in particular and we add to it
```

```
#routing functionality
```

```
#so its not actually a router, but it is virtually deployed to function as one
```

```
#libraries for Mininet/netorking topologies/ command-line applications / info/ debugging
```

```
#networking nodes such as controller/ switches and hosts
```

```
from Mininet.topo import Topo
```

```
from Mininet.net import Mininet
```

```
from Mininet.cli import CLI
```

```
from Mininet.log import setLogLevel, info, debug
```

```
from Mininet.node import Host, RemoteController
```

```
# quagga is the interface that helps enabling the bgp protocol
```

```
# writing yes to the quagga file as a configuration in the correct variable
```

```

# enabling the bgp protocol
QUAGGA_DIR = '/usr/lib/quagga'
# Must exist and be owned by quagga user (quagga:quagga by default on Ubuntu)
QUAGGA_RUN_DIR = '/var/run/quagga'
CONFIG_DIR = 'configs'
#Create a vRouter host class to integrate the explained vRouter functionality
class vRouterHost(Host):
    def __init__(self, name, ip, route, *args, **kwargs):
        Host.__init__(self, name, ip=ip, *args, **kwargs)

        self.route = route

    def config(self, **kwargs):
        Host.config(self, **kwargs)

        debug("configuring route %s" % self.route)

        self.cmd('Ip route add default via %s' % self.route)

#create the router class to integrate the router functionality
class vRouter(Host):
    def __init__(self, name, quaggaConfFile, zebraConfFile, intfDict, *args, **kwargs):
        Host.__init__(self, name, *args, **kwargs)

        self.quaggaConfFile = quaggaConfFile
        self.zebraConfFile = zebraConfFile
        self.intfDict = intfDict
    def config(self, **kwargs):
        Host.config(self, **kwargs)
        self.cmd('sysctl net.ipv4.ip_forward=1')

        for intf, attrs in self.intfDict.items():
            self.cmd('ip addr flush dev %s' % intf)
            if 'mac' in attrs:

```

```

        self.cmd('ip link set %s down' % intf)
        self.cmd('ip link set %s address %s' % (intf, attrs['mac']))
        self.cmd('ip link set %s up ' % intf)
    for addr in attrs['ipAddrs']:
        self.cmd('ip addr add %s dev %s' % (addr, intf))

    self.cmd('/usr/lib/quagga/zebra -d -f %s -z %s/zebra%s.api -i %s/zebra%s.pid' %
(self.zebraConfFile, QUAGGA_RUN_DIR, self.name, QUAGGA_RUN_DIR, self.name))
    self.cmd('/usr/lib/quagga/bgpd -d -f %s -z %s/zebra%s.api -i %s/bgpd%s.pid' %
(self.quaggaConfFile, QUAGGA_RUN_DIR, self.name, QUAGGA_RUN_DIR, self.name))

    def terminate(self):
        self.cmd("ps ax | egrep 'bgpd%s.pid|zebra%s.pid' | awk '{print $1}' | xargs kill" %
(self.name, self.name))
        Host.terminate(self)
#class that creates the vRouter topology needed for the exact script
class vRouterTopo( Topo ):
    """***** Creating the vRouter topology*****"""
    def build( self ):
        #adding the only switch of the topology that is a vRouter
        s1 = self.addSwitch('s1', dpid='00000000000000b1')
        #include the zebra configuration file
        zebraConf = '%s/zebra.conf' % CONFIG_DIR

        #setting up ethernets of the router
        eth0 = { 'mac' : '00:00:00:00:00:01' ,
                'ipAddrs' : ['10.0.0.1/24'] }
        eth1 = { 'ipAddrs' : ['192.168.1.254/24'] }
        intfs = { '%s-eth0' % name : eth0,
                '%s-eth1' % name : eth1 }
        quaggaConf = '%s/quagga%s.conf' % (CONFIG_DIR, 1)

        #add the router functionality
        router = self.addHost(name, cls=Router, quaggaConfFile=quaggaConf,

```

```

        zebraConfFile=zebraConf, intfDict=intfs)

#add link between switch and router
self.addLink(router, s1)

#add hosts in the topology between switch and router
for i in range(1, 2):
    host = self.addHost('h%s' % i, cls=vRouterHost,
                        ip='192.168.1.1/24' % i,
                        route='192.168.1.254' % i)

    #connect the added hosts with the switch
    self.addLink(host,s1)

# Set up the internal BGP speaker
bgpEth0 = { 'mac':'00:00:00:00:00:01',
            'ipAddrs' : ['10.0.2.1/24',
                        '10.0.2.2/24',
                        '10.0.2.3/24',
                        '10.0.2.4/24',] }
bgpEth1 = { 'ipAddrs' : ['10.10.10.1/24'] }
bgpIntfs = { 'bgp-eth0' : bgpEth0,
            'bgp-eth1' : bgpEth1 }

bgp = self.addHost( "bgp", cls=Router,
                    quaggaConfFile = '%s/quagga-sdn.conf' % CONFIG_DIR,
                    zebraConfFile = zebraConf,
                    intfDict=bgpIntfs )

#adding link between the switch and the bgp so it can peer
self.addLink( bgp, s1 )

# Connect BGP speaker to the root namespace so it can peer with ONOS
root = self.addHost( 'root', inNamespace=False, ip='10.10.10.2/24' )
self.addLink( root, bgp )
self.plotGraph(max_x=100, max_y=100)

#give a plot of the topology made

```

```

#net.plotGraph(max_x=100, max_y=100)

topos = { 'vRouter' : vRouterTopo }
print '*****VROUTER TOPOLOGY*****'
if __name__ == '__main__':
    setLogLevel('debug')
    topo = vRouterTopo()
    #create the network in Mininet
    net = Mininet(topo=topo, controller=RemoteController)
    #network starts functioning
    net.start()
    info('***** Starting network*****\n')
    #plot the network topology
    net.plotGraph(max_x=100, max_y=1000)
    CLI(net)
    #network stops functioning
    net.stop()
    info('***** Stopping network*****')

```

Ομοίως, για τις τοπολογίες, που σχετίζονται με τα κινητά δίκτυα, IPRAN.py και heterogeneous.py. Στην περίπτωση αυτή, δομούνται οι κινητές τοπολογίες και εισάγονται τα διάφορα κινητά στοιχεία. Στην IPRAN εισάγονται οι σταθμοί βάσης και τα σημεία πρόσβασης, ενώ στην ετερογενή περίπτωση εμφανίζονται και τα τερματικά και οι μεταγωγείς. Αναλυτικά, ο κώδικας για αυτά παρατίθεται παρακάτω:

*IPRAN.py:*

Η συγκεκριμένη τοπολογία αναφέρεται σε δίκτυο με σταθμούς βάσης και σημεία πρόσβασης. Για να εκτελεστεί επιτυχώς απαιτείται μηχανήμα, το οποίο έχει εγκατεστημένο mininet-wifi, καθώς και τον αντίστοιχο χρησιμοποιούμενο ελεγκτή δικτύου. Η αντίστοιχη υλοποίηση παρατίθεται πιο κάτω. Εντολή για να τρέξει η τοπολογία είναι:

```
Sudo mn - -wifi - -custom ~/mininet-wifi/custom/IPRAN.py - - topo my topo - -controller remote
```

```
#!/usr/bin/python
```

```
#making a simple IPRAN topology
```

```
#importing libraries concerning Mininet/ Controllers/ Onos etc
```

```
from Mininet.net import Mininet
```

```
from Mininet.node import Controller, RemoteController, OVSKernelSwitch
```

```
from Mininet.link import TCLink
```

```
from Mininet.cli import CLI
```

```
from Mininet.log import setLogLevel
```

```
def topology():
```

```
#making a network with a remote controller and a OVS switch
```

```
net = Mininet( controller=remote, link=TCLink, switch=OVSKernelSwitch )
```

```
print "***** Creating nodes*****"
```

```
#creating two access points explaining their exact configuration
```

```
ap1 = net.addBaseStation( 'ap1', ssid= 'ssid-ap1', mode= 'g', channel= '1', position='10,30,0',  
range='20' )
```

```
#creating two sta1 points explaining their exact configuration
```

```
sta1 = net.addStation( 'sta1', mac='00:00:00:00:00:01', ip='10.0.0.1/8', position='10,20,0' )
```

```
sta2 = net.addStation( 'sta2', mac='00:00:00:00:00:02', ip='10.0.0.2/8', position='50,20,0' )
```

```
#creating the quagga Configuration for router
```

```
router = net.addHost(name, cls=Router,  
quaggaConfFile=quaggaConf,zebraConfFile=zebraConf, intfDict=intfs)
```

```

print "***** Creating links and associations*****"
net.addLink( c0, ap1 )
net.addLink( c0, router )
net.addLink( ap1, sta1 )
net.addLink( sta1, sta2 )
#Connect BGP speaker to the root namespace so it can peer with ONOS
root = net.addHost( 'root', inNamespace=False, ip='10.10.10.2/24' )
net.addLink( root, bgp )

print "***** Starting network*****"
print "***** Creating IPRAN network*****"
net.build()
ap1.start( [c0] )

print "***** Running CLI*****"
CLI( net )
print "***** Stopping network*****"
net.stop()

if __name__ == '__main__':
    setLogLevel( 'info' )
    topology()

```

### *Heterogeneous.py:*

Η συγκεκριμένη τοπολογία αναφέρεται σε δίκτυο με σταθμούς βάσης, σημεία πρόσβασης, καθώς και τερματικά. Για να εκτελεστεί επιτυχώς απαιτείται μηχανήμα, το οποίο έχει εγκατεστημένο mininet, mininet-wifi, καθώς και τον αντίστοιχο χρησιμοποιούμενο ελεγκτή δικτύου. Η αντίστοιχη υλοποίηση παρατίθεται πιο κάτω. Η αντίστοιχη εντολή για να τρέξει η τοπολογία είναι:

```
Sudo mn - -wifi - -custom ~/mininet-wifi/custom/Heterogeneous.py - - topo my topo - - controller remote
```

```
#!/usr/bin/python
```

```
#making a heterogeneous topology including switches and hosts
```

```
#base stations and access points
```

```
#importing libraries concerning Mininet/ Controllers/ Onos etc
```

```
from mininet.net import Mininet
```

```
from mininet.node import Controller, RemoteController, OVSKernelSwitch
```

```
from mininet.link import TCLink
```

```
from mininet.cli import CLI
```

```
from mininet.log import setLogLevel
```

```
def topology():
```

```
#making a network with a remote controller and a OVS switch
```

```
net = Mininet( controller=remote, link=TCLink, switch=OVSKernelSwitch )
```

```
print "***** Creating nodes*****"
```

```
#creating access point including their exact configuration
```

```
ap1 = net.addBaseStation( 'ap1', ssid= 'ssid-ap1', mode= 'g', channel= '1',  
position='10,30,0', range='20' )
```

```
#creating two base stations declaring their exact configuration
```

```
sta1 = net.addStation( 'sta1', mac='00:00:00:00:00:01', ip='10.0.0.1/8', position='10,20,0' )
```

```
sta2 = net.addStation( 'sta2', mac='00:00:00:00:00:02', ip='10.0.0.2/8', position='50,20,0' )
```

```
#declare a switch for the topology
```

```
print "***** Creating switches & hosts*****"
```



```

s1= net.addSwitch('s1', dpid='0000000000000001')
#create 4 hosts and add Links between them and the switch
h1= net.addHost={ 'mac' : '00:00:00:00:00:01' % i,
                  'ipAddrs' : ['10.0.0.1/24' % i] }
h2= net.addHost={ 'mac' : '00:00:00:00:00:02' % i,
                  'ipAddrs' : ['10.0.0.2/24' % i] }
h3= net.addHost={ 'mac' : '00:00:00:00:00:03' % i,
                  'ipAddrs' : ['10.0.0.3/24' % i] }
h4= net.addHost={ 'mac' : '00:00:00:00:00:04' % i,
                  'ipAddrs' : ['10.0.0.4/24' % i] }

router = net.addHost(name, cls=Router,
quaggaConfFile=quaggaConf,zebraConfFile=zebraConf, intfDict=intfs)

#creating links between stations, access points and controller-switch
print "***** Creating links and associations*****"
net.addLink( ap1, c0 )
net.addLink( ap1, sta1 )
net.addLink( ap2, sta2 )
net.addLink( c0 , s1 )
net.addLink (h1, s1)
net.addLink (h2 , s1)
net.addLink (h3 , s1)
net.addLink (h4 , s1)
#Connect BGP speaker to the root namespace so it can peer with ONOS
root = net.addHost( 'root', inNamespace=False, ip='10.10.10.2/24' )
#create the bgp connection
net.addLink( root, bgp )
net.plotGraph(max_x=100, max_y=100)

print "***** Starting network*****"
print "***** Creating IP RAN network*****"

```

```
net.build()
```

```
c0.start()
```

```
ap1.start( [c0] )
```

## Παράρτημα Β: Δημοσιεύσεις

1. Bouras, C., Kokkinos, V., Kollia, A., & Papazois, A. (2015, August). Techno-economic analysis of ultra-dense and DAS deployments in mobile 5G. In *Wireless Communication Systems (ISWCS), 2015 International Symposium on* (pp. 241-245). IEEE. [92]- Περίληψη: Οι υπέρ-πυκνές αρχιτεκτονικές και οι DAS αποτελούν θεμέλιο λίθο για την επίτευξη των υψηλών ρυθμών μετάδοσης δεδομένων και καθυστερήσεων, που υπόσχεται η μελλοντική γενιά κινητών δικτύων επικοινωνίας, καθώς υπόσχονται να διασφαλίσουν την εξαιρετική κάλυψη σε εσωτερικούς χώρους και προσφέρουν τη δυνατότητα να συναντήσουν τους βασικούς δείκτες σε χαμηλότερο κόστος. Στην εν λόγω μελέτη, εξετάζονται οι τεχνοοικονομικές πλευρές των πιο πάνω τεχνολογιών. Εκτός από την παρουσίαση των αρχιτεκτονικών και των πλεονεκτημάτων, παρουσιάζονται τεχνοοικονομικά μοντέλα των συγκεκριμένων τεχνολογιών. Τελικά, το κόστος των femtocells είναι μικρότερο σε σχέση με αυτό των DAS.
2. Bouras, C., Kollia, A., & Papazois, A. (2017). Dense Deployments and DAS in 5G: A Techno-Economic Comparison. *Wireless Personal Communications*, 94(3), 1777-1797. [93]-Περίληψη: Οι 5G ασύρματες τηλεπικοινωνίες απαιτούν ταχεία κίνηση δεδομένων και υψηλή ταχύτητα δικτύου. Επομένως, είναι σημαντικό να επικεντρωθούμε σε τεχνολογίες, που είναι σε θέση να ανταποκριθούν σε αυτά τα αιτήματα. Από την άλλη πλευρά, ο υπολογισμός του κόστους εγκατάστασης, συντήρησης και λειτουργίας ενός δικτύου, διαδραματίζει σημαντικό ρόλο για την υιοθέτησή του από μια επιχείρηση ή πάροχο. Σε αυτό το άρθρο, παρουσιάζεται ένα μοντέλο κόστους για τα DAS και τα small cells, επειδή αυτές οι δύο τεχνολογίες προσφέρουν σημαντικά οφέλη και πληρούν τις ανάγκες της επόμενης γενιάς δικτύων κινητής τηλεφωνίας. Μια μελέτη εφικτότητας πολλών στοιχείων του δικτύου, όπως το διαθέσιμο εύρος ζώνης, το κόστος λειτουργίας, το περιοδικό, το επιτόκιο, τον σταθμό βάσης, τον εξοπλισμό, την κατανάλωση ενέργειας, το backhauling, το κόστος υλοποίησης κλπ. αποδίδει ποιες παράμετροι κόστους έχουν τη μεγαλύτερη επίδραση στο μοντέλο. Τα πειράματα, που συντελούνται χρησιμοποιώντας παραμέτρους και μεταβλητές για να τις αντιπροσωπεύουν σε μαθηματικές εξισώσεις καταλήγουν σε πρόβλεψη κόστους για τα επόμενα 5 χρόνια. Στη συνέχεια, το συνολικό και τα επί μέρους κόστη υπολογίζονται, δηλαδή το συνολικό κόστος ιδιοκτησίας, το κόστος κεφαλαίου και οι λειτουργικές δαπάνες για πολλές τιμές πυκνότητας ροής σύμφωνα με τα προτεινόμενα μοντέλα τιμολόγησης.

3. Bouras, C., Kollia, A., & Papazois, A. (2016, April). Sensitivity analysis of small cells and DAS techno-economic models in mobile 5G. In *Wireless Communications and Networking Conference (WCNC), 2016 IEEE* (pp. 1-6). IEEE. [94]-Περίληψη: Η επόμενη γενιά κινητών δικτύων απαιτεί υψηλούς ρυθμούς δεδομένων και χαμηλές καθυστερήσεις. Οι δαπάνες εγκατάστασης του δικτύου, της συντήρησης και της λειτουργίας προσδίδουν υψηλά κόστη. Υπολογίζεται το κόστος σε DAS και small cells, περιγράφοντας ενημερωμένα μοντέλα κόστους για καθένα από αυτά. Παρουσιάζεται μια μελέτη εφικτότητας για ορισμένα κόστη, συμπεριλαμβανομένου του εύρους ζώνης, του κόστους λειτουργίας, του επιτοκίου, των σταθμών βάσης, του εξοπλισμού, της κατανάλωσης ενέργειας, της επιστροφής, του κόστους υλοποίησης και της πυκνότητα της παραγωγής. Περιλαμβάνεται μία πρόβλεψη για το κόστος το έτος 2016 και διεξάγονται διάφορα πειράματα, με βάση την ανωτέρω ανάλυση, εξετάζοντας πολλές διαφορετικές τιμές παραμέτρων. Υπολογίζονται το συνολικό κόστος ιδιοκτησίας, το κόστος κεφαλαίου και οι λειτουργικές δαπάνες. Τέλος, προκύπτουν σημαντικά συμπεράσματα συγκρίνοντας τις δύο βασικές τεχνολογίες κόστους, ενώ αξιολογούνται οι παράμετροι κόστους και οι σχετικές μεταβλητές, διαπιστώνοντας ποιοι συμβάλουν τα μέγιστα στη διαμόρφωση των υψηλών τιμών.
4. Bouras, C., Kollia, A., & Papazois, A. (2017). Analyzing Small - cells and Distributed Antenna Systems from Techno - economic Perspective. Retrieved October 2, 2017, from International Journal of Wireless Networks and Broadband Technologies (IJWNBT) [95]-Περίληψη: Οι νέες γενιές κινητών δικτύων επικοινωνίας απαιτούν οικονομικά βιώσιμες λύσεις με σκοπό να ικανοποιήσουν τις απαιτήσεις, που έχουν σημειωθεί από τους επιστήμονες. Στο συγκεκριμένο άρθρο, οι συγγραφείς πραγματοποιούν περίληψη των διαθέσιμων ερευνητικών ενεργειών και παρουσιάζουν μία αρχιτεκτονική για το DAS και μία για τα femtocells και ένα μαθηματικό μοντέλο αναλύοντας τα επί μέρους κόστη, αφού οι τεχνολογίες έχουν αποδειχθεί πολύ ενδιαφέρουσες ως προς τα κινητά δίκτυα. Υπάρχουν λεπτομερή πειράματα σχετικά με το κόστος κεφαλαίου, το λειτουργικό και το συνολικό κόστος εξετάζοντας και τις δύο τεχνολογίες σε σχέση με τις τεχνολογίες καλωδίου, του μεγέθους του κτηρίου, τα έτη επενδύσεων για έναν πάροχο. Τα κύρια αποτελέσματα είναι ότι τα femtocells αποτελούν μία πολύ ελκυστικότερη λύση στα μικρότερα κτήρια, ενώ η εναλλακτική αποτελεί ευνοϊκότερη για μεγάλες υποδομές.
5. [http://ru6.cti.gr/ru6/system/files/bouras\\_site/ergasies/diplwmatikes/Kollia\\_diplomatiki.pdf?language=el](http://ru6.cti.gr/ru6/system/files/bouras_site/ergasies/diplwmatikes/Kollia_diplomatiki.pdf?language=el) [96]

6. Bouras, C., Kollia, A., & Papazois, A. (2017, March). SDN & NFV in 5G: Advancements and challenges. In Innovations in Clouds, Internet and Networks (ICIN), 2017 20th Conference on (pp. 107-111). IEEE. [97]-Περίληψη: Η επόμενη γενιά δικτύων κινητής τηλεφωνίας έχει αυξήσει τις προσδοκίες και έχει προκαλέσει μια εντελώς νέα προσέγγιση στο μέλλον της δικτύωσης. Αυτή η μελέτη συνοψίζει τις λύσεις, που πληρούν όλες τις υφιστάμενες απαιτήσεις και ενσωματώνουν SDN και NFV στην κινητή δικτύωση. Η κύρια συμβολή αυτής της ερευνητικής δραστηριότητας είναι ένα εργαλείο αναφοράς βιβλιογραφίας για επιστήμονες και μηχανικούς, γιατί παρουσιάζει και συγκρίνει τις πιο θεμελιώδεις λύσεις και τις μελλοντικές κατευθύνσεις. Σε αυτή την εργασία, τα κύρια χαρακτηριστικά των SDN και NFV συνοψίζονται ως θεμελιώδεις εναλλακτικές λύσεις, που συμβάλλουν στην επιτυχία των στόχων, που τέθηκαν από το 5G. Τα κύρια αιτήματα και οι προκλήσεις, που αντιμετωπίζουν αυτές οι λύσεις και οι πιο ωφέλιμες εφαρμογές του συνδυασμού SDN με NFV περιγράφονται.
7. Bouras, C., Kollia, A., & Papazois, A. (2017, July). Teaching network security in mobile 5G using ONOS SDN controller. In Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on (pp. 465-470). IEEE. [98]-Περίληψη: Το SDN αποτελεί βασική τεχνολογική λύση, που ανταποκρίνεται στις βασικές προκλήσεις της 5G. Η ασφάλεια ακόμα παραμένει ένα από τα πιο αμφιλεγόμενα θέματα. Η ασφάλεια έχει σκοπό τη δημιουργία αξιόπιστων και δικτύων σε on-line εφαρμογές, που ικανοποιούν τις απαιτήσεις των SLA. Ως εκ τούτου, η διδασκαλία της ασφάλειας στα SDN και NFV είναι θεμελιώδης για τον ακαδημαϊκό κόσμο αυτές τις μέρες. Σε αυτή την εργασία, θα συνοψιστούν τα πιο θεμελιώδη ζητήματα, που σχετίζονται με τις προκλήσεις ασφάλειας στο SDN και με προβλήματα, που εμφανίζονται σε μελλοντικά δίκτυα κινητής τηλεφωνίας SDN. Παρουσιάζονται, επίσης, πειράματα τοπολογιών με χρήση σεναρίων επίθεσης με σκοπό την ανάδειξη μεθόδων διδασκαλίας. Τα πειράματα διεξάγονται χρησιμοποιώντας τον ONOS, κάτι, που δείχνει ότι η διδασκαλία της ασφάλειας με τον ελεγκτή ONOS είναι εύκολη και μπορεί να προσφέρει πολλά οφέλη.
8. Bouras, C., Kollia, A., & Papazois, A. (2017, July). Teaching 5G networks using the ONOS SDN controller. In Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on (pp. 312-317). IEEE. [99]-Περίληψη: Τα SDN και NFV αποτελούν σημαντικές απαντήσεις στις απαιτήσεις της επόμενης γενιάς κινητών δικτύων. Η ασύρματη και η κινητή δικτύωση γίνεται μία απόλυτη αναγκαιότητα καθώς τα NFV και το SDN δημιουργούν μία συνολικά νέα προσέγγιση για αυτούς τους τύπους δικτύων και είναι

υποψήφιες λύσεις για την πέμπτη γενιά. Παρουσιάζουμε διάφορες ιδέες για διδασκαλία του συνδυασμού SDN και NFV σε μελλοντικά κινητά δίκτυα, που χρησιμοποιούν τον ελεγκτή δικτύων ONOS και διάφορες περιπτώσεις χρήσης του. Το αρχιτεκτονικό σχέδιο, που πειραματίζεται εξηγείται λεπτομερώς. Υπάρχουν πολλές προσομοιώσεις δικτύου χρησιμοποιώντας τις περιπτώσεις χρήσης vRouter, IP-RAN και MC-CORD, που δείχνουν πόσο σημαντικός είναι ο ONOS και πώς συμβάλλει στην εξήγηση της 5G και των SDN στη διαδικασία διδασκαλίας. Τελικά, τα πειράματα δείχνουν ότι ο ONOS είναι κατάλληλος για τη διδασκαλία της SDN και NFV στη 5G.

9. Bouras, C., Kollia, A., & Papazois, A. (pending). Exploring SDN & NFV in 5G Using ONOS & POX Controllers. International Journal of Interdisciplinary Telecommunications and Networking (IJITN). [100]-Περίληψη: Νέες λειτουργίες θα προκύψουν από τη δικτύωση cloud και θα αντικαταστήσουν σταδιακά την υπάρχουσα υποδομή των κινητών δικτύων με εικονικά. Δύο τεχνολογίες, συγκεκριμένα οι SDN και NFV, προσφέρουν τα σημαντικά οφέλη τους και ένας συνδυασμός αυτών είναι μια απάντηση στις απαιτήσεις που τέθηκαν, όπως το CORD. Τα ONOS και POX είναι ελεγκτές SDN και προσφέρουν τη δυνατότητα συνδυασμού SDN και NFV για την αντιμετώπιση πολλών προβλημάτων στον τομέα των κινητών δικτύων. Στο παρόν άρθρο, οι τεχνολογίες και οι ελεγκτές συγκρίνονται και αντιπαραβάλλονται. Ενδεικτικές περιπτώσεις τοπολογιών προσομοιώνονται και βοηθούν στην αξιολόγηση και των δύο ελεγκτών. Σύμφωνα με τα πειραματικά ευρήματα, ο ONOS είναι ένας από τους σημαντικότερους ελεγκτές για πρακτικούς, θεωρητικούς, ερευνητικούς και εκπαιδευτικούς σκοπούς, ενώ το POX είναι ένας χρήσιμος και απλούστερος ελεγκτής για άλλες εκπαιδευτικές εφαρμογές.