ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΛΕΤΗ ΤΕΧΝΟΛΟΓΙΩΝ ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΩΝ ΔΙΑΜΟΙΡΑΣΜΟΥ ΣΥΝΔΕΣΕΩΝ WI-FI

Διπλωματική Εργασία

του

Βαμβακά Φιλίππου

Θεσσαλονίκη, Φεβρουάριος 2019

ΜΕΛΕΤΗ ΤΕΧΝΟΛΟΓΙΩΝ ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΩΝ ΔΙΑΜΟΙΡΑΣΜΟΥ ΣΥΝΔΕΣΕΩΝ WI-FI

Βαμβακάς Φίλιππος του Ιωάννη

Πτυχίο Μηχανικού Πληροφορικής και Τηλεπικοινωνιών, Λάρισα, 2011
ΜΔΕ στη Διοίκηση των Επιχειρήσεων, Καστοριά, 2014

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής:
Παπαδημητρίου Παναγιώτης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 04/03/2019

Παπαδημητρίου Παναγιώτης	Μαμάτας Ελευθέριος	Πετρίδου Σοφία
.....	.....	.....

Βαμβακάς Φίλιππος

.....

Περίληψη

Ο διαμοιρασμός συνδέσεων Wi-Fi έχει προσελκύσει σημαντική προσοχή, δεδομένου του αυξανόμενου ενδιαφέροντος για ευρύτερη και φθηνότερη πρόσβαση στο Διαδίκτυο. Ο διαμοιρασμός πρόσβασης στο Διαδίκτυο αποφέρει σημαντικά οφέλη για το ευρύτερο κοινό που μπορεί να έχει πρόσβαση στο Διαδίκτυο δωρεάν μέσω διαμοιραζόμενων σημείων πρόσβασης (hotspots), αξιοποιώντας την πυκνότητα των σημείων πρόσβασης Wi-Fi σε κατοικημένες περιοχές.

Παρόλα αυτά, ο διαμοιρασμός συνδέσεων Wi-Fi εγείρει σημαντικές ανησυχίες τόσο για τους διαμοιραστές όσο και για τους επισκέπτες, το οποίο μπορεί να εξαλείψει τα κίνητρα των κατόχων σημείων πρόσβασης να μοιραστούν την σύνδεσή τους ή αντίθετα, να αποτρέψουν τους χρήστες από το να δημιουργήσουν συνδέσεις στα διαμοιραζόμενα σημεία πρόσβασης.

Από αυτή την άποψη, μελετάμε διάφορες αρχιτεκτονικές και τεχνολογίες που χρησιμοποιούνται στον διαμοιρασμό πρόσβασης στο Διαδίκτυο. Αναλύουμε ιδιαιτέρως πτυχές διαμοιρασμού Wi-Fi, όπως την αυθεντικοποίηση, την λογοδοσία, το εύρος ζώνης και την απομόνωση κίνησης, προκειμένου να παρέχονται κίνητρα τόσο στους διαμοιραστές όσο και στους χρήστες. Ως τομείς εφαρμογής του διαμοιρασμού πρόσβασης στο Διαδίκτυο, εστιάζουμε στο Wi-Fi και στα ασύρματα δίκτυα πλέγματος, με το FON και Freifunk να είναι μερικά αξιοσημείωτα παραδείγματα, αντίστοιχα.

Λέξεις κλειδιά: Διαμοιρασμός συνδέσεων, ασύρματα δίκτυα, ασύρματα δίκτυα πλέγματος, κοινωνικά δίκτυα, δίκτυα οριζόμενα μέσω λογισμικού

Abstract

Wi-Fi sharing has attracted significant attention, given the increasing interest in wider and cheaper Internet access. Internet access sharing yields significant benefits for the wider public who can access Internet for free through shared hotspots, exploiting the density of Wi-Fi access points in residential areas.

Nevertheless, Wi-Fi sharing raises significant concerns both for sharers and guests, which may essentially eliminate any incentives for hotspot owners to share their connection or, conversely, put off users from establishing connections to shared hotspots.

In this respect, we study various architectures and technologies employed for Internet access sharing. We particularly analyze Wi-Fi sharing aspects, such as authentication, accountability, bandwidth and traffic isolation in order to provide incentives both for sharers and guests. As application domains of Internet access sharing, we focus on Wi-Fi and wireless mesh networks, with FON and Freifunk being some notable examples, respectively.

Keywords: Internet access sharing, Wi-Fi networks, wireless mesh networks, community networks, software-defined networks

Πρόλογος – Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω τον καθηγητή κύριο Παπαδημητρίου Παναγιώτη για το θέμα που μου ανάθεσε και για την πολύτιμη βοήθεια που μου έδωσε προκειμένου να διεκπεραιώσω την διπλωματική μου εργασία. Επίσης, θα ήθελα να ευχαριστήσω τους γονείς μου και την οικογένειά μου που στάθηκαν δίπλα μου, πίστεψαν σε μένα και με βοήθησαν με τον τρόπο τους για να φέρω εις πέρας την εργασία μου. Τέλος, θα ήθελα να ευχαριστήσω ακόμα όλους εκείνους τους φίλους και γνωστούς που στάθηκαν στο πλάι μου, τους ταλαιπώρησα λίγο με την συμπεριφορά μου, αλλά εν' τέλει κατάφεραν με τον τρόπο τους να μου δώσουν δύναμη και ενέργεια για να προσπαθήσω περισσότερο μέχρι που τελικά κατάφερα να πετύχω τους στόχους μου.

Πίνακας περιεχομένων

Κατάλογος Εικόνων

Συμβολισμοί

AAA	Authentication Authorization Accounting	Αυθεντικοποίηση Εξουσιοδότηση Λογοκρισία
ACL	Access Control List	Λίστα Ελέγχου Πρόσβασης
ANQP	Access Network Query Protocol	Πρωτόκολλο Ερώτησης στο Δίκτυο Πρόσβασης
AODV	Ad hoc On demand Distance Vector	Ανά άλμα Κατά παραγγελίας Απόστασης Διανύσματος
AP	Access Point	Σημείο Πρόσβασης
API	Application Programming Interface	Διεπαφή Προγραμματισμού Εφαρμογής
API	Authentication Programming Interface	Διεπαφή Αυθεντικοποίησης Προγραμματισμού
ARP	Address Resolution Protocol	Πρωτόκολλο Διευθυνσιοδότησης Διευθύνσεων
B.A.T.M.A.N.	Better Approach To Mobile Adhoc Networking	Καλύτερη Προσέγγιση στην Κινητή Δικτύωση ανά Άλμα
BF	Bloom Filter	Φίλτρο Άνθησης
BSA	Basic Service Area	Βασική Περιοχή Υπηρεσιών
BSS	Basic Service Set	Βασικό Σετ Υπηρεσιών
CS	Card Sharing	Διαμοιρασμός Κάρτας
DHCP	Dynamic Host Configuration Protocol	Πρωτόκολλο Δυναμικής Διαμόρφωσης Παρόχου
DNS	Domain Name Server	Τομέας Ονόματος Διακομιστή
DoS	Denial of Service	Άρνηση Εξυπηρέτησης
DRA	Distributer Recognition and Accountability	Κατανεμημένη Αναγνώριση και Λογοκρισία
DS	Distributed System	Σύστημα Διανομής
EAP	Extensible Authentication Protocol	Πρωτόκολλο Επεκτάσιμης Αυθεντικοποίησης
ESS	Extended Service Set	Επεκτάσιμο Σετ Υπηρεσιών
FON	Fonero Network	Δίκτυο Fonero
HWMP	Hybrid Wireless Mesh Protocol	Υβριδικό Ασύρματο Δίκτυο Πλέγματος
IBSS	Independent Basic Service Set	Ανεξάρτητο Βασικό Σετ Υπηρεσιών
ISP	Internet Service Provider	Υπηρεσία Παροχής Δικτύου
LAN	Local Area Network	Δίκτυο Τοπικής Περιοχής
LLDP	Link Layer Discover Protocol	Πρωτόκολλο Ανίχνευσης Στρώματος Συνδέσμου
MAC	Media Access Control	Έλεγχος Πρόσβασης Πολυμέσων
MPRs	Multipoint Relays	Πολλαπλά Σημεία
NAT	Network Address Translation	Μεταφραστής Διευθύνσεων Δικτύου
NETCONF	Network Configuration Protocol	Πρωτόκολλο Διαμόρφωσης Δικτύου
OGM	Originator Messages	Πρωτότυπα Μηνύματα
OLSR	Optimized Link State Routing	Δρομολόγηση Βελτιστοποιημένης Κατάστασης Σύνδεσης
OP	Operator	Διαχειριστής
OSN	Online Social Network	Κοινωνικά σε Απευθείας σύνδεση Δίκτυα
PAWS	Public Access Wi-Fi Service	Υπηρεσία Δημόσιας Πρόσβασης Wi-Fi

PCP	Priority Code Point	Σημείο Κώδικα Προτεραιότητας
PERR	Path Error	Διαδρομή Σφάλματος
PREP	Path Reply	Απάντηση Διαδρομής
PREQ	Path Request	Αίτηση Διαδρομής
QoS	Quality of Service	Ποιότητα Υπηρεσίας
RANN	Root Announcement	Αναγγελία Ρίζας
REX	Reputation based Extension	βασισμένο σε Επέκταση Φήμης
RPC	Remote Procedure Call	Κλήση Απομακρυσμένης Διαδικασίας
SDN	Software Defined Network	Τεχνολογία Δικτύωσης Λογισμικού
SHF	Super High Frequency	Υπερβολικά Υψηλή Συχνότητα
SSID	Service Set Identifier	Αναγνωριστικό Συνόλου Υπηρεσίας
TTL	Time To Leave	Χρόνος για να Φύγει
TX	Trust based Extension	βασισμένο σε Εμπιστοσύνη Επέκτασης
UHF	Ultra High Frequency	Εξαιρετικά Υψηλή Συχνότητα
VLAN	Virtual Local Area Network	Εικονικό Τοπικό Δίκτυο Περιοχής
VOP	Virtual Operator	Εικονικός Διαχειριστής
VPN	Virtual Private Network	Εικονικά Ιδιωτικά Δίκτυα
VpuN	Virtual public Network	Εικονικό δημόσιο Δίκτυο
VRF	Virtual Routing and Forwarding	Εικονική Δρομολόγηση και Προώθηση
WEP	Wireless Equivalent Privacy	Ασύρματη Ισοδύναμη Ιδιωτικοποίηση
Wi-Fi	Wireless Fidelity	Ασύρματη Πιστότητα
WLAN	Wireless Local Area Network	Ασύρματη Τοπικής Περιοχής Δικτύου
WMN	Wireless Mesh Network	Ασύρματο Δίκτυο Πλέγματος
WPA	Wireless Protected Access	Ασύρματη Προστατευόμενη Πρόσβαση
XML	Extensible Markup Language	Γλώσσα Επεκτάσιμης Σήμανσης
YANG	Yet Another Next Generation	Ακόμη Μία Νέα Γενιά

1 Εισαγωγή

Ζούμε σε μία κοινωνία συνεχόμενα τεχνολογικά αναπτυσσόμενη, με την ανάγκη για σύνδεση στο Διαδίκτυο ολοένα και περισσότερο χρήσιμη και απαραίτητη στη ζωή μας. Ο κόσμος γύρω μας το χρησιμοποιεί ολοένα και περισσότερο σε διάφορους τομείς της ζωής του, όπως δουλειά, επικοινωνία με φίλους και οικογένεια, ενασχόληση, παιχνίδια και πολλές άλλες δραστηριότητες, για καθένα διαφορετική και συνάμα χρήσιμη.

Οι συσκευές παράλληλα που χρησιμοποιεί ο κάθε χρήστης, διαφέρουν και εξελίσσονται με τέτοιο ρυθμό, που καθιστούν αναγκαία την ύπαρξη πολλών συσκευών στα σπίτια, στην εργασία και έξω στο δρόμο, του καθενός ξεχωριστά, ανάλογα με τα θέλω και τη μόδα της εποχής. Πλέον κάθε άνθρωπος έχει τουλάχιστον μία κινητή συσκευή (αν όχι δύο), ο υπολογιστής δεν λείπει από το σπίτι ή τον χώρο εργασίας και είναι ένα απαραίτητο εργαλείο για πολλές χρήσεις, όπως επίσης και διάφορες συσκευές όπως tablet, τηλεόραση, αυτοκίνητο και άλλες που διαθέτει και χρησιμοποιεί ο καθένας διαφορετικά.

Όλες αυτές οι συσκευές παρέχουν διάφορες λειτουργίες και έχουν εφαρμογές, η καθεμία ξεχωριστά, στον τρόπο με τον οποίο παρέχουν διάφορες υπηρεσίες στους χρήστες τους, ανάλογα με τις ανάγκες τους. Αυτό όμως που τις καθιστά περισσότερο χρήσιμες και απαιτητικές είναι η διασύνδεσή τους στο Διαδίκτυο, με τέτοιο τρόπο, που όχι μόνο παρέχουν τις υπηρεσίες που χρειάζεται ο χρήστης, αλλά και μπορούν να συνδεθούν πολλές φορές και να επικοινωνήσουν η μία με την άλλη με τέτοιο τρόπο, ώστε να ανταλλάξουν μεταξύ τους πληροφορίες και δεδομένα, γρήγορα, εύκολα και αποτελεσματικά.

Αν και ο ασφαλέστερος και αποδοτικότερα εφικτός τρόπος σύνδεσης των διαφόρων συσκευών μεταξύ τους είναι μέσω καλωδίου, δηλαδή ενσύρματα, παρόλα αυτά, υπάρχει και ένας άλλος με περισσότερα οφέλη τρόπος, αυτός της ασύρματης σύνδεσης. Συσκευές μπορούν να επικοινωνήσουν μεταξύ τους και να συνδεθούν στο Διαδίκτυο μέσω δεδομένων ή με έναν ακόμα καλύτερο και με περισσότερες δυνατότητες χρησιμοποιημένο τρόπο, της **ασύρματης πιστότητας** (**Wireless Fidelity**

–Wi-Fi). Περισσότερα πράγματα, όπως επίσης και σαν επίκεντρο της συζήτησής μας, θα αναφερθούμε περισσότερο στην επόμενη ενότητα.

Για να γίνει κάτι τέτοιο εφικτό και να επικοινωνήσουν οι διάφοροι χρήστες μεταξύ τους πρέπει να συνδεθούν σε κάποιο δίκτυο. Το δίκτυο, ανάλογα με διάφορους κανόνες και πρωτόκολλα που χρησιμοποιεί, είναι υπεύθυνο για το σωστό διαμοιρασμό των πληροφοριών, και λαμβάνοντας υπόψη διάφορους παράγοντες όπως το εύρος ζώνης, την απόσταση, την αυθεντικοποίηση των χρηστών, τις συσκευές που χρησιμοποιούνται, και το τι μπορεί η κάθε μία να παρέχει, έτσι ώστε η πληροφορία να είναι αξιόπιστη και να φθάσει στον προορισμό της, θέτει τις βάσεις για την επίτευξη ενός μεγαλύτερου στόχου, δηλαδή την μετάδοση της πληροφορίας από τη μία μεριά της γης στην άλλη, με ασφάλεια, συνοχή και ταχύτητα.

Στις μέρες μας, οι άνθρωποι χρειάζεται να έχουν πρόσβαση στο Διαδίκτυο καθημερινά και ψάχνουν οποιοδήποτε τρόπο προκειμένου κάτι τέτοιο να συμβεί, ακόμα και σε πιο απομακρυσμένες περιοχές, σε περιοχές που δεν έχει σήμα και ακόμα περισσότερο, όταν έχουν σήμα, αυτό να παραμένει σταθερό και να μην χάνεται. Ο διαμοιρασμός των αρχείων σε τέτοιες περιπτώσεις είναι αναγκαίος και η ύπαρξη του Wi-Fi είναι απαραίτητη για να επιτευχθεί κάτι τέτοιο. Ωστόσο, οι άνθρωποι δεν έχουν πάντα την οικονομική ευχέρεια για να ανταποκριθούν στις αλλαγές του Διαδικτύου. Γι' αυτό υπάρχουν και ελεύθερες δυνατότητες σύνδεσης σε μακρινές αποστάσεις μέσω του Wi-Fi και των δυνατοτήτων που προσφέρει στους ολοένα και αυξανόμενους χρήστες του.

Παρόλα αυτά, δυσκολίες και προβλήματα μπορεί να προκύψουν στην σύνδεση ή στην μετάδοση της πληροφορίας από την μία συσκευή στην άλλη. Φόβος και ανησυχίες μπορεί να προκύψουν όχι μόνο σε αυτόν που διαμοιράζεται ένα μέρος της σύνδεσής του, αλλά και στον επισκέπτη που θα χρησιμοποιήσει την σύνδεση του παρόχου, προκειμένου να εξυπηρετηθεί και να του παρέχονται οι δυνατότητες της σύνδεσής του στο Διαδίκτυο. Θα μελετήσουμε παρακάτω τις μεθόδους επίλυσης των διαφόρων ζητημάτων που παρουσιάζονται στον διαμοιρασμό των αρχείων, τον τρόπο κρυπτογράφησης και απόκρυψης της πληροφορίας από δυνητικά επικίνδυνους και κακόβουλους χρήστες, τον τρόπο λειτουργίας των διαφόρων πρωτοκόλλων που χρησιμοποιούνται και τη σημασία τους.

1.1 Αρχιτεκτονική ασύρματων δικτύων

Αρχικά, τα ασύρματα δίκτυα μπορούν πλέον να επιτρέπουν σε ηλεκτρονικές συσκευές (από υπολογιστές μέχρι οποιαδήποτε περιφερειακή) να επικοινωνούν μεταξύ τους και να ανταλλάσσουν δεδομένα χωρίς χρήση καλωδίων. Σε όλα τα νέα πρότυπα ασύρματων δικτύων που έχουν αναπτυχθεί, πλέον, δεν είναι απαραίτητη η οπτική επαφή. Σε κάθε ασύρματο δίκτυο υπάρχουν δύο μέρη:

- **η ασύρματη κάρτα δικτύου** ή wireless LAN adapter, η οποία μπορεί να επικοινωνεί με άλλες συσκευές που έχουν ασύρματη κάρτα δικτύου, ή με τον πομποδέκτη-κόμβο και το σημείο πρόσβασης που λειτουργεί και ως γέφυρα με το ενσύρματο δίκτυο.
- **μια μικρή κεραία** [52].

Ο πομποδέκτης έχει τις διαστάσεις ενός βιβλίου και, εκτός από την κεραία, έχει και τα κατάλληλα βύσματα για σύνδεση με σταθερό δίκτυο. Ακόμα και τα πιο πολλά ασύρματα δίκτυα χρησιμοποιούν για λόγους ασφάλειας, μεθόδους εξουσιοδότησης των συνδεόμενων και κρυπτογράφησης των δεδομένων [17]. Αρκετά πρότυπα χρησιμοποιούν την τεχνική εναλλαγής συχνότητας (frequency hopping) σύμφωνα με την οποία ο κάθε πομποδέκτης αλλάζει συχνότητα μετά την αποστολή/λήψη ενός πακέτου δεδομένων, αποφεύγοντας έτσι τα παράσιτα.

Ως προς την τοπολογία, οι δύο βασικότερες κατηγορίες για ασύρματα δίκτυα είναι οι ακόλουθες :

- τα ανεξάρτητα δίκτυα (independent networks)
- τα δίκτυα υποδομής (infrastructure networks)

1.1.1 Ανεξάρτητα δίκτυα

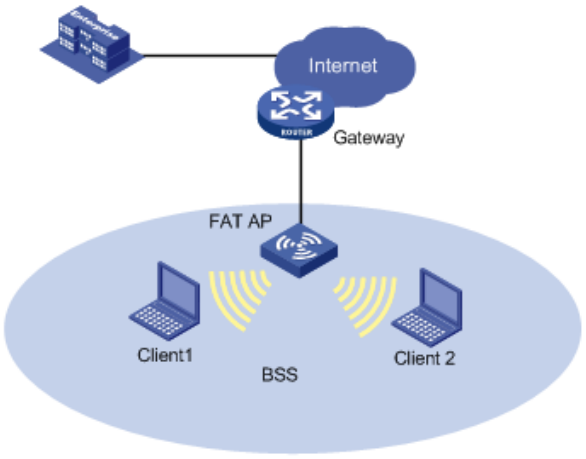
Η πρώτη κατηγορία, το **βασικό σετ υπηρεσιών (Basic Service Set –BSS)** αποτελείται από δύο ή περισσότερους ασύρματους κόμβους ή αλλιώς σταθμούς. Κάθε σταθμός μπορεί να επικοινωνεί απευθείας με όλους τους υπόλοιπους, εφόσον όμως βρίσκεται μέσα στη περιοχή ραδιοκάλυψής του. Το βασικό σετ υπηρεσιών σε αυτή την περίπτωση ονομάζεται και **ανεξάρτητο βασικό σετ υπηρεσιών (Independent**

Basic Service Set -IBSS) και είναι συνήθως προσωρινό, δηλαδή δημιουργείται για κάποιο σκοπό και στη συνέχεια διαλύεται. Πρόκειται για τον απλούστερο τύπο ασύρματου δικτύου.

1.1.2 Δίκτυα υποδομής

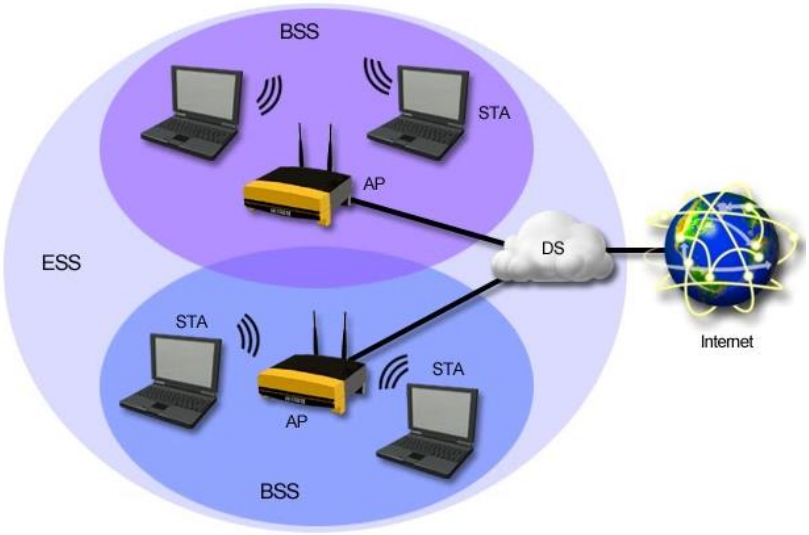
Το βασικό σετ υπηρεσιών περιλαμβάνει ένα κάθε φορά **σημείο πρόσβασης (Access Point –AP)**. Το σημείο πρόσβασης είναι υπεύθυνο για τη σύνδεση του βασικού σετ υπηρεσιών με κάποιο ενσύρματο δίκτυο, αναλαμβάνει την ανταλλαγή των πλαισίων μεταξύ των σταθμών και τον συνολικό έλεγχο της λειτουργίας του βασικού σετ υπηρεσιών. Όταν ένα σημείο θέλει να στείλει ένα πλαίσιο σε ένα άλλο σημείο, δεν του το στέλνει απευθείας, αλλά το πλαίσιο αποστέλλεται πρώτα στο σημείο πρόσβασης και αυτό με τη σειρά του, το στέλνει στον τελικό προορισμό.

Η **βασική περιοχή υπηρεσιών (Basic Service Area –BSA**) είναι η περιοχή ραδιοκάλυψης του σημείου πρόσβασης. Δηλαδή οι σταθμοί πρέπει να βρίσκονται στην περιοχή ραδιοκάλυψης του σημείου πρόσβασης για να επικοινωνούν μεταξύ τους, χωρίς να παίζει ρόλο η μεταξύ τους απόσταση όπως στην περίπτωση του ανεξάρτητου βασικού σετ υπηρεσιών. Για να συμμετέχει ένας σταθμός στο βασικό σετ υπηρεσιών θα πρέπει να ακολουθήσει τη διαδικασία σύνδεσης (association) με το σημείο πρόσβασης. Η διαδικασία αυτή ξεκινάει με πρωτοβουλία του σταθμού και είναι απόφαση του σημείου πρόσβασης αν ο σταθμός θα γίνει δεκτός στο βασικό σετ υπηρεσιών [50].



Εικόνα 1-1: BSS

Ένας αριθμός από βασικά σετ υπηρεσιών μπορούν να συνδεθούν και να αποτελέσουν ένα **επεκτάσιμο σετ υπηρεσιών (Extended Service Set -ESS)**. Στο επεκτάσιμο σημείο πρόσβασης τα σημεία πρόσβασης των βασικών σετ υπηρεσιών συνδέονται μέσω ενός ενσύρματου δικτύου κορμού, που ονομάζεται **σύστημα διανομής (Distribution System –DS)**. Με αυτόν τον τρόπο είναι εφικτή η επικοινωνία μεταξύ σταθμών που ανήκουν σε διαφορετικά βασικά σετ υπηρεσιών, αλλά στο ίδιο επεκτάσιμο σετ υπηρεσιών [51]. Σε αυτή την περίπτωση πρέπει τα σημεία πρόσβασης να επικοινωνούν στο στρώμα ζεύξης δεδομένων μέσω του δικτύου κορμού, επιτελώντας τη λειτουργία της γέφυρας για τους σταθμούς διαφορετικών βασικών σετ υπηρεσιών. Το επεκτάσιμο σετ υπηρεσιών τελειώνει, όταν παρεμβληθεί μεταξύ των σημείων πρόσβασης, οντότητα δικτύου που να λειτουργεί σε υψηλότερο στρώμα, όπως είναι ο δρομολογητής (router).



Εικόνα 1-2: ESS

1.2 Wi-Fi

Η **ασύρματη πιστότητα** (**Wireless Fidelity –Wi-Fi**) είναι τεχνολογία για ασύρματη τοπική δικτύωση συσκευών με βάση τα πρότυπα IEEE 802.11. Το Wi-Fi είναι το εμπορικό σήμα της συμμαχίας Wi-Fi, το οποίο περιορίζει τη χρήση του όρου

πιστοποιημένη ασύρματη πιστότητα σε προϊόντα που ολοκληρώνουν με δοκιμές πιστοποίησης διαλειτουργικότητας.

Οι συσκευές που μπορούν να χρησιμοποιούν τεχνολογίες Wi-Fi περιλαμβάνουν επιτραπέζιους και φορητούς υπολογιστές, κονσόλες βιντεοπαιχνιδιών, κινητά και tablet, έξυπνες τηλεοράσεις, ψηφιακοί ήχοι, αυτοκίνητα και σύγχρονοι εκτυπωτές [53]. Οι συμβατές συσκευές Wi-Fi μπορούν να συνδεθούν στο Διαδίκτυο μέσω ασύρματης τοπικής περιοχής δικτύου (Wireless Local Area Network –WLAN) και ενός ασύρματου σημείου πρόσβασης (Access Point –AP). Ένα τέτοιο σημείο πρόσβασης (ή hotspot) έχει μια περιοχή περίπου 20 μέτρων σε εσωτερικούς χώρους και μεγαλύτερη εμβέλεια σε εξωτερικούς χώρους. Η κάλυψη καυτού σημείου (hotspot) μπορεί να είναι τόσο μικρή όσο ένα μονό δωμάτιο με τοίχους που μπλοκάρουν τα ραδιοκύματα, ή τα τετραγωνικά χιλιόμετρα που επιτυγχάνονται με τη χρήση πολλαπλών επικαλυπτόμενων σημείων πρόσβασης.

Εικόνα 1-3: Wi-Fi

Διαφορετικές εκδόσεις του Wi-Fi υπάρχουν, με διαφορετικές σειρές, ζώνες ραδιοφώνου και ταχύτητες. Το Wi-Fi χρησιμοποιεί συνηθέστερα τις ραδιοζώνες των 2.4 gigahertz εξαιρετικά υψηλής συχνότητας (Ultra High Frequency –UHF) και 5.8 gigahertz υπερβολικά υψηλής συχνότητας (Super High Frequency –SHF). Αυτές οι ζώνες υποδιαιρούνται σε πολλαπλά κανάλια. Κάθε κανάλι μπορεί να μοιραστεί με χρόνο από πολλά δίκτυα [54]. Αυτά τα μήκη κύματος λειτουργούν καλύτερα για την οπτική επαφή. Πολλά συνηθισμένα υλικά απορροφούν ή τα αντανακλούν, τα οποία περιορίζουν περαιτέρω την εμβέλεια, αλλά μπορούν να συμβάλλουν στην ελαχιστοποίηση των παρεμβολών μεταξύ διαφορετικών δικτύων σε συνωστισμένα

περιβάλλοντα. Σε κοντινή απόσταση, ορισμένες εκδόσεις του Wi-Fi, που εκτελούνται με κατάλληλο υλικό, μπορούν να επιτύχουν ταχύτητες άνω του 1 Gbit/s.

1.2.1 Πλεονεκτήματα Wi-Fi

Η εξάπλωση των ασύρματων δικτύων και συγκεκριμένα του Wi-Fi οφείλεται κυρίως στα εξής πλεονεκτήματα:

- **Κινητικότητα χρήστη**. Οι χρήστες μπορούν να μετακινούνται εντός της εμβέλειας του ασύρματου δικτύου, δηλαδή σε χώρο που θα έχουν επαρκές σήμα, διατηρώντας την συνδεσιμότητα τους με αυτό. Αυτό έχει σαν αποτέλεσμα την μεγαλύτερη παραγωγικότητα - αποτελεσματικότητα στο εργασιακό περιβάλλον και όχι μόνο.
- **Ευκολία, ευελιξία και απλότητα εγκατάστασης.** Δε χρειάζεται να εγκαταστήσουμε καλωδιώσεις μέσα από τοίχους και ταβάνια. Μπορεί να γίνει η δικτύωση σε μέρη όπου η καλωδίωση θα ήταν αδύνατη, ή μη επιθυμητή, όπως η δικτύωση γραφείων τα οποία βρίσκονται σε απόσταση μεταξύ τους. Η εγκατάσταση στις περισσότερες περιπτώσεις μπορεί να γίνει εύκολα αν ακολουθηθούν κάποιοι βασικοί κανόνες εγκατάστασης.
- **Κλιμάκωση, δυνατότητα επέκτασης.** Τα ασύρματα δίκτυα μπορούν να διαρθρωθούν σε ένα πλήθος από τοπολογίες, ώστε να ταιριάξουν στις απαιτήσεις των εφαρμογών. Οι τοπολογίες αλλάζουν εύκολα και επεκτείνονται από απλά δίκτυα με μικρό αριθμό χρηστών, ως μεγάλες δομές δικτύων με εκατοντάδες χρήστες και δυνατότητα περιαγωγής (roaming).
- **Κόστος.** Παρόλο που το αρχικό κόστος εγκατάστασης είναι υψηλότερο σε σχέση με λύσεις ενσύρματης δικτύωσης, το κόστος για όλη τη διάρκεια ζωής της επένδυσης μπορεί να είναι μικρότερο, ιδιαίτερα σε δυναμικό περιβάλλον που απαιτεί συχνές αλλαγές, αναδιαρθρώσεις και μετακινήσεις. Επιπλέον το κόστος υλοποίησης - εγκατάστασης και συντήρησης - διαχείρισης του δικτύου είναι πολύ μικρό. Το σημαντικότερο κομμάτι του κόστους είναι η αγορά του εξοπλισμού.

- **Ταχύτητες μετάδοσης**. Όσο αναπτύσσεται η τεχνολογία γίνεται δυνατή η μετάδοση μεγαλύτερων ρυθμών δεδομένων. Ήδη ο μέγιστος ρυθμός μετάδοσης δεδομένων, από τα 2Mbps που μπορούσαν να επιτευχθούν αρχικά, έφτασε σήμερα σε ταχύτητες πάνω από 200Mbps ενώ ήδη έχουν εξαγγελθεί ακόμα μεγαλύτερες ταχύτητες.
- **Αξιοπιστία – ανεξαρτησία**. Ένα ασύρματο δίκτυο κατάλληλα διαμορφωμένο μπορεί να έχει μεγάλη αξιοπιστία. Έτσι μπορεί να σχεδιαστεί έτσι ώστε να μπορεί να εργάζεται όταν συμβαίνουν διακοπές ρεύματος και να περιλαμβάνει πολλές εναλλακτικές διαδρομές.
- **Εμβέλεια.** Η εμβέλεια ενός ασύρματου δικτύου σε περιβάλλον γραφείου μπορεί να είναι μερικές δεκάδες μέτρα. Τα ραδιοκύματα σε εσωτερικό χώρο έχουν να διαπεράσουν τοίχους και οροφές οπότε υφίστανται σημαντική απόσβεση. Σε ανοικτό χώρο όπου υπάρχει οπτική επαφή ανάμεσα στις ασύρματες συσκευές, οι αποστάσεις που μπορεί να καλυφθούν είναι μεγαλύτερες.
- **Συμβατότητα με το υπάρχον δίκτυο.** Τα περισσότερα ασύρματα δίκτυα έχουν προτυποποιημένο τρόπο σύνδεσης με τα υπάρχοντα ενσύρματα δίκτυα. Έτσι, η προσθήκη ασύρματης δικτύωσης σε υπάρχουσες δομές δικτύων μπορεί να γίνει με τον ευκολότερο τρόπο. Πολλές φορές δεν αποτελούν επέκταση ενός ενσύρματου δικτύου.

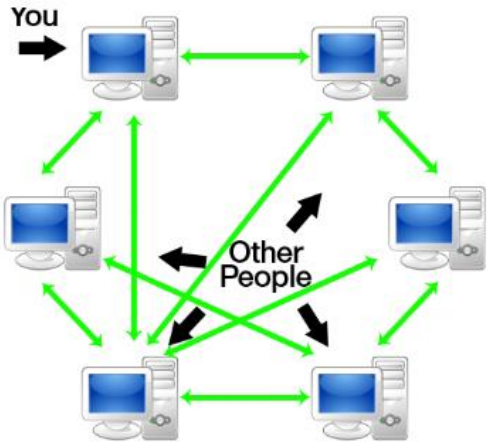
με πιο σημαντικά την **κινητικότητα** (mobility) και το **χαμηλό κόστος** [54].

1.2.2 Σχεδιασμός ασύρματης σύνδεσης

Τα **ασύρματα τοπικά δίκτυα περιοχής (Wireless Local Area Network – WLAN)** μπορούν να επιτευχθούν, με έναν αριθμό τρόπων, ανάλογα με την επιθυμητή πολυπλοκότητα. Τα WLANs είναι συνήθως τριών ειδών:

1. **Ομότιμος με ομότιμο (Peer –to –Peer):**

Ένα τέτοιο δίκτυο είναι ένα WLAN στην βασική του μορφή. Δύο υπολογιστές εξοπλισμένοι με ασύρματες κάρτες προσαρμογής είναι όλα αυτά που χρειάζονται για να δημιουργήσεις ένα peer-to-peer δίκτυο, δίνοντας τη δυνατότητα στους υπολογιστές να διαμοιράζουν πληροφορίες με τους υπόλοιπους [48]. Αν και αυτού του τύπου δίκτυο δεν χρειάζεται διαχείριση ή διαμόρφωση από πριν, δεν επιτρέπει σε κάθε υπολογιστή να έχει πρόσβαση σε έναν κεντρικό διαχειριστή (server), παρεμποδίζοντας έτσι την επικοινωνία πελάτη/διαχειριστή (client/server).



Εικόνα 1-4: Ομότιμοι χρήστες

Σχεδιάζοντας ένα δίκτυο peer-to-peer περιλαμβάνει τρία κύρια χαρακτηριστικά:

1) Οι σταθμοί πρέπει να είναι κατανεμημένοι ώστε όλοι να είναι μέσα στα επιτρεπτά όρια απόστασης.
2) Όλοι οι σταθμοί πρέπει να στέλνουν και να λαμβάνουν στην ίδια συχνότητα μετάδοσης. (Οι περισσότερες ασύρματες κάρτες δικτύων έχουν μία εργοστασιακά ορισμένη συχνότητα)
3) Το πρόβλημα του κρυφού κόμβου πρέπει να αποφευχθεί, έτσι ώστε κάθε σταθμός να επικοινωνεί με όλους τους υπόλοιπους.

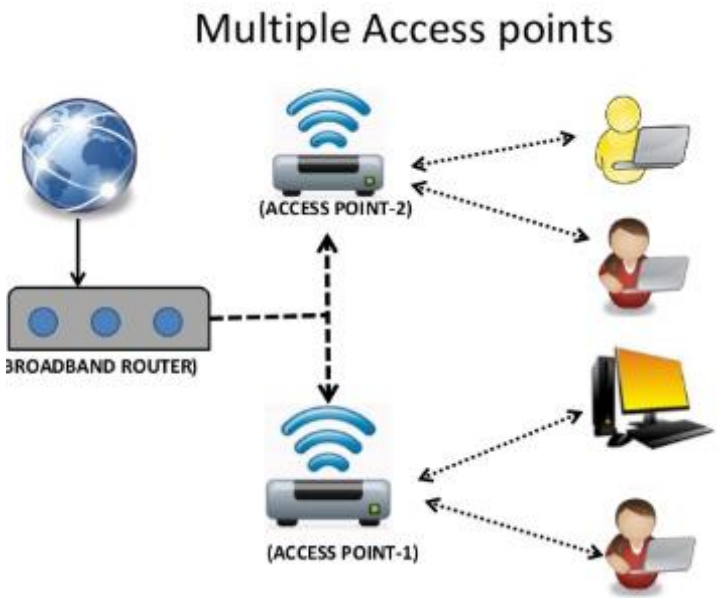
2. **Πελάτη και σημείου πρόσβασης (Client & Access Point):**

Σε ένα τέτοιο δίκτυο οι χρήστες, όχι μόνο επωφελούνται από δυνατότητες εκτεταμένης εμβέλειας, αλλά επωφελούνται και από πληροφορίες του διαχειριστή, καθώς το AP είναι συνδεδεμένο με το ενσύρματο δίκτυο ραχοκοκαλιάς. Οι αριθμοί των χρηστών που μπορούν να υποστηριχτούν από αυτού του τύπου το δίκτυο ποικίλει ανά τεχνολογία και από τη φύση και των αριθμών των εμπλεγμένων μεταδόσεων. Γενικά, μπορούν να υποστηρίξουν 15 με 20 χρήστες.

Εικόνα 1-5: Πελάτης και AP

3. **Πολλαπλά σημεία πρόσβασης (Multiple Access Points):**

Αν και οι περιοχές κάλυψης σε μέγεθος από προϊόν σε προϊόν και σε διαφορετικό περιβάλλον αλλάζουν, τα συστήματα WLAN είναι εκ’ φύσεως κλιμακωτά. Αν και τα AP έχουν περιορισμένη κάλυψη, μεγάλες εγκαταστάσεις όπως αποθήκες και πανεπιστημιουπόλεις συχνά βρίσκουν απαραίτητο να εγκαταστήσουν πολλά σημεία πρόσβασης, δημιουργώντας μεγάλες περιοχές πρόσβασης. APs, όπως κυψελωτές σελίδες σε κυψελικά τηλεφωνικά εφαρμογές, υποστηρίζουν περιαγωγή και από AP σε AP μεταβίβαση. Μεγάλες εγκαταστάσεις που απαιτούν πολλαπλά σημεία πρόσβασης τα τοποθετούν με σχεδόν τον ίδιο τρόπο όπως στα κυψελωτά μέρη, δημιουργώντας επικαλυπτόμενα κελιά για συνεχόμενη σύνδεση στο Διαδίκτυο. Όσο η χρήση του δικτύου αυξάνεται, επιπλέον σημεία πρόσβασης μπορούν εύκολα να τοποθετηθούν.



Εικόνα 1-6: Πολλαπλά APs

1.3 Εμπόδια και προβληματισμοί παρόχου και επισκέπτη σύνδεσης

Όπως αναφερθήκαμε ήδη, το να συνδεθεί κάποιος στο ίντερνετ δεν απαιτεί και πολλά πράγματα, αρκεί η συσκευή ενός χρήστη να διαθέτει έναν ελεγκτή διεπαφής δικτύου με τον οποίο να συνδέεται σε ένα δίκτυο Wi-Fi και εφόσον υπάρχει ένα AP ή όχι, να μπορεί να επικοινωνήσει κάποιος χρήστης με κάποιον άλλο ή με μία βάση δεδομένων. Υπάρχουν δύο πλευρές χρηστών. Αυτοί οι οποίοι επιθυμούν να διαμοιράσουν την σύνδεσή τους στο δίκτυο, έτσι ώστε να μπορούν να συνδεθούν άλλοι χρήστες, οι λεγόμενοι **πάροχοι ή διαμοιραστές (hosts or sharers)** και εκείνοι οι οποίοι χρησιμοποιούν την σύνδεση των παρόχων, προκειμένου να εισέλθουν στο ίντερνετ, οι λεγόμενοι **επισκέπτες ή πελάτες (clients or guests)**.

Και οι δύο έχουν διαφορετικούς στόχους και προσπαθούν καθένας για τους λόγους του να επωφεληθούν από αυτόν τον διαμοιρασμό. Ωστόσο, υπάρχουν πολλά προβλήματα και ανησυχίες που μπορεί να προκύψουν τόσο από τη μία μεριά, δηλαδή του διαμοιραζόμενου, του παρόχου, αλλά και του επισκέπτη. Και στις δύο περιπτώσεις θα πρέπει καθένας να λάβει υπόψη του, από τη δική του σκοπιά, τις δυσκολίες και τα προβλήματα που μπορούν να προκύψουν, και έχοντας ανησυχίες και ανασφάλειες για την επιτυχία της σύνδεσής του, να υπολογίσει διάφορους παράγοντες που μπορεί να προκύψουν στην προσπάθεια σύνδεσής τους ή ακόμα και στον διαμοιρασμό των

πληροφοριών. Έχοντας αυτές τις ανησυχίες μπορούν εν τέλει να μην προβούν σε κάποια ενέργεια, να αποθαρρυνθούν και να αποφασίσουν να μην γίνει καμία ενέργεια και ο διαμοιρασμός να μην υπάρξει καθόλου. Παρακάτω ελέγχουμε τις ανησυχίες του καθενός ξεχωριστά [6].

1.3.1 Ανησυχίες παρόχου

Ο πάροχος είναι υπεύθυνος και υπόλογος για τον αριθμό και την προστασία των πληροφοριών που επιθυμεί να διαμοιράσει, δεδομένου μιας **υπηρεσίας παροχής διαδικτύου (Internet Service Provider).** Ένας αριθμός AP δεν έχει μείνει ασφαλισμένος, είτε επειδή οι πάροχοι ιδεολογικά θέλουν να υποστηρίξουν την δωρεάν ασύρματη πρόσβαση, είτε επειδή δεν έχουν την τεχνογνωσία για να αλλάξουν τις προεπιλεγμένες εργοστασιακές ρυθμίσεις των AP τους. Οι πάροχοι AP που είναι ενήμεροι για τους πιθανούς κινδύνους και τις νομικές συνέπειες του διαμοιρασμού της σύνδεσής τους από κακόβουλους επισκέπτες, σχεδόν πάντα ασφαλίζουν τους AP τους.

Μία φυσική ανησυχία των παρόχων είναι η πιθανή απώλεια του εύρους ζώνης. Ένας ασυνείδητος επισκέπτης δεν πρέπει να είναι σε θέση να χρησιμοποιεί όλο το εύρος ζώνης σε βαθμό που ο πάροχος δεν είναι σε θέση να έχει επαρκής πρόσβαση στο Διαδίκτυο. Μπορεί να υπάρχει η ανάγκη για να ελέγχει το εύρος ζώνης του επισκέπτη ακόμα και όταν ο πάροχος δεν χρησιμοποιεί το Διαδίκτυο, προκειμένου να διατηρηθεί η συνολική κίνηση μέσα στα αποδεκτά όρια του προμηθευτή υπηρεσίας διαδικτύου (Internet Service Provider –ISP) παρόχου.

Ακόμα μία ανησυχία είναι, ότι αν και πολλοί πάροχοι Wi-Fi δεν είναι ενήμεροι για αυτή τη πιθανότητα, ένας κακόβουλος επισκέπτης μπορεί να επιτεθεί και να μολύνει άλλους υπολογιστές στο δίκτυο του παρόχου ή ακόμα στον ασύρματό του δρομολογητή. Ένα πιο δύσκολο πρόβλημα είναι ότι ένας επισκέπτης μπορεί να κατεβάσει παράνομο περιεχόμενο, όπως αρχεία πολυμέσων που προστατεύονται από πνευματικά δικαιώματα ή πορνογραφία [6]. Οι περισσότεροι ISPs όροι υπηρεσιών ρητά απαγορεύουν τους πελάτες τους που εκτελούν ή συνεργάζονται με τέτοιες παράνομες πράξεις, και οι συνέπειες θα ήταν στον πάροχο που θα παραβίαζε αυτούς τους όρους, εξαιτίας των ενεργειών των επισκεπτών.

1.3.2 Ανησυχίες επισκέπτη

Όπως και στην περίπτωση του παρόχου, έτσι και βασικό ζήτημα και μέλημα του επισκέπτη στο δίκτυο, είναι να διαφυλάξει τα προσωπικά του δεδομένα και η σύνδεσή του να είναι όσο πιο ασφαλής γίνεται, έτσι ώστε να μην έχει κυρώσεις και να μην παραβιάζει τους νόμους και κανόνες που επιτρέπουν στον πάροχο να διαμοιράζει το περιεχόμενο που επιθυμεί.

Τα σύγχρονα λειτουργικά συστήματα προσπαθούν να κάνουν σύνδεση σε ένα νέο ασύρματο δίκτυο, ανώδυνα και εύκολα. Αυτό οδήγησε σε απρόσεκτη και ακόμα πιο ξέγνοιαστη συμπεριφορά, που πολλοί χρήστες δεν διστάζουν να συνδεθούν σε οποιαδήποτε ξένο ασύρματο δίκτυο που είναι ελεύθερα διαθέσιμο. Ωστόσο, κλέβοντας κρυφά εύρο ζώνης είναι αμφισβητήσιμο από ηθική και νομική άποψη.

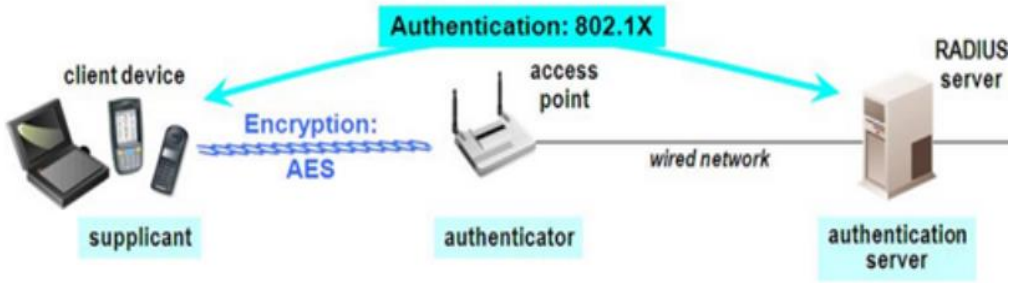
Επίσης, οι συνετοί επισκέπτες θα πρέπει να συνειδητοποιούν την ευαισθησία σε επιθέσεις και μολύνσεις από έναν κακόβουλο πάροχο, με τον ίδιο παρόμοιο τρόπο που ένας κακόβουλος επισκέπτης μπορεί να επιτεθεί σε έναν πάροχο. Ακόμη χειρότερα, εάν χρησιμοποιείται το **πρωτόκολλο δυναμικής διαμόρφωσης παρόχου (Dynamic Host Configuration Protocol –DHCP)**, το δίκτυο του κεντρικού υπολογιστή μπορεί να αναθέσει στον επισκέπτη μια ψεύτικη διεύθυνση IP **τομέα ονόματος διακομιστή (Domain Name Server –DNS)**, διαμορφώνοντας τη βάση για μια εξελιγμένη επίθεση ηλεκτρονικού ψαρέματος (pharming attack). Με την ανακατεύθυνση των αιτημάτων DNS για προσωπικά ονόματα ιστοτόπων (ηλεκτρονικό ταχυδρομείο, τραπεζικές ιστοσελίδες κλπ.) σε ψεύτικους διακομιστές που αναπαράγουν προσεκτικά την εμφάνιση και την αίσθηση του ιστοτόπου που ζητήθηκε, ο επισκέπτης μπορεί να αποκαλύψει κωδικούς πρόσβασης και άλλες ευαίσθητες πληροφορίες.

Στόχος και σκοπός κάθε επισκέπτη και διαμοιραστή είναι να διαφυλάξουν το ιδιωτικό τους απόρρητο (ιδιωτικότητα –privacy) ή της εμπιστευτικότητας (confidentiality). Τα 3 στάνταρ που καθορίζουν την ασφαλή επικοινωνία μεταξύ διαμοιραστή και επισκέπτη είναι η **αυθεντικοποίηση, εξουσιοδότητη και ευθύνη (Authentication Authorization Accounting –AAA)** [6]. Παρακάτω θα αναφερθούμε στην αυθεντικοποίηση και τον ρόλο που παίζει στον ασφαλή διαμοιρασμό των συνδέσεων.

1.4 Αυθεντικοποίηση και ασφάλεια

Ο έλεγχος ταυτότητας είναι η διαδικασία προσδιορισμού του αν κάποιος ή κάτι είναι στην πραγματικότητα ποιος ή τι δηλώνει ότι είναι. Η τεχνολογία ελέγχου ταυτότητας παρέχει έλεγχο πρόσβασης για τα συστήματα, ελέγχοντας αν τα διαπιστευτήρια ενός χρήστη αντιστοιχούν στα διαπιστευτήρια σε μια βάση δεδομένων εξουσιοδοτημένων χρηστών ή σε ένα διακομιστή ελέγχου ταυτότητας δεδομένων.

Ο έλεγχος ταυτότητας χρήστη πραγματοποιείται στις περισσότερες αλληλεπιδράσεις ανθρώπου-χρήστη εκτός των λογαριασμών επισκεπτών, των λογαριασμών που έχουν συνδεθεί αυτόματα και των συστημάτων ηλεκτρονικών υπολογιστώ[27]. Γενικά, ο χρήστης πρέπει να επιλέξει ένα όνομα χρήστη ή αναγνωριστικό χρήστη και να παράσχει έναν έγκυρο κωδικό πρόσβασης για να αρχίσει να χρησιμοποιεί ένα σύστημα. Ο έλεγχος ταυτότητας χρηστών επιτρέπει την αλληλεπίδραση ανθρώπου με το μηχάνημα σε λειτουργικά συστήματα και εφαρμογές, καθώς και σε ενσύρματα και ασύρματα δίκτυα, ώστε να επιτρέπεται η πρόσβαση σε δικτυωμένα συστήματα, εφαρμογές και πόρους.



Εικόνα 1-7: Αυθεντικοποίηση

Κατά τη διάρκεια του ελέγχου ταυτότητας, τα διαπιστευτήρια που παρέχει ο χρήστης συγκρίνονται με αυτά που βρίσκονται σε αρχείο σε μια βάση δεδομένων με πληροφορίες εξουσιοδοτημένων χρηστών είτε στο τοπικό λειτουργικό σύστημα είτε μέσω ενός διακομιστή ελέγχου ταυτότητας. Εάν τα διαπιστευτήρια ταιριάζουν και η αυθεντικοποιημένη οντότητα είναι εξουσιοδοτημένη να χρησιμοποιεί τον πόρο, η διαδικασία ολοκληρώνεται και ο χρήστης έχει πρόσβαση. Τα δικαιώματα και οι φάκελοι που επιστρέφονται καθορίζουν τόσο το περιβάλλον που βλέπει ο χρήστης όσο

και τον τρόπο με τον οποίο μπορεί να αλληλεπιδράσει μαζί του, συμπεριλαμβανομένων των ωρών πρόσβασης και άλλων δικαιωμάτων όπως το μέγεθος του χώρου αποθήκευσης πόρων [30].

Όποιος βρίσκεται εντός εμβέλειας με NID μπορεί να επιχειρήσει πρόσβαση σε δίκτυο. Γι' αυτόν τον λόγο, το Wi-Fi είναι πιο ευάλωτο σε επίθεση (αποκαλούμενη υποκλοπή) από τα ενσύρματα δίκτυα. Το Wi-Fi προστατευόμενης πρόσβασης (Wi-Fi Protected Access –WPA) είναι μια οικογένεια τεχνολογιών που δημιουργήθηκε για την προστασία πληροφοριών που μετακινούνται μέσω δικτύων Wi-Fi και περιλαμβάνει λύσεις για προσωπικά και επιχειρηματικά δίκτυα. Τα χαρακτηριστικά ασφαλείας του WPA περιείχαν ισχυρότερες προστασίες και νέες πρακτικές ασφάλειας καθώς το τοπίο ασφαλείας έχει αλλάξει με την πάροδο του χρόνου και θα μελετηθεί περισσότερο στο επόμενο κεφάλαιο.

Η πρόσβαση στο Διαδίκτυο μέσω κοινόχρηστων ευρυζωνικών συνδέσεων μπορεί να εγείρει ζητήματα ασφάλειας και ευθύνης, τόσο για τον διαμοιραστή της σύνδεσης όσο και για τον επισκέπτη. Ο διαμοιραστής θα ανησυχήσει για το κατά πόσο ένας επισκέπτης είναι νόμιμος, δεδομένου ότι ο διαμοιραστής μπορεί να θεωρηθεί υπεύθυνος για οποιεσδήποτε κακόβουλες ενέργειες των επισκεπτών όπως **επιθέσεις άρνησης εξυπηρέτησης (Denial-of-Service attacks –DoS)** και λήψης παράνομου περιεχομένου. Αντίθετα, οι επισκέπτες μπορούν να γίνουν θύματα κακόβουλων διαμοιραστών που διαφημίζουν ψεύτικα **αναγνωριστικά συνόλου υπηρεσιών (Service Set Identifiers –SSID)**, στην προσπάθειά τους να υποκλέψουν ή να "κρυφακούσουν" την κίνηση των επισκεπτών και να ανακτήσουν ιδιωτικές πληροφορίες που μεταδίδονται μέσω ενός διαμοιραζόμενου Wi-Fi.

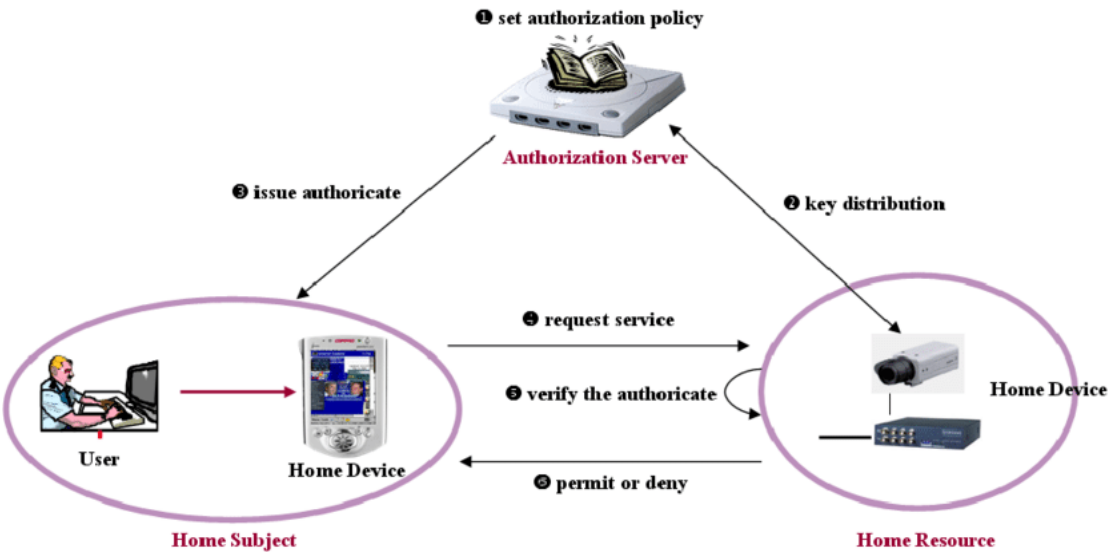
Τα κοινωνικά δίκτυα αυξάνουν την ανάγκη για την ανακάλυψη και αυθεντικοποίηση δικτύου βασιζόμενο σε κοινωνικές σχέσεις. Επί του παρόντος, στα SSID βασιζόμενα δίκτυα ανακάλυψης και υπάρχων μεθόδων αυθεντικοποίησης, δεν πληρούνται αυτές οι απαιτήσεις. Πιο συγκεκριμένα, τα αναγνωριστικά συνόλου υπηρεσιών που είναι βασισμένα σε ανακαλύψεις Wi-Fi έχουν αποδειχθεί ότι είναι ανασφαλή, όπως και το μήκος των 32 byte του SSID είναι ανεπαρκές για την ενθυλάκωση της κοινωνικής πληροφορίας, δεδομένου του μεγάλου αριθμού φίλων που σχετίζονται με τα περισσότερα κοινωνικά προφίλ. Επιπλέον, οι υπάρχουσες

μέθοδοι επαλήθευσης εντοπίζουν τα διαμοιραζόμενα μυστικά, τα οποία δεν είναι εφικτά να διανεμηθούν μεταξύ μεγάλου αριθμού κοινωνικών δικτυακών συμμετεχόντων.

Αυτά τα θέματα μπορούν να αποτρέψουν τους χρήστες από το να διαμοιράζουν την σύνδεσή τους στο Διαδίκτυο και τους δυνητικούς επισκέπτες από την εγκαθίδρυση συνδέσεων σε ένα κοινόχρηστο Wi-Fi από άγνωστους ιδιοκτήτες. Ουσιαστικά, οι περισσότεροι ιδιοκτήτες Wi-Fi κλειδώνουν τα σημεία πρόσβασής τους (hotspots) δημιουργώντας κοινά μυστικά, αποτρέποντας την δυνατότητα να τα διαμοιραστούν με άλλους.

1.5 Εξουσιοδότηση

Η **εξουσιοδότηση (authorization)** περιλαμβάνει τη διαδικασία μέσω της οποίας ένας διαχειριστής παρέχει δικαιώματα σε χρήστες που έχουν πιστοποιηθεί, καθώς και τη διαδικασία ελέγχου των δικαιωμάτων λογαριασμού χρήστη για να επαληθεύσει ότι ο χρήστης έχει λάβει πρόσβαση σε αυτούς τους πόρους. Τα δικαιώματα και οι προτιμήσεις που παρέχονται για τον εξουσιοδοτημένο λογαριασμό εξαρτώνται από τα δικαιώματα του χρήστη, τα οποία αποθηκεύονται είτε τοπικά είτε στο διακομιστή ελέγχου ταυτότητας. Οι ρυθμίσεις που ορίζονται για όλες αυτές τις μεταβλητές περιβάλλοντος καθορίζονται από τον διαχειριστή.



Εικόνα 1-8: Εξουσιοδότηση

Τα συστήματα και οι διαδικασίες μπορεί επίσης να χρειαστεί να επιτρέψουν τις αυτοματοποιημένες ενέργειές τους μέσα σε ένα δίκτυο. Οι υπηρεσίες ηλεκτρονικής δημιουργίας αντιγράφων ασφαλείας, τα συστήματα επιδιόρθωσης και ενημέρωσης και τα συστήματα απομακρυσμένης παρακολούθησης, όπως αυτά που χρησιμοποιούνται στην τεχνολογία της τηλεϊατρικής και των τεχνολογιών έξυπνου δικτύου, όλα πρέπει να πιστοποιούνται με ασφάλεια, προτού εξακριβώσουν ότι πρόκειται για το εξουσιοδοτημένο σύστημα που εμπλέκεται σε οποιαδήποτε αλληλεπίδραση και όχι για χάκερ [57].

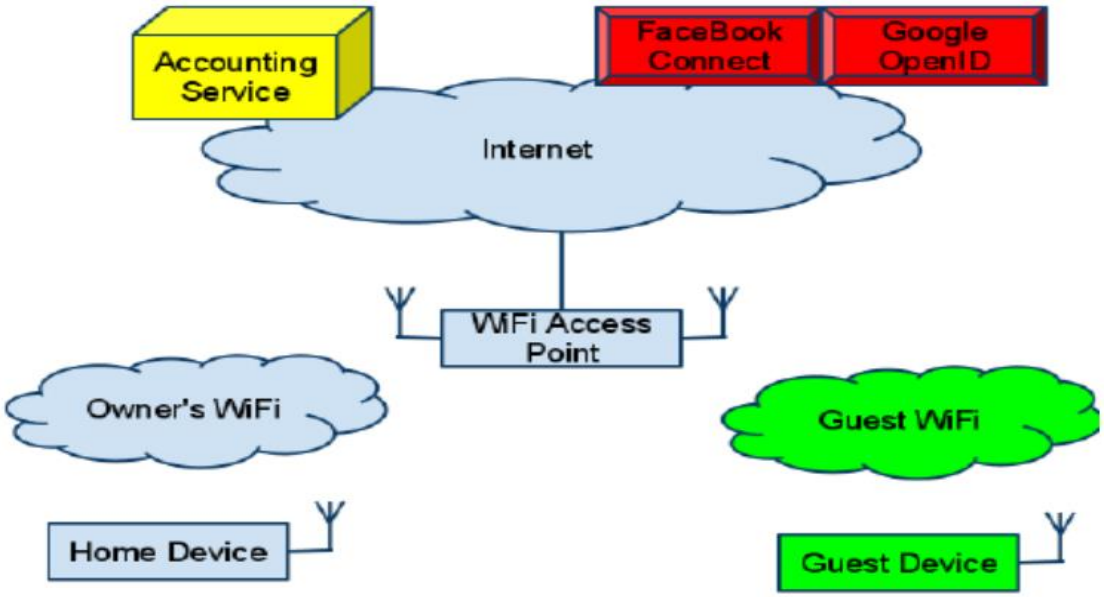
Ένας ISP εξουσιοδοτεί σε κάποιον διαμοιραστή να παρέχει πληροφορίες και δεδομένα σε άλλους χρήστες, με την προϋπόθεση να μην παραβιάζονται θέματα ασφάλειας και η επικοινωνία με τους διαφόρους χρήστες να είναι μέσα σε πλαίσια νομικά και να μην θίγονται θέματα προσωπικών δεδομένων. Από την μεριά τους οι πάροχοι των πληροφοριών εξουσιοδοτούν στους επισκέπτες την σύνδεσή τους σε δίκτυο, με νόμιμο και ασφαλή τρόπο, έτσι ώστε να μην παραβιάζουν ούτε οι ίδιοι, ούτε οι επισκέπτες προσωπικά ζητήματα που μπορούν να επιφέρουν κυρώσεις και στους δύο.

1.6 Λογοδοσία

Η **λογοδοσία (accounting)** αποτελεί ουσιαστικό μέρος ενός σχεδίου ασφάλειας των πληροφοριών. Η φράση σημαίνει ότι κάθε άτομο που συνεργάζεται με ένα πληροφοριακό σύστημα θα πρέπει να έχει συγκεκριμένες ευθύνες για τη διασφάλιση της πληροφόρησης. Τα καθήκοντα για τα οποία ένα άτομο είναι υπεύθυνο αποτελούν μέρος του συνολικού σχεδίου ασφάλειας πληροφοριών και μπορούν εύκολα να μετρηθούν από ένα πρόσωπο που έχει διευθυντική ευθύνη για τη διασφάλιση της πληροφόρησης.

Η λογοδοσία στο Διαδίκτυο αντιστοιχεί σε όλες τις μεθόδους που αναγνωρίζουν, διαχωρίζουν και τιμωρούν την «κακή συμπεριφορά». Το εγγενές στο αρχικό σχέδιο του διαδικτύου είναι ανοιχτή πεποίθηση, στην οποία βασίζονται πάντα οι φιλοξενούμενοι και οι χρήστες, μέσω της συνδεδεμένης απαίτησης λογοδοσίας. Μια

τέτοια απεικόνιση της ανοιχτής πεποίθησης επιτρέπει στους κακόβουλους χρήστες να χρησιμοποιούν εκθέσεις στο σύνολο των συνδέσεων και των συσκευών για να ξεκινήσουν μια ποικιλία επιθέσεων που παράγονται από υπολογιστή, ενώ επωφελούνται από την ανακούφιση που δεν ακολουθούνται [31].



Εικόνα 1-9: Λογοδοσία

Το Διαδίκτυο δεν παρέχει δεδομένα σχετικά με την τύχη των πληροφοριών που μεταδίδονται. Κατά συνέπεια, όταν τα πακέτα χάνονται ή αναβάλλονται, δεν υπάρχει σαφής μέθοδος για τα υπερβολικά μέρη να περιορίσουν την αποτυχία και να την επιδιορθώσουν, εάν είναι περιορισμένη, για αποζημίωση αν μια συμφωνία σε επίπεδο υπηρεσίας έχει αποθαρρυνθεί ή ακόμα να μελετηθεί από αυτήν (π.χ., να αναθεωρήσει μια συμφωνία μεταξύ ομότιμων μέσω μιας με χαμηλή απόδοση ομάδας). Εξαιρετικά εργαλεία παρόμοια με την ιχνυλάτηση θα είναι ικανά να βοηθήσουν στον περιορισμό της βλάβης του δικτύου. Από την άλλη, απεικονίζουν τους τερματισμούς που προέρχονται από το πεπρωμένο της έρευνας και όχι από την πραγματική ανταλλαγή, γεγονός που τις καθιστά ευπαθείς στην εκμετάλλευση από δίκτυα μεταφοράς. Επιπλέον, τέτοια εργαλεία συχνά αποκαλύπτουν τις εσωτερικές ρυθμίσεις και στρατηγικές εύρεσης κατεύθυνσης των παρόχων υπηρεσιών διαδικτύου, και αυτό δίνει στον δεύτερο ένα κίνητρο για να αφήσει απροστάτευτα τα δίκτυά τους σε επιθέσεις.

Ένας αλγόριθμος που έχει αναπτυχθεί για το σκοπό αυτό είναι ο **αλγόριθμος κατανεμημένης αναγνώρισης και λογοδοσίας (Distributed Recognition and Accountability –DRA)** και ο κύριος στόχος του είναι να έχει μια ισχυρή ευθύνη για όλες τις μεμονωμένες κινήσεις στο δίκτυο και να βρει τους χρήστες που προσπαθούν να συνδεθούν με διαφορετικά αναγνωριστικά χρήστη και να κρύβει την ταυτότητά τους [32].

Ένας άλλος στόχος είναι η ομαδοποίηση όλων των δραστηριοτήτων που εκτελούνται από ένα μόνο χρήστη βάσει του αναγνωριστικού δικτύου. Ο DRA έχει κάποιες βασικές συνθήκες. Για παράδειγμα, δεν θεωρεί απώλεια πακέτων δεδομένων, συγχρονισμό με το δίκτυο κ.ο.κ. Κάθε περιουσιακό στοιχείο θα πρέπει να ανήκει σε ένα άτομο του οργανισμού, το οποίο είναι υπεύθυνο σε κάθε μία από αυτές. Τα καθήκοντα και οι ευθύνες όλων των εργαζομένων, καθώς σχετίζονται με τη διασφάλιση των πληροφοριών, πρέπει να διευκρινιστούν λεπτομερώς. Διαφορετικά, η προσπάθεια δημιουργίας και διατήρησης της ασφάλειας των πληροφοριών είναι τυχαία και σχεδόν απουσιάζει.

1.7 Απομόνωση

Ένας άλλος παράγοντας που πρέπει να ληφθεί υπόψη είναι εκτός από την ασφάλεια, το θέμα **απομόνωσης (isolation)**. Με αυτόν τον τρόπο πρέπει να παρέχεται η δυνατότητα σε κάθε χρήστη να παραμένει ανώνυμος, αλλά παράλληλα να διατηρεί τα δικαιώματα που έχει στο δίκτυο που του γίνεται ο διαμοιρασμός. Θα πρέπει δηλαδή, με κάποιον τρόπο να μπορεί να επικοινωνεί με τη βάση δεδομένων του παρόχου και να χρησιμοποιεί το Διαδίκτυο με τον ίδιο τρόπο όπως και κάθε άλλος επισκέπτης.

Όσοι περισσότεροι χρήστες εισέρχονται σε ένα δίκτυο, τόσο μεγαλώνουν και οι προσδοκίες συντήρησής του. Εκτός από τα θέματα ασφάλειας και πιστοποίησης που δημιουργούνται τόσο για τον πάροχο, όσο και για τον επισκέπτη, όπως είδαμε και παραπάνω εγείρονται θέματα ποιότητας και ταχύτητας του δικτύου [23]. Τα πακέτα πρέπει να μεταδίδονται με σταθερό ρυθμό και ο επισκέπτης να διατηρεί την σύνδεσή του στο ίντερνετ. Παρόλα αυτά, θέματα όπως το εύρος ζώνης που χρησιμοποιεί και διαθέτει ο πάροχος, ο τρόπος με τον οποίο μπορεί να τον διαμοιραστεί με τους

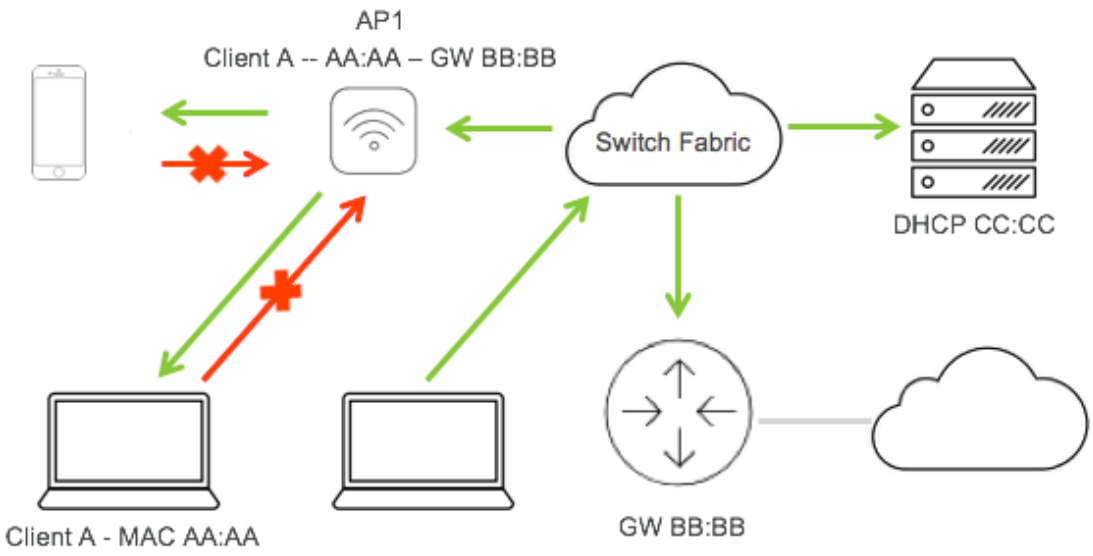
διάφορους επισκέπτες του δικτύου, αλλά και το γεγονός ότι όσο περισσότεροι συνδέονται σε αυτό, μπορεί να υπάρξει σύγχυση, και να προκύψουν θέματα υλοποίησης και συντονισμού, προκαλούν ανησυχίες και για τους δύο [28].

Προκειμένου να επιτευχθεί καλύτερη απομόνωση του δικτύου και των χρηστών θα ασχοληθούμε με δύο ειδών απομονώσεις: α) **την ασύρματη απομόνωση των επισκεπτών** και β) **την απομόνωση των σημείων πρόσβασης**. Σε επόμενο κεφάλαιο θα αναφερθούμε και θα μελετήσουμε περαιτέρω, και τεχνικά, για την απομόνωση κίνησης και θα δούμε την χρήση και λειτουργία των **εικονικών ιδιωτικών δικτύων (Virtual Private Networks –VPN)**.

1.7.1 Ασύρματη απομόνωση επισκεπτών

Η **απομόνωση ασύρματου επισκέπτη (Wireless Client Isolation)** είναι ένα χαρακτηριστικό ασφάλειας που εμποδίζει τους ασύρματους πελάτες να επικοινωνούν μεταξύ τους. Αυτή η λειτουργία είναι χρήσιμη για SSID επισκεπτών προσθέτοντας ένα επίπεδο ασφάλειας για τον περιορισμό των επιθέσεων και των απειλών μεταξύ συσκευών που είναι συνδεδεμένες στα ασύρματα δίκτυα [29].

Στην απομόνωση αυτή χρησιμοποιείται η απομόνωση τρόπου γέφυρας πελάτη (Bridge Mode Client Isolation), η οποία είναι διαθέσιμη για SSID που έχουν ρυθμιστεί για λειτουργία γέφυρας, που είναι ωστόσο απενεργοποιημένη από προεπιλογή. Όταν ένα SSID έχει διαμορφωθεί για τη λειτουργία γεφυρών, οι πελάτες γεφυρώνονται μέσω του σημείου πρόσβασης ενδεχομένως σε ένα συγκεκριμένο **εικονικό τοπικό δίκτυο περιοχής (Virtual Local Area Network –VLAN).** Μετά τη σύνδεση με το AP, οι πελάτες θα έχουν τη δυνατότητα να κάνουν αίτηση DHCP στα VLAN που τους έχουν εκχωρηθεί. Μετά την ολοκλήρωση του DHCP, η διεύθυνση **ελέγχου πρόσβασης πολυμέσων (Media Access Control –MAC)** της προεπιλεγμένης πύλης παρακολουθείται για τον συγκεκριμένο πελάτη. Στη συνέχεια επιτρέπεται η διεύθυνση MAC της προεπιλεγμένης πύλης σε ένα τείχος προστασίας (firewall) επιπέδου 2 που περιορίζει την υπόλοιπη κίνηση προς και από τον ασύρματο πελάτη.



Εικόνα 1-10: Ασύρματη απομόνωση επισκέπτη

Με την ενεργοποίηση του προγράμματος ασύρματης απομόνωσης του πελάτη, οι πελάτες θα μπορούν να επικοινωνούν μόνο με την προεπιλεγμένη πύλη και δεν θα μπορούν να επικοινωνούν με άλλες συσκευές στον ίδιο VLAN (ή τομέα μετάδοσης). Προκειμένου ο ασύρματος πελάτης να επικοινωνήσει με άλλη συσκευή, πρέπει να χρησιμοποιηθεί μία έναντι ρεύματος (upstream) πύλη, για να ενεργοποιηθεί αυτή η επικοινωνία (π.χ. Inter VLAN routing και **λίστες ελέγχου πρόσβασης (Access Control Lists –ACLs)**,). Οποιαδήποτε κίνηση που δεσμεύει μια διεύθυνση στο ίδιο VLAN ως συσκευή στην απομόνωση του πελάτη θα απορριφθεί. Η κυκλοφοριακή σύνδεση για άλλα VLANs θα προωθηθεί και θα δρομολογηθεί κανονικά. Στο επόμενο κεφάλαιο θα ασχοληθούμε περισσότερα με τα VLAN και θα δούμε πως κάτι τέτοιο μπορεί να γίνει εφικτό.

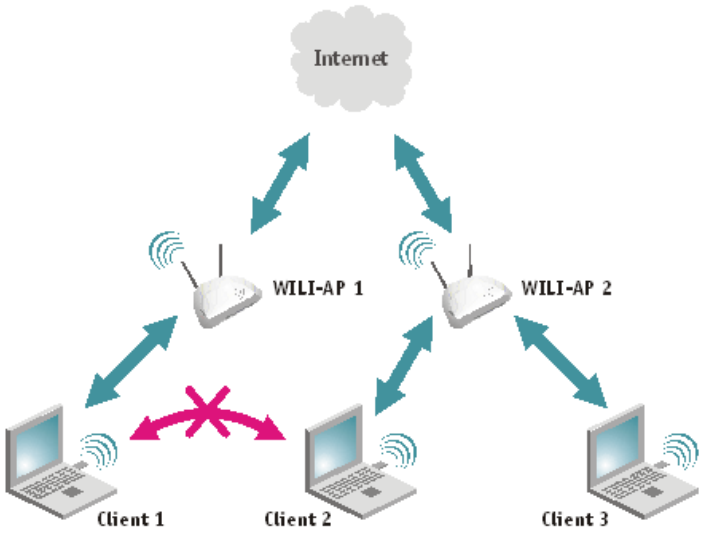
1.7.2 Ασύρματη απομόνωση σημείου πρόσβασης

Ένας άλλος και πιο βασικός τρόπος απομόνωσης του δικτύου είναι μέσω της **απομόνωσης σημείου πρόσβασης (Access Point Isolation).** Αν και δεν διαφέρει και με την ασύρματη απομόνωση επισκέπτη, θα δούμε τι επιπλέον προσφέρει και πως μπορεί το παραπάνω να γίνει επιτευκτό.

Εικόνα 1-11: Επικοινωνία συσκευών με σημείο πρόσβασης

Πρόκειται για έναν άλλο τρόπο για να παρέχει ο πάροχος πρόσβαση στο Διαδίκτυο στους επισκέπτες, ενώ ταυτόχρονα να αποκλείει την εσωτερική υποδομή του δικτύου του. Οι επισκέπτες είναι σε θέση να συνδεθούν στο ίντερνετ -αλλά ο δικτυακός εξοπλισμός του παρόχου παραμένει εκτός ορίων [29]. Οι διακομιστές αρχείων, τα τελικά σημεία, οι συσκευές - τα πάντα στο LAN - δεν είναι προσβάσιμα μέσω ενός δρομολογητή ή ενός σημείου πρόσβασης, με ενεργοποιημένες τις ρυθμίσεις απομόνωσης AP. Τα οφέλη είναι παρόμοια με ένα δίκτυο επισκεπτών από αυτή την άποψη.

Επιπλέον, εμποδίζει τις συσκευές σε ασύρματο δίκτυο να επικοινωνούν απευθείας μεταξύ τους. Εξ ορισμού, η απομόνωση AP δημιουργεί ένα εικονικό δίκτυο μοναδικό για κάθε συσκευή στο WLAN. Γιατί θα ήθελε κάποιος να διασφαλίσει ότι τα τελικά σημεία δεν μπορούν να επικοινωνήσουν στο WLAN του παρόχου; Γιατί, εμποδίζει τους χάκερς να χρησιμοποιούν δημόσιο Wi-Fi για να κλέψουν δεδομένα από άλλους χρήστες του δικτύου [28]. Επίσης, σταματά κάποιον να “ρίχνει” το ασύρματο δίκτυο κατακλύζοντάς το με κίνηση (flooding).



Εικόνα 1-12: Απομόνωση σημείου πρόσβασης

Η απομόνωση AP σταματά μια κακόβουλη τεχνική που ονομάζεται ARP δηλητηρίαση (poisoning or spoofing), που ονομάζεται επίσης **επίθεση ενδιάμεσου (Man-in-the-Middle Attack).** Το ARP αντιπροσωπεύει το **πρωτόκολλο διευθυνσιοδότησης διευθύνσεων Address Resolution Protocol –ARP)**, μια μέθοδο δικτυακής επικοινωνίας που ανακαλύπτει τη φυσική διεύθυνση ethernet μιας συσκευής στέλνοντας IP (κάνοντας δηλαδή ping). Εδώ ένας επιτιθέμενος μπορεί να συνδέσει μια συσκευή συνδεδεμένη με ενσύρματα στο τοπικό δίκτυο LAN, υπονομεύοντας τη διεύθυνση IP ενός δημόσιου σημείου πρόσβασης στο ίδιο τοπικό δίκτυο. Η ψεύτικη IP στέλνει σήμα στην άλλη συσκευή εκθέτοντας τη φυσική διεύθυνση MAC της, η οποία καθιστά τα δεδομένα και τις επικοινωνίες της ορατά στον εισβολέα. Η ενεργοποίηση της απομόνωσης AP στον δρομολογητή προστατεύει από την επίθεση, διακόπτοντας αυτόν τον τύπο επικοινωνίας [23].

Η χρήση του δρομολογητή του παρόχου για τη δημιουργία ενός δικτύου επισκεπτών είναι ένας άλλος τρόπος για να διαχωρίσει τους επισκέπτες χρησιμοποιώντας το ίντερνετ και τις δικτυακές συσκευές και εξοπλισμό του. Πρόκειται για ξεχωριστό WLAN με το δικό του όνομα - το οποίο ονομάζεται τυπικά SSID (αναγνωριστικό συνόλου υπηρεσιών) στη διαχείριση δικτύου. Η κατοχή δύο δικτύων Wi-Fi επιτρέπει στον πάροχο να ρυθμίσει τις παραμέτρους για να καλύψει τις ανάγκες των επισκεπτών του, σε εύρος ζώνης και προσβασιμότητας, προστατεύοντας

ταυτόχρονα τα δεδομένα της επιχείρησής του στο LAN και την πρωτεύουσα σύνδεση Wi-Fi.

Ακόμα, αν θα ήθελε ο πάροχος να ρυθμίσει την επιχείρησή του ασύρματα, χωρίς να αφιερώσει ένα SSID επισκεπτών, η ενεργοποίηση της απομόνωσης AP θα εμποδίσει το δικτυακό του εξοπλισμό από το να δει ο ένας τον άλλον. Οι υπολογιστές που είναι ενσύρματοι στο LAN δεν θα μπορέσουν να μιλήσουν με τις ασύρματες συσκευές και αυτές δεν μπορούν να έχουν πρόσβαση σε κοινά στοιχεία όπως διακομιστές αρχείων και εφαρμογές που φιλοξενούνται σε εσωτερική υποδομή.

Με τη διαχείριση δικτύου επισκεπτών, ο πάροχος κάνει λεπτομερείς ελέγχους για να ρυθμίσει τη χρήση ενός καθορισμένου ασύρματου δικτύου επισκεπτών. Μπορεί να ρυθμίσει τους περιορισμούς **ποιότητας της υπηρεσίας (Quality of Service –QoS)** που καλύπτουν το διαθέσιμο εύρος ζώνης ή να θέσει περιορισμούς χρόνου για το χρονικό διάστημα κατά το οποίο κάποιος μπορεί να το χρησιμοποιήσει. Αν θέλει να διακόψει την επικοινωνία μεταξύ τελικών σημείων, η απομόνωση AP είναι καλύτερη για την εξασφάλιση ασύρματου δικτύου.

1.8 Στόχοι – Συνεισφορά

Στόχος της συγκεκριμένης έρευνας είναι η μελέτη όλων εκείνων των αρχιτεκτονικών μέσω των οποίων μπορεί να γίνει επιτευκτός ο διαμοιρασμός συνδέσεων Wi-Fi μεταξύ των διαφόρων χρηστών μεταξύ τους. Αναλύονται τα διάφορα πρωτόκολλα που χρησιμοποιούνται και καθορίζουν την ταχύτητα, το εύρος ζώνης και την ομαλή λειτουργία και διασύνδεση των διαφόρων συσκευών μεταξύ τους. Επίσης, μελετώνται οι τεχνολογίες και τα λογισμικά που χρησιμοποιούνται, τα οποία με κατάλληλες ρυθμίσεις, μπορούν να επεκτείνουν το δίκτυο και να παρέχουν πρόσβαση σε χρήστες, ακόμα και σε απομακρυσμένες περιοχές. Αναλύονται σε θεωρητικό επίπεδο ο τρόπος χρήσης των ασύρματων δικτύων και συγκεκριμένα των δικτύων πλέγματος και γίνεται αναφορά και μελέτη στα PAWS, FON και Freifunk.

Η συνεισφορά της διατριβής έχει εκτός από θεωρητική προσέγγιση και πρακτική, καθώς θα δούμε πως εφαρμόζεται στο Freifunk και στο OTE Wi-Fi FON. Θα ασχοληθούμε με τον τρόπο διαμοιρασμού της σύνδεσης κάθε χρήστη στο δίκτυο,

τι κινδύνους μπορεί να προκύψουν και πως μπορούμε να τους αποφύγουμε. Ακόμα, θα δούμε τι τεχνικές χρησιμοποιεί η κάθε εφαρμογή του κάθε δικτύου και πως μπορεί κάποιος να συνδεθεί σε ένα και να γίνει μέλος.

Σημαντικό ζήτημα τίθεται πάντα η ασφάλεια και η αυθεντικοποίηση του χρήστη, τα οποία αποτελούν σημαντικό παράγοντα στον τρόπο σύνδεσης των χρηστών, διατηρώντας εκτός από την ανωνυμία τους και το απόρρητο της σύνδεσής τους. Μέσω των διαφόρων τεχνικών όπως τα VPN, NAT, σηράγγων και μεθόδων κρυπτογράφησης, διαμοιράζονται οι πληροφορίες και τόσο ο πάροχος όσο και ο χρήστης ακολουθώντας διαφόρων ειδών κανόνες μπορούν να έχουν ασφαλή πρόσβαση στο Διαδίκτυο.

1.9 Διάρθρωση της διπλωματικής

Αρχικά, στο δεύτερο κεφάλαιο μελετάμε τις διάφορες τεχνολογίες που χρησιμοποιούνται στον διαμοιρασμό σύνδεσης Wi-Fi, εστιάζοντας στο πρωτόκολλο επεκτάσιμης αυθεντικοποίησης (Extensible Authentication Protocol –EAP), στον τρόπο απομόνωσης της πληροφορίας μέσω των ιδιωτικών εικονικών δικτύων (Virtual Private Networks –VPN), καθώς επίσης και την κρυπτογράφηση του κειμένου με την χρήση της ασύρματης προστατευόμενης πρόσβασης (Wireless Protected Access - WPA).

Στο τρίτο κεφάλαιο επικεντρωνόμαστε στα δίκτυα πλέγματος (Mesh networks) και συλλέγουμε πληροφορίες από τον τρόπο σύνδεσής τους., βλέπουμε τον τρόπο χρήσης των πρωτοκόλλων δρομολόγησης του υβριδικού ασύρματου δικτύου πλέγματος (Hybrid Wireless Mesh Network), Babel και της καλύτερης προσέγγισης στην κινητή δικτύωση ανά άλμα (Better Approach To Mobile Adhoc Networking), και σχολιάζουμε τα οφέλη που μας προσφέρουν στον διαμοιρασμό συνδέσεων.

Στο τέταρτο κεφάλαιο βλέπουμε τη χρήση των τεχνολογιών σε συστήματα διαμοιρασμού δικτύων στα κοινωνικά δίκτυα (Community Networks). Ασχολούμαστε με το κοινωνικά Wi-Fi (Social Wi-Fi) και την υπηρεσία δημόσιας πρόσβασης Wi-Fi (Public Access Wi-Fi Service). Ακόμα, επικεντρωνόμαστε στο FON και συγκεκριμένα στο OTE Wi-Fi FON, όπου αναλύουμε τον τρόπο λειτουργίας του.

Στο πέμπτο κεφάλαιο μελετάμε την χρήση και λειτουργία του δικτύου Freifunk που δραστηριοποιείται στην Γερμανία. Παρουσιάζονται οι τεχνολογίες και αρχιτεκτονικές που χρησιμοποιεί και όλο εκείνο το εύρος των περιοχών που καλύπτει. Ακόμα, μελετώνται τρόποι εξέλιξής του και πως μπορεί να επωφελήσει τον διαμοιρασμό των συνδέσεων.

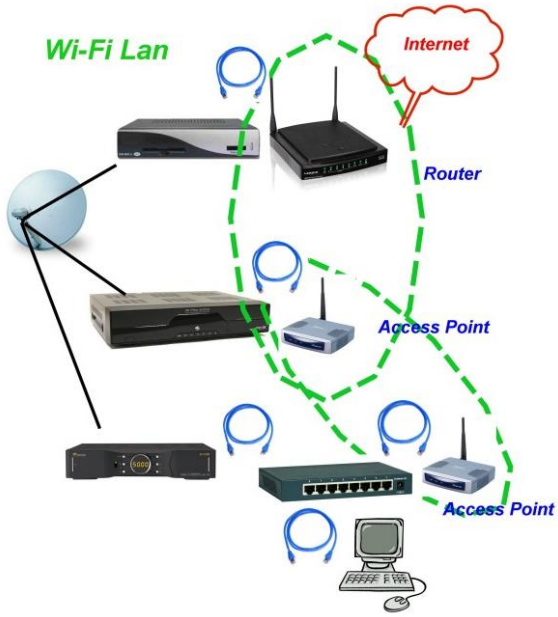
Στο τελευταίο κεφάλαιο γίνεται μία σύνοψη της διπλωματικής εργασίας και προτείνονται μελλοντικές επεκτάσεις της μελέτης και των διαθέσιμων τεχνολογιών που μπορούν να βελτιώσουν τον διαμοιρασμό των συνδέσεων. Γίνεται τέλος, ανασκόπηση της λειτουργίας και του τρόπου σύνδεσης των ασύρματων δικτύων και που αυτά οφελούν στη σύνδεση των χρηστών.

2 Τεχνολογίες διαμοιρασμού σύνδεσης Wi-Fi

Προκειμένου να γίνει ο σωστός διαμοιρασμός συνδέσεων Wi-Fi, όπως είδαμε και παραπάνω θα πρέπει να χρησιμοποιηθούν εκτός από δρομολογητές, AP τα οποία ενώ θα λαμβάνουν σήμα Ethernet μέσω καλωδίου UTP, το εκπέμπουν στην περιοχή των 2.4GHz. Όπως ακριβώς δύο υπολογιστές μπορούν να συνδεθούν μεταξύ τους μέσω AP, έτσι ακριβώς και δύο δορυφορικοί δέκτες μπορούν να συνδεθούν ασύρματα, να συντάξουν ένα δίκτυο LAN και μέσω αυτού να εφαρμόσουν την τεχνολογία του διαμοιρασμού κάρτας (Card Sharing –CS).

Η ρύθμιση των μονάδων για το ασύρματο δίκτυο, είτε είναι AP, είτε δρομολογητής με ενσωματωμένο AP, δεν διαφέρει σε παραμετροποίηση από την ρύθμισης ενός ασύρματου δικτύου υπολογιστών. Μία ακόμα όμως σημαντική ρύθμιση που πρέπει να γίνει στα AP, είναι η επιλογή της κατάστασης λειτουργίας. Με βάση την κατάσταση λειτουργίας, ένα AP μπορεί να λειτουργήσει ως:

- σταθμός εκπομπής πάνω στον οποίο θα συνδέονται τα υπόλοιπα AP
- πελάτης που θα συνδέεται σε ένα σταθμό εκπομπής (AP Client)
- ασύρματη γέφυρα για να επικοινωνεί με ένα και μοναδικό AP που θα έχει την ίδια ρύθμιση (Wireless Bridge)
- επαναλήπτης σήματος για την επέκταση του ασύρματου δικτύου (repeat mode). Η βασική διαφορά με την κατάσταση AP Client, είναι ότι με την πρώτη ρύθμιση το AP μπορεί να τροφοδοτήσει και περαιτέρω συσκευές.



Εικόνα 2-1: Χρήση AP στον διαμοιρασμό συνδέσεων

Θα ασχοληθούμε παρακάτω για το πώς μπορούν να γίνουν συγκεκριμένες ρυθμίσεις στα AP, έτσι ώστε να γίνει ο διαμοιρασμός των συνδέσεων γρήγορα, εύκολα, αλλά και πως χρησιμοποιούνται οι διάφορες τεχνικές, τα πρωτόκολλα δρομολόγησης που είναι υπεύθυνα για τον σωστό διαμοιρασμό των πληροφοριών, καθώς επίσης και τα μοντέλα κρυπτογράφησης που διασφαλίζουν ασφάλεια, αυθεντικότητα και εξουσιοδότηση, τόσο στον πάροχο, όσο και στον επισκέπτη.

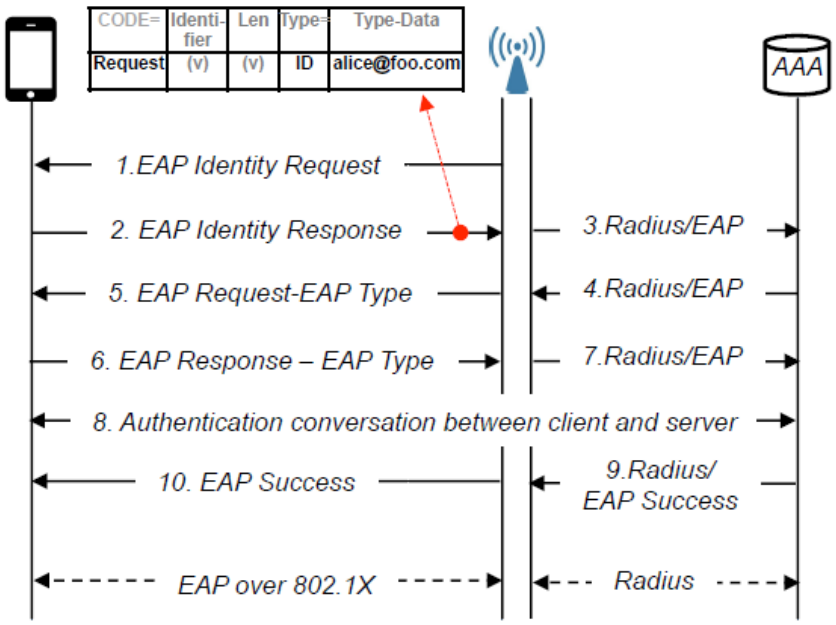
2.1 Οικογένεια πρωτοκόλλων EAP

Τα δίκτυα χρησιμοποιούν ένα σύνολο από πρωτόκολλα προκειμένου να επικοινωνήσουν οι διάφορες συσκευές μεταξύ τους, να ανταλλάσσουν πληροφορίες και δεδομένα, και διασφαλίζουν ότι η επικοινωνία θα γίνει με βάση κάποια πρότυπα, όπου οι συμμετέχοντες θα πρέπει να ακολουθούν κάποιους κανόνες [39]. Πρόκειται δηλαδή, για ένα σύνολο από κανόνες, οι οποίοι καθορίζουν το πώς διακινούνται τα δεδομένα, το πώς γίνεται ο έλεγχος και ο χειρισμός των λαθών, ακόμα και αν ανήκουν σε ίδια ή διαφορετικού τύπου δίκτυα.

Ένας χρήστης, δεδομένου ότι θέλει να συνδεθεί σε ένα AP θα πρέπει να επιτύχει μία σύνδεση, στην οποία θα υπάρχει αυθεντικότητα της χρήσης, αλλά και να

συνδέεται εύκολα χωρίς να εισάγει συνέχεια κωδικούς και να μπορεί να βρίσκει τα διαθέσιμα AP χωρίς κάποιον περαιτέρω κόπο. Γι' αυτό το λόγο υπάρχουν και θα μελετήσουμε τα παρακάτω πρωτόκολλα που διευκολύνουν την πρόσβαση του χρήστη στο δίκτυο.

Το **πρωτόκολλο επεκτάσιμης αυθεντικοποίησης (Extensible Authentication Protocol –EAP)** είναι το πρότυπο πλαίσιο ελέγχου ταυτότητας που υιοθετήθηκε από τους περισσότερους Wi-Fi προμηθευτές και παρόχους υπηρεσιών. Στο παρακάτω σχήμα φαίνεται μία τυπική EAP αυθεντικοποίηση, μεταξύ ενός πελάτη ,ενός AP και ενός (Authentication Authorization Accounting –AAA) διακομιστή [1].



Εικόνα 2-2: Ροή αυθεντικοποίησης EAP

Μετά από την επιχείρηση της συσκευής του πελάτη να συνδεθεί με το AP, το AP εκκινεί αυθεντικοποίηση στέλνοντας ένα EAP αίτημα ταυτότητας (EAP Identity Request) (1ο μήνυμα). Ο πελάτης απαντάει με το δικό του αίτημα ταυτότητας (2ο μήνυμα). Το AP ενθυλακώνει το μήνυμα σε μία ακτίνα κύκλου (Radius) και το προωθεί στον αντίστοιχο διακομιστή AAA (3ο μήνυμα). Στη συνέχεια, ο AAA διακομιστής διαλέγει μία συγκεκριμένη μέθοδο αυθεντικοποίησης EAP (EAP-TTLS/ EAP-PEAP) και ενεργοποιεί την αμοιβαία αυθεντικοποίηση (4ο-8ο μήνυμα). Μετά από μία επιτυχημένη αυθεντικοποίηση, αποστέλλεται μήνυμα επιτυχίας (9ο μήνυμα).

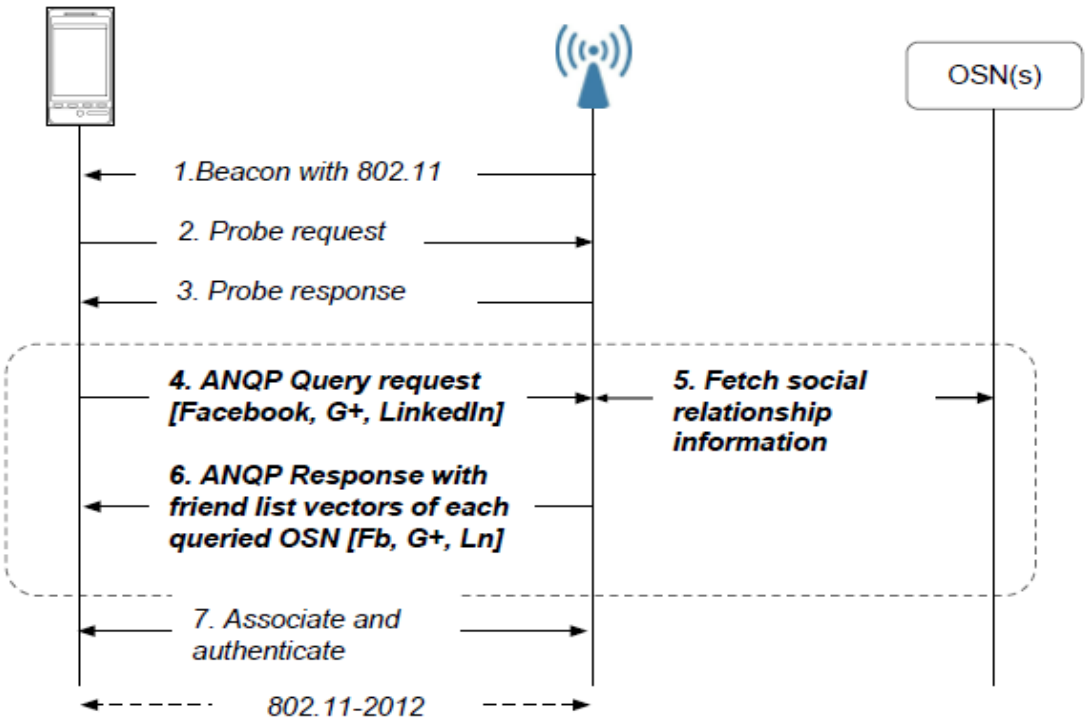
Κατά τη διάρκεια του αμοιβαίου ελέγχου ταυτότητας, ο πελάτης και ο διακομιστής αποδεικνύουν την ιδιοκτησία τους για ένα συγκεκριμένο πιστοποιητικό ή γνώση ενός προδιαμοιρασμένου μυστικού [38]. Για παράδειγμα, στο EAP-TTLS, ο διακομιστής χρησιμοποιεί ένα πιστοποιητικό και ο πελάτης έναν κωδικό. Δεδομένου ότι δεν υπάρχουν τέτοια διαπιστευτήρια στα κοινωνικά Wi-Fi, προτείνεται η μέθοδος αυθεντικοποίησης EAP-Social, στην οποία και τα δύο μέλη χρησιμοποιούν πληροφορίες από τα σε απευθείας σύνδεση κοινωνικά δίκτυα για την εδραίωση εμπιστοσύνης [1].

2.1.1 Πρωτόκολλο ANQP

Προκειμένου να μπορέσουν οι χρήστες να ανακαλύψουν τα διαθέσιμα Wi-Fi σημεία πρόσβασης που λειτουργούν από τους παρόχους, χρησιμοποιείται ένα πρωτόκολλο που παρέχεται από το πιο προηγμένο πρότυπο 802.11-2012, το οποίο ονομάζεται **πρωτόκολλο ερώτησης στο δίκτυο πρόσβασης (Access Network Query Protocol –ANQP).**

Το ANQP στοχεύει στην παροχή καλύτερων μεταφορών Wi-Fi υπηρεσιών με μία καλύτερη δυνατότητα εντοπισμού δικτύου και υποστηρίζεται από πολλές κινητές συσκευές κατασκευαστών και προμηθευτών εξοπλισμού δικτύου. Ουσιαστικά, το ANQP επιτρέπει στη συσκευή του επισκέπτη να ρωτάει συγκεκριμένες πληροφορίες σχετικά με το δίκτυο πρόσβασης πρωτού συνδεθεί με αυτό. Αυτή η λειτουργία είναι πολύ χρήσιμη και μπορεί να επεκταθεί για να επιτρέψει σε επισκέπτες να διερευνήσουν την κοινωνική σχέση τους με τον ιδιοκτήτη του σημείου πρόσβασης.

Στο παρακάτω σχήμα απεικονίζεται η διαδικασία εντοπισμού διαθέσιμου δικτύου.



Εικόνα 2-3: Εντοπισμός δικτύου Wi-Fi

Όπως και στο EAP στόχος αρχικά της συσκευής μας είναι να επικοινωνήσει με έναν AP. Όταν η φιλοξενούμενη συσκευή έρχεται κοντά στο σημείο πρόσβασης, λαμβάνει σήματα από το δίκτυο ανακοινώνοντας την υποστήριξή του ANQP (1ο μήνυμα). Μετά την εκπομπή του δικτύου για την ύπαρξή του (2ο και 3ο μήνυμα), η συσκευή στέλνει ένα ANQP ερώτημα στο δίκτυο (4ο μήνυμα). Αυτή η αίτηση περιέχει την λίστα των OSNs που ο χρήστης θέλει να ρωτήσει, όπως το Facebook, Google+ και LinkedIn. Το AP στη συνέχεια ανακτά τη λίστα πληροφοριών του φίλου από το συγκεκριμένο OSN με ανάκληση στα αντίστοιχα APIs (5ο μήνυμα). Μετά την απόκτηση της λίστας των φίλων, το AP τα στέλνει στη συσκευή του επισκέπτη (6ο μήνυμα). Εάν ο επισκέπτης ανακαλύψει ότι ανήκει στις λίστες φίλων, συσχετίζει και πιστοποιεί στο δίκτυο (7ο μήνυμα) [1].

2.1.2 Πρωτόκολλο OLSR

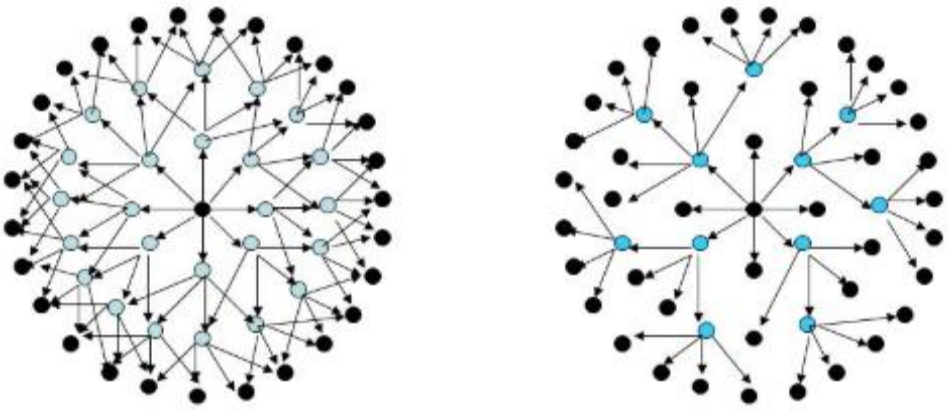
Το **πρωτόκολλο δρομολόγησης βελτιστοποιημένης κατάστασης σύνδεσης (Optimized Link State Routing Protocol –OLSR)** είναι ένα πρωτόκολλο δρομολόγησης IP βελτιστοποιημένο για δίκτυα ad hoc. Χρησιμοποιεί μηνύματα hello

και τοπολογία ελέγχου για να ανακαλύψει και να διαδώσει τις πληροφορίες κατάστασης σύνδεσης στο υπόλοιπο δίκτυο. Οι μεμονωμένοι κόμβοι χρησιμοποιούν αυτές τις πληροφορίες τοπολογίας για να υπολογίσουν τους επόμενους προορισμούς για όλους τους κόμβους του δικτύου χρησιμοποιώντας το μικρότερο αριθμών κόμβων του μονοπατιού.

Αρχικά, κάθε κόμβος πρέπει τοπικά να υπολογίζει το ρυθμό μετάδοσης (transmission rate) για κάθε διεπαφή του. Την πληροφορία αυτή την παίρνουμε από το περιβάλλον του χρήστη μέσω της **διεπαφής προγραμματισμού εφαρμογών (Application Programming Interface –API)** για καθεμιά από τις διεπαφές που συμμετέχει στη διαδικασία της δρομολόγησης. Στη συνέχεια κάθε κόμβος θα πρέπει να γνωστοποιήσει το ρυθμό μετάδοσης του σε όλους τους γειτονικούς του κόμβους (one-hop neighbours) [36].

Όπως και στα Link State πρωτόκολλα, χρησιμοποιεί πίνακες δρομολόγησης για να αποθηκεύει τις καλύτερες διαδρομές ανάμεσα στους κόμβους, οι οποίες υπολογίζονται χρησιμοποιώντας τον αλγόριθμο δρομολόγησης του Dijkstra. Είναι κατάλληλο για συνθήκες στις οποίες τα δύο άκρα αλλάζουν με τον χρόνο για το λόγο ότι δεν χρειάζεται επιπλέον κίνηση με δεδομένα ελέγχου, καθώς διατηρούνται διαρκώς οι διαδρομές προς όλα τα σημεία.

Μέσω των **πολλαπλών σημείων (Multipoint Relays –MPRs)** τα οποία μεταδίδουν μηνύματα μεταξύ κόμβων, επιλέγεται και παίζει ρόλο στην δρομολόγηση της κατάλληλης διαδρομής από οποιαδήποτε πηγή σε οποιοδήποτε επιθυμητό κόμβο προορισμού. Το OLSR ελαχιστοποιεί την επιβάρυνση του δικτύου από την κίνηση πολυάριθμων μηνυμάτων ελέγχου, χρησιμοποιώντας μονάχα επιλεγμένους κόμβους MPRs για την αναμετάδοση των μηνυμάτων ελέγχου, όπως φαίνονται και στην παρακάτω εικόνα.



Εικόνα 2-4: Μηχανισμός πλημμύρας στο OLSR

Οι κόμβοι αυτού που έχουν επιλεγεί ως MPR από κάποιους γειτονικούς τους κόμβους, ανακοινώνουν αυτοί την πληροφορία περιοδικά στα μηνύματα ελέγχου που αποστέλλουν. Με αυτόν τον τρόπο ένας κόμβος ανακοινώνει στο δίκτυο, ότι έχει επαφή αυτή τη στιγμή με τους κόμβους που τον έχουν επιλέξει ως MPR. Στον υπολογισμό των διαδρομών, οι κόμβοι MPR χρησιμεύουν για να χαραχθεί το μονοπάτι από έναν δεδομένο κόμβο σε οποιονδήποτε προορισμό στο δίκτυο.

Συνοψίζοντας, μερικά από τα πλεονεκτήματα που προσφέρει στο δίκτυο το OLSR είναι τα ακόλουθα:

- Έχει σχεδιαστεί να λειτουργεί απολύτως κατανεμημένα, και δεν εξαρτάται από καμία κεντρική οντότητα.
- Είναι ιδιαίτερα καλό για δίκτυα όπου η κίνηση είναι τυχαία και σποραδική ανάμεσα σε έναν μεγάλο αριθμό κόμβων, παρά σε καταστάσεις όπου η κίνηση αφορά σχεδόν αποκλειστικά ένα μικρό και συγκεκριμένο σετ από κόμβους.
- Είναι κατάλληλο για μεγάλα και πυκνά κινητά δίκτυα, καθώς η βελτιστοποίηση που επιτυγχάνεται με τη χρήση των MPR δουλεύει καλύτερα σε τέτοιες συνθήκες.
- Χρησιμοποιεί βήμα-προς-βήμα (hop-by-hop) δρομολόγηση, με άλλα λόγια, κάθε κόμβος χρησιμοποιεί την δική του τοπική πληροφόρηση για τη δρομολόγηση των πακέτων.
- Διατηρεί διαρκώς πληροφορία για τις διαδρομές προς όλους τους προορισμούς στο δίκτυο, και ως εκ τούτου είναι ιδανικό για την κίνηση που δημιουργείται

μεταξύ ενός μεγάλου αριθμού κόμβων όπου η δυάδα [αφετηρία – προορισμός] αλλάζει διαρκώς.

- Δεν απαιτείται αξιόπιστη μετάδοση των μηνυμάτων ελέγχου: ο κάθε κόμβος αποστέλλει μηνύματα ελέγχου περιοδικά, και μπορεί να αντέξει απώλεια μηνυμάτων σε λογικά πλαίσια, χωρίς προβλήματα. Αυτές οι απώλειες είναι σύνηθες φαινόμενο στις ασύρματες επικοινωνίες.
- Επίσης δεν απαιτείται η μετάδοση των μηνυμάτων με συγκεκριμένη σειρά. Κάθε μήνυμα ελέγχου είναι αριθμημένο αυξητικά. Με αυτόν τον τρόπο, ο παραλήπτης μπορεί να γνωρίζει ανά πόσα στιγμή ποια πληροφορία απ' αυτές είναι η πιο πρόσφατη, ακόμα και εάν έχουν μεταδοθεί με λάθος σειρά [45].

2.2 Διαχείριση δικτύων Wi-Fi

Το ίδιο το δίκτυο πρέπει να έχει ένα στρώμα αφαίρεσης υλικού. Αυτό το στρώμα πρέπει να είναι εύκολο να περικοπεί έτσι ώστε πολλά διαφορετικά δίκτυα να μπορούν να τρέχουν ταυτόχρονα χωρίς να παρεμβαίνουν μεταξύ τους, σε μια ποικιλία διαφορετικών υλικών, συμπεριλαμβανομένων των διακοπτών (switches), δρομολογητών , των σημείων πρόσβασης, κλπ.

Πάνω από το επίπεδο αφαίρεσης υλικού, θέλουμε νέα πρωτόκολλα και μορφές διευθύνσεων να εκτελούνται ανεξάρτητα με τη δική τους απομονωμένη φέτα του ίδιου φυσικού δικτύου, επιτρέποντας τη βελτιστοποίηση των δικτύων για τις εφαρμογές που εκτελούνται σε αυτά, ή προσαρμοσμένες για τον ιδιοκτήτη που τα διαθέτει.

Προκειμένου να εικονοποιήσουμε ένα δίκτυο, θα πρέπει να γνωρίζουμε ποια κομμάτια του θα τεμαχίσουμε για την καλύτερη μετάδοση της πληροφορίας. Θα δούμε παρακάτω πως μπορεί κάτι τέτοιο να γίνει επιτευκτό και τι μπορεί να μας προσφέρει.

2.2.1 SDN/ OpenFlow

Με την **τεχνολογία δικτύωσης λογισμικού (Software Defined Network – SDN)**, η οποία είναι μια προσέγγιση στον υπολογισμό του σύννεφου που διευκολύνει τη διαχείριση δικτύου και επιτρέπει προγραμματισμό αποδοτικής διαμόρφωσης δικτύου, βελτιώνεται η απόδοση και η παρακολούθηση του δικτύου. Το SDN

αποσκοπεί να αντιμετωπίσει το γεγονός ότι η στατική αρχιτεκτονική των παραδοσιακών δικτύων είναι αποκεντρωμένη και πολύπλοκη, ενώ τα τρέχοντα δίκτυα απαιτούν μεγαλύτερη ευελιξία και εύκολη αντιμετώπιση προβλημάτων [37].

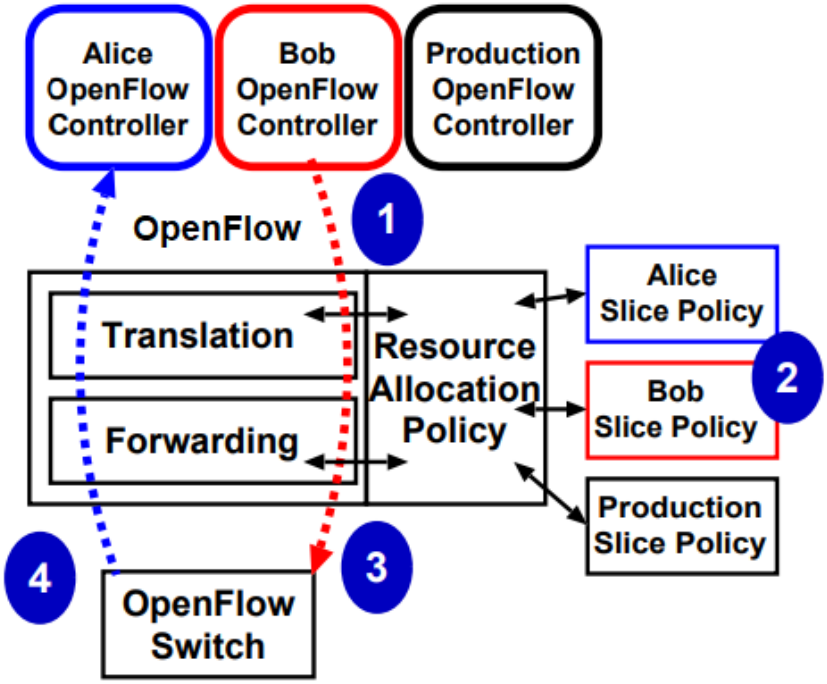
Η SDN επιχειρεί να συγκεντρώσει τη νοημοσύνη δικτύου σε ένα στοιχείο δικτύου αποσυνδέοντας τη διαδικασία προώθησης πακέτων δικτύου (επίπεδο δεδομένων) από τη διαδικασία δρομολόγησης (επίπεδο ελέγχου). Το επίπεδο ελέγχου αποτελείται από έναν ή περισσότερους ελεγκτές οι οποίοι θεωρούνται ως ο εγκέφαλος του δικτύου SDN όπου ενσωματώνεται ολόκληρη η νοημοσύνη. Ωστόσο, η συγκέντρωση πληροφοριών έχει τα δικά της μειονεκτήματα όταν πρόκειται για την ασφάλεια, την επεκτασιμότητα και την ελαστικότητα και αυτό είναι το κύριο θέμα της SDN [2].

Το SDN προσφέρει πολλά οφέλη επίσης όμως, συμπεριλαμβανόμενης της παροχής κατά παραγγελία, της αυτοποιημένης εξισορρόπησης φορτίου, της βελτιωμένης φυσικής υποδομής και της ικανότητας κλιμάκωσης των πόρων του δικτύου με κλειδαριές, με τις ανάγκες εφαρμογής και δεδομένων.

Ακόμα, παρέχει υπηρεσίες δικτύου γρήγορα, με κέρδος και σε μεγάλη κλίμακα. Μπορεί να:

- Προσαρμόσει και να βελτιώσει δίκτυα σε πραγματικό χρόνο, ώστε να μπορεί να έχει μεγαλύτερη αξία από τα υπάρχοντα στοιχεία
- Δημιουργεί υπηρεσίες δικτύου σε λιγότερο από το ήμισυ του χρόνου και τα παρέχει σε δευτερόλεπτα
- Γεφυρώνει το χάσμα μεταξύ αυτοματοποίησης υπηρεσιών και αυτοματοποίησης δικτύου
- Προσθέτει την ευαισθητοποίηση του δικτύου στην παροχή υπηρεσιών κατά παραγγελία, ώστε να μπορεί να αξιοποιήσει με τον καλύτερο τρόπο τα διαθέσιμα περιουσιακά στοιχεία του δικτύου
- Προσθέτει την ευαισθητοποίηση σχετικά με την υγιεινή των υπηρεσιών στην δυναμική βελτιστοποίησης δικτύου για να διασφαλίσει την ποιότητα των υπηρεσιών και την αποτελεσματικότητα του δικτύου.

Το πρωτόκολλο **ανοιχτής ροής (OpenFlow)** θεωρείται ένα από τα πρώτα πρότυπα δικτύωσης που ορίζονται από το λογισμικό SDN. Αρχικά ορίστηκε το πρωτόκολλο επικοινωνίας σε περιβάλλοντα SDN που επιτρέπει στον ελεγκτή SDN να αλληλεπιδρά άμεσα με το επίπεδο προώθησης των συσκευών δικτύου, όπως οι διακόπτες και οι δρομολογητές, τόσο φυσικοί όσο και εικονικοί , ώστε να μπορούν να προσαρμόζονται καλύτερα στις μεταβαλλόμενες επιχειρηματικές απαιτήσεις.



Εικόνα 2-5: Λειτουργία OpenFlow

Το OpenFlow παρακολουθεί τα μηνύματα από τους ελεγκτές του επισκέπτη (1) και χρησιμοποιώντας τα στοιχεία του χρήστη (2), διαγράφει με διαφάνεια (3) το μήνυμα που ελέγχει μόνο ένα κομμάτι του δικτύου. Μηνύματα από μεταγωγείς (4) προωθούνται μόνο στους επισκέπτες, αν αυτό ταιριάζει με την πολιτική κομματιού τους [25].

Ένα κρίσιμο σημείο της εικονικοποίησης στο OpenFlow είναι της απομόνωσης μεταξύ κομματιών. Επειδή οι μηχανισμοί απομόνωσης ποικίλλουν ανάλογα με τον πόρο, παρακάτω βλέπουμε κάποιους μηχανισμούς απομόνωσης που προσφέρει στο δίκτυο:

a) Απομόνωση εύρους ζώνης:

Ενώ δεν εκθέτει τον έλεγχο, εξακολουθεί να είναι σε θέση για να αξιοποιήσει τις υπάρχουσες δυνατότητες απομόνωσης εύρους ζώνης μεταγωγής σημειώνοντας τα VLAN προτεραιότητας bits σε πακέτα. Οι ετικέτες VLAN έχουν ένα πεδίο τριών δυαδικών ψηφίων, το σημείο κώδικα προτεραιότητας (Priority Code Point –PCP) VLAN, που είναι ένας τυπικός μηχανισμός για την χαρτογράφηση ενός πακέτου σε μία από τις οχτώ ουρές προτεραιότητας. Το OpenFlow εκθέτει τη δυνατότητα διαχείρισης των ετικετών VLAN και των σε προτεραιότητα bits, έτσι ώστε να είναι δυνατόν να επισημανθούν όλα τα πακέτα σε μια ροή με μία συγκεκριμένη ποσότητα.

Έτσι, για να επιβάλλει την απομόνωση του εύρους ζώνης, ξαναγράφει όλες τις προσθήκες του πίνακα προώθησης για να συμπεριλάβει μία ενέργεια "ορισμός VLAN προτεραιότητας", ορίζοντας την προτεραιότητα σε μία από τις οχτώ ουρές προτεραιότητας. Όλη η κίνηση από ένα δεδομένο κομμάτι, αντιστοιχεί στην τάξη κυκλοφορίας που καθορίζεται από την πολιτική κατανομής πόρων. Το ακριβές νόημα κάθε κατηγορίας κυκλοφορίας πρέπει να ρυθμιστεί εκτός ζώνης από τον διαχειριστή του δικτύου [34].

b) Απομόνωση τοπολογίας:

Οι ελεγκτές ανακαλύπτουν τους κόμβους και τους συνδέσμους του δικτύου μέσω του OpenFlow. Σε μία εικονική ρύθμιση, ο ελεγκτής ανακαλύπτει μία συσκευή δικτύου όταν η συσκευή συνδέεται ενεργά με τη θύρα TCP ακρόασης του ελεγκτή. Δεδομένου ότι λειτουργεί ως εναλλακτική λύση μεταξύ του διακόπτη και του ελεγκτή, προωθεί μόνο τις συνδέσεις σε έναν ελεγκτή επισκέπτη για τους διακόπτες στην εικονική τοπολογία του επισκέπτη.

Ακόμα, υπάρχει ένα μήνυμα για τη λίστα των διαθέσιμων φυσικών θυρών σε έναν διακόπτη. Το OpenFlow επεξεργάζεται την απάντηση μηνύματος για να αναφέρει μόνο τις θύρες που εμφανίζονται στην εικονική τοπολογία. Λαμβάνεται επίσης μία ιδιαίτερη μέριμνα για την διαχείριση μηνυμάτων πρωτοκόλλου ανίχνευσης στρώματος συνδέσμου (Link Layer Discover Protocol –LLDP). Τα μηνύματα LLDP αποστέλλονται σε κάθε θύρα μεταγωγής για να κάνουν εντοπισμό του γείτονα. Όταν τα μηνύματα παραλαμβάνονται από τον γειτονικό διακόπτη, δεν αντιστοιχούν σε

κανένα κανόνα προώθησης και συνεπώς αποστέλλονται στον ελεγκτή. Δεδομένου ότι τα μηνύματα έχουν μία συγκεκριμένη, πολύ γνωστή μορφή, το OpenFlow διασταυρώνει και βάζει ετικέτες στο μήνυμα με το αναγνωριστικό κομματιών αποστολής, έτσι ώστε αυτές να αποστέλλονται πίσω στο σωστό κομμάτι όταν παραλαμβάνονται και πάλι [34].

c) Απομόνωση ροής χώρου:

Κάθε κομμάτι πρέπει να περιορίζεται να επηρεάζει μόνο τις ροές στον χώρο ροής τους. Το OpenFlow εκτελεί επανεγγραφή μηνυμάτων για να διασφαλίσει διαφανώς ότι μόνο ένα κομμάτι έχει έλεγχο στις δικές του ροές και δεν μπορεί να επηρεάσει άλλες ροές κομματιών. Δεν είναι δυνατόν να ξαναγραφούν όλοι οι κανόνες ώστε να ταιριάζουν σε ένα κομμάτι. Έτσι, το OpenFlow κάνει τους κανόνες πιο συγκεκριμένους.

Εάν ο ελεγκτής ενός επισκέπτη προσπαθήσει να δημιουργήσει έναν κανόνα που να επηρεάζει όλη την κίνηση, το OpenFlow θα ξαναγράψει τον κανόνα για να επηρεάσει μόνο την επισκεψιμότητα TCP στη θύρα 80. Ωστόσο, δεν θα ξαναγράψει έναν κανόνα που να επηρεάζει την κυκλοφορία της θύρας 22 μόνο για να επηρεάσει την κίνηση στην θύρα 20. Στην περίπτωση κανόνων που δεν μπορούν να ξαναγραφούν, το OpenFlow στέλνει ένα μήνυμα σφάλματος στον ελεγκτή, υποδεικνύοντας ότι η καταχώρηση ροής δεν μπορεί να προστεθεί [34].

d) Απομόνωση ελέγχου:

Εκτός από τους φυσικούς πόρους, το ίδιο κανάλι ελέγχου OpenFlow πρέπει να είναι εικονικό και απομονωμένο. Για παράδειγμα, όλα τα μηνύματα στο OpenFlow περιλαμβάνουν ένα μοναδικό αναγνωριστικό συναλλαγής, όπου θα πρέπει να ξαναγράψει την ταυτότητα συναλλαγής, έτσι ώστε να διασφαλίσει ότι τα μηνύματα από διαφορετικούς ελεγκτές επισκεπτών δεν χρησιμοποιούν το ίδιο αναγνωριστικό.

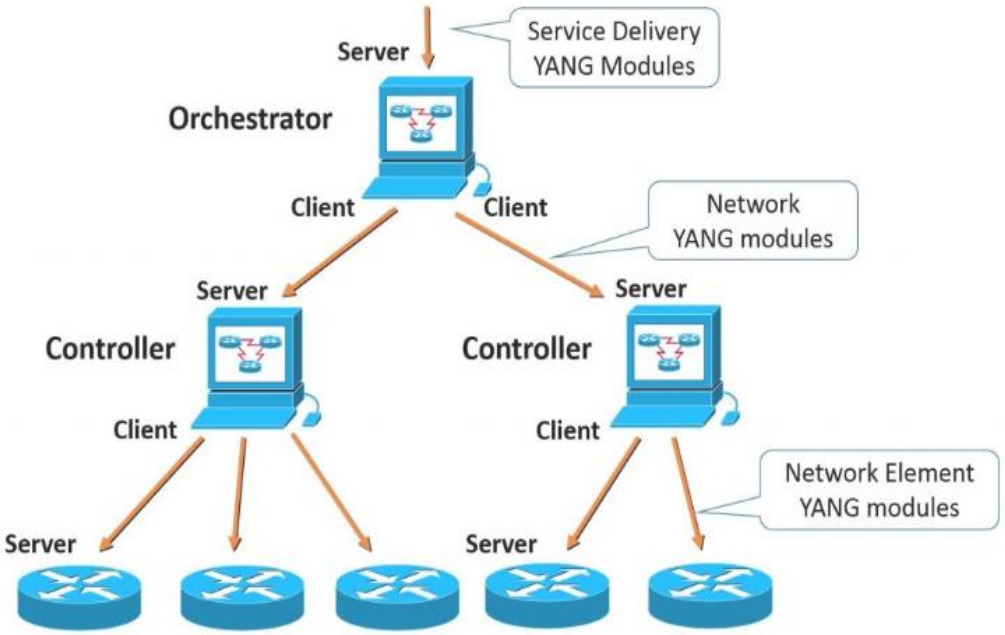
Ομοίως, το OpenFlow χρησιμοποιεί έναν ακέραιο 32-bit για την αναγνώριση του ρυθμιστή, όπου ένα πακέτο βρίσκεται στην ουρά, όσο κατά την αποστολή της απόφασης που στέλνεται στον ελεγκτή. Τα μηνύματα κατάστασης , π.χ. η διασύνδεση σε μία θύρα, έχει να αντιγραφεί σε όλα τα κομμάτια που έχουν επηρεαστεί.

Εικονοποιώντας το κανάλι ελέγχου, καθίστανται ευκολότερο, επειδή του OpenFlow πρωτόκολλο ορίζει μόνο 16 τύπους μηνυμάτων.

2.2.2 NETCONF

Το **πρωτόκολλο διαμόρφωσης δικτύου (Network Configuration Protocol –NETCONF)** είναι ένα πρωτόκολλο διαχείρισης δικτύου το οποίο αναπτύχθηκε και τυποποιήθηκε από το IETF. Το NETCONF παρέχει μηχανισμούς για την εγκατάσταση, χειρισμό και διαγραφή της διαμόρφωσης των συσκευών δικτύου [18]. Οι λειτουργίες του υλοποιούνται πάνω από ένα απλού **κλήσης απομακρυσμένης διαδικασίας (Remote Procedure Call –RPC)** επίπεδο. Το πρωτόκολλο NETCONF χρησιμοποιεί κωδικοποίηση δεδομένων βασισμένη σε **γλώσσα επεκτάσιμης σήμανσης (Extensible Markup Language –XML)** για τα δεδομένα διαμόρφωσης, καθώς και για τα μηνύματα πρωτοκόλλου. Τα μηνύματα πρωτοκόλλου ανταλλάσσονται πάνω από ένα ασφαλές πρωτόκολλο μεταφοράς.

Αρχικά παρέχει πρόσβαση στις εγγενείς δυνατότητες μιας συσκευής μέσα σε ένα δίκτυο, καθορίζοντας μεθόδους για να χειριστεί τη βάση δεδομένων διαμόρφωσης, να ανακτήσει λειτουργικά δεδομένα και να επικαλεστεί συγκεκριμένες λειτουργίες. Το **ακόμα μία επόμενη γενιά (Yet Another Next Generation –YANG),** το οποίο είναι μία γλώσσα μοντελοποίησης δεδομένων για τον ορισμό των δεδομένων που αποστέλλονται μέσω του πρωτοκόλλου διαμόρφωσης δικτύου NETCONF, παρέχει τα μέσα για τον προσδιορισμό του περιεχομένου που μεταφέρεται μέσω του NETCONF, τόσο για δεδομένα όσο και για λειτουργίες. Μαζί, βοηθούν τους χρήστες να δημιουργούν εφαρμογές διαχείρισης δικτύου που να ανταποκρίνονται στις ανάγκες των φορέων εκμετάλλευσης δικτύου [35].



Εικόνα 2-6: NETCONF

Το NETCONF και YANG προσθέτουν διάφορες λειτουργίες και αντιμετωπίζουν διάφορες αδυναμίες στα δίκτυα Wi-Fi όπως:

- **Συναλλαγές διαμόρφωσης:**

Οι ρυθμίσεις παραμέτρων NETCONF βασίζονται σε ατομικές συναλλαγές που αποτελούνται από πολλαπλές εντολές διαμόρφωσης που απαιτούνται για να μετακινήσουν ένα δίκτυο από μία κατάσταση A στην κατάσταση B. Η σειρά των αποσπασμάτων διαμόρφωσης μιας συναλλαγής δεν έχει σημασία και η επιτυχία μιας συναλλαγής βασίζεται στην επιτυχία από όλα τα αποσπάσματα εντολών. Εάν αποτύχει οποιαδήποτε εντολή, ολόκληρη η συναλλαγή αποτυγχάνει. Επομένως, δεν υπάρχει ενδιάμεση λανθασμένη κατάσταση, είτε είναι στην κατάσταση A (εάν κάποια εντολή της συναλλαγής αποτύχει) είτε στην κατάσταση B (εάν η συναλλαγή είναι επιτυχής στο σύνολό της).

- **Επικύρωση και επαναφορά σε επίπεδο δικτύου:**

Κάθε διακομιστής NETCONF διατηρεί μια "βάση υποψηφίων" (παράλληλα με τη "βάση δεδομένων ρυθμίσεων εκτέλεσης"). Χρησιμοποιώντας αυτόν τον κατάλογο υποψήφιων δεδομένων, ένας διαχειριστής NETCONF μπορεί να εφαρμόσει μια συναλλαγή σε ολόκληρο το δίκτυο αποστέλλοντας μια παραμετροποίηση στον

υποψήφιο της κάθε συσκευής, επικυρώνοντας τον υποψήφιο, και εάν όλοι οι συμμετέχοντες είναι εντάξει, τους ενημερώνει να δεσμεύσουν τις αλλαγές. Εάν τα αποτελέσματα δεν είναι ικανοποιητικά, ο διαχειριστής μπορεί να ζητήσει την επαναφορά όλων των συσκευών.

- **Ολοκληρωμένη ενορχηστρωμένη ενεργοποίηση δικτύου:**

Υπάρχει διάκριση μεταξύ της διανομής μιας διαμόρφωσης σε όλες τις συσκευές δικτύωσης και της ενεργοποίησής της. Για παράδειγμα, εάν ο χειριστής θέλει να ρυθμίσει ένα VPN σε ένα δίκτυο συσκευών ταυτόχρονα, το NETCONF παρέχει την ευελιξία να διανείμει τη διαμόρφωση, να την επικυρώσει, να κλειδώσει όλες τις διαμορφώσεις συσκευών, να δεσμεύσει τη διαμόρφωση και να ξεκλειδώσει. Αυτό το σύνολο ενεργειών θα οδηγήσει στην ενεργοποίηση ενός VPN σε ολόκληρο το δίκτυο ταυτόχρονα, με ενορχηστρωμένο, συγχρονισμένο τρόπο.

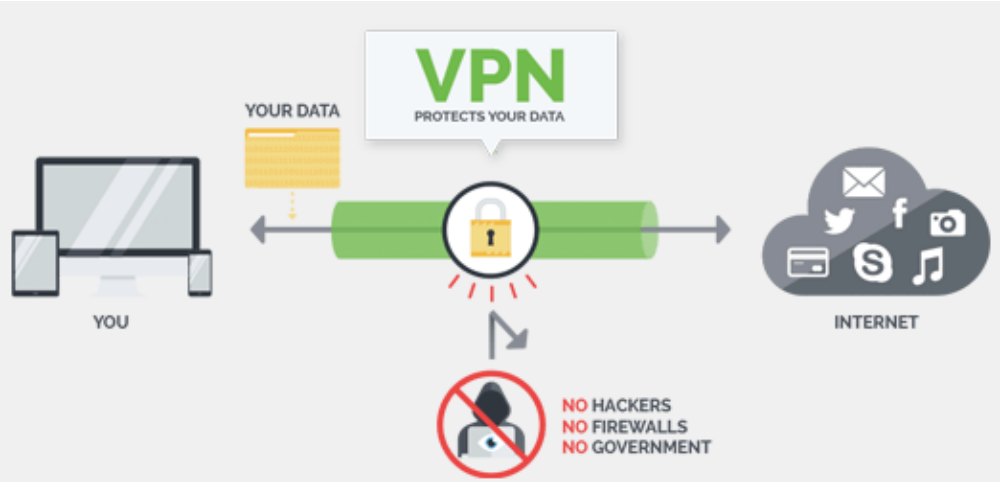
- **Αποθήκευση και επαναφορά των ρυθμίσεων:**

Ο διαχειριστής του NETCONF μπορεί να πραγματοποιήσει αντίγραφα ασφαλείας των ρυθμίσεων της συσκευής δικτύου, όποτε χρειάζεται και να το επαναφέρει στέλνοντας την αποθηκευμένη διαμόρφωση σε οποιαδήποτε συσκευή δικτύου [33].

2.3 VPN

Αναφερθήκαμε ελάχιστα προηγουμένως στα VPN. Θα ασχοληθούμε περισσότερο σε αυτήν την ενότητα για το ποια είναι, που χρησιμοποιούνται και πως ωφελούν στην διασύνδεση και στον διαμοιρασμό των δικτύων σε Wi-Fi συνδέσεις. Ένα **εικονικό ιδιωτικό δίκτυο** (συνήθως αναφέρεται σαν **VPN, Virtual Private Network**) είναι ένα δίκτυο που χρησιμοποιεί κατά κύριο λόγο δημόσια τηλεπικοινωνιακή υποδομή, όπως το Διαδίκτυο, και δίνει τη δυνατότητα σε απομακρυσμένα γραφεία ή σε χρήστες που ταξιδεύουν να έχουν πρόσβαση σε ένα κεντρικό οργανωτικό δίκτυο.

Ένα VPN συνήθως απαιτεί από τους απομακρυσμένους χρήστες του δικτύου πιστοποίηση, και συχνά ασφαλίζει τα δεδομένα με τεχνολογίες κρυπτογράφησης για να εμποδιστεί η διάδοση των ιδιωτικών πληροφοριών σε μη εξουσιοδοτημένους τρίτους. Ένα VPN μπορεί να δημιουργείται για τη λειτουργικότητα του δικτύου που βρίσκεται σε οποιοδήποτε δίκτυο, όπως η κοινή χρήση των δεδομένων και η πρόσβαση σε πόρους δικτύου, εκτυπωτές, βάσεις δεδομένων, ιστοσελίδες, κλπ. [58].



Εικόνα 2-7: VPN

Ένας χρήστης VPN αντιμετωπίζει συνήθως το κεντρικό δίκτυο με τρόπο που είναι ταυτόσημος με το να συνδέεται άμεσα με το κεντρικό δίκτυο. Η τεχνολογία VPN μέσω του κοινόχρηστου διαδικτύου έχει αντικαταστήσει την ανάγκη διατήρησης ακριβών μισθωμένων γραμμών τηλεπικοινωνιακών κυκλωμάτων σε ευρείες περιοχές εγκαταστάσεων του δικτύου. Η τεχνολογία VPN μειώνει το κόστος, επειδή δεν χρειάζεται φυσική μισθωμένη γραμμή για τη σύνδεση απομακρυσμένων χρηστών σε ένα intranet.

Αν και απλό στην περιγραφή του, ένα VPN έχει πολλές διαφορετικές χρήσεις:

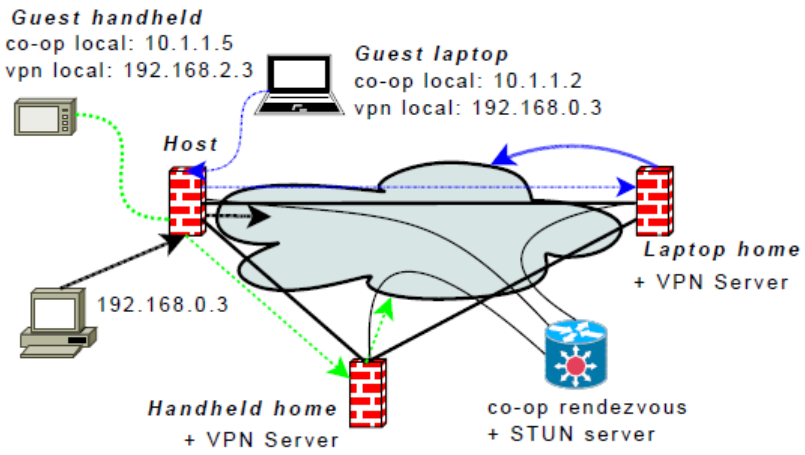
- **Ασφαλής πρόσβαση στο δίκτυο της εργασίας μας εξ' αποστάσεως**: Χρήστες που ταξιδεύουν συχνά και δεν βρίσκονται στον χώρο τους, μπορούν να χρησιμοποιήσουν VPN στημένο στην επιχείρησή τους, προκειμένου να έχουν πρόσβαση σε όλους τους τοπικούς πόρους.
- **Ασφαλής πρόσβαση στο οικιακό μας δίκτυο εξ' αποστάσεως**: Αν κάποιος θέλει να στήσει ένα VPN στο σπίτι του, θα μπορεί από οπουδήποτε να έχει

πρόσβαση σε υπηρεσίες, να κατεβάσει υλικό, είτε να παίξει παιχνίδια μέσω ίντερνετ σαν να ήταν στο ίδιο τοπικό δίκτυο LAN.

- **Απόκρυψη της δραστηριότητάς μας από το τοπικό δίκτυο ή τον ISP μας**: Στην ελεύθερη σύνδεση Wi-Fi (δημόσια ή ιδιωτική), σε όποια σελίδα μπαίνει κανείς που δεν είναι ασφαλής HTTP (HTTPS), όλη η δραστηριότητα είναι εμφανής σε οποιονδήποτε ενδιαφέρεται να κοιτάξει. Ενώ, αν συνδεθεί κανείς σε ένα VPN, το μόνο που θα φαίνεται είναι η ασφαλής σύνδεση με το VPN, και όλα τα άλλα δεδομένα θα παραμείνουν κρυμμένα στο VPN. Ούτε ο ISP δεν θα ξέρει τις κινήσεις του χρήστη μέσω VPN.
- **Παράκαμψη Τοπικής Λογοκρισίας**: Συνδεδεμένοι με ένα VPN μπορεί κανείς να πλοηγηθεί ελεύθερα, όπου θέλει και σε όποια σελίδα επιθυμεί, δίχως να χρειάζεται να του μπλοκάρουν την πρόσβαση [3].

2.3.1 Σήραγγα

Εμπόδια του παρόχου και του επισκέπτη σύνδεσης μπορούν να επιλυθούν εάν η μοναδική πρόσβαση που παρέχεται στον επισκέπτη είναι μία **σήραγγα (tunnel)** σε ένα σημείο στο Διαδίκτυο που εμπιστεύεται ο επισκέπτης. Οι κοινές πρακτικές ασφάλειας δικτύων θα συνεχιστούν στο τέλος του κεντρικού υπολογιστή του παρόχου, συμπληρώνοντας τις σήραγγες. Για βασική προστασία από κακόβουλους επισκέπτες, τα τείχη προστασίας πρέπει να ενεργοποιούνται στον ασύρματο δρομολογητή ή/και στους υπολογιστές του παρόχου. Ορισμένοι ασύρματοι δρομολογητές όπως εμπορικοί (π.χ. FON) και ανοιχτού κώδικα λογισμικού (π.χ. DD-WRT) επιτρέπουν τον καθορισμό ορίων εύρους ζώνης.



Εικόνα 2-8: Μοντέλο σήραγγας

Η επισκεψιμότητα επισκεπτών μεταφέρεται στον πάροχο μέσω σήραγγας. Το τελικό άκρο της σήραγγας του παρόχου είναι ένας διακομιστής VPN και πιστοποιεί τους επισκέπτες. Το άκρο του παρόχου είναι ένα τείχος προστασίας επιτρέποντας μόνο πακέτα με εγχώρια πρόσβαση. Ένας STUN διακομιστής βοηθά στην δημιουργία σηράγγων όταν τα μέλη βρίσκονται πίσω από **μεταφραστή διευθύνσεων δικτύου (Network Address Translation –NAT)**. Οι επισκέπτες απευθύνονται διαμέσου μίας σταθερής τοπικής διεύθυνσης IP στο δίκτυο του παρόχου και μίας VPN τοπικής διεύθυνσης IP στο οικιακό τους δίκτυο. Και οι δύο διευθύνσεις μπορούν να επαναχρησιμοποιηθούν εκτός του πεδίου εφαρμογής τους [6].

Οι επισκέπτες δεν θα πρέπει να επιτρέπεται να χρησιμοποιούν τον ξένο πάροχο ως εναλλακτικό σημείο πρόσβασης στο ίντερνετ, κυρίως για να αποφεύγουν περιορισμούς που μπορεί να είναι στον χώρο τους ή σε άλλο προεπιλεγμένο σημείο πρόσβασης. Αυτοί οι περιορισμοί περιλαμβάνουν τους όρους παροχής υπηρεσιών του οικιακού ISP ή αποδεκτές πολιτικές χρήσης, όπως επίσης και κάθε οικογενειακού ελέγχου λογισμικό που είναι βασισμένο σε δρομολογητή.

Μία σήραγγα δεν επιλύει άμεσα αυτό το πρόβλημα. Αντιθέτως, εκχωρεί αυτή την ευθύνη στο τελικό σημείο απομακρυσμένης σήραγγας. Ο λόγος είναι ότι εάν ο επισκέπτης έχει το δικαίωμα πρόσβασης στο Διαδίκτυο από ένα σημείο, τότε αυτό το σημείο θα πρέπει να έχει την ευθύνη και την εξουσία για να περιορίσει την πρόσβαση στο περιεχόμενο.

Με τον μηχανισμό των σηράγγων, η κίνηση από τον επισκέπτη δια μέσου οποιοδήποτε παρόχου τελικά οδηγείται μέσω ενός μόνο κομβικού σημείου, του σπιτιού του παρόχου. Αυτό περιορίζει την ενίσχυση που ένας κακόβουλος επισκέπτης μπορεί να επιτύχει καλύτερο εύρος ζώνης από το ήδη διαθέσιμο στο σπίτι. Με μία σήραγγα, ο επισκέπτης εκτίθεται μόνο στον δικό του ISP και η πρόσβαση σε υπηρεσίες υψηλής ποιότητας δεν διαρρέει [6].

Ο εξαναγκασμός του επισκέπτη να δημιουργήσει μία ασφαλή σήραγγα καταργεί την ικανότητα του παρόχου να εποπτεύει δραστηριότητες παραβίασης, η οποία μπορεί να αποτελεί νομική ευθύνη για έναν πάροχο σημείου πρόσβασης. Έτσι, είναι προς το συμφέρον του επισκέπτη να έχει πρόσβαση στο δημόσιο Διαδίκτυο μέσω μιας σήραγγας του δικού του ISP, του οποίου οι όροι υπηρεσίας είναι γνωστοί σε αυτόν.

Η αναγκαστική πρόσβαση μέσω του οικείου δικτύου του επισκέπτη βελτιώνει επίσης της υπευθυνότητα στις καταστάσεις αντιστοίχισης IP, αφού ο οικείος κόμβος είναι πλέον μέρος οποιασδήποτε διαδρομής ανίχνευσης και μπορούν να επιβληθούν νομικά δεσμευτικοί όροι υπηρεσίας του δικού του ISP. Πολλοί ISP έχουν όρους υπηρεσίας που απαγορεύουν την επαναπώληση συνδεσιμότητας στο Διαδίκτυο. Με τον περιορισμό της επισκεψιμότητας κίνησης σε μία σήραγγα, ο πάροχος είναι σε θέση να διαμοιράζει το Wi-Fi χωρίς να μοιράζεται βασικές υπηρεσίες που παρέχονται από τον ISP, όπως αναζητήσεις DNS, προκαθορισμένες διαδρομές ή εκχωρήσεις διευθύνσεων IP.

Επίσης, δεδομένου ότι η σήραγγα είναι κρυπτογραφημένη, όλοι εκτός από τον επισκέπτη και τον πάροχο θα αντιληφθούν την κίνηση του επισκέπτη ως προερχόμενη από τον χώρο του. Η ίδια κυκλοφορία σήραγγας θα εμφανιστεί παρόμοια με τις ροές από ομότιμους χρήστες, όπως το bittorrent και το skype που ήδη υπάρχουν στο Διαδίτκυο. Ακόμα και έτσι, οι ISPs έχουν πολύ έλεγχο από τότε που θα μπορούσαν να απαγορεύσουν συμβατικά την κυκλοφορία της κίνησης ή να επηρεάσουν την προθυμία του παρόχου για να διαμοιράζεται το Wi-Fi αλλάζοντας το μοντέλο τιμολόγησης. Σε πρακτικές καταστάσεις, οι συνεταιρισμοί θα μπορούσαν να χωρίσουν το κόστος της ένταξης με τους ISPs για να μεταφέρουν την κυκλοφορία της σήραγγας.

2.3.2 NAT

Η **μετάφραση διεύθυνσης δικτύου (Network Address Translation – NAT)** είναι ειδικό πρωτόκολλο που εκτελούν οι πύλες (gateways) και έχει σαν αποτέλεσμα να αλλάζει την IP διεύθυνση ενός πακέτου που ξεκινά από έναν υπολογιστή εντός του τοπικού δικτύου και προωθείται εκτός του δικτύου [16].

Πιο συγκεκριμένα, το NAT δουλεύει ως εξής: Κάθε υπολογιστής ενός ιδιωτικού δικτύου που ζητάει να συνδεθεί με κάποιον εκτός δικτύου, κάνει αίτηση στον μεταφραστή διεύθυνσης δικτύου (που υπάρχει στην πύλη (gateway ή firewall)) για να πάρει μία νέα διεύθυνση. Το NAT διαθέτει ένα σύνολο διαθέσιμων IP διευθύνσεων (address pool) και μία από αυτές τις αναθέτει στον υπολογιστή. Ταυτόχρονα, κρατάει μία βάση δεδομένων στην οποία καταγράφει τη διεύθυνση που απέδωσε σε κάθε υπολογιστή (διαδικασία MAP). Έτσι, κάθε πακέτο που φεύγει από τον υπολογιστή του ιδιωτικού δικτύου και «ταξιδεύει» στο Διαδίκτυο έχει σαν διεύθυνση αποστολέα τη νέα αυτή διεύθυνση.

Αντίστροφα, κάθε υπολογιστής που θέλει να στείλει δεδομένα στον συγκεκριμένο υπολογιστή του ιδιωτικού δικτύου, στέλνει πακέτα με διεύθυνση παραλήπτη τη νέα διεύθυνση. Το NAT είναι πάλι υπεύθυνο σε αυτήν την περίπτωση για να παραλάβει ο υπολογιστής τα πακέτα που προορίζονται για αυτόν: συγκεκριμένα, το NAT κοιτάει τη βάση 45 δεδομένων και βλέπει ποια είναι η πραγματική IP διεύθυνση του υπολογιστή (δηλαδή η διεύθυνση που έχει στο ιδιωτικό του δίκτυο) και με βάση αυτήν την πληροφορία, δρομολογεί τα εισερχόμενα πακέτα.

Ένα πρότυπο που βρίσκει εφαρμογή σε τοπικά δίκτυα των οποίων οι υπολογιστές μοιράζονται μια κοινή σύνδεση ίντερνετ εκτός από το NAT, είναι και η προώθηση θυρών (port forwarding). Το NAT, ορίζει σε κάθε ηλεκτρονικό υπολογιστή του τοπικού δικτύου μια διαφορετική εσωτερική διεύθυνση IP, της μορφής 192.168.x.x ή 10.1.x.x και μια κοινή εξωτερική IP με την οποία αναγνωρίζονται από άλλα συστήματα συνδεμένα στο ίντερνετ [24].

Το NAT βρίσκει εφαρμογή σε ιδιωτικά και εταιρικά δίκτυα που συνδέονται στο ίντερνετ μέσω δρομολογητών και συνδέσεων ADSL ή μισθωμένων γραμμών. Πολλές φορές ο διαχειριστής των δικτύων αυτών θα πρέπει να ρυθμίσει κατάλληλα τους κανόνες NAT, ώστε να είναι εφικτή η πρόσβαση από το ίντερνετ σε υπηρεσίες

και εφαρμογές που εκτελούνται σε συγκεκριμένο υπολογιστή του εσωτερικού δικτύου. Η ρύθμιση αυτή ονομάζεται port forwarding. Επειδή όλοι οι ηλεκτρονικοί υπολογιστές εμφανίζονται στο Διαδίκτυο με την ίδια διεύθυνση IP, ένας κανόνας NAT ή port forwarding καθορίζει σε ποιον από όλους θα πρέπει να αναζητηθεί μια συγκεκριμένη υπηρεσία. Αυτό γίνεται με την αντιστοίχιση της θύρας της εν λόγω υπηρεσίας (π.χ. port 80 για HTTP server) στην εσωτερική διεύθυνση του υπολογιστή του τοπικού δικτύου όπου αυτή εκτελείται [6].

2.3.3 Απομόνωση κίνησης

Η εικονικοποίηση του δικτύου βελτιώνει την κατανομή πόρων, επιτρέπει στους φορείς εκμετάλλευσης να ελέγχουν το δίκτυό τους πριν από τις αλλαγές και επιτρέπει στους ανταγωνιστικούς πελάτες να μοιράζονται τον ίδιο εξοπλισμό με ελεγχόμενο και απομονωμένο τρόπο. Κρίσιμα, εικονικά δίκτυα υπόσχονται επίσης να παρέχουν ένα ασφαλές και ρεαλιστικό περιβάλλον να αναπτύξουν και να αξιολογήσουν πειραματικά πρωτόκολλα [28].

Τα VLAN χρησιμοποιούνται για την εικονικοποίηση του πίνακα γεφύρωσης των μεταγωγών επιπέδου 2 και για τη δημιουργία εικονικών μεταγωγικών τοπολογιών που επικαλύπτουν το φυσικό δίκτυο. Η κυκλοφορία που ταξιδεύει σε μία τοπολογία (π.χ. VLAN) δεν μπορεί να διαπερνά μια άλλη τοπολογία. Με αυτόν τον τρόπο, η επισκεψιμότητα από μια ομάδα χρηστών ή συσκευών μπορεί να παραμείνει απομονωμένη από άλλους χρήστες ή συσκευές.

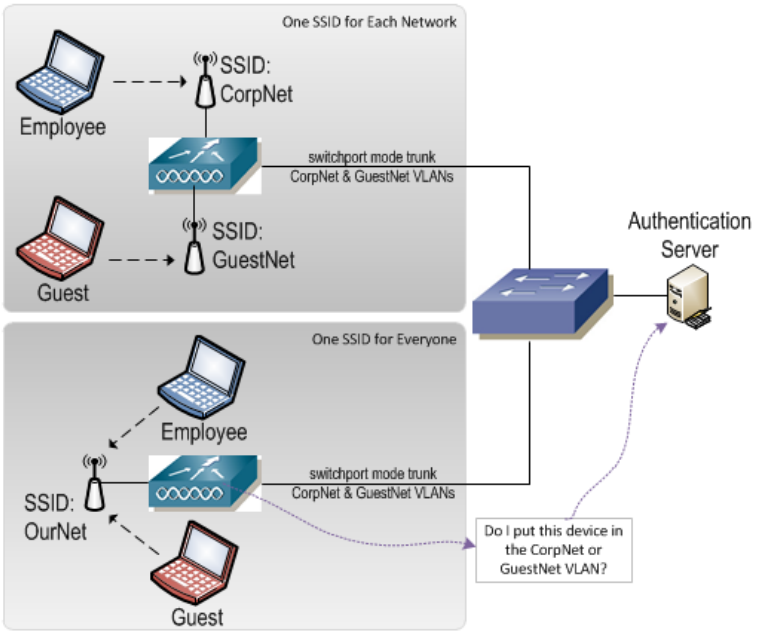
Υπάρχει ένας τρόπος για να διατηρηθεί η απομόνωση της κυκλοφορίας μεταξύ των συσκευών του επιπέδου 3. Ονομάζεται **εικονική δρομολόγηση και προώθηση (Virtual Routing and Forwarding –VRF)**. Η VRF επιτρέπει τον εικονικοποίηση του πίνακα δρομολόγησης σε ένα διακόπτη επιπέδου 3 ή δρομολογητή. Κάθε εικονικός πίνακας περιέχει το δικό του μοναδικό σύνολο καταχωρήσεων προώθησης. Η κυκλοφορία που εισέρχεται σε δρομολογητή θα προωθηθεί χρησιμοποιώντας τον πίνακα δρομολόγησης που συσχετίζεται με το ίδιο VRF με τον οποίο συνδέεται η διεπαφή εισόδου και αποστέλλεται μια διεπαφή εξόδου που σχετίζεται με το ίδιο VRF. Όπως τα VLAN, τα VRF εξασφαλίζουν τη λογική απομόνωσης της κυκλοφορίας καθώς διασχίζουν μια κοινή υποδομή φυσικού δικτύου.

Η χρήση των VRF εστιάζει κυρίως στα ακόλουθα στοιχεία:

- **Έλεγχο πρόσβασης:**

Ο έλεγχος πρόσβασης αναφέρεται στον τρόπο προσδιορισμού των τερματικών συσκευών και στην κατάτμηση στην άκρη του δικτύου (γνωστός και ως στρώμα πρόσβασης). Οι χρήστες πρέπει να είναι κατακερματισμένοι πριν εισάγουν την κυκλοφορία στο δίκτυο, έτσι ώστε το δίκτυο να γνωρίζει ποιο εικονικό δίκτυο θα συνδέσει την κυκλοφορία του.

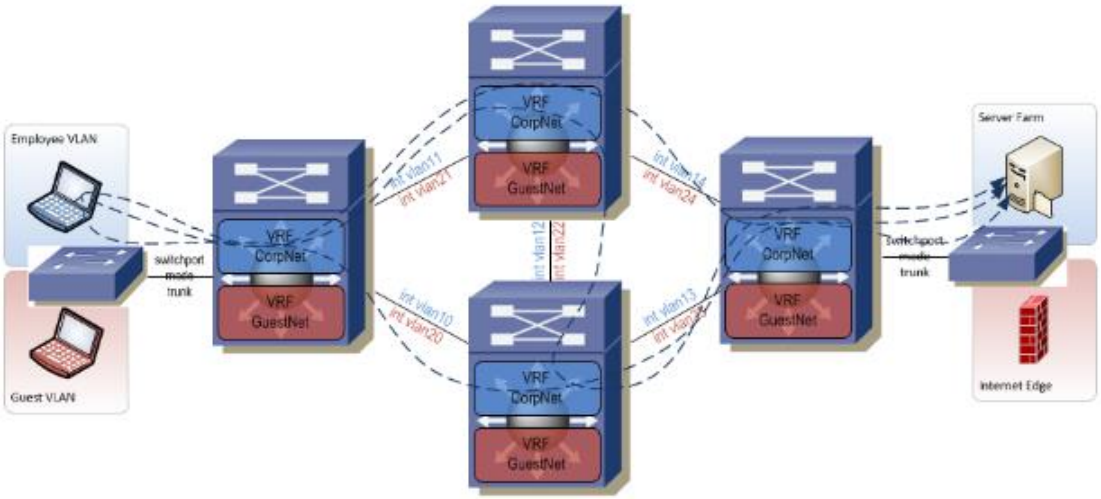
Στα ασύρματα δίκτυα οι συσκευές τερματισμού μπορούν να κατατμηθούν μέσω ξεχωριστών SSID για διαφορετικές ομάδες χρηστών. Μπορεί να δημιουργηθεί ένα SSID για τους παρόχους, τους επισκέπτες και τους διαμοιραστές, το καθένα από τα οποία δεσμεύεται στο δικό του VLAN στην πλευρά ανερχόμενης ζεύξης του ασύρματου ελεγκτή. Μηχανισμοί όπως το 802.1X μπορούν επίσης να χρησιμοποιηθούν σε ασύρματες συνδέσεις για τη σύνδεση μιας τελικής συσκευής με ένα συγκεκριμένο VLAN αφού συνδεθεί με το ασύρματο δίκτυο.



Εικόνα 2-9: Έλεγχος πρόσβασης

- **Απομόνωση διαδρομής:**

Μια πιο κλιμακωτή εναλλακτική λύση για το hop-by-hop είναι η ενθυλάκωση της κυκλοφορίας κάθε VRF μέσα σε μια σήραγγα. Δεδομένου ότι μια σήραγγα μπορεί να παρέχεται απευθείας μεταξύ δύο άκρων δρομολογητών, τίποτα δεν χρειάζεται να αγγίξει στον πυρήνα του δικτύου. Στην πραγματικότητα, τα VRF δεν χρειάζεται καν να παρέχονται στον πυρήνα του δικτύου (υποθέτοντας ότι δεν υπάρχουν συσκευές ακμής συνδεδεμένες με τον πυρήνα). Αυτό απλοποιεί την παροχή διαδρομών μέσω του δικτύου και εξαλείφει τον κίνδυνο σφάλματος σε έναν κεντρικό δρομολογητή κατά τη διάρκεια της παροχής. Εάν προβλέπεται σωστά, μια σήραγγα παρέχει επίσης ενσωματωμένο πλεονασμό διαδρομής (σε αντίθεση με το hop-by-hop το οποίο πρέπει να υπολογιστεί χειροκίνητα).

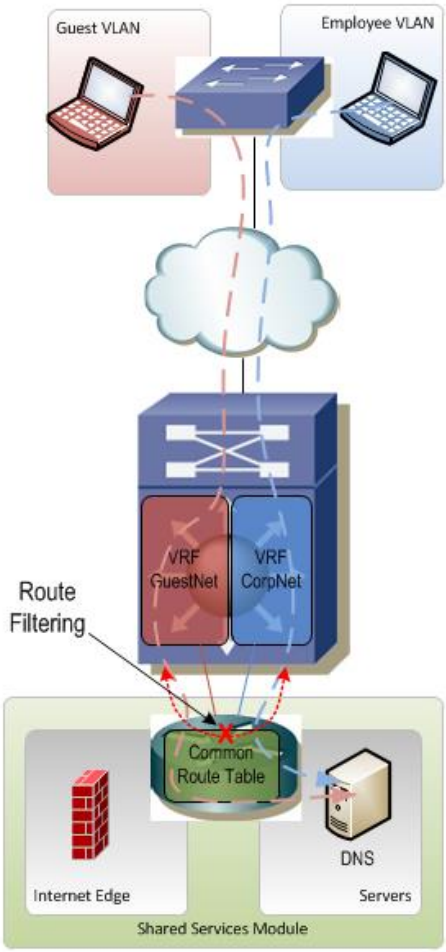


Εικόνα 2-10: Απομόνωση διαδρομής

- **Μοιραζόμενες υπηρεσίες:**

Οι υπηρεσίες κοινής χρήσης βρίσκονται συνήθως στη δική τους μικρή μονάδα που κρέμεται από την άκρη του δικτύου. Αυτή η ενότητα είναι ένα από τα πιο δύσκολα τμήματα ενός δικτύου με δυνατότητα VRF, επειδή είναι πολύ εύκολο να επιτρέψει κατά λάθος να διαρρεύσει κυκλοφορία μεταξύ VRFs εάν δεν ληφθούν σωστά μέτρα. Δεδομένου ότι οι διακομιστές και οι συσκευές ακροδεκτών του διαδικτύου που βρίσκονται στην ενότητα κοινόχρηστων υπηρεσιών πρέπει να επικοινωνήσουν με συσκευές τερματισμού σε όλα τα VRF, αυτό το μοντέλο πρέπει να περιέχει διαδρομές για όλα τα VRF. Θα ήταν πολύ εύκολο να επιτρέψουμε τυχαία τις διαδρομές από το

VRF A να διαφημίζονται μέσω της μονάδας κοινόχρηστων υπηρεσιών σε VRF B (και αντίστροφα) επιτρέποντας έτσι στις συσκευές A και B να επικοινωνούν ελεύθερα [58].



Εικόνα 2-11: Μοιραζόμενες υπηρεσίες

2.4 Τεχνολογίες κρυπτογράφησης

Η κρυπτογράφηση είναι ένα από τα πιο σημαντικά βήματα για την εξασφάλιση του δικτύου Wi-Fi, επομένως δεν είναι κάτι που πρέπει να παραλείψει κάποιος. Όταν ενεργοποιεί κανείς την κρυπτογράφηση, το δίκτυο Wi-Fi απαιτεί έναν κωδικό πρόσβασης, έτσι ώστε να μην μπορεί κανείς άλλος να συνδεθεί [13]. Ωστόσο, δεν είναι μόνο ο κωδικός πρόσβασης που είναι σημαντικός, αλλά και ο τύπος κρυπτογράφησης.

Υπάρχουν πολλές επιλογές που μπορεί να υποστηρίξει ο δρομολογητής όταν πρόκειται για ασύρματη κρυπτογράφηση. Αν χρησιμοποιείται μια ξεπερασμένη

μέθοδο κρυπτογράφησης, οι εισβολείς δεν χρειάζονται καν τον κωδικό του χρήστη, επειδή μπορούν να σπάσουν την παλιά κρυπτογράφηση.

Εφόσον τα δημόσια hotspots γενικά δεν χρησιμοποιούν κρυπτογράφηση, θα πρέπει να υποθέσει κανείς , ότι ο καθένας μπορεί να δει την επισκεψιμότητά του στο Διαδίκτυο, εκτός εάν λάβει προφυλάξεις.

- Να βεβαιωθεί ότι είναι νόμιμο hotspot. Υπάρχουν άνομοι τύποι που έχουν στηθεί σε πειρατικούς δρομολογητές με γνωστά SSID ονόματα και στη συνέχεια τα χρησιμοποιούν για να καταγράψουν τις ανυποψίαστες πληροφορίες σύνδεσης των χρηστών και άλλα ιδιωτικά δεδομένα.
- Να βεβαιωθεί ότι το τείχος προστασίας λογισμικού του υπολογιστή του χρήστη είναι ενεργοποιημένο και ότι η λειτουργία κοινής χρήσης αρχείων των Windows είναι απενεργοποιημένη.
- Να μην στέλνει τραπεζικούς κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών, εμπιστευτικά μηνύματα ηλεκτρονικού ταχυδρομείου ή άλλα ευαίσθητα δεδομένα, εκτός εάν είναι βέβαιος κανείς ότι βρίσκεται σε ασφαλή τοποθεσία. Καλό είναι να αναζητήσει κανείς το εικονίδιο κλειδώματος στην κάτω δεξιά γωνία του προγράμματος περιήγησης, καθώς και ένα URL στην γραμμή διευθύνσεων που ξεκινά με το https. Τέτοιες τοποθεσίες ενσωματώνουν την δική του κρυπτογράφηση.
- Πάντα να απενεργοποιεί κανείς την συχνότητα Wi-Fi όταν δεν είναι σε ένα hotspot. Ο λόγος είναι, ότι οι χάκερ μπορούν να το χρησιμοποιήσουν για να δημιουργήσουν συνδέσεις Wi-Fi από ομότιμους χρήστες με τον υπολογιστή του και να έχουν απευθείας πρόσβαση [15].

Η πρώτη γραμμή υπεράσπισης για το δίκτυό Wi-Fi είναι η κρυπτογράφηση, η οποία κωδικοποιεί τα δεδομένα που μεταδίδονται μεταξύ του υπολογιστή ή των άλλων ασύρματων συσκευών και του ασύρματου δρομολογητή. Δυστυχώς, οι περισσότεροι δρομολογητές δρομολογούν τα πακέτα με απενεργοποιημένη κρυπτογράφηση και πολλοί χρήστες δεν την ενεργοποιούν, αφήνοντας τους εαυτούς τους πλήρως εκτεθειμένους. Εάν δεν το έχει κάνει ήδη, θα πρέπει να ενεργοποιήσει την κρυπτογράφηση του δρομολογητή του και να χρησιμοποιήσει ισχυρότερη μορφή που

υποστηρίζει το δίκτυό του. Υπάρχουν 2 ειδών πρωτόκολλα, το πρωτόκολλο ασύρματης κρυπτογράφησης (WEP) που είναι λιγότερο ασφαλές και το πρωτόκολλο ασύρματης προστατευμένης πρόσβασης (WPA), με πιο πρόσφατο το WPA2.

2.4.1 WEP

Το **πρωτόκολλο ασύρματης κρυπτογράφησης (Wireless Equivalent Privacy –WEP)**, αποτελεί την παλαιότερη μέθοδο κρυπτογράφησης δεδομένων, μόνο που επειδή η τεχνολογία είναι παλαιότερη δεν την καθιστά και καλύτερη. Πρακτικά το WEP μπορεί να προστατεύσει το δίκτυο κάποιου χρήστη από τις βασικότερες μόνο επιθέσεις και να εγγυηθεί απλώς πως κάποιος τυχαίος που δεν γνωρίζει τον κωδικό πρόσβασης, δεν θα είναι σε θέση να συνδεθεί σε αυτό. Λίγες στοιχειώδεις γνώσεις να διαθέτει όμως αυτός ο «κάποιος τυχαίος» και η ασφάλεια του δικτύου του θα είναι σε κίνδυνο [13].

2.4.2 WPA2

Το **πρωτόκολλο ασύρματης προστατευμένης πρόσβασης (Wireless Protected Access –WPA)**, καθώς και η επέκτασή του **WPA2** αποτελεί τον διάδοχο του WEP αφού ουσιαστικά αναπτύχθηκε ακριβώς για να διορθώσει τις ατέλειές του. Θα πρέπει να βεβαιωθεί κάποιος ότι έχει αλλάξει το προεπιλεγμένο όνομα δικτύου και τον κωδικό πρόσβασης του δρομολογητή του. Με αυτόν τον τρόπο θα είναι πιο δύσκολο για του επιτιθέμενους να έχουν πρόσβαση στον δρομολογητή του και να χειριστούν τις ρυθμίσεις του.

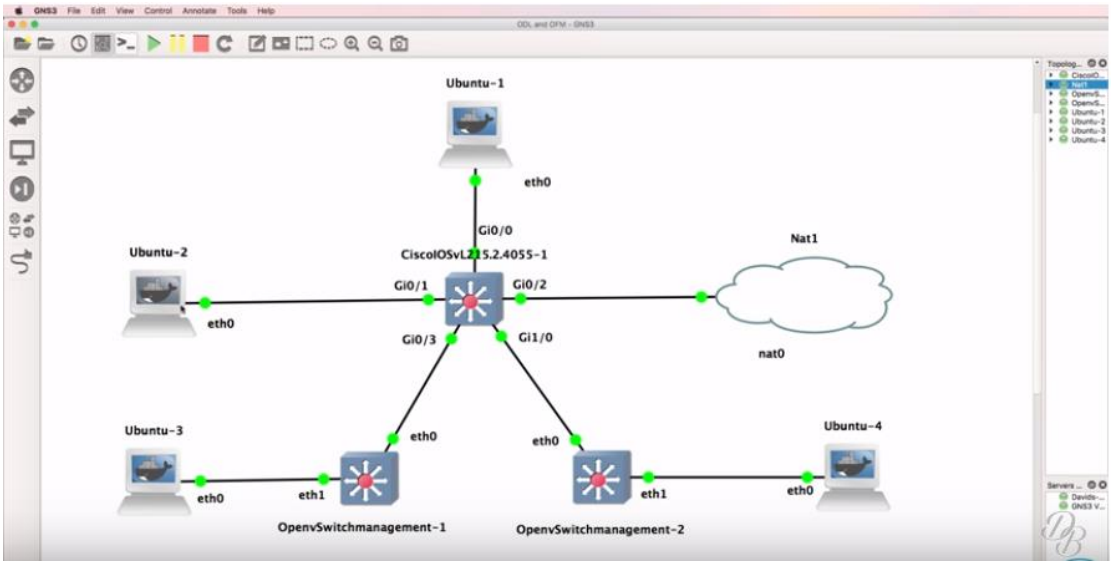
Αν κάποιος έχει παλαιότερο δρομολογητή που υποστηρίζει μόνο WEP, θα είναι ασφαλέστερο εάν χρησιμοποιήσει κλειδιά WEP 128-bit -, αλλά επίσης θα πρέπει να ελεγχθεί η τοποθεσία Web του κατασκευαστή για μια ενημέρωση λογισμικού που θα προσθέσει υποστήριξη WPA. Αν δεν είναι πιθανή μια τέτοια ενημέρωση, θα πρέπει να αντικατασταθούν παλιοί προσαρμογείς και δρομολογητές με νεότερα μοντέλα που υποστηρίζουν WPA. Καλύτερη επιλογή θα ήταν ο δρομολογητής να υποστηρίζει την υβριδική λειτουργία WPA + WPA2, η οποία επιτρέπει την χρησιμοποίηση ισχυρότερης κρυπτογράφηση WPA2 με προσαρμογείς που την υποστηρίζουν, διατηρώντας ταυτόχρονα τη συμβατότητα με τους προσαρμογείς WPA [13].

2.5 Εφαρμογές

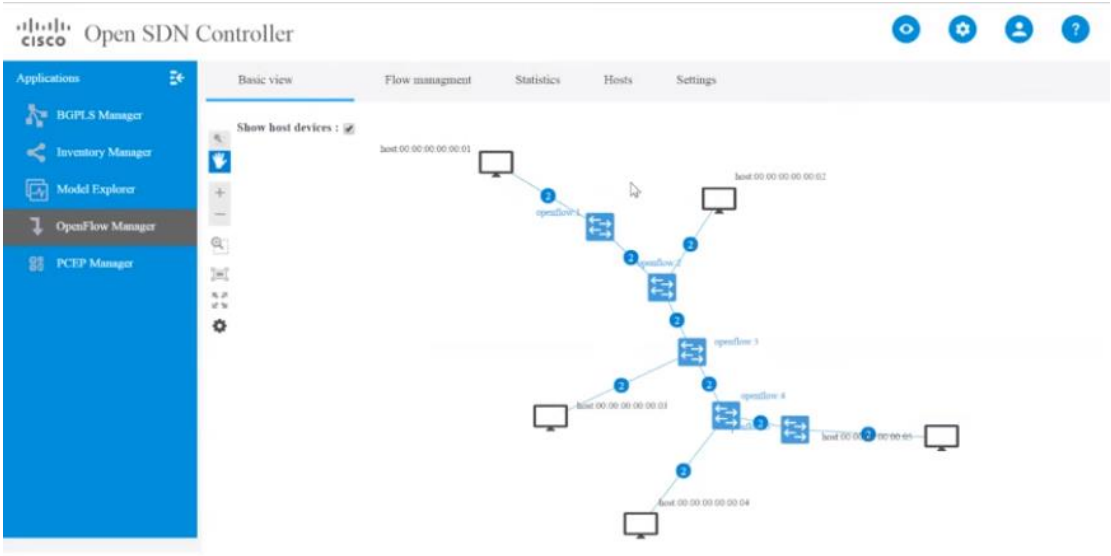
2.5.1 OpenFlow

Όπως είδαμε και αναφερθήκαμε και παραπάνω, εκτός από τις ενέργειες τεμαχισμού της πληροφορίας, χωρίζοντάς την σε κομμάτια, το OpenFlow είναι υπεύθυνο για τον σωστό διαμοιρασμό των δεδομένων ,χρησιμοποιώντας μεθόδους απομόνωσης και βελτιώνοντας έτσι τη ροή και την κίνηση στο Διαδίκτυο, προσφέροντας συνάμα και ασφάλεια στο δίκτυο του εκάστοτε παρόχου και επισκέπτη [25].

Μία εφαρμογή που μπορεί κανείς να διαχειριστεί τις συσκευές, να δει την κίνηση και με διάφορες παραμέτρους να μελετήσει περισσότερο ή να στήσει ένα εικονικό δίκτυο είναι μέσω της εφαρμογής OpenFlow Manager –OFM της Cisco ή του Open SDN Controller. Παρακάτω βλέπουμε ενδεικτικές εικόνες των εφαρμογών.



Εικόνα 2-12: OpenFlow

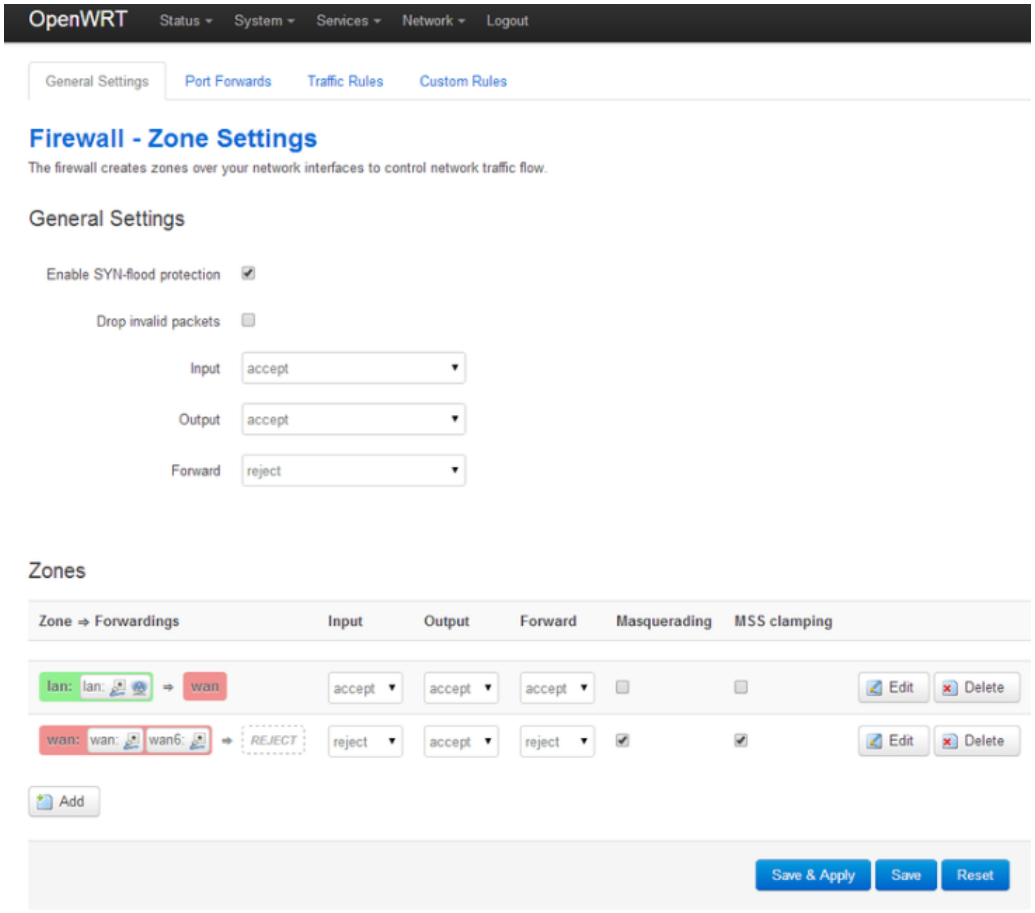


Εικόνα 2-13: Open SDN Controller

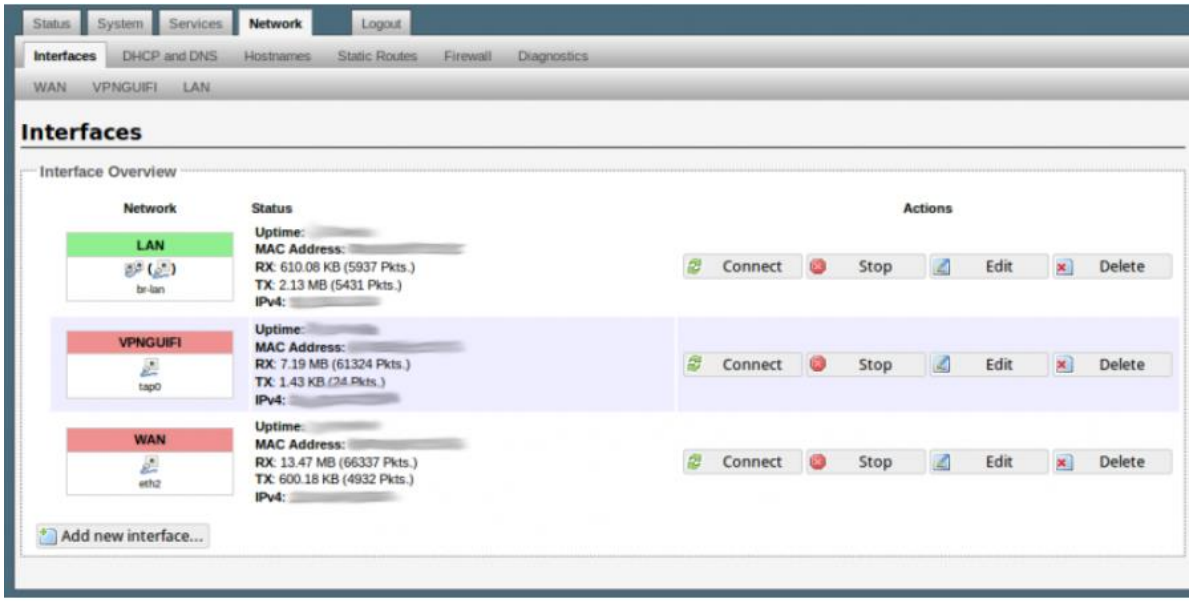
2.5.2 OpenWrt

Το OpenWrt είναι ένα λογισμικό που βασίζεται σε Linux. Λειτουργεί καλύτερα σε ένα δρομολογητή και διανέμει ενσωματωμένες συσκευές. Δεν λειτουργεί ως στατικό λογισμικό/ Οι χρήστες μπορούν να χειριστούν το OpenWrt και να διαμορφώσουν διαφορετικά είδη πράξεων και υπηρεσιών [41].

Με την χρήση του λογισμικού μπορεί κάποιος ρυθμίζοντας τις IP διευθύνσεις και αλλάζοντας τις επιλογές για το LAN ή WAN της σύνδεσης να δοκιμάσει να στείλει και να λάβει πακέτα, με τέτοιον τρόπο έτσι ώστε να ελέγχεται ο διαμοιρασμός των δεδομένων, να λάβει μετρήσεις και να αναλύσει περισσότερο τα αποτελέσματα. Ενδεικτικές εικόνες της συγκεκριμένης εφαρμογής είναι οι ακόλουθες.



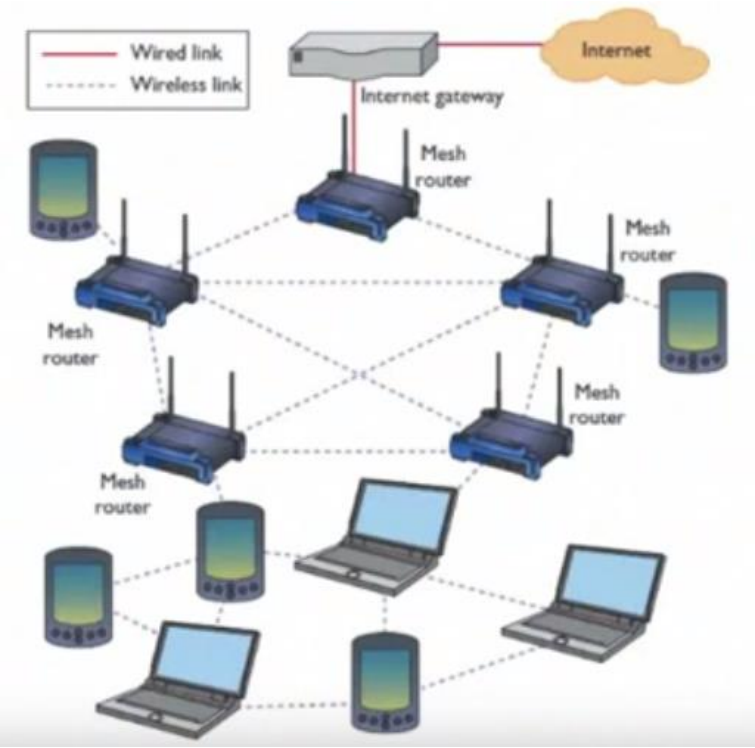
Εικόνα 2-14: OpenWrt



Εικόνα 2-15: OpenWrt διεπαφές

3 Δίκτυα πλέγματος (Mesh networks)

Ένα **ασύρματο δίκτυο πλέγματος (Wireless Mesh Network –WMN)** είναι ένα δίκτυο επικοινωνιών αποτελούμενο από ραδιοζεύκτες που οργανώνονται σε μια τοπολογία πλέγματος. Είναι ακόμα, μία μορφή ασύρματου δικτύου ad hoc. Ένα πλέγμα αναφέρεται σε πλούσια διασύνδεση μεταξύ συσκευών ή κόμβων. Τα δίκτυα ασύρματων δικτύων αποτελούνται συχνά από πελάτες πλέγματος, πλέγματος δρομολογητές και πύλες. Η κινητικότητα των κόμβων είναι λιγότερο συχνή. Εάν οι κόμβοι μετακινούνται συνεχώς ή συχνά, το πλέγμα δαπανά περισσότερο χρόνο για την ενημέρωση διαδρομών παρά για την παράδοση δεδομένων [20].



Εικόνα 3-1: Δίκτυο πλέγματος (Mesh)

Σε ένα ασύρματο δίκτυο πλέγματος, η τοπολογία τείνει να είναι πιο στατική, έτσι ώστε οι υπολογισμοί των διαδρομών να μπορούν να συγκλίνουν και να είναι εφικτή η παράδοση των δεδομένων στους προορισμούς τους. Ως εκ τούτου, πρόκειται για κεντρική μορφή δικτύου ad hoc με χαμηλή κινητικότητα. Ακόμα, επειδή μερικές φορές βασίζεται σε στατικούς κόμβους για να λειτουργήσουν ως πύλες, δεν είναι ένα πραγματικά αμιγώς ασύρματο ad hoc δίκτυο [43].

Οι πελάτες πλέγματος είναι συχνά υπολογιστές, κινητά τηλέφωνα και άλλες ασύρματες συσκευές. Οι δρομολογητές πλέγματος προωθούν την κίνηση σε και από πύλες, οι οποίες μπορούν, αλλά δεν χρειάζεται να είναι συνδεδεμένες στο ίντερνετ. Η περιοχή κάλυψης όλων των κόμβων συχνοτήτων που λειτουργούν σα ένα δίκτυο καλείται μερικές φορές σύννεφο πλέγματος. Η πρόσβαση σε αυτό το σύννεφο πλέγματος εξαρτάται από του κόμβους συχνοτήτων που εργάζονται μαζί για να δημιουργήσουν ένα ασύρματο δίκτυο[47].

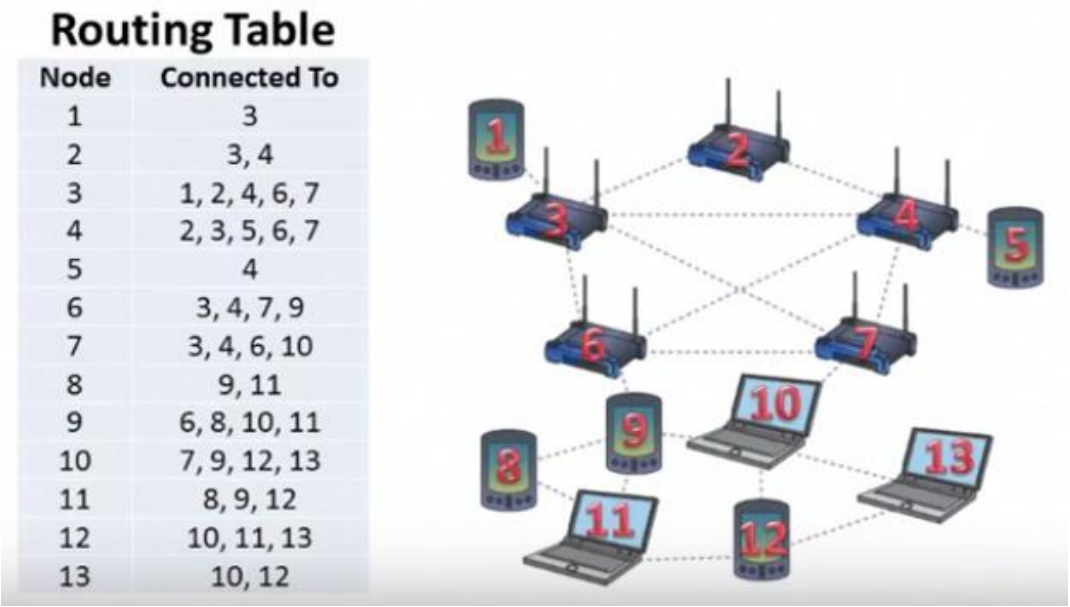
Το δίκτυο πλέγματος είναι αξιόπιστο και προσφέρει πλεονασμό. Όταν ένας κόμβος δεν μπορεί πλέον να λειτουργήσει, οι υπόλοιποι κόμβοι μπορούν ακόμα να επικοινωνούν μεταξύ τους, απευθείας ή μέσω ενός ή περισσοτέρων ενδιάμεσων κόμβων. Τα δίκτυα αυτά μπορούν να διαμορφωθούν και να θεραπευτούν από μόνα τους. Τα ασύρματα δίκτυα πλέγματος λειτουργούν με διαφορετικές ασύρματες τεχνολογίες, συμπεριλαμβανομένων των 802.11, 802.15, 802.16, κυψελοειδών τεχνολογιών και δεν χρειάζεται να περιορίζονται σε οποιαδήποτε τεχνολογία ή πρωτόκολλο.

3.1 Λειτουργία

Ο τρόπος με τον οποίο λειτουργούν τα δίκτυα πλέγματος είναι απλός. Αρχικά κάθε κόμβος, δηλαδή υπολογιστής, κινητό ή ασύρματη συσκευή συνδέεται ενσύρματα ή και ασύρματα με έναν δρομολογητή. Οι υπόλοιποι κόμβοι συνδέονται μεταξύ τους ασύρματα ενισχύοντας το σήμα, παρέχοντας παράλληλα και μεγαλύτερο εύρος διαθέσιμης περιοχής κάλυψης. Κάθε κόμβος έχει τη δική του κάρτα δικτύωσης επιτρέποντας έτσι να επικοινωνεί με τους υπόλοιπους κόμβους [26].

Κάθε κόμβος αποφασίζει να στείλει ή να δεχτεί δεδομένα από άλλους κόμβους του δικτύου. Για να γίνει κάτι τέτοιο εφικτό χρησιμοποιούνται διάφορα πρωτόκολλα δρομολόγησης ανάλογα με το φάσμα περιοχής που πρόκειται να καλύψουν. Τα πρωτόκολλα δρομολόγησης ορίζουν εκείνους τους κανόνες σύμφωνα με τους οποίους θα γίνει η μετάβαση της πληροφορίας από τον έναν κόμβο στον άλλο, διαμορφώνοντας ο κάθε κόμβος ξεχωριστά, τον δικό του πίνακα δρομολόγησης (routing table) σύμφωνα με τον οποίο αποθηκεύει όλες τις διαθέσιμες διαδρομές, την βέλτιστη ανάλογα με τα

διάφορα άλματα που πρέπει να κάνει ο ένας κόμβος στον επόμενο ή ανάλογα το εύρος και την συχνότητα που εκπέμπει ο κάθε κόμβος και η κάθε διαδρομή ξεχωριστά. [49].



Routing Table

Node	Connected To
1	3
2	3, 4
3	1, 2, 4, 6, 7
4	2, 3, 5, 6, 7
5	4
6	3, 4, 7, 9
7	3, 4, 6, 10
8	9, 11
9	6, 8, 10, 11
10	7, 9, 12, 13
11	8, 9, 12
12	10, 11, 13
13	10, 12

Εικόνα 3-2: Πίνακας δρομολόγησης

Στα δίκτυα πλέγματος υπάρχει η δυνατότητα επικοινωνίας μεταξύ κόμβων αφού κάθε συσκευή-κόμβος επικοινωνεί με μία άλλη, μέχρι να στείλει στον προορισμό που θέλει τα απαραίτητα δεδομένα. Τι συμβαίνει όμως όταν κάποιος κόμβος τερματίζει την επικοινωνία ή βγαίνει από το δίκτυο ή παθαίνει μία δυσλειτουργία? Η πληροφορία δεν χάνεται, μιας και επικοινωνεί ο κόμβος με τον αμέσως επόμενο διαθέσιμο κόμβο, ενημερώνοντας έτσι τη διαδρομή και η πληροφορία συνεχίζει να μεταδίδεται. Ακόμα και σε περίπτωση δημιουργίας καινούργιας σύνδεσης κόμβου στο δίκτυο, ενημερώνονται όλοι οι υπόλοιποι κόμβοι για την παρουσία του και γίνεται επικοινωνία για τη βέλτιστη διαδρομή [44].

Εικόνα 3-3: Ευρεία κάλυψη περιοχής

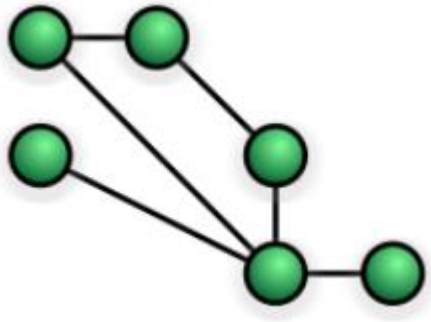
3.2 Τοπολογίες

Η δικτυακή πλέγματος είναι ένας τύπος τοπολογίας δικτύου στον οποίο μια συσκευή (κόμβος) μεταδίδει τα δικά της δεδομένα καθώς και λειτουργεί ως αναμετάδοση για άλλους κόμβους. Οι δρομολογητές χρησιμοποιούνται για να παρέχουν την καλύτερη και αποτελεσματικότερη διαδρομή δεδομένων για αποτελεσματική επικοινωνία. Σε περίπτωση αποτυχίας υλικού, πολλές διαδρομές είναι διαθέσιμες για να συνεχιστεί η διαδικασία επικοινωνίας δικτύου.

Η τιμή των πλήρως δικτύων πλέγματος είναι ανάλογη προς τον εκθέτη του αριθμού των συνδρομητών, υποθέτοντας ότι οι ομάδες επικοινωνίας οποιωνδήποτε δύο τελικών σημείων, μέχρι και όλων των τελικών σημείων. Υπάρχουν δύο ειδών τοπολογίες δικτύων πλέγματος, η μερική τοπολογία και η ολική [21].

3.2.1 Μερική τοπολογία mesh

Σε αυτό το είδος τοπολογίας ορισμένοι κόμβοι συνδέονται με ακριβώς έναν άλλο κόμβο, αλλά μερικοί κόμβοι συνδέονται με δύο ή περισσότερους κόμβους με έναν σύνδεσμο από σημείο σε σημείο [26]. Αυτό καθιστά δυνατή τη χρήση κάποιου από το πλεόνασμα της τοπολογίας πλέγματος που είναι φυσικά πλήρως συνδεδεμένο, χωρίς τις δαπάνες και την πολυπλοκότητα που απαιτούνται για μια σύνδεση μεταξύ κάθε κόμβου στο δίκτυο. Αυτό είναι λιγότερο δαπανηρό για την εφαρμογή σε σύγκριση με την ολικής τοπολογίας πλέγματος, αλλά έχει λιγότερη πλεονασμό.



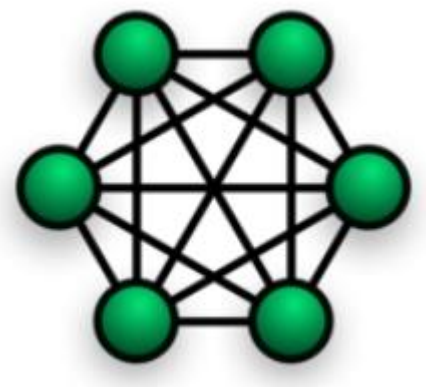
Εικόνα 3-4: Μερική τοπολογία mesh

3.2.2 Ολική τοπολογία mesh

Σε αυτό το είδος τοπολογίας κάθε κόμβος του δικτύου είναι συνδεδεμένος με όλους τους άλλους κόμβους με απευθείας συνδέσμους. Αυτό παρέχει μεγαλύτερη πλεονασμό, διότι αν κάποιος κόμβος αποτύχει, η κίνηση του δικτύου μπορεί να κατευθυνθεί χρησιμοποιώντας άλλους κόμβους. Κάθε κόμβος προσεγγίζει τους κόμβους εργασίας σε κοντινή απόσταση και βρίσκει την καλύτερη διαδρομή για αποτελεσματική και αξιόπιστη επικοινωνία. Το απλούστερο πλήρως συνδεδεμένο δίκτυο είναι ένα δίκτυο δύο κόμβων. Ένα πλήρως συνδεδεμένο δίκτυο δεν χρειάζεται να χρησιμοποιεί μεταγωγή πακέτων ή εκπομπή. Ωστόσο, ο αριθμός των συνδέσεων αυξάνεται τετραδικά με τον αριθμό των κόμβων:

$$c = \frac{n(n-1)}{2}$$

Αυτό καθιστά μη πρακτικό για μεγάλα δίκτυα. Αυτού του είδους η τοπολογία δεν εκπέμπει και δεν επηρεάζει άλλους κόμβους του δικτύου [20].



Εικόνα 3-5: Ολική τοπολογία mesh

3.3 Πρωτόκολλα δρομολόγησης

Τα δίκτυα πλέγματος χρησιμοποιούν και αυτά με την σειρά τους πρωτόκολλα τα οποία τους επιτρέπουν την δρομολόγηση των πακέτων, προσφέροντας εκτός από ευελιξία κίνησης, διαμόρφωση των τοπολογιών του δικτύου και ανακατεύθυνση σε περίπτωση δυσλειτουργίας κάποιας συσκευής, ασφάλεια και προστασία από διάφορες επιθέσεις [19]. Τα κυριότερα πρωτόκολλα που χρησιμοποιούνται είναι το υψηλής απόδοσης ασύρματο δίκτυο πλέγματος (HWMN), το Babel, όπως επίσης και το καλύτερης απόδοσης στην κινητή δικτύωση adhoc (B.A.T.M.A.N.), τα οποία θα συζητήσουμε τους ρόλους που έχουν στο διαμοιρασμό των δικτύων παρακάτω.

3.3.1 Πρωτόκολλο HWMP

Το **υβριδικό ασύρματο δίκτυο πλέγματος (Hybrid Wireless Mesh Protocol –HWMP)** είναι ένα υβριδικό πρωτόκολλο ασύρματου δικτύου που λειτουργεί στο επίπεδο 2 και χρησιμοποιεί διευθύνσεις MAC για την επιλογή διαδρομής. Ονομάζεται ένα υβριδικό πρωτόκολλο, καθώς συνδυάζει τόσο τις ενεργές όσο και τις προοδευτικές στρατηγικές δρομολόγησης. Συνδυάζει την ευελιξία της επιλογής διαδρομής κατ' απαίτηση με προεκτατικές επεκτάσεις δέντρων τοπολογίας. Ο συνδυασμός αντιδραστικών και προληπτικών στοιχείων του HWMP επιτρέπει την αποτελεσματική επιλογή διαδρομής για μια μεγάλη ποικιλία δικτύων πλέγματος [12]. Το HWMP βασίζεται σε **πρωτόκολλο ανά άλμα κατά παραγγελία απόστασης διανύσματος (Ad**

hoc On demand Distance Vector –AODV) προσαρμοσμένο για την επιλογή διαδρομής βάσει MAC διευθύνσεων και τη σύνδεση μετρικής συνείδησης.

Το HWMP χρησιμοποιεί τέσσερα διαφορετικά είδη στοιχείων πληροφοριών (IE). Οι αιτήσεις διαδρομής (Path Request –PREQ), η απάντηση διαδρομής (Path Reply –PREP) και η αναγγελία των ριζών (Root Announcement –RANN) χρησιμοποιούνται στη διαδικασία επιλογής διαδρομής, ενώ η διαδρομή σφάλματος (Path Error –PERR) χρησιμοποιείται για τη συντήρηση της διαδρομής. Στο HWMP, μια διαδρομή προς τον προορισμό περιγράφεται από το επόμενο άλμα σε κάθε ενδιάμεσο σταθμό πλέγματος. Όταν μια πηγή θέλει να στείλει δεδομένα σε έναν προορισμό για τον οποίο δεν έχει ακόμα διαδρομή, ξεκινά μια ανακάλυψη διαδρομής μεταδίδοντας ένα PREQ [46].

Προκειμένου να αποφευχθούν διαφόρων ειδών επιθέσεων είτε στην κίνηση των πακέτων, είτε στους διάφορους κόμβους, χρησιμοποιούνται δύο επεκτάσεις του HWMP, το βασισμένο σε εμπιστοσύνη ασφαλούς δρομολόγησης (HWMP Trust based Extension –TX) και το βασισμένο σε επεκτάσεις φήμης (HWMP Reputation based Extension –REX).

Και τα δύο προστατεύουν το δίκτυο και προσφέρουν ασφάλεια ενάντια στις εξής επιθέσεις:

- **Επίθεση πλημμύρας:**

Ένας εσωτερικός κακόβουλος κόμβος μπορεί να παράγει οποιονδήποτε αριθμό από PREQ ζητώντας διαδρομές προς μη υπαρκτούς προορισμούς. Αυτή η επίθεση μπορεί εύκολα να αντιμετωπιστεί περιορίζοντας τον αριθμό των αιτημάτων που μπορεί να δημιουργήσει ένας κόμβος ανάλογα με τη δική του φήμη. Το HWMP-TX μπορεί φυσικά να χειριστεί αυτό το είδος της επίθεσης καθώς τα αιτήματα από έναν κόμβο υποβάλλονται σε επεξεργασία αν και μόνο εάν πληρούν το κριτήριο της ελάχιστης εμπιστοσύνης. Όπως και το HWMP-REX δεν δημιουργεί κατώτατο όριο στο επίπεδα φήμης, ένας κόμβος μπορεί να πλημμυρίσει το δίκτυο με ψεύτικες αιτήσεις.

- **Αντιμετώπιση μετρικής:**

Η πιο συνηθισμένη επίθεση τροποποίησης σε ένα δίκτυο υψηλής ταχύτητας είναι μια επίθεση μετρικού χειρισμού. Οι κακόβουλοι κόμβοι μπορούν να χειριστούν το μετρικό πεδίο, που πρέπει να συμπεριλάβουν οι ίδιοι στο επιλεγμένο μονοπάτι και στη συνέχεια να ξεκινήσουν διαφορετικές απορρίψεις πακέτων. Αυτές οι επιθέσεις μπορούν να ξεκινήσουν με επιτυχία πριν αρχίσουν οι κόμβοι την επεξεργασία παρακολούθησης. Μόλις δημιουργηθούν σχέσεις εμπιστοσύνης και οι κόμβοι αρχίζουν τη διαδικασία παρακολούθησης, το ποσοστό επιτυχίας αυτών των επιθέσεων πέφτει δραστικά. Στα HWMP-REX και HWMP-TX, καθώς οι κόμβοι με χαμηλότερη φήμη αποφεύγονται στη διαδικασία επιλογής διαδρομής, αυτό το είδος επίθεσης μπορεί να ανιχνευθεί συνήθως με την πάροδο του χρόνου.

- **Επίθεση σκουληκότρυπας:**

Οι κακόβουλοι μπορούν να ενεργήσουν σε συνεννόηση για την καταγραφή πακέτων στο ένα άκρο του δικτύου και να το επαναλάβουν στο άλλο. Ο κύριος στόχος αυτής της επίθεσης είναι να πείσει δύο μακριά κόμβους ως γείτονες. Μόλις δημιουργηθεί μια σκουληκότρυπα, οι κόμβοι μπορεί να ξεκινήσουν αρκετές επιθέσεις πτώσης πακέτων. Το HWMP-REX δεν εντοπίζει επιθέσεις από τέτοιους συν εννοημένους κόμβους όπως το ο θεματοφύλακας δεν εγγυάται τη λήψη στον δέκτη. Το HWMP-TX μπορεί να ταυτοποιήσει ανεξάρτητα τους κόμβους αυτούς με τη βοήθεια άλλων κόμβων που μοιράζονται γειτονικότητα με έναν τέτοιο κακόβουλο κόμβο και μπορεί να ανιχνεύσει επιθέσεις πτώσης πακέτων.

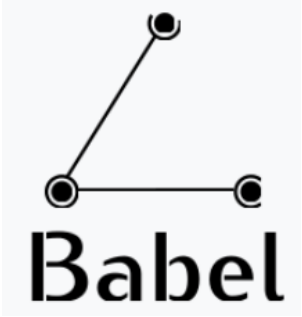
- **Επίθεση κατασκευής:**

Οι εγωιστικοί κόμβοι μπορούν να κατασκευάζουν μηνύματα για να αποφεύγουν την κατανάλωση των πόρων τους. Για παράδειγμα, ένας κόμβος μπορεί να κατασκευάσει ένα μήνυμα PERR για την ενημέρωση των κόμβων που κατεβάζουν για μία ενεργή σύνδεση ως σπασμένη. Το HWMP-REX δεν μπορεί να χειριστεί μια τέτοια επίθεση, καθώς δεν υπάρχει τρόπος να γίνει διάκριση μεταξύ ενός γνήσιου και κατασκευασμένου μηνύματος PERR. Στο HWMP-TX, για έναν κόμβο για τη διατήρηση γειτονικών σχέσεων, πρέπει να κρατήσει τους συνδέσμους ενεργούς και αυτό περιορίζει έναν κόμβο από την παραγωγή συχνά κατασκευασμένων μηνυμάτων [12].

3.3.2 Πρωτόκολλο Babel

Το Babel είναι ένα πρωτόκολλο δρομολόγησης διάνυσμα-αποφυγής βρόχου για IPv6 και IPv4 με γρήγορες ιδιότητες σύγκλισης. Βασίζεται στις ιδέες των DSDV, AODV και EIGRP της Cisco, αλλά έχει σχεδιαστεί για να λειτουργεί καλά όχι μόνο σε ενσύρματα δίκτυα αλλά και σε ασύρματα δίκτυα mesh και έχει επεκταθεί με υποστήριξη για δίκτυα επικάλυψης. Το Babel βρίσκεται στη διαδικασία να γίνει πρότυπο του IETF.

Όταν εντοπίζει μια ασύρματη σύνδεση, το Babel απενεργοποιεί όλες τις βελτιστοποιήσεις και χρησιμοποιεί μια μέτρηση που βασίζεται στην απώλεια πακέτων που έχει σχεδιαστεί για το Wi-Fi MAC (μέτρηση ETX). Αυτό επιβραδύνει τη σύγκλιση, αλλά διασφαλίζει ότι τα ιδιόμορφα χαρακτηριστικά των ασύρματων ζεύξεων δεν σταματάνε τη δρομολόγηση [9].



Εικόνα 3-6: Babel

Το Babel είναι ισχυρό στη παρουσία κινητικότητας: σε ένα δίκτυο καθαρού πλέγματος, το Babel δεν δημιουργεί ποτέ ένα βρόχο δρομολόγησης και σε ένα δίκτυο που βασίζεται στο πρόθεμα, όλοι οι βρόχοι δρομολόγησης είναι εγγυημένοι ότι θα εξαφανιστούν μόλις μια ενημέρωση μεταβεί γύρω από ένα βρόχο (δεν υπάρχει "καταμέτρηση στο άπειρο").

Το Babel απολαμβάνει αρκετά γρήγορη σύγκλιση. Δεδομένου ότι το Babel χρησιμοποιεί ενεργοποιημένες ενημερώσεις και ρητά αιτήματα για πληροφορίες δρομολόγησης, συνήθως συγκλίνει σχεδόν αμέσως μετά την ολοκλήρωση του μέτρου ποιότητας συνδέσμων. Αυτή η αρχική λύση δεν είναι βέλτιστη -αφού συγκλίνει σε ένα απλά ικανοποιητικό σύνολο διαδρομών. Επίσης, το Babel θα πάρει το χρόνο του πριν

βελτιστοποιήσει τους πίνακες δρομολόγησης. Σε περίπτωση απώλειας πολλών πακέτων, η σύγκλιση σε ένα βέλτιστο σύνολο διαδρομών μπορεί να διαρκέσει έως και 40 δευτερόλεπτα (με το προεπιλεγμένο διάστημα ενημέρωσης 16 δευτερολέπτων).

Το Babel μπορεί προαιρετικά να λάβει υπόψη την ραδιοσυχνότητα προκειμένου να αποφευχθεί η παρεμβολή. Αυτό βελτιώνει δραματικά την απόδοση σε δίκτυα πολλαπλών συχνοτήτων [10].

3.3.3 Πρωτόκολλο B.A.T.M.A.N.

Είναι ένα πρωτόκολλο δρομολόγησης που αναπτύσσεται από την γερμανική κοινότητα Freifunk και προορίζεται να αντικαταστήσει το OLSR. Το κρίσιμο σημείο της **καλύτερης προσέγγισης στην κινητή δικτύωση ανά άλμα (Better Approach To Mobile Adhoc Networking –B.A.T.M.A.N.)** είναι η αποκέντρωση της γνώσης σχετικά με την καλύτερη διαδρομή μέσω του δικτύου, μιας και κανένας κόμβος δεν έχει όλα τα δεδομένα. Αυτή η τεχνική εξαλείφει την ανάγκη διάδοσης πληροφοριών σχετικά με αλλαγές δικτύου σε κάθε κόμβο του δικτύου. Ο επιμέρους κόμβος αποθηκεύει μόνο πληροφορίες σχετικά με την "κατεύθυνση" που έλαβε δεδομένα και αποστέλλει τα δεδομένα του ανάλογα. Δημιουργείται ένα δίκτυο συλλογικής νοημοσύνης, μιας και τα δεδομένα μεταφέρονται από τον ένα κόμβο στον άλλο και τα πακέτα λαμβάνουν δυναμικές και δημιουργικές διαδρομές [8].

Εικόνα 3-7: B.A.T.M.A.N.

Η προσέγγιση του αλγορίθμου B.A.T.M.A.N. είναι να διαιρέσει τη γνώση σχετικά με τις καλύτερες διαδρομές άκρου προς άκρο μεταξύ κόμβων στο πλέγμα σε όλους τους συμμετέχοντες κόμβους. Κάθε κόμβος αντιλαμβάνεται και διατηρεί μόνο τις πληροφορίες για το καλύτερο επόμενο βήμα προς όλους τους άλλους κόμβους. Έτσι, η ανάγκη για μια παγκόσμια γνώση σχετικά με τις τοπικές αλλαγές τοπολογίας

καθίσταται περιττή [11]. Επιπρόσθετα, ένα βασισμένο σε γεγονότα αλλά όχι διαχρονικό (διαχρονικό με την έννοια ότι το B.A.T.M.A.N. δεν προγραμματίζει ποτέ ούτε τις πληροφορίες τοπολογίας χρονικού ορίου για τη βελτιστοποίηση των αποφάσεων δρομολόγησης του), αποτρέπει τη συσσώρευση αντιφατικών πληροφοριών τοπολογίας (ο συνήθης λόγος ύπαρξης βρόχων δρομολόγησης) και περιορίζει ποσότητα μηνυμάτων τοπολογίας που πλημμυρίζουν το πλέγμα, αποφεύγοντας έτσι την υπερβολική επιβάρυνση της κυκλοφορίας ελέγχου). Ο αλγόριθμος έχει σχεδιαστεί για να ασχολείται με δίκτυα που βασίζονται σε αναξιόπιστους συνδέσμους.

Ο αλγόριθμος πρωτοκόλλου του B.A.T.M.A.N. μπορεί να περιγραφεί ως εξής. Κάθε κόμβος μεταδίδει μηνύματα εκπομπής (τα ονομαζόμενα **πρωτότυπα μηνύματα (Originator Messages –OGM)** για να ενημερώσει τους γειτονικούς κόμβους για την ύπαρξή του. Οι γείτονες αυτοί αναμεταδίδουν τα OGM σύμφωνα με συγκεκριμένους κανόνες για να ενημερώσουν τους γείτονές τους για την ύπαρξη του αρχικού εκκινητή αυτού του μηνύματος και ούτω καθεξής. Έτσι, το δίκτυο πλημμυρίζεται με μηνύματα εντολέα. Τα OGM είναι μικρά, το τυπικό μέγεθος ακατέργαστου πακέτου είναι 52 byte συμπεριλαμβανομένων των εξόδων IP και UDP. Τα OGM περιέχουν τουλάχιστον τη διεύθυνση του δημιουργού, τη διεύθυνση του κόμβου που μεταδίδει το πακέτο, ένα χρόνο για να φύγει (Time To Leave –TTL) και έναν αριθμό ακολουθίας.

Τα OGMs ακολουθούν ένα μονοπάτι όπου η ποιότητα των ασύρματων ζεύξεων είναι ασθενής ή κορεσμένη, με συνέπεια να χαθούν πακέτα ή να καθυστερήσουν στο δρόμο τους στο πλέγμα. Επομένως, τα OGM που ταξιδεύουν σε καλές διαδρομές θα διαδοθούν ταχύτερα και πιο αξιόπιστα. Προκειμένου να διαπιστωθεί εάν τα OGM έχουν ληφθεί μία φορά ή περισσότερες φορές, υπάρχει ένας αύξοντας αριθμός, ο οποίος δίνεται από τον δημιουργό του OGM. Κάθε κόμβος εκπέμπει εκ νέου κάθε OGM που έλαβε το πολύ μία φορά και μόνο εκείνα που έλαβε από τον γείτονα που έχει αναγνωριστεί ως το καλύτερο επόμενο άλμα (γείτονας με την καλύτερη κατάταξη) προς τον αρχικό εκκινητή του OGM.

Με αυτόν τον τρόπο τα OGMs πλημμυρίζουν επιλεκτικά μέσω του πλέγματος και ενημερώνουν τους κόμβους λήψης για την ύπαρξη άλλων κόμβων. Ένας κόμβος X θα μάθει για την ύπαρξη ενός κόμβου Y στην απόσταση λαμβάνοντας τα OGM του,

όταν τα OGM του κόμβου Υ αναμεταδίδονται από τους γείτονές του με ένα μόνο λυκίσκο. Εάν ο κόμβος Χ έχει περισσότερους από έναν γείτονες, μπορεί να πει από τον αριθμό των μηνυμάτων εντολέα που λαμβάνει πιο γρήγορα και πιο αξιόπιστα μέσω ενός από τους γείτονές του με ένα μόνο λυκίσκο, που ο γείτονας πρέπει να επιλέξει να στείλει δεδομένα στον απομακρυσμένο κόμβο.

Ο αλγόριθμος τότε επιλέγει αυτόν τον γείτονα ως το καλύτερο επόμενο άλμα προς τον δημιουργό του μηνύματος και διαμορφώνει τον πίνακα δρομολόγησης αντίστοιχα [8].

3.4 Πλεονεκτήματα και μειονεκτήματα

Τα δίκτυα πλέγματος προσφέρουν δυνατότητες να διαμοιράζουν οι διάφοροι κόμβοι πληροφορίες ο ένας στον άλλο. Κάποια από τα πλεονεκτήματα της χρήσης τους είναι:

a) **Μηδαμινά έως ελάχιστα προβλήματα κυκλοφορίας:** Κάθε κόμβος επικοινωνεί με τον επόμενο και σε περίπτωση μη δυνατότητας, υπάρχει εναλλακτική διαδρομή παρέχοντας έτσι ομαλή και αποτελεσματική αποστολή και λήψη της πληροφορίας.
b) **Μέγιστη ασφάλεια:** Χρησιμοποιώντας τα διάφορα πρωτόκολλα και μηχανισμούς κρυπτογράφησης που διαθέτει ο κάθε κόμβος, καθιστά πιο δύσκολη τη πρόσβαση σε έναν.
c) **Ευελιξία και εύκολη ανίχνευση σφαλμάτων:** Πιθανή αστοχία ενός κόμβου ή καναλιού δεν οδηγεί στην αχρήστευση ολόκληρου του δικτύου και με βάση τον πίνακα δρομολόγησης ενημερώνονται όλοι οι υπόλοιποι κόμβοι για την επιλογή της νέας βέλτιστης διαδρομής
d) **Διαμοιρασμός μίας σύνδεσης Διαδικτύου σε όλους τους υπολογιστές του δικτύου:** Αυτό σημαίνει ότι η ύπαρξη μιας και μοναδικής σύνδεσης με το Διαδίκτυο αρκεί για να παράσχει πρόσβαση σε όλους τους υπολογιστές ή ασύρματες συσκευές του τοπικού ή ευρύτερου δικτύου.
e) **Παρέχουν καλύτερο σήμα από τους αναμεταδότες:** Σε αντίθεση με τους αναμεταδότες ή ενισχυτές, που ενισχύουν το σήμα, παράλληλα εξασθενούν

την ταχύτητα του δικτύου, διότι πρέπει να επικοινωνούν και με το router και με τον κόμβο για να στέλνουν και να δέχονται δεδομένα. Από την άλλη πλευρά στα δίκτυα πλέγματος επικοινωνεί ο κάθε κόμβος με τον επόμενο παρέχοντας κατευθείαν τα δεδομένα.

Κάποια από τα μειονεκτήματα ωστόσο των δικτύων πλέγματος είναι:

- **Υψηλό κόστος:** Ανάλογα με τον αριθμό των συσκευών στο δίκτυο το κόστος υλοποίησης και συντήρησης είναι υπερβολικά υψηλό, ειδικά όσο περισσότερες συσκευές συνδέονται σε αυτό.
- **Χαμηλή ταχύτητα ανάλογα με τον αριθμό των κόμβων:** Αν και εύκολη η εγκατάσταση ενός δικτύου πλέγματος, όσο αυξάνονται οι συσκευές, μπορεί να καλύπτουν μεγαλύτερο φάσμα σήματος, αλλά παράλληλα ελαττώνουν την ταχύτητα σύνδεσης όσο συνδέονται ολοένα και περισσότερες συσκευές [20].

4 Συστήματα διαμοιρασμού δικτύων Wi-Fi

Όσο αυξάνεται η ανάγκη χρήσης του Wi-Fi και σε περισσότερες περιοχές, αυξάνεται η περιοχή κάλυψης, οι συσκευές που πρέπει να συνδεθούν με τέτοιον τρόπο έτσι ώστε να επεκτείνουν το διαθέσιμο εύρος κάλυψης είναι περισσότερο χρήσιμες και η σημαντικότητα του διαμοιρασμού συνδέσεων αποκτάει περισσότερο νόημα και ουσία στην χρήση του δικτύου, τόσο για τον πάροχο, όσο και για τον επισκέπτη.

Παρόλα αυτά, όπως αναφερθήκαμε και παραπάνω, θα πρέπει να δοθεί προτεραιότητα στην εμπιστευτικότητα και ασφάλεια, τόσο από τη μεριά του παρόχου, όπου θέλει να προστατεύσει τα δεδομένα και την σύνδεσή του, αλλά και του επισκέπτη, που ενώ θέλει να κρατήσει την ανωνυμία του, να μην παραβιάζει όρους χρήσης και να μπορεί να χρησιμοποιεί σταθερά και γρήγορα την ταχύτητα και το διαθέσιμο εύρος ζώνης του δικτύου που του γίνεται ο διαμοιρασμός.

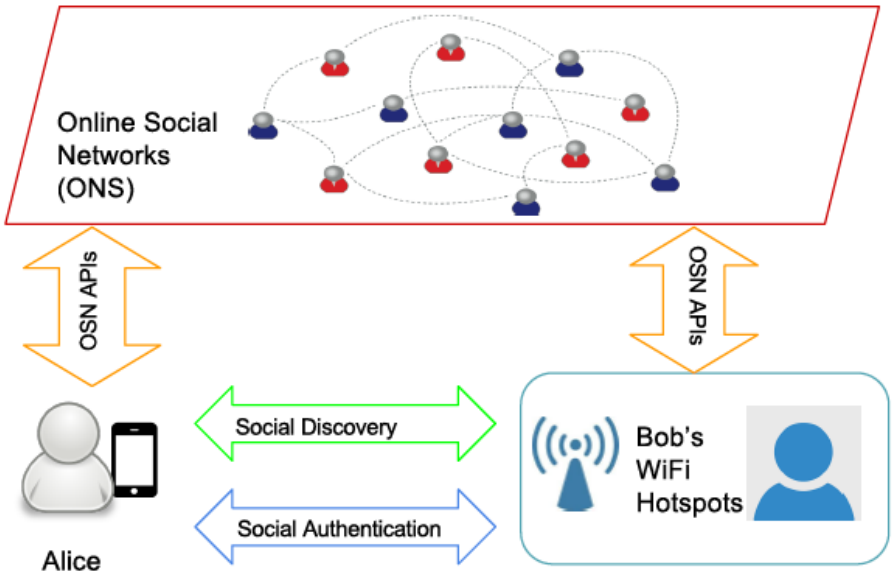
Μία τέτοια κοινοτική χρήση του Wi-Fi δίνει κίνητρα και κινητοποιεί τη συμμετοχή των χρηστών, δεδομένου ότι είναι ουσιαστικά αμοιβαία. Παρόλα αυτά, η αρχιτεκτονική του Wi-Fi δεν είναι τόσο ασφαλής στο κοινοτικό διαμοιραζόμενο μηχανισμό.

Γι’ αυτό τον λόγο υπάρχουν διάφορα συστήματα, τα οποία επιτρέπουν την κοινή χρήση ευρυζωνικών συνδέσεων του σπιτιού με τους επισκέπτες, εκμεταλλευόμενα το εύρος ζώνης του ασύρματου σημείου πρόσβασης σε κατοικημένες περιοχές. Η κοινή χρήση μπορεί να προσφέρεται δωρεάν, όπως γίνεται στα δίκτυα PAWS με τη χρήση VpuN, είτε να είναι διαθέσιμη μόνο σε συνδρομητές, όπως είναι το FON. Παρακάτω θα δούμε τι οφέλη προσφέρει η κάθε χρήση και πως μπορεί, εκτός από την ασφάλεια, να εκμεταλλευτεί κανείς το διαθέσιμο εύρος ζώνης.

4.1 Κοινωνικά Wi-Fi

Τα **Κοινωνικά Wi-Fi (Social Wi-Fi)**, είναι μία αρχιτεκτονική η οποία επιτρέπει στους ιδιοκτήτες Wi-Fi να διαμοιράζουν το δίκτυό τους με τους σε απευθείας σύνδεση (Online Social Networks –OSN) φίλους τους. Το Social Wi-Fi επιτρέπει σε έναν χρήστη να ανακαλύψει ένα Wi-Fi δίκτυο που λειτουργεί από έναν από τους

φίλους του και να αυθεντικοποιήσει στο δίκτυο, επικυρώνοντας την κοινωνική τους σχέση. Στο παρακάτω σχήμα απεικονίζεται μια επισκόπηση των προτεινόμενων μηχανισμών [1].



Εικόνα 4-1: Δείγμα Social Wi-Fi

Ο Bob έχει Wi-Fi και διαφημίζει την λίστα των φίλων του. Όταν η Alice έρχεται κοντά στο hotspot του Bob, ανακαλύπτει ότι είναι φίλη του Bob μέσω της διαφημιζόμενης πληροφορίας. Η αναζήτηση του Social Wi-Fi ακολουθείται από την αμοιβαία αυθεντικοποίηση μεταξύ της Alice και του Bob, κατά την οποία επικυρώνεται μέσω πληροφοριών που αποκτήθηκαν μέσω του κοινωνικού δικτύου της **διεπαφής αυθεντικοποίησης προγραμματισμού (Authentication Programming Interface –API)**.

4.1.1 Τρόπος λειτουργίας

Τα κοινωνικά Wi-Fi απαιτούν έναν αποτελεσματικό τρόπο για τους επισκέπτες για να ανακαλύψουν τα hotspots που διατίθενται μέσω των δικτυακών τους φίλων. Όπως αναφερθήκαμε και σε προηγούμενο κεφάλαιο, αυτό γίνεται μέσω του πρωτοκόλλου ANQP, το οποίο είναι υπεύθυνο μέσω της αποστολής αιτημάτων από το AP και τους σε απευθείας σύνδεση φίλους, μέσω εφαρμογών όπως το Facebook, το

LinkedIn, το Google+ και άλλων, να διαμοιράζονται οι πληροφορίες στους διαφόρους φίλους μεταξύ τους.

Το ANQP στοχεύει στην παροχή υπηρεσιών Wi-Fi με φερεγγυότητα, με καλύτερη δυνατότητα εντοπισμού δικτύου και υποστηρίζεται από πολλούς κατασκευαστές κινητών συσκευών και προμηθευτές εξοπλισμού δικτύου [1].

Εκτός από το ANQP, τα κοινωνικά δίκτυα χρησιμοποιούν μεθόδους αυθεντικοποίησης όπως το EAP προκειμένου η πληροφορία που θα διαμοιραστεί όχι μόνο να είναι ασφαλής αλλά και να διαφυλάξει την ακεραιότητα της κάθε σύνδεσης και του κάθε χρήστη μέσω ανταλλαγής κωδικών, με τη μέθοδο χειραψίας δηλαδή, από τον ένα χρήστη στον άλλο [38].

Γι’ αυτό τον λόγο οι υπάρχουσες μέθοδοι επαλήθευσης απαιτούν ένα μυστικό προτίμησης ή ένα προκαθορισμένο πιστοποιητικό για έλεγχο ταυτότητας. Η χρήση τέτοιων τεχνικών στα κοινωνικά δίκτυα θα απαιτούσε τη διανομή διαπιστευτηρίων μεταξύ μεγάλου αριθμού συμμετεχόντων στο κοινωνικό δίκτυο. Το κοινωνικό WiFi αποφεύγει αυτή την ανάγκη επιτρέποντας τον αμοιβαίο έλεγχο ταυτότητας μεταξύ του επισκέπτη και του χρήστη. Αυτό επιτυγχάνεται με την επικύρωση της φιλίας τους μέσω μιας διαδικασίας πρόκλησης-αντίδρασης .Δεδομένου ότι ένας σε απευθείας σύνδεση φίλος δεν έχει μυστικό, δεν μπορούμε να βασιζόμαστε σε υπάρχουσες μεθόδους αμοιβαίας εξακρίβωσης της ταυτότητας. Αντ' αυτού, προτείνεται μια νέα μέθοδο επαλήθευσης ταυτότητας που ονομάζεται EAP-Social [1].

Ειδικότερα, οι ιδιοκτήτες των hotspot θα καταχωρούν τα AP τους στο σύννεφο (Cloud) AAA, και το εξουσιοδοτούν να επικαλεστεί τα αντίστοιχα API κοινωνικού δικτύου. Στη συνέχεια, το Cloud AAA θα φέρει τη λίστα των φίλων και θα τη συμπιέσει σε φίλτρα Bloom για ανακάλυψη, που θα δούμε στη συνέχεια. Απαιτείται να εφαρμοστεί μόνο το EAP-Social στο Cloud AAA για να χειριστεί τον κοινωνικό έλεγχο ταυτότητας. Η προσέγγιση αυτή αποφέρει σημαντικά οφέλη. Αρχικά, τα AP θα εκτελούνται σε ένα διαμέσου μοντέλου, παρακάμπτοντας την ανάγκη σημαντικών ενημερώσεων υλικού ή λογισμικού. Επιπλέον, το κεντρικό Cloud AAA είναι υπεύθυνο για τον κοινωνικό έλεγχο ταυτότητας, γεγονός που εξαλείφει την ανάγκη για αυτόνομη ανάπτυξη AAA σε κάθε σημείο πρόσβασης.

4.1.2 Χρήση Bloom φίλτρων

Εκτός από την αυθεντικοποίηση στα κοινωνικά δίκτυα προκύπτουν και άλλα δύο ζητήματα, όπως η ιδιωτικότητα και η συμπίεση των δεδομένων. Πιο συγκεκριμένα, η αποκάλυψη ονομάτων φίλων παραβιάζει το απόρρητο. Επιπλέον, η ενθυλάκωση όλων των ονομάτων φίλων σε ένα μήνυμα δεν είναι εφικτή, ειδικά όταν οι φίλοι του κατόχου του hotspot που είναι σε σύνδεση, είναι της τάξης των εκατοντάδων ή χιλιάδων. Για να επιδιορθωθεί αυτό, χρησιμοποιούνται **φίλτρα άνθησης (Bloom Filter –BF)** για συμπίεση δεδομένων και προστασία της ιδιωτικής ζωής. Το φίλτρο Bloom (BF) είναι μια ευρέως χρησιμοποιούμενη δομή δεδομένων για τη συμπίεση ενός αυθαίρετου συνόλου δεδομένων σε ένα διάνυσμα δυαδικών ψηφίων και την παροχή αναζήτησης μέλους.

Οι λίστες φίλων αρχικά συμπιέζονται σε BF, και στη συνέχεια, το AP εισάγει τα BFs. Στη συνέχεια, η συσκευή επισκέπτη πραγματοποιεί αναζήτηση BF για να ελέγξει εάν το όνομα του επισκέπτη βρίσκεται στις λίστες φίλων. Μόνο εάν υπάρχει ταίριασμα, η φιλοξενούμενη συσκευή προσπαθεί να συσχετιστεί και να επικυρωθεί στο δίκτυο. Τα BF φέρνουν τρία σημαντικά οφέλη στην ανακάλυψη δικτύου:

a) διατηρεί την ιδιωτική ζωή επειδή δεν αποκαλύπτει ονόματα φίλων
b) επιτυγχάνει υψηλή συμπίεση των λιστών φίλων
c) η απόδοση αναζήτησης δεν υποβαθμίζεται με την αύξηση του μεγέθους της λίστας φίλων.

Ωστόσο, υπάρχουν δύο ζητήματα που τίθενται στα BF. Η διαγραφή ενός φίλου από τη λίστα και τα ψεύτικα θετικά. Αυτά τα θέματα μπορούν να αντιμετωπιστούν καθώς ένα όνομα φίλου μπορεί να αφαιρεθεί χρησιμοποιώντας το BF μέτρησης, το οποίο αποθηκεύει μια τιμή μετρητή παρά ένα ψηφίο σε κάθε υποδοχή. Ο μετρητής μειώνεται όταν αφαιρείται ένας φίλος.

Όσο ο μετρητής είναι μεγαλύτερος από μηδέν, η μέτρηση BF θα βρει ένα ταίριασμα.

Από την άλλη πλευρά, τα ψεύτικα θετικά μπορούν να οδηγήσουν σε λάθος αποτελέσματα αναζήτησης. Υπάρχει περίπτωση δύο χρήστες να έχουν την ίδια τιμή. Αν και μόνο ο ένας χρήστης στην πραγματικότητα περιλαμβάνεται στη λίστα φίλων,

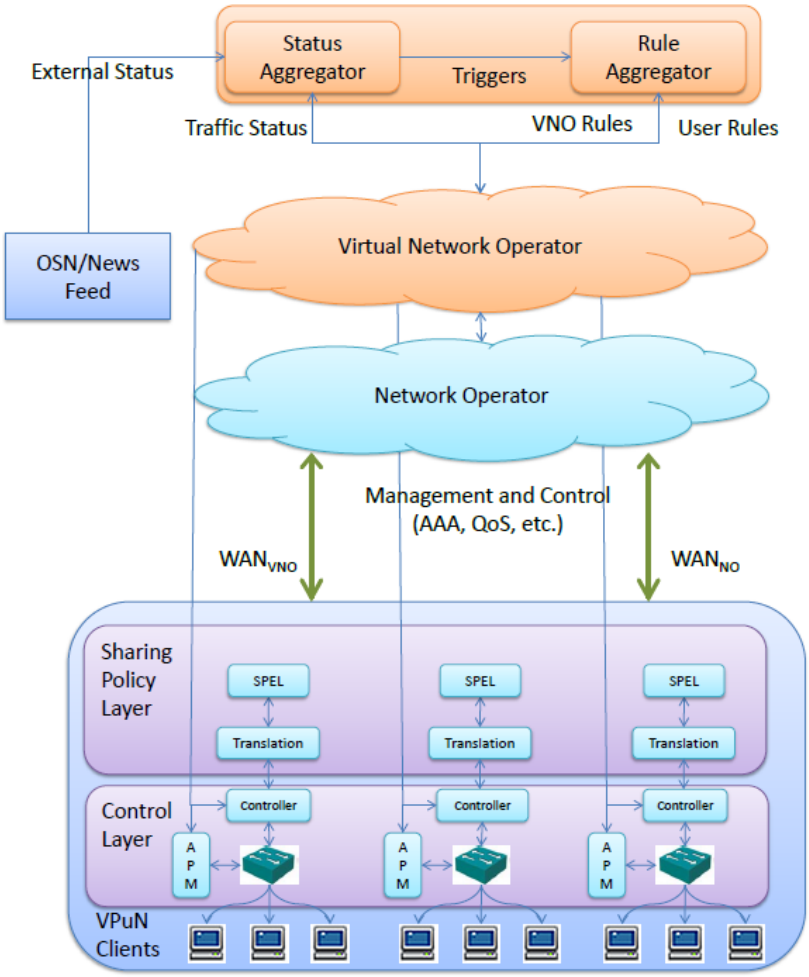
η BF θα αναφέρει ένα ταίριασμα και για τους δύο. Παρ 'όλα αυτά, τα ψεύτικα θετικά δεν προκαλούν σοβαρές συνέπειες μιας και αρχίζουν την εξακρίβωση της ταυτότητας, η οποία θα είναι ανεπιτυχής, δεδομένου ότι η σχέση του OSN μεταξύ του επισκέπτη και του κατόχου του hotspot δεν θα επικυρωθεί [1].

4.1.3 VPuN

Τα VPN, όπως αναφερθήκαμε και σε προηγούμενο κεφάλαιο, είναι υπεύθυνα με τη χρήση σηράγγων για την απομόνωση της κίνησης, προσφέρουν ευελιξία και διαμοιράζουν με τέτοιο τρόπο την πληροφορία, έτσι ώστε και ο πάροχος και ο επισκέπτης να διατηρούν την ανωνυμία τους και να μπορεί να υπάρχει αυθεντικοποίηση και εμπιστευτικότητα στην χρήση του διαδικτύου. Μία παρόμοια τεχνική είναι η χρήση των VpuN που χρησιμοποιείται στα κοινωνικά δίκτυα με τη διαφορά ότι πρόκειται για δημόσια εικονικά δίκτυα [37].

Η αρχιτεκτονική **δημόσιου VPN (VPuN)** όπως φαίνεται και στο παρακάτω σχήμα, διανέμεται σε οικιακά δίκτυα, σε διαχειριστές δικτύου (Network Operators – OP) και σε εικονικούς διαχειριστές δικτύου (Virtual Network Operators -VOP). Σύμφωνα με τις απαιτήσεις VPuN, ένας οικιακός δρομολογητής με δυνατότητα SDN, ένας ελεγκτής, ένας διαχειριστή σημείου πρόσβασης και ένα σύστημα για τη μετάφραση των εκφράσεων κοινής πολιτικής, αναπτύσσεται σε κάθε ένα από το οικιακό δίκτυο.

Επιπρόσθετα με τα βασικά API που περιγράφονται εκεί, ο διαχειριστής σημείου πρόσβασης θα παρέχει επίσης τη δυνατότητα δημιουργίας, τροποποίησης και ρύθμισης παραμέτρων ασύρματων SSID. Μία εναλλακτική προσέγγιση θα ήταν να χρησιμοποιηθεί ένα στρώμα τεμαχισμού (π.χ. όπως στο OpenFlow) για τον οικιακό δρομολογητή, που επιτρέπει τόσο τον OP του οικιακού δικτύου όσο και τον VOP να ελέγχουν τα αντίστοιχα κομμάτια τους, ενώ επιβάλλουν την απομόνωση αυτών των κομματιών [2].



Εικόνα 4-2: Αρχιτεκτονική VPuN

Τα VPuN προβλέπονται για την επίτευξη στόχων υψηλού επιπέδου όπως στο να εκθέσουν μια δυναμική και φιλική προς τον χρήστη άντληση στους ενδιαφερόμενους σε διάφορα επίπεδα του δικτύου για να καθορίσουν τις απαιτήσεις των πόρων του δικτύου. Επίσης, όταν εξωτερικοί παράγοντες χρειάζονται, θα πρέπει τα VPuN να ρυθμίζονται αυτόματα ή να αναδιαμορφώνονται. Κάτι τέτοιο είναι χρήσιμο σε καταστάσεις έκτακτης ανάγκης ή σε φυσικές καταστροφές, όπου τα σημεία πρόσβασης μπορούν να συνδέονται αυτόματα με σημεία πρόσβασης άλλων χρηστών ή προσωπικών συσκευών βάσει τάσεων κοινωνικής δικτύωσης στο Διαδίκτυο, ή όταν οι φορείς εκμετάλλευσης των δικτύων πρέπει να κατανείμουν δυναμικά την χωρητικότητα, ώστε να ικανοποιηθούν τα εξελισσόμενα αιτήματα [2].

Προκειμένου να εκπληρώσουν αυτούς τους υψηλούς στόχους τα VPuN πρέπει:

- Να παρέχουν στους ενδιαφερόμενους τη δυνατότητα να καθορίσουν τις απαιτήσεις τους και τις παραμέτρους που επηρεάζουν αυτές τις απαιτήσεις με άλλο τρόπο.
- Να δώσουν τη δυνατότητα να μεταφράσουν αυτές τις απαιτήσεις σε ροές ελέγχου που πρέπει να εγκατασταθούν σε διάφορα σημεία του δικτύου.
- Να συγκεντρώσουν και να εξατομικεύσουν δεδομένα από εξουσιοδοτημένα μέσα κοινωνικής δικτύωσης και πηγές, και να αποτελέσουν το ίδιο το δίκτυο για την εξακρίβωση του περιβάλλοντος.
- Να χρησιμοποιήσουν τις πληροφορίες που συλλέγονται, παίρνοντας έξυπνες αποφάσεις για την αυτόματη αναδιαμόρφωση του δικτύου.

Εκτός από τις απαιτήσεις χαρακτηριστικών, τα VPuN θα πρέπει να πληρούν κάποιες απαιτήσεις, έτσι ώστε να μπορούν να ενσωματωθούν άψογα σε οποιαδήποτε στοίβα SDN. Θα πρέπει:

- Να παρέχουν συμβατότητα με τα υπάρχοντα πρωτόκολλα δικτύου.
- Να παρέχουν την δυνατότητα να επεκτείνουν και να υποστηρίξουν άλλες προδιαγραφές SDN που θα μπορούσαν να εξελίσσονται πέρα από το OpenFlow.
- Να παρέχουν διαφανή API και βιβλιοθήκες, που θα μπορούσαν να χρησιμοποιηθούν για την κατασκευή εξωτερικών εφαρμογών προστιθέμενης αξίας, όπως ένα εργαλείο παρακολούθησης ανταμοιβής για τη διανομή χωρητικότητας [2].

4.2 PAWS

Η **υπηρεσία δημόσιας πρόσβασης Wi-Fi (Public Access Wi-Fi Service – PAWS)** είναι μια υπηρεσία κοινής ωφέλειας που βασίζεται σε κοινότητα χρηστών και χρησιμοποιεί μια σειρά από τεχνικές που κάνουν χρήση της διαθέσιμης αχρησιμοποίητης χωρητικότητας στα οικιακά ευρυζωνικά δίκτυα, επιτρέποντας την πρόσβαση σε αυτούς τους πόρους [4]. Η PAWS υιοθετεί μια προσέγγιση συμμετοχής σε επίπεδο κοινότητας, όπου οι συνδρομητές ευρυζωνικών υπηρεσιών στο σπίτι

μπορούν να δώσουν ελεγχόμενη αλλά δωρεάν χρήση του ευρυζωνικού τους δικτύου υψηλής ταχύτητας στους συμπολίτες τους.

Η PAWS αναπτύχθηκε με 20 προσαρμοσμένους δρομολογητές PAWS τοποθετημένους σε μια υποβαθμισμένη κοινότητα στο Νότιγχαμ και δοκιμάστηκε επίσης στην αγροτική Ουαλία. Το PAWS είναι ουσιαστικά ένα κοινόχρηστο δίκτυο πρόσβασης κοινόχρηστων χρηστών για τους μειονεκτούντες χρήστες σε αστικές και αγροτικές κοινότητες. Το PAWS αντιμετωπίζει συνεχιζόμενες προκλήσεις ανάπτυξης, όπως η περιορισμένη κάλυψη, που προέρχεται από την κοινή χρήση χρηστών.

Συγκεκριμένα, κατά τη διάρκεια της δοκιμαστικής ανάπτυξης του PAWS, παρατηρήθηκε ότι οι οικιακοί χρήστες δεν μοιράζονταν την ευρυζωνική σύνδεση τους, σε περιόδους κατά τις οποίες χρειάζονταν, είτε ολόκληρο το εύρος ζώνης, είτε όλες τις θύρες του οικιακού δρομολογητή (δηλαδή, η PAWS χρησιμοποιεί ένα σημείο πρόσβασης συνδεδεμένο με το δρομολογητή του σπιτιού για κοινή χρήση πρόσβασης στο Διαδίκτυο). Ουσιαστικά, η PAWS είναι ένα κοινόχρηστο δίκτυο με ένα μόνο σημείο πρόσβασης ανά επισκέπτη και ως εκ τούτου, η κοινή χρήση πρόσβασης στο Διαδίκτυο εξαρτάται σε μεγάλο βαθμό από τις πολιτικές κοινής χρήσης χρηστών (δηλαδή από τις περιόδους κατά τις οποίες ο χρήστης μοιράζεται τη σύνδεσή του στο Διαδίκτυο).

Η πρόθεση της PAWS είναι να διερευνήσει την παροχή μιας περιορισμένης υπηρεσίας που είναι δωρεάν στο σημείο χρήσης, στοχεύοντας τα δημογραφικά στοιχεία που θέλουν και χρειάζονται, αλλά δεν μπορούν να έχουν πρόσβαση στο Διαδίκτυο [4].

4.2.1 Αρχιτεκτονική

Η τεχνολογία πρόσβασης που παρέχεται από το PAWS είναι το πρότυπο Wi-Fi 802.11 b/a/g/n, η πανταχού παρούσα παρουσία των ευρυζωνικών εφαρμογών (που παρέχει επαρκείς δυνατότητες και χωρητικότητα για κοινή χρήση) και των συσκευών πελάτη (που παρέχουν επαρκείς ευκαιρίες για χρήση) εύλογη επιλογή.

Σε αυτό το δίκτυο γίνεται ο διαμοιρασμός της σύνδεσης ενός συνδρομητή (παρόχου), διαθέτοντας ένα ποσό του εύρους ζώνης του σε άλλου κατοίκους (πολίτες) μέσω VPN συνδεσιμότητας ενός ανοιχτού δικτύου. Με τον τρόπο αυτό είναι και

ασφαλές το κανάλι επικοινωνίας των χρηστών και απροσπέλαστο από διάφορους εισβολείς (κακόβουλους χρήστες). Η εφαρμογή της PAWS χρησιμοποιώντας VPN τεχνολογίας προσεγγίζεται μέσω ενός SSID.

Το Wi-Fi είναι σχεδόν πανταχού παρόν σε συσκευές πελάτη (τηλέφωνα, tablet, επιτραπέζιους και φορητούς υπολογιστές) και οι περισσότερες συσκευές διαθέτουν ενσωματωμένη υποστήριξη για VPN πρωτόκολλα.

Κάθε χρήστης διαθέτει έναν δρομολογητή που χρησιμοποιείται σαν πύλη για το σπίτι του διαμοιραστή. Κάθε πύλη είναι συνδεδεμένη με ένα ενσύρματο καλώδιο Ethernet στον δρομολογητή του διαμοιρασθέντα χώρου και διαφημίζει μία μη ασφαλή Wi-Fi σύνδεση μέσω ενός SSID PAWS στο δικό του VLAN στα 2.4GHz σαν επιλογή αυτόματου καναλιού [4]. Κάθε σημείο πρόσβασης ρυθμίζεται για την γεφύρωση μόνο της ασύρματης διεπαφής στην ενσύρματη διεπαφή, προσφέροντας IP διευθύνσεις σε συνδεδεμένες συσκευές μέσω DHCP εύρους διευθύνσεων.

4.2.2 Διαχείριση κίνησης

Στο PAWS πρέπει να εφαρμόσουμε ένα όριο εύρους ζώνης, για τη συνολική χρήση των πολιτών ανά πύλη, για να διασφαλιστεί ότι μπορεί να παρέχονται απλές εγγυήσεις στους συμμετέχοντες, σχετικά με τον πιθανό αντίκτυπο στη δική τους υπηρεσία διαδικτύου. Οι πύλες PAWS ενεργοποιούν την κίνηση μεταξύ του PAWS WLAN και του διακομιστή VPN χρησιμοποιώντας

ιεραρχική πειθαρχία κοπής του κουτιού συμβολοσειρών: όλη η κυκλοφορία PAWS έχει εκχωρηθεί στην προεπιλεγμένη κλάση που έχει μετακινηθεί σε λήψη 2Mb/s και μεταφόρτωση 512kb/s.

Κάθε πύλη εφαρμόζει πολιτικές τείχους προστασίας που επιτρέπουν πρωτόκολλα ελέγχου όπως DHCP, ICMP και DNS και αποκλείουν κάθε άλλη κίνηση εκτός από τη διαχείριση συσκευών διακομιστή, τον διακομιστή VPN και τον διακομιστή μέτρησης. Οποιεσδήποτε αιτήσεις ιστού (HTTP / HTTPS) που έχουν αποκλειστεί, ανακατευθύνονται σε μια σελίδα στην ιστοσελίδα του έργου, δίνοντας πληροφορίες σχετικά με τις οδηγίες PAWS και εγγραφής. Βασικός στόχος αυτής της χρήσης είναι να αποκαλυφθούν οι χρήσεις που μπορεί να προσφέρει ένα σύστημα

όπως το PAWS και έτσι έχει επιλεγεί να μην περιορίζεται η πρόσβαση σε εξωτερικούς ιστότοπους ή υπηρεσίες.

Για να μετριαστεί οποιαδήποτε απειλή ασφάλειας, επιβάλλεται η χρήση κρυπτογραφημένης, επικυρωμένης σύνδεσης VPN από άκρο σε άκρο μεταξύ της συσκευής του πολίτη και του διαδικτυακού PAWS που παρέχεται. Αυτό εξασφαλίζει την προστασία της ιδιωτικής ζωής για την κυκλοφορία του πολίτη και παρέχει τουλάχιστον κάποια εγγύηση στον πολίτη ότι είναι πραγματικά συνδεδεμένο με το δίκτυο PAWS [4].

Ένας ακόμη σκοπός που εξυπηρετείται από το VPN είναι να αποτρέψει τους πολίτες από τη χρήση του δικτύου ανώνυμα. Όλη η πρόσβαση είναι μέσω μιας περιόδου σύνδεσης με το διακομιστή VPN, ώστε να μπορέσει να βρεθεί ποιος συνδέεται επακριβώς και χρησιμοποιεί το δίκτυο PAWS, σε τι έχουν πρόσβαση, σε πόσος χρόνος χρησιμοποιείται στην σύνδεση. Αυτό μετριάζει τον κίνδυνο για τους πολίτες που χρησιμοποιούν το δίκτυο ακατάλληλα, καθώς γίνεται επιτρεπτό να συλλεχθούν δεδομένα για ανάλυση.

4.3 FON

Ένα άλλο δίκτυο το οποίο χρησιμοποιείται ευρέως και έχει μεγάλο εύρος κάλυψης είναι το FON. Το **FON (Fonero Network)** είναι το όνομα μιας κοινότητας Wi-Fi που χρησιμοποιεί κοινωνική δρομολόγηση. Τα μέλη της μοιράζονται την ασύρματη πρόσβασή τους και σε αντάλλαγμα μπορούν να χρησιμοποιήσουν ελεύθερα το Wi-Fi όταν βρουν άλλο σημείο πρόσβασης Fonero [55]. Αυτά τα σημεία πρόσβασης παρέχονται από άλλα μέλη της FOM. Το FON είναι μία προσέγγιση από το χρήστη σε Wi-Fi από ομότιμους χρήστες (peer-to-peer). Για να προσφέρει κάποιος ένα σημείο πρόσβασης FON θα πρέπει να χρησιμοποιούν συμβατό ασύρματο δρομολογητή (router), που ονομάζεται La Fonera, ο οποίος διατίθεται από το FON.

Εφευρέτης του FON είναι ο Martin Varsavsky (γεννημένος το 1960 στο Buenos Aires), ο οποίος είναι ένας Αργεντίνος επιχειρηματίας με έδρα την Ισπανία και ίδρυσε πολλές εταιρίες σε όλο τον κόσμο, περιλαμβάνοντας και την Urban Capital, Viatel, EINSTEINet, Ya.com, και Eolia. Στα τέλη του 2005 ξεκίνησε την επιχείρηση

FON στη Μαδρίτη, η οποία παρέχει διεθνείς υπηρεσίες Wi-Fi χρησιμοποιώντας υποδομή που δημιουργούν οι χρήστες. Η FON υποστηρίζεται από τους επενδυτές μετοχών Google, Skype, Microsoft, Index Ventures και Deutsche Telekom. Το 2012, το δίκτυο έφθασε σε περισσότερα από 7 εκατομμύρια Wi-Fi hotspot σε αρκετές χώρες. Σήμερα, μετράει πάνω από 21 εκατομμύρια hotspots.

Όσοι ανήκουν στην κοινότητα FON ονομάζονται Foneros. Στην ομάδα των Foneros υπάρχουν τρία βασικά επίπεδα συμμετοχής:

1) **Χρήστες:** Αυτοί που μοιράζονται το Wi-Fi τους και σε αντάλλαγμα μπορούν να έχουν δωρεάν Wi-Fi όταν χρησιμοποιούν ένα σημείο πρόσβασης FON.
2) **Ξένοι χρήστες:** Αυτοί που δεν μοιράζονται το δικό τους Wi-Fi αλλά πληρώνουν μία αμοιβή για να χρησιμοποιήσουν ένα σημείο πρόσβασης FON.
3) **Κερδοφόροι χρήστες:** Αυτοί που βγάζουν χρήματα από το Wi-Fi τους. Οι χρήστες κερδίζουν ένα ποσοστό της αμοιβής που πληρώνουν οι ξένοι χρήστες για να χρησιμοποιήσουν το FON.

Υπάρχει κάποια διαμάχη σχετικά με το FON και τις υπηρεσίες του, που προκύπτει κυρίως γύρω από τα νομικά ζητήματα που συνδέονται με τους παρόχους υπηρεσιών διαδικτύου (ISPs). Μερικοί χρήστες του Διαδικτύου που είναι μέλη των χρηστών ίσως παραβιάζουν τους όρους παροχής υπηρεσιών ISP, καθώς ο πάροχος υπηρεσιών τους ενδέχεται να μην επιτρέπει στους χρήστες του να μοιράζονται τις συνδέσεις Wi-Fi ή να μεταπωλούν το εύρος ζώνης τους [56].

4.4 OTE Wi-Fi FON

Η Cosmote σε συνεργασία με την εταιρεία FON, δίνει τη δυνατότητα στους συνδρομητές της να διαμοιράζουν μέρος της σύνδεσής τους, ώστε να μπορεί ένας συνδρομητής να συνδεθεί στο router άλλου, με την προϋπόθεση και ο ίδιος να παρέχει αυτή τη δυνατότητα μέσω του router του. Δημιουργείται δηλαδή, μία κοινότητα όπου οι χρήστες διαμοιράζουν μεταξύ τους μέρος της σύνδεσής τους προς όφελος όλων.

Με την ενεργοποίηση της υπηρεσίας FON, το router εκπέμπει 2ο SSID (Service Set Identifier) με την ονομασία OTE WIFI FON στο οποίο η πρόσβαση γίνεται χωρίς

την εισαγωγή κλειδιού. Όταν όμως επιχειρήσουμε να επισκεφτούμε μία σελίδα, μεταφερόμαστε αυτόματα στο FON Portal και ζητούνται τα στοιχεία σύνδεσης Otenet (Internet Credentials). Κάθε καινούργιος συνδρομητής Cosmote έχει τα δικά του προσωπικά στοιχεία για να συνδεθεί και αν τα ξεχάσει ή τα χάσει μπορεί καλώντας στο 13888 (τεχνική υποστήριξη πελατών Cosmote) από τον αριθμό σύνδεσης που καλεί και εφόσον είναι ο κάτοχος της γραμμής, με κάποια επιβεβαίωση στοιχείων από τον ίδιο, να σταλούν το username (ονομασία) και το password (κωδικός) της σύνδεσής τους, σε κάποιο κινητό που αυτός επιθυμεί [56].

Η υπηρεσία απευθύνεται μόνο σε συνδρομητές Cosmote, αρκεί το router τους να έχει εκπέμψει δίκτυο FON τις τελευταίες 30 ημέρες. Αυτό σημαίνει ότι το router πρέπει να είναι ανοιχτό και να λειτουργεί είτε κάποιος είναι συνδεδεμένος στην υπηρεσία ή όχι. Για λόγους ασφαλείας, ο συνδρομητής που συνδέεται σε δίκτυο FON, χρησιμοποιεί 2ο VLAN (192.168.182.1) και η WAN IP που φαίνεται προς τα έξω είναι διαφορετική από την WAN IP του router.

4.4.1 Λειτουργία χρήσης

Μπορεί κάποιος να κατεβάσει δωρεάν την εφαρμογή που είναι διαθέσιμη για συσκευές Android και iOS, δίνοντας έτσι τη δυνατότητα να:

- συνδέεσαι αυτόματα σε ένα Wi-Fi Spot
- δοκιμάζεις την ταχύτητα της σύνδεσής σου
- αποθηκεύεις τα αγαπημένα σου Wi-Fi Spots για να τα βρίσκεις ακόμα και όταν βρίσκεσαι offline
- παίρνεις ειδοποιήσεις όταν συνδέεσαι σε ένα Wi-Fi Spot
- έχεις πρόσβαση σε έναν εύχρηστο χάρτη με τα Wi-Fi σημεία, ώστε να τα εντοπίζεις και να συνδέεσαι όσο πιο εύκολα γίνεται

4.4.2 Εξοπλισμός

Η ταχύτητα της σύνδεσης των χρηστών δεν επηρεάζεται, ακόμα και όταν μοιράζονται μέρος αυτής, γιατί οι συσκευές που είναι συνδεδεμένες στο ιδιωτικό σου δίκτυο έχουν πάντα προτεραιότητα έναντι των συνδεδεμένων FON επισκεπτών.

Επομένως, η πλοήγησή σου στο Διαδίκτυο δεν επηρεάζεται. Αυτό ισχύει για τους κατόχους εξοπλισμού των κάτωθι router:

- Speedport Entry 2i
- Speedport Entry 2i Plus
- Speedport W724
- ZTE H108NS
- ZTE 931VII

Η μέγιστη ταχύτητα download (κατεβάσματος) είναι 1 Mbps ανά χρήστη, ενώ ο μέγιστος αριθμός ταυτόχρονα συνδεδεμένων επισκεπτών/χρηστών σε ένα δίκτυο Wi-Fi είναι 2. Στις περιπτώσεις μόνο των ZTE δρομολογητών η ταχύτητα είναι 512 Kbps (μέχρι να γίνει Update) και πιθανώς κάποιος να αντιληφθεί χαμηλότερη downlink ταχύτητα όταν 2 επισκέπτες είναι συνδεδεμένοι ταυτόχρονα και κάνουν απαιτητική χρήση (π.χ. κατέβασμα αρχείων, αναπαραγωγή online βίντεο).

Μπορείς να χρησιμοποιήσεις την υπηρεσία, π.χ. από το laptop σου, κινητό ή tablet, μέσω browser ακολουθώντας τα εξής βήματα:

1) Αναζητάς στη mobile συσκευή σου το ασύρματο δίκτυο με όνομα (SSID) «OTE Wi-Fi FON» και το επιλέγεις.
2) Ανοίγεις έναν browser (google chrome, firefox, opera, internet explorer) που χρησιμοποιείς για να σερφάρεις στο Διαδίκτυο.
3) Καταχωρείς το username και password της Cosmote Home Double Play σύνδεσής σου, στα αντίστοιχα πεδία. Αυτό θα χρειαστεί να γίνει μόνο την 1^{η} φορά που θα χρησιμοποιήσεις τον browser [53].

4.4.3 Χώρες δραστηριοποίησης FON

Εκτός Ελλάδας, η FON δραστηριοποιείται στις παρακάτω χώρες με τις αντίστοιχες εταιρίες:

- Αυστραλία (Telstra)
- Βέλγιο (Proximus)
- Βραζιλία (Oi)
- Γαλλία (SFR)

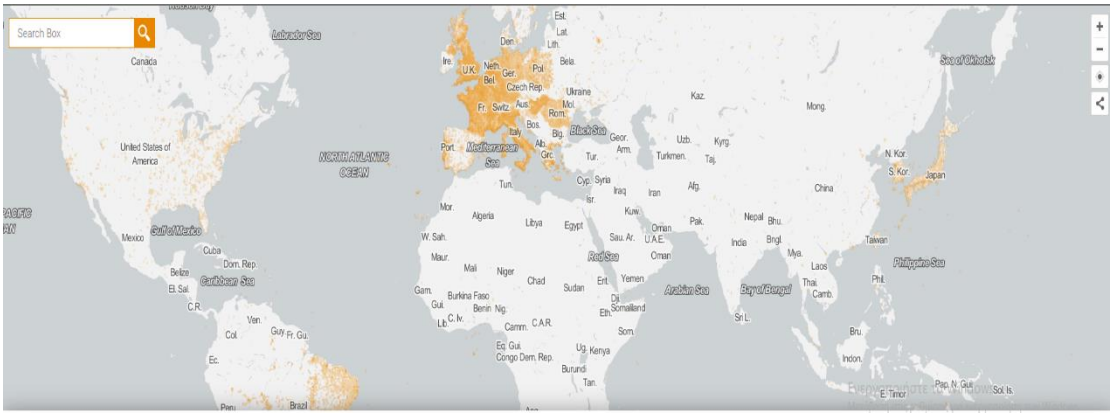
- Γερμανία (DT)
- Ηνωμένο Βασίλειο (BT)
- Ιταλία (Vodafone)
- Ισπανία (Vodafone)
- Ολλανδία (KPN)
- Ουγγαρία (MT)
- Πολωνία (Netia)
- Πορτογαλία (NOS)
- Ρουμανία (MTC)
- Ιαπωνία (SoftBank)
- Ν. Αφρική (MWEB)
- Ν. Κορέα (KT)

4.4.4 Εφαρμογές και hotspots

Το OTE Wi-Fi FON είναι ασφαλές γιατί η υπηρεσία έχει σχεδιαστεί και υλοποιηθεί με τέτοιο τρόπο ώστε να διασφαλίζεται η ακεραιότητα και η ασφάλεια της σύνδεσής σου από κακόβουλους επισκέπτες.

Συγκεκριμένα, το ιδιωτικό/τοπικό δίκτυο του σπιτιού σου είναι εντελώς διακριτό/διαφορετικό από το δημόσιο ασύρματο δίκτυο OTE Wi-Fi FON που είναι διαθέσιμο προς κοινή χρήση. Σε κάθε επισκέπτη του spot αποδίδεται διαφορετική δημόσια IP διεύθυνση. Συνεπώς, οι επισκέπτες του Wi-Fi Spot δεν μπορούν να έχουν άμεση πρόσβαση στο τοπικό, για προσωπική σου χρήση δίκτυο [53].

Μπορεί κάποιος να βρει τα διάφορα hotspots ανάλογα με την περιοχή που βρίσκεται βάζοντας τη χώρα, την πόλη ή τη συγκεκριμένη περιοχή που βρίσκεται μέσω GPS ή ψάχνοντας μέσω του site: https://fon.com/maps/ το οποίο εμφανίζει την παρακάτω εικόνα:



Εικόνα 4-3 Χάρτης σημείων hotspots για Wi-Fi FON

Εκτός από τη συγκεκριμένη σελίδα, κάποιος μπορεί να περιηγηθεί εύκολα και γρήγορα μέσω των κινητών συσκευών που συνδέεται καθένας καθημερινά, μέσα από την εφαρμογή που μπορεί να κατεβάσει κάποιος δωρεάν, είτε χρησιμοποιεί android συσκευή, είτε iPhone. Η εφαρμογή είναι η COSMOTE FON και το λογότυπό της είναι το ακόλουθο:

Εικόνα 4-4: Cosmote FON App

Εικόνα 4-5: FonSpots

5 Freifunk

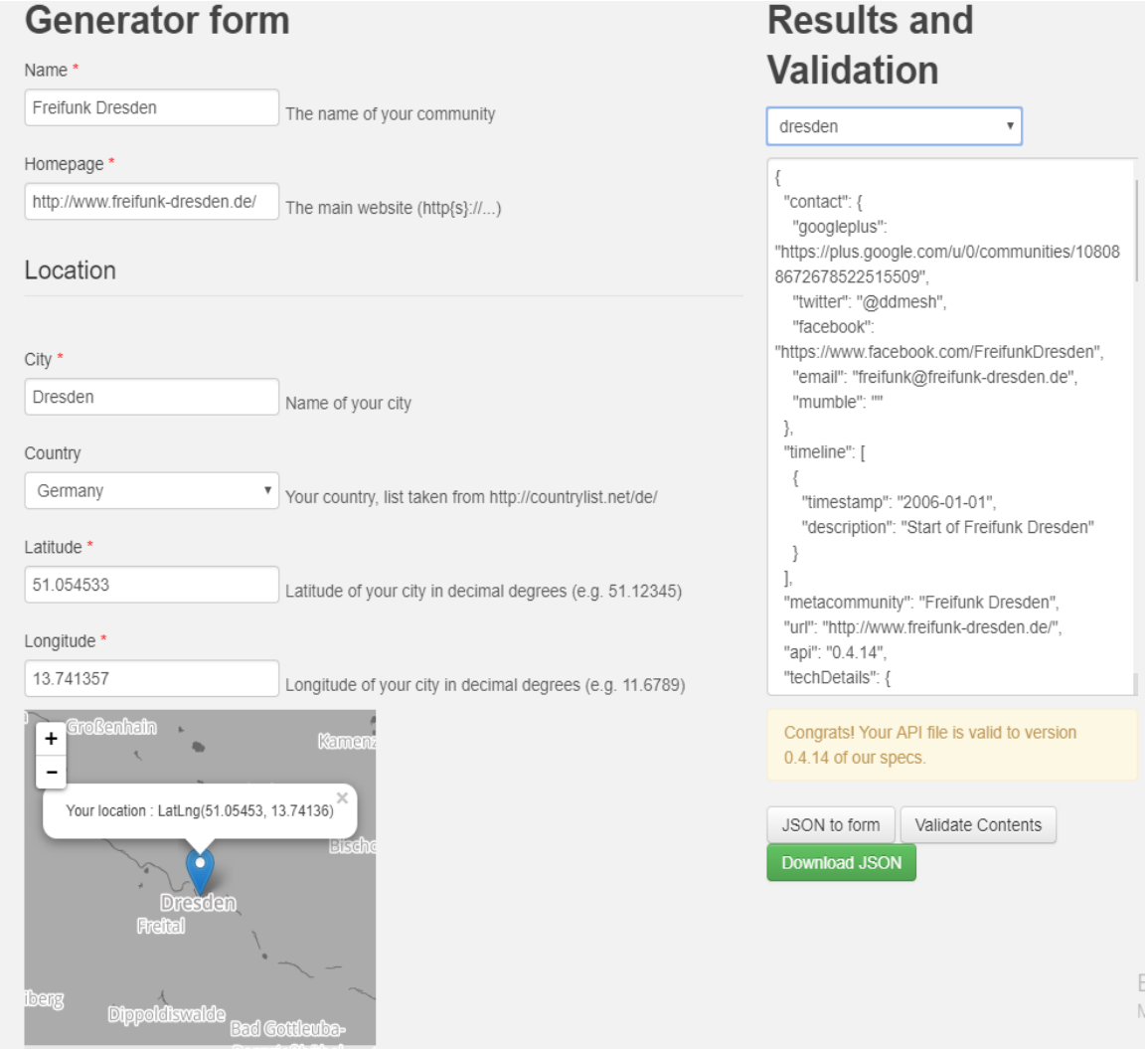
5.1 Λειτουργία

Ένα άλλο δίκτυο πλέγματος είναι το Freifunk, το οποίο δραστηριοποιείται στην Γερμανία. Τα Freifunk (Γερμανική μετάφραση ελεύθερου ραδιοφώνου, πιο κατάλληλη: δωρεάν ασύρματη δικτύωση) είναι μια πρωτοβουλία που υποστηρίζει την ανάπτυξη εργαλείων για δίκτυα πλέγματος που αναφερθήκαμε και προηγουμένως. Εκτός αυτού, η πρωτοβουλία υποστηρίζει κοινότητες που αναπτύσσουν τεχνογνωσία για να δημιουργήσουν τα δικά τους δίκτυα [7].

Ήδη από το 2002, οι γερμανοί ακτιβιστές της Freifunk, μη εμπορικού λαϊκού ομίλου, αποφάσισαν να αυτοοργανωθούν για να παρέχουν δωρεάν και αυτόνομη υποδομή διαδικτύου για όλους. Το 2014, οι άμισθοι του Münster από το τοπικό χάκερ Space Warpzone αποφάσισαν να αναπτύξουν ένα δίκτυο πλέγματος για το συγκρότημα των κτιρίων τους. Επισκέφτηκαν μια γειτονική κοινότητα Freifunk στο Bielefeld, η οποία τους προσέφερε μια σειρά μαθημάτων στη σχετική τεχνολογία, η οποία παρέχεται κυρίως από το εθνικό δίκτυο Freifunk.

Εικόνα 5-1: Freifunk

Το API Freifunk επιτρέπει στις τοπικές ομάδες να προβάλλονται αυτόματα σε εφαρμογές όπως ο χάρτης κοινότητας, το ημερολόγιο και οι παρατιθέμενοι μέσα στον συσσωρευτή feed. Αυτή η γεννήτρια API υποστηρίζει την προετοιμασία του απαιτούμενου αρχείου JSON για να παρέχει ακόμα περισσότερες πληροφορίες σχετικά με την τοπική κοινότητα [40].



Εικόνα 5-2: Γεννήτρια διεπαφής προγράμματος εφαρμογής

5.2 Πρωτόκολλα και ανάλυση

Η κοινότητα Freifunk είναι μέρος ενός δικτύου έργων που αναπτύσσουν εργαλεία για δίκτυα πλέγματος, συμπεριλαμβανομένων των έργων Λογισμικού Freifunk και OpenWrt, πρωτόκολλα δρομολόγησης όπως OLSR και BATMAN, εργαλεία όπως χάρτες για δίκτυα (π.χ. freimap), εργαλεία σάρωσης όπως το εργαλείο horst και πολλά περισσότερα. Πρόσφατα, οι άνθρωποι άρχισαν επίσης να αναπτύσσουν το ανοιχτό λογισμικό όπως η πατάτα πλέγματος για villagetelco.

Πολλοί παρέχουν επίσης πρόσβαση στο ίντερνετ και επιτρέπουν σε άλλους να έχουν πρόσβαση στο παγκόσμιο δίκτυο. Τα δίκτυα ελεύθερης ραδιοεπικοινωνίας είναι

αυτό-κατασκευαζόμενα δίκτυα. Για τη ρύθμισης χρησιμοποιείται το firmware του Freifunk στους δρομολογητές WLAN, μια ειδική διανομή Linux. Οι τοπικές κοινότητες στη συνέχεια διαθέτουν το δικό τους προσαρμοσμένο λογισμικό στους ιστοτόπους τους. Στα χωριά και στις πόλεις υπάρχουν όλο και πιο ελεύθερες ομάδες που συναντώνται τακτικά.

Με το λογισμικό του Freifunk είναι σχετικά εύκολο να εμφανιστούν νέα ασύρματα δίκτυα πλέγματος χρησιμοποιώντας ad-hoc επίπεδο επικοινωνίας WLAN2 και δρομολόγηση επιπέδου 3 με OLSR, BATMAN και άλλα πρωτόκολλα. Προερχόμενη από τη Γερμανία, η Freifunk αναπτύχθηκε με επιτυχία σε πολλές χώρες. Το έργο OLPC στο Αφγανιστάν χρησιμοποιεί το Freifunk για την ανάπτυξη δικτύων για τη διανομή ψηφιακών βιβλίων, ειδήσεων και εκπαιδευτικών μέσων. Στη Γκάνα, το Freifunk χρησιμοποιείται για να γεφυρώσει το ψηφιακό χάσμα στα χωριά. Στο Βιετνάμ, το Freifunk χρησιμοποιείται για να προσφέρει συνδέσεις στο Διαδίκτυο σε εκδηλώσεις ελεύθερες and ανοιχτού κώδικα όπως το FOSSASIA. Στην Ευρώπη και στην Αμερική, τα δίκτυα πόλεων και χωριών μειώνουν το κόστος για τις κοινότητες και τις μικρές και μεσαίες επιχειρήσεις που μοιράζονται κοινές συνδέσεις στο Διαδίκτυο, ADSL, τηλεφωνικές ή δορυφορικές ανερχόμενες σε απομακρυσμένες περιοχές.

5.3 Τρόπος διαμοιρασμού

Η ιδέα είναι ότι κάθε δρομολογητής WiFi μπορεί να μετατραπεί σε σημείο πρόσβασης που επικοινωνεί απευθείας με άλλους δρομολογητές, μεταφέροντας πληροφορίες μεταξύ τους και σχηματίζοντας έτσι ένα "πλέγμα" συνδέσεων δρομολογητή-δρομολογητή. Με αυτόν τον τρόπο, οι χρήστες μπορούν να στείλουν δεδομένα από οποιοδήποτε σημείο του δικτύου χωρίς καν να συνδεθούν στο Διαδίκτυο. Η υποδομή ανήκει και συντηρείται από τους ακτιβιστές, οι οποίοι σχημάτισαν μια ένωση που χειρίζεται νομικές και οικονομικές πρακτικές.

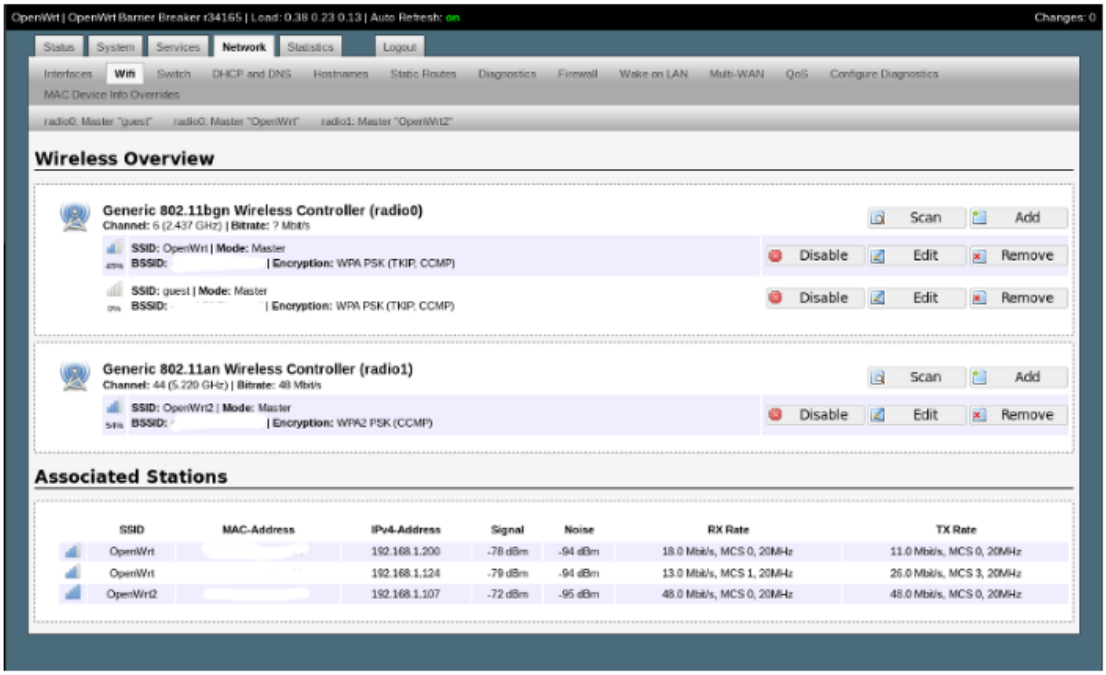
Το ελεύθερο ασύρματο δίκτυο διαμορφώνει τη δική του υποδομή, ανεξάρτητη από το Διαδίκτυο, στο οποίο οι άνθρωποι μπορούν να λειτουργούν τοπικούς διακομιστές web και δωρεάν υπηρεσίες για την ανταλλαγή δεδομένων, την

πραγματοποίηση τηλεφωνικών κλήσεων ή την πραγματοποίηση ραδιοφώνου. Μπορούν να πληρώσουν σε ένα σημείο την πρόσβαση στο Διαδίκτυο, να συνδέσουν το μόντεμ μέσω καλωδίου σε έναν δρομολογητή και να το διαθέσουν στους γείτονες. Το ίδιο πράγμα λειτουργεί και με την πρόσβαση στη σταθερή τηλεφωνία. Πολλοί δίνουν ένα μέρος του εύρους ζώνης τους στο δίκτυο και άλλοι χρηματοδοτούν την πρόσβαση μαζί. Προκειμένου βέβαια να προστατευθούν οι ιδιωτικοί πάροχοι πρόσβασης στο Διαδίκτυο σε ελεύθερα δίκτυα από την έλλειψη ευθύνης από παρεμβολές, οι δρομολογητές συσσωρεύουν την κίνηση στο Διαδίκτυο και δρομολογούν μέσω των δικών τους πυλών [42].

Εκτός από τους κανονικούς εσωτερικούς δρομολογητές WLAN, οι κοινότητες χρησιμοποιούν αδιάβροχες εξωτερικές εγκαταστάσεις στις οποίες το λογισμικό Freifunk λειτουργεί ως λειτουργικό σύστημα και βελτιστοποιεί τις συνδέσεις με κατευθυντικές κεραίες. Τα δίκτυα πλέγματος μπορούν να περιλαμβάνουν σταθερές ή κινητές ασύρματες συσκευές. Για παράδειγμα, οι φορητοί υπολογιστές και τα τηλέφωνα μπορούν επίσης να διαμορφωθούν ως κόμβοι σε δίκτυα Freifunk. Το υλικό αυτό αναπτύχθηκε ακόμη και για ειδικά δίκτυα κοινότητας, οπότε η Freifunk χρησιμοποίησε ως πρότυπο το έργο Village Telco, το οποίο έχει ως στόχο την κατασκευή ελεύθερων και ανοικτών ασύρματων τηλεφωνικών δικτύων.

Εικόνα 5-3: Εγκατάσταση κεραιών Freifunk

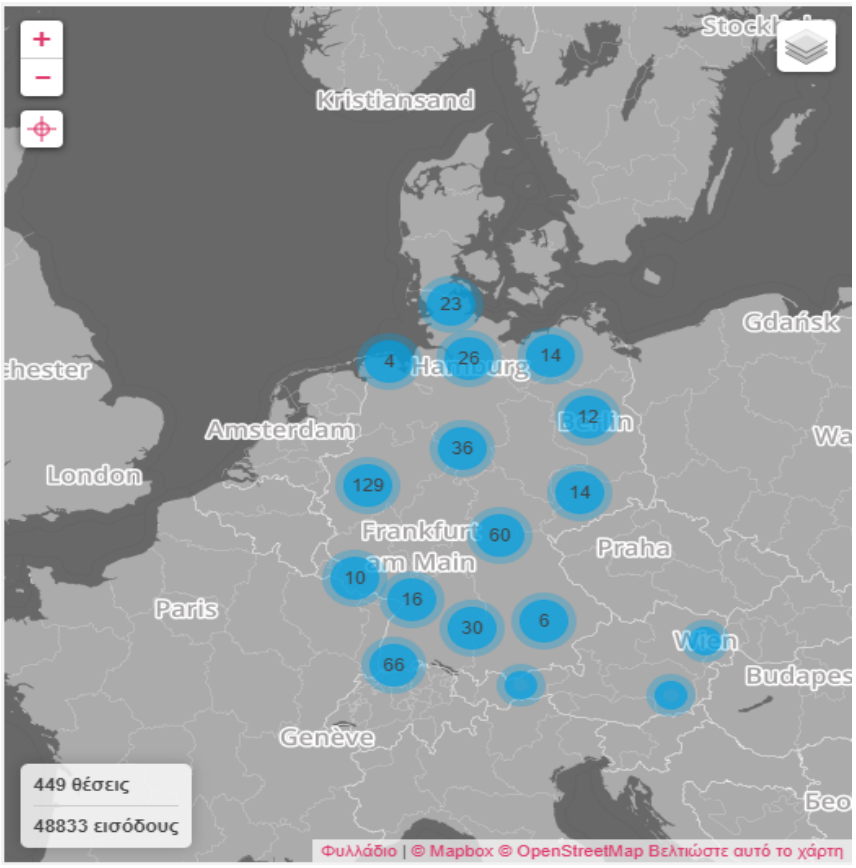
Το υλικό καταγράφεται με το λογισμικό του Freifunk, μια τροποποιημένη έκδοση του OpenWrt. Σε αντίθεση με τα περισσότερα λειτουργικά συστήματα που παρέχονται από τους κατασκευαστές, το OpenWrt μπορεί να ρυθμιστεί πλήρως από τον χρήστη. Για το σκοπό αυτό, ο δρομολογητής "flash" έχει μια διεπαφή χρήστη στην οποία μπορούμε να κάνουμε ρυθμίσεις με τους "κανονικούς" ασύρματους δρομολογητές. Η διεπαφή ιστού δημιουργείται σε LuCl, για την οποία υπάρχουν προ-διαμορφωμένες προσθήκες [7].



Εικόνα 5-4: OpenWrt in Freifunk

5.4 Περιοχές κάλυψης

Παρακάτω μπορούμε να δούμε τις περιοχές της Γερμανίας όπου έχουν εγκατασταθεί κεραίες Freifunk προκειμένου να εξυπηρετήσουν περισσότερους συνδρομητές κόμβους, επεκτείνοντας έτσι το δίκτυο και παρέχοντας ασύρματες υπηρεσίες σχεδόν σε όλες τις πόλεις της Γερμανίας.



Εικόνα 5-5: Χάρτης Freifunk

6 Συμπεράσματα

Αρχικά, είδαμε τη χρήση και σημαντικότητα του Wi-Fi στη ζωή μας και το πως μπορεί κάποιος να συνδεθεί σε κάποιο δίκτυο. Μιλήσαμε και επικεντρωθήκαμε στα ασύρματα δίκτυα, τον ρόλο των δρομολογητών, κεραιών και άλλων σημείων πρόσβασης, που είναι απαραίτητα όχι μόνο στην σύνδεση κάποιου χρήστη στο Διαδίκτυο, αλλά και στον σωστό διαμοιρασμό των συνδέσεων μεταξύ τους.

Αφού μελετήθηκαν όλες εκείνες οι τεχνολογίες και ο τρόπος με τον οποίο μπορεί να γίνει ο διαμοιρασμός των συνδέσεων των χρηστών ανά τον κόσμο, είδαμε τα οφέλη αλλά και τις δυσκολίες που αντιμετωπίζει κανείς στη σύνδεσή του σε κάποιο δίκτυο. Τόσο ο πάροχος, όσο και ο επισκέπτης πρέπει να λάβουν υπόψη τους την ασφαλή σύνδεσή τους στο δίκτυο, δίχως να καταπατούν κανόνες όπως εμπιστευτικότητα και σωστή χρήση του διαδικτύου, έτσι ώστε να επωφελούνται από μία σύνδεση και να μην δρουν ενάντια στην χρήση του άλλου.

Σημαντικός παράγοντας που πρέπει να ληφθεί υπόψη στο διαμοιρασμό των συνδέσεων είναι η απομόνωση της κίνησης, το εύρος ζώνης που επιλέγεται κάθε φορά να διαμοιραστεί (έτσι ώστε να επωφελούνται και οι 2 μεριές, του παρόχου και του επισκέπτη), καθώς επίσης η σημαντικότητα της λογοδοσίας, εξουσιοδότησης του κάθε χρήστη, όπως και ζητήματα αυθεντικοποίησης και ασφάλειας. Θα πρέπει κάθε φορά να ληφθούν υπόψη τα ακριβή στοιχεία του χρήστη και μέσω διαδικασιών όπως χειραψίας και ανταλλαγής προσωπικών στοιχείων μεταξύ χρηστών να μπορεί να γίνει επιτευκτή μία σύνδεση μεταξύ τους.

Είδαμε πως μπορεί ένα δίκτυο να είναι λειτουργικό και όλα εκείνα τα πρωτόκολλα που χρησιμοποιούνται για την επίτευξη ενός τέτοιου σκοπού. Με την χρήση του ANQP μπορούν όχι μόνο να βρεθούν διαθέσιμες συνδέσεις στους χρήστες, αλλά μέσω δυναμικής ενημέρωσης των πινάκων του κάθε σημείου πρόσβασης να μπορεί να γίνει αυτόματα η σύνδεση σε κάποιο δίκτυο. Ακόμα, είδαμε πόσο σημαντικά βοηθάει στην ασφάλεια του δικτύου μας το EAP και πως μπορεί κάθε χρήστης να ανταλλάξει πληροφορίες με τους υπολοίπους. Με το OLSR ακόμα και κάποιο σημείο πρόσβασης να σταματήσει να λειτουργεί, μπορεί μέσω της σύνδεσης των συσκευών

του δικτύου με τέτοιο τρόπο, να μπορεί να βρεθεί ο ακριβώς επόμενος γειτονικός κόμβος και ένας χρήστης να συνδεθεί σε αυτόν δίχως να χρειαστεί να αλλάξει κάτι στις ρυθμίσεις της συσκευής του.

Με την SDN τεχνολογία είδαμε πως μπορεί κανείς να διαχειριστεί το δίκτυο με τέτοιο τρόπο ώστε να προσθέσει επιπλέον υπηρεσίες και να το κάνει περισσότερο λειτουργικό. Ένα από τα πρωτόκολλα που βασίζεται είναι το OpenFlow το οποίο μπορεί να απομονώσει εκτός από την κίνηση και τον έλεγχο, την τοπολογία, αλλά και τη ροή του χώρου, επιτρέποντας έτσι καλύτερη κίνηση στο δίκτυο και τη σωστή διαχείριση των συσκευών, αποτρέποντας συσσώρευση και κάνοντας το δίκτυο περισσότερο ευέλικτο. Ένα άλλο πρωτόκολλο που εξυπηρετεί τη διαχείριση του δικτύου είδαμε ότι είναι το NETCONF, το οποίο με την επικύρωση του κάθε χρήστη, βοηθάει στις συναλλαγές μεταξύ των χρηστών και διαμορφώνει με επιτυχία μαζί με το YANG τις ρυθμίσεις του δικτύου.

Χάρις τα VPN μπορεί να απομονωθεί η κίνηση, να υπάρχει ασφαλής πρόσβαση στο δίκτυο και να προστατευτούν τα απόρρητα στοιχεία του κάθε χρήστη. Είδαμε ότι μέσω των σηράγγων και του πρωτοκόλλου NAT γίνεται η σύνδεση με το Διαδίκτυο και με άκρο προς άκρο στους χρήστες εύκολη, ασφαλής και δύσκολα προσπελάσιμη από κακόβουλους χρήστες.

Μέσω του firmware OpenWrt και του API OpenFlow, μπορεί κανείς να ρυθμίσει την κίνηση του φορτίου και να επιλέξει εκείνα τα στοιχεία που θα κάνουν ένα δίκτυο περισσότερο ευέλικτο με διάφορες δοκιμές και χρήσεις.

Ασχοληθήκαμε κυρίως με την αρχιτεκτονική των δικτύων και είδαμε περισσότερο πως λειτουργούν στην εγκατάσταση τους, τα δίκτυα πλέγματος. Μέσω και πάλι πρωτοκόλλων και κυρίως του Babel και B.A.T.M.A.N. επιτυγχάνεται καλύτερη διαδρομή στην διάδοση της πληροφορίας των χρηστών. Τέτοια δίκτυα είναι τα κοινωνικά, το FON, τα PAWS, όπως και το Freifunk. Κάθε ένα από αυτά χρησιμοποιούν τα πρωτόκολλα που περιγράψαμε και μπορούν να συνδεθούν οι χρήστες με τέτοιο τρόπο μεταξύ τους που μπορούν μέσω του διαμοιρασμού της σύνδεσής τους να επικοινωνούν και να έχουν πρόσβαση στο Διαδίκτυο, ακόμα και σε άλλες χώρες και απομακρυσμένες περιοχές.

Θα πρέπει να μπορεί κάθε χρήστης να διαμοιράζει περισσότερο εύρος ζώνης της σύνδεσής του, να μπορεί να έχει πρόσβαση ακόμα και σε περιοχές που δεν υποστηρίζεται το Wi-Fi, όχι μόνο λόγω εμβέλειας αλλά και διαφόρων παρεμβολών, καθώς επίσης να μπορεί να επιλύει ζητήματα ταχύτητας, είσοδο περισσότερων χρηστών στο δίκτυο, όπως και προβλήματα που μπορεί να παρουσιαστούν στην διασύνδεση των χρηστών μεταξύ τους.

Τέλος, θα πρέπει όσο βελτιώνεται η τεχνολογία, όχι μόνο να εφευρίσκονται καινούργια πρωτόκολλα αλλά και αρχιτεκτονικές αντιμετώπισης των διαφόρων εισβολέων, αλλά και ο τρόπος μετάδοσης της πληροφορίας και της διασύνδεσης της χρήσης του δικτύου να είναι πιο σταθερός, χωρίς απώλειες, διατηρώντας την ανωνυμία των χρηστών, αλλά και παρέχοντας το κυριότερο ρόλο της ασφάλειας της κάθε σύνδεσης στο δίκτυο.

Βιβλιογραφία

[1] Z. Cao, J. Fitschen and P. Papadimitriou. *Social WiFi: Hotspot Sharing with Online Friends*.

[2] A. Abujoda, D. Dietrich, P. Papadimitriou and A. Sathiaseelan. *Software-defined wireless mesh networks for internet access sharing*. pp. 359-372. 2015.

[3] A. Sathiaseelan, C. Rotsos, S. C.S., D. Trossen, P. Papadimitriou and J. Crowcroft. *Virtual Private Networks*.

[4] A. Sathiaseelan, R. Mortier, M. Goulden, C. Greiffenhagen, M. Radenkovic, J. Crowcroft and D. McAuley. *A Feasibility Study of an In-the-Wild Experiment Public Access WiFi Network*.

[5] A. Sathiaseelan and J. Crowcroft. *LCD-Net: Lowest Cost Denominator Networking*.

[6] N. Sastry, J. Crowcroft and K. Sollins. *Architecting Citywide Ubiquitous Wi-Fi Access*.

[7] "Freifunk". [Online]. Available at: https://freifunk.net/worum-geht-es/. [Accessed: 25-Jan-2019].

[8] "B.A.T.M.A.N. protocol concept". [Online]. Available at: https://www.open-mesh.org/projects/open-mesh/wiki/BATMANConcept. [Accessed: 8-Jan-2019].

[9] "Babel (protocol)". [Online]. Available at: https://en.wikipedia.org/wiki/Babel_(protocol). [Accessed: 8-Jan-2019].

[10] "Babel –a loop-avoiding distance-vector routing protocol". [Online]. Available at: https://www.irif.fr/~jch/software/babel/. [Accessed: 8-Jan-2019].

[11] "B.A.T.M.A.N.". [Online]. Available at: https://en.wikipedia.org/wiki/B.A.T.M.A.N.. [Accessed: 8-Jan-2019].

[12] P. Subhash and S.Ramachandram. (2015). *Trust based HWMP Protocol in High-Performance Wireless Mesh Networks*.

[13] "How to Encrypt Your Wireless Network". [Online]. 22-Jan-2019. Available at: https://www.lifewire.com/how-to-encrypt-your-wireless-network-2487653. [Accessed: 25-Jan-2019].

[14] “How to Secure Your Wireless Network”. [Online]. 9-Apr-2007. Available at: https://www.pcworld.com/article/130330/article.html. [Accessed: 25-Jan-2019].

[15] “Κρυπτογράφηση Wi-Fi: πόσο καλά έχετε «κλειδώσει» το Wi-Fi σας;”. [Online]. 6-Sep-2016. Available at: http://popaganda.gr/kriptografisi-wi-fi/. [Accessed: 25-Jan-2019].

[16] “Network Configuration Protocol”. [Online]. Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cns/configuration/15-mt/cns-15-mt-book/cns-netconf.pdf. [Accessed: 21-Dec-2018].

[17] V. Maglaris. (2017). *Αρχιτεκτονικές Διαχείρισης Δικτύων*.

[18] “NETCONF”. [Online]. Available at: https://en.wikipedia.org/wiki/NETCONF. [Accessed: 21-Dec-2018].

[19] “Πρωτόκολλα Επικοινωνίας”. [Online]. Available at: https://diktia.weebly.com/uploads/6/4/5/1/6451366/_protokolla_epikoinonias.pdf. [Accessed: 14-Dec-2018].

[20] “Mesh networking”. [Online]. Available at: https://www.techopedia.com/definition/24398/mesh-networking. [Accessed: 14-Jan-2019].

[21] “Network topology”. [Online]. Available at: https://en.wikipedia.org/wiki/Network_topology. [Accessed: 14-Jan-2019].

[22] “Εικονικό ιδιωτικό δίκτυο”. [Online]. Available at: https://el.wikipedia.org/wiki/Εικονικό_ιδιωτικό_δίκτυο. [Accessed: 4-Feb-2019].

[23] J. Knight. (2011). *An Introduction to Layer 3 Traffic Isolation*.

[24] “Network address translation”. [Online]. Available at: https://en.wikipedia.org/wiki/Network_address_translation. [Accessed: 4-Feb-2019].

[25] R. Sherwood, G. Gibb, K. Yap, G. Appenzeller, M. Casado, N. McKeown and G. Parulkar. (2009). *FlowVisor: A Network Virtualization Layer*.

[26] D. Roos. “How Wireless Mesh Networks Work”. [Online]. Available at:https://computer.howstuffworks.com/how-wireless-mesh-networks-work.htm. [Accessed: 14-Jan-2019].

[27] W. Lou and K. Ren. *Security, Privacy, and Accountability in Wireless Access Networks*.

[28] "Wireless Client Isolation". [Online]. Available at: https://documentation.meraki.com/MR/Firewall_and_Traffic_Shaping/Wireless_Client_Isolation. [Accessed: 8-Dec-2018].

[29] "Secure a Wireless Network with Access Point Isolation". [Online]. 7-Mar-2018. Available at: https://www.neweggbusiness.com/smartbuyer/networking/access-point-isolation-secure-wireless/. [Accessed: 8-Dec-2018].

[30] M. Rouse. (2018). *authentication*.

[31] "Accountability". [Online]. Available at: https://www.computer-security-glossary.org/accountability.html. [Accessed: 4-Dec-2018].

[32] Z. Xiao, N. Kathiresshan and Y. Xiao. (2012). *A survey of accountability in computer networks and distributed systems*.

[33] S. Mozumdar. (2018). *NETCONF and YANG: De facto Network Management for SDN*.

[34] "OpenFlow". [Online]. Available at: https://en.wikipedia.org/wiki/OpenFlow. [Accessed: 18-Jan-2019].

[35] "YANG". [Online]. Available at: https://en.wikipedia.org/wiki/YANG. [Accessed: 18-Jan-2019].

[36] B. Mitchell. (2018). *Network Application Programming Interfaces (APIs)*.

[37] "Software-defined networking". [Online]. Available at: https://en.wikipedia.org/wiki/Software-defined_networking. [Accessed: 17-Jan-2019].

[38] "Extensible Authentication Protocol". [Online]. Available at: https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol. [Accessed: 4-Jan-2019].

[39] "Extensible Authentication Protocols". [Online]. Available at: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/access_registrar/7-0/user/guide/user_guide/eap.pdf. [Accessed: 4-Jan-2019].

[40] "freifunk.net". [Online]. Available at: https://wiki.freifunk.net/Kategorie:English. [Accessed: 3-Feb-2019].

[41] “Welcome to the OpenWrt Project”. [Online]. Available at: https://openwrt.org/. [Accessed: 28-Dec-2018].

[42] “Freifunk”. [Online]. Available at: https://en.wikipedia.org/wiki/Freifunk. [Accessed: 3-Feb-2019].

[43] “Wireless mesh network”. [Online]. Available at: https://en.wikipedia.org/wiki/Wireless_mesh_network. [Accessed: 5-Jan-2019].

[44] “Wireless ad hoc network”. [Online]. Available at: https://en.wikipedia.org/wiki/Wireless_ad_hoc_network. [Accessed: 5-Jan-2019].

[45] “Optimized Link State Routing Protocol”. [Online]. Available at: https://en.wikipedia.org/wiki/Optimized_Link_State_Routing_Protocol. [Accessed: 28-Dec-2018].

[46] “Hybrid Wireless Mesh Protocol”. [Online]. Available at: https://en.wikipedia.org/wiki/Hybrid_Wireless_Mesh_Protocol. [Accessed: 28-Dec-2018].

[47] “Mesh networking”. [Online]. Available at: https://en.wikipedia.org/wiki/Mesh_networking. [Accessed: 28-Dec-2018].

[48] Z. Yan, P. Zhang, and T. Virtanen. (2003). *Trust evaluation based security solution in ad hoc networks*.

[49] F. Akyidliz, X. Wang and W. Wang. (2005). *Wireless mesh networks: A survey*.

[50] P. Nikopolitidis, M. Obaidat, G. Papadimitriou and A. Pobortsis. *Ασύρματα δίκτυα*.

[51] W. Stallings. (2002). *Wireless Communications and Networks*.

[52] Q. Bi, I. Zysman and H. Menkes. (2001). *Wireless Mobile Communications at the Start of the 21st Century*.

[53] “Δωρεάν WiFi”. [Online]. Available at: https://www.cosmote.gr/cs/cosmote/gr/new_my_wifi.html. [Accessed: 30-Jan-2019].

[54] “Να πούμε ΟΧΙ στην υπηρεσία Fon WiFi του ΟΤΕ! Να πούμε ΝΑΙ σε δικά μας δίκτυα WiFi”. [Online]. Available at: https://athens.indymedia.org/post/1515127/. [Accessed: 30-Jan-2019].

[55] Georgakopoulos. (2014). *Δοκιμή: OTE My Wifi*.

[56] “fon”. [Online]. Available at: https://fon.com//. [Accessed: 30-Jan-2019].

[57] “Η χρήση των free WiFi εγκυμονεί σοβαρό κίνδυνο κλοπής προσωπικών δεδομένων”. [Online]. 17-Nov-2017. Available at: https://www.liberal.gr/arthro/177207/ygeia/eidiseis/isoni-chrisi-ton-free-WiFi-egkumonei-sobaro-kinduno-klopis-prosopikon-dedomenonsin.html. [Accessed: 8-Jan-2019].

[58] A. Kyritsis. “Τι είναι το VPN – Virtual Private Network – και γιατί μπορεί να χρειάζεστε ένα”. [Online]. 18-Jan-2013. Available at: https://www.pcsteps.gr/1376-vpn-technology-explained/. [Accessed: 20-Jan-2019].