ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

# Σχεδίαση και ανάπτυξη ασφαλούς πρωτοκόλλου διαχείρισης και ελέγχου συσκευών για μεγάλης κλίμακας BPL δίκτυα

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αρτέμης Χ. Βουλκίδης

**Επιβλέπων : Παναγιώτης Κωττής**

Καθηγητής ΕΜΠ

Αθήνα, Νοέμβριος 2007

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

# Σχεδίαση και ανάπτυξη ασφαλούς πρωτοκόλλου διαχείρισης και ελέγχου συσκευών για μεγάλης κλίμακας BPL δίκτυα

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αρτέμης Χ. Βουλκίδης

**Επιβλέπων :** Παναγιώτης Κωττής

Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 28η Νοεμβρίου 2007.

| | | |
|---|---|---|
| ..... | ..... | ..... |
| Παναγιώτης Κωττής | Καψάλης Χρήστος | Κανελλόπουλος Ιωάννης |

Αθήνα, Νοέμβριος 2007

.....

Αρτέμης Χ. Βουλκίδης

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

# Περίληψη

Σκοπός αυτής της διπλωματικής εργασίας είναι ο σχεδιασμός και ανάπτυξη ενός ασφαλούς πρωτοκόλλου διαχείρισης και ελέγχου συσκευών για μεγάλης κλίμακας Broadband over Power Line (BPL) δίκτυα. Τα δίκτυα BPL είναι δίκτυα επικοινωνιών τα οποία επιτρέπουν την ευρυζωνική μετάδοση πληροφορίας πάνω από τις γραμμές μεταφοράς μέσης τάσης του εκάστοτε υπάρχοντος ηλεκτρικού δικτύου. Εκτός από τα τηλεπικοινωνιακά οφέλη που τα συστήματα BPL μπορούν να προσφέρουν στα πλαίσια μιας απελευθερωμένης αγοράς τηλεπικοινωνιών, ένας άλλος κλάδος που αναμένεται να ωφεληθεί σημαντικά από αυτά είναι και τα έξυπνα δίκτυα ενέργειας, τα οποία ως στόχο έχουν την αποτελεσματικότερη διαχείριση και αξιοποίηση τόσο των παραδοσιακών όσο και των εναλλακτικών πηγών ενέργειας. Στα πλαίσια των προτύπων διαχείρισης που προτείνουν τα έξυπνα δίκτυα σχεδιάστηκε και υλοποιήθηκε ένα πρωτόκολλο ελέγχου βασισμένο στην XML τεχνολογία Universal Plug and Play, με ταυτόχρονη συνύπαρξη κατάλληλων σχημάτων συνάθροισης και κρυπτογράφησης παρόμοιων με αυτών που παρουσιάζονται στα ασύρματα δίκτυα αισθητήρων. Το τελικό πρωτόκολλο είναι ένας γρήγορος, αυτόνομος, ασφαλής και αποτελεσματικός τρόπος απομακρυσμένου ελέγχου του δικτύου BPL. Οι σχετικές πειραματικές μετρήσεις κατέδειξαν ότι το δίκτυο ανταποκρίνεται ικανοποιητικά όταν οι περιφέρειες που διακρίνονται ανά σημείο συνάθροισης είναι συγκεκριμένου μεγέθους, γεγονός που εισάγει στο σύστημα ένα σημαντικό παράγοντα επίδοσης ικανό να επηρεάσει την ορθή λειτουργία του δικτύου. Η σημαντική επίδραση του μεγέθους συναθροιστικών περιφερειών αποτελεί μελλοντικό σημείο προς μελέτη, καθώς με χρήση θεωρίας παιγνίων μπορεί να μοντελοποιηθεί η συμπεριφορά του συστήματος με απώτερο στόχο την εύρεση του ιδανικού, ως προς τη συνολική επίδοση του πρωτοκόλλου, μεγέθους.

Το πρωτόκολλο που δημιουργήθηκε μπορεί να χρησιμοποιηθεί σε οποιοδήποτε κατανεμημένο δίκτυο ελέγχου με την ίδια επιτυχία, και τους ίδιους παράγοντες. Η γενικότητά του αυτή οφείλεται στο γεγονός ότι το πρωτόκολλο Universal Plug and Play λειτουργεί πανομοιότυπα ανεξάρτητα φυσικού μέσου ή συνδεσμολογίας.



## Λέξεις κλειδιά

Broadband over Power Line, Έξυπνα δίκτυα ενέργειας, Αυτόνομα συστήματα, Αυτόνομος υπολογισμός, Ασύρματα δίκτυα αισθητήρων, Τεχνολογίες XML, Πρωτόκολλο Universal Plug and Play, Συνάθροιση, Κρυπτογράφηση

# Abstract

The scope of this diploma thesis was the design and implementation of a secure device management protocol mainly targeted to large scale Broadband over Power Line (BPL) networks. BPL networks are telecommunication networks that allow the broadband transmission of the signals using the existing medium voltage power line networks. Apart from the obvious telecommunication profit that BPL are able to offer given a liberalized telecommunication market, another field that is expected to considerably take advantage of this new technology, is the one of Smart Energy Grids. Smart Grids aim to effectively manage and exploit not only the traditional but also the alternative energy sources. The designed control protocol was based, in the context of the management patterns implied by the Smart Grid concepts, on the Universal Plug and Play protocol, with the simultaneous use of aggregation and cryptographic schemes inspired by the Wireless Sensor Networks. The implemented protocol is a fast, autonomic, secure and effective way to remotely manage BPL networks. The respective experimental results showed that the network acts sufficiently when the aggregation region consists of a maximum number of control devices. This fact adds a critical performance parameter in the general system design and implementation, capable to affect the whole response profile of it. The impact of the size of the aggregation region on the overall network performance is a future field of study, because it can be modelized by game theoretic models, in order to find the optimum, concerning the effect on the network performance, region size.

The protocol can be effectively used in almost any other similar control network. This universality is due to the fact that the UPnP protocol can operate identically, independently of the physical layer or the configuration of the network.



# Key Words

Broadband Over Power Line, Smart Energy Grids, Autonomic Systems, Autonomic Computing, Wireless Sensor Networks, XML Technologies, Universal Plug and Play Protocol, Aggregation, Cryptography

# Ευχαριστήριο Σημείωμα

Στο σημείο αυτό, θα ήθελα να ευχαριστήσω όλους όσους συνέβαλαν, είτε άμεσα είτε έμμεσα, στην επιτυχή ολοκλήρωση της διπλωματικής αυτής εργασίας.

Ιδιαιτέρως θα ήθελα να ευχαριστήσω θερμά τον Καθηγητή ΕΜΠ και επιβλέποντα της εργασίας μου, κο Παναγιώτη Κωττή, για την εμπιστοσύνη που έδειξε στο πρόσωπό μου με την ανάθεση αυτής της εργασίας. Επιπλέον, θα ήθελα να εκφράσω τις ευχαριστίες μου για το ενδιαφέρον του καθ' όλη τη διάρκεια της εργασίας αυτής, όπως και για την προσοχή με την οποία με συμβούλευσε κατά την εκπόνηση και συγγραφή της.

Επίσης, οφείλω ένα μεγάλο ευχαριστώ στον υποψήφιο Διδάκτορα ΕΜΠ Μάρκο Αναστασόπουλο, για την προσφορά των γνώσεων και των ιδεών του προς όφελος της εργασίας αυτής, καθώς και για την άψογη και πολύ ευχάριστη συνεργασία μας, την οποία εύχομαι να ανανεώσουμε μελλοντικά.

Τέλος, θα ήθελα να αποδώσω ένα ειλικρινές ευχαριστώ σε όλους όσοι με στήριξαν και με πίστεψαν σε όλα τα χρόνια της φοίτησής μου, κυρίως δε την οικογένειά μου για την αμέριστη και αδιάκοπη συμπαράσταση και αγάπη τους.

Αφιερώνεται στον παππού μου Νίκο

# Περιεχόμενα

**ΠΕΡΙΕΧΟΜΕΝΑ** ..... **13**

**ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ** ..... **17**

**1 ΕΙΣΑΓΩΓΗ ΣΤΟ BPL** ..... **19**

**1.1 Εισαγωγικά** ..... **19**

**1.2 Αρχιτεκτονικές συστημάτων BPL** ..... **21**

1.2.1 Αρχιτεκτονική #1 ..... 21

1.2.2 Αρχιτεκτονική #2 ..... 23

1.2.3 Αρχιτεκτονική #3 ..... 25

1.2.4 Πιθανά μελλοντικά συστήματα ..... 26

**2 ΑΥΤΟΝΟΜΑ ΣΥΣΤΗΜΑΤΑ – SMART GRIDS** ..... **29**

**2.1 Αυτόνομα Συστήματα (Autonomic Systems)** ..... **29**

2.1.1 Εισαγωγικά ..... 29

2.1.2 Γενικές Αρχές Αυτόνομων Συστημάτων ..... 30

2.1.2.1 Αυτο–προσαρμογή ..... 31

2.1.2.2 Αυτο–ίαση ..... 31

2.1.2.3 Αυτο–βελτιστοποίηση ..... 31

2.1.2.4 Αυτο–προστασία ..... 32

2.1.3 Βασικές Έννοιες των Αυτόνομων Συστημάτων ..... 32

2.1.3.1 Αυτόνομος Ελεγκτής ..... 33

2.1.3.2 Ελεγχόμενοι πόροι ..... 35

2.1.3.3 Πολλαπλά επίπεδα Αυτόνομων Ελεγκτών ..... 35

2.1.3.4 Συνεργασία Αυτόνομων Ελεγκτών ..... 36

2.1.4 Πολιτικές για Αυτόνομους Ελεγκτές ..... 37

2.1.5 Η αξία των Αυτόνομων Συστημάτων ..... 37

2.1.5.1 Επιχειρήσεις ..... 38

2.1.5.2 Επιχειρήσεις ..... 39

**2.2 Έξυπνα δίκτυα (Smart Grid)** ..... **40**

2.2.1 Εισαγωγικά ..... 40

2.2.2 Η προέλευση των Έξυπνων Δικτύων ..... 42
2.2.3 Οι λόγοι που οδήγησαν στα Έξυπνα Δίκτυα ..... 44
2.2.3.1 Τεχνολογίες νέας γενιάς ..... 45
2.2.3.2 Οι στόχοι που έχουν τεθεί ..... 46
2.2.4 Οφέλη των έξυπνων δικτύων ..... 47
2.2.4.1 Επιτάχυνση υιοθέτησης νέων τεχνολογιών ..... 48
2.2.4.2 Μειωμένα κόστη υποδομών ..... 48
2.2.4.3 Λιγότερα blackout και ενεργειακές διαταραχές ..... 50
2.2.4.4 Βελτιωμένη ενεργειακή απόδοση ..... 50
2.2.4.5 Μείωση εκπομπών αερίων του θερμοκηπίου ..... 51
2.2.4.6 Καθαρή ενεργειακή αγορά ..... 51
2.2.4.7 Ευρείας κλίμακας αξιοποίηση ανανεώσιμων πηγών ενέργειας ..... 52
2.2.4.8 Ενσωμάτωση κατανεμημένων σταθμών παραγωγής ..... 53
2.2.4.9 Μειωμένα κόστη για ενέργεια «ψηφιακής ποιότητας» ..... 53
2.2.4.10 Μικροδίκτυα ..... 54
2.2.4.11 Μειωμένες απώλειες γραμμών μεταφοράς ..... 54
2.2.4.12 Συνδυασμένη θερμότητα – ενέργεια ..... 54
2.2.4.13 Δημιουργία θέσεων εργασίας ..... 55
2.2.5 Ποιοι επηρεάζονται από τα Έξυπνα Δίκτυα ..... 55
2.2.6 Σύνοψη ..... 58

**3 Η ΕΦΑΡΜΟΓΗ ΕΛΕΓΧΟΥ– ΤΟ ΠΡΩΤΟΚΟΛΛΟ UPNP ..... 61**

**3.1 Εισαγωγικά ..... 61**

**3.2 Το πρωτόκολλο Universal Plug and Play ..... 62**
3.2.1 Εισαγωγικά ..... 62
3.2.2 Η λειτουργία του πρωτοκόλλου ..... 65
3.2.2.1 Ανεύρεση (Discovery) ..... 66
3.2.2.2 Περιγραφή (Description) ..... 67
3.2.2.3 Έλεγχος (Control) ..... 68
3.2.2.4 Συγχρονισμός (Eventing) ..... 69
3.2.2.5 Παρουσίαση (Presentation) ..... 70
3.2.3 Το σημείο ελέγχου και η αλληλεπίδραση με τη συσκευή ..... 70
3.2.4 Η αρχιτεκτονική του SDK ..... 73
3.2.4.1 Η εφαρμογή της συσκευής και του σημείου ελέγχου ..... 74
3.2.4.2 SDK API ..... 74
3.2.4.3 SSDP ..... 75

3.2.4.4 Mini Web Server ..... 75
3.2.4.5 GENA ..... 76
3.2.4.6 SOAP ..... 76
3.2.4.7 HTTP ..... 76
3.2.4.8 Mini server ..... 77
3.2.4.9 Η βιβλιοθήκη ThreadUtil ..... 78
3.2.4.10 XML Parser ..... 78
3.2.4.11 Στρώμα BSD Socket ..... 79
3.2.5 Εικονικοί Κατάλογοι ..... 79

**3.3 Η εφαρμογή ελέγχου ..... 81**
3.3.1 Εισαγωγικά ..... 81
3.3.2 Η εφαρμογή της UPnP συσκευής ..... 83
3.3.2.1 Διαμόρφωση και αρχικοποίηση ..... 84
3.3.2.1.1 Η αρχικοποίηση του SDK ..... 84
3.3.2.1.2 Ορισμός ριζικού καταλόγου ..... 85
3.3.2.1.3 Εγγραφή ριζικής συσκευής ..... 86
3.3.2.1.4 Αρχικοποίηση συσκευής ..... 87
3.3.2.1.5 Διαφήμιση της συσκευής ..... 87
3.3.2.2 Διαχείριση αιτήσεων ..... 88
3.3.2.2.1 Αιτήσεις εγγραφής ..... 89
3.3.2.2.2 Αιτήσεις λήψης παραμέτρων ..... 90
3.3.2.2.3 Αιτήσεις ενεργειών ..... 92
3.3.2.3 Αποστολή Γεγονότων ..... 93
3.3.2.4 Διακοπή λειτουργίας ..... 95
3.3.3 Η εφαρμογή του σημείου ελέγχου ..... 95
3.3.3.1 Διαμόρφωση και αρχικοποίηση ..... 96
3.3.3.1.1 Αρχικοποίηση του SDK ..... 96
3.3.3.1.2 Αρχικοποίηση σχετική με το σημείο ελέγχου ..... 97
3.3.3.1.3 Εγγραφή σημείου ελέγχου ..... 97
3.3.3.2 Αναζήτηση για υπηρεσίες ενδιαφέροντος ..... 98
3.3.3.3 Λήψη περιγραφών ..... 101
3.3.3.4 Αναμονή γεγονότων ..... 102
3.3.3.5 Πρόκληση ενεργειών ..... 103
3.3.3.6 Διακοπή λειτουργίας ..... 105

**3.4 Σύνοψη ..... 106**

**4 ΣΥΝΑΘΡΟΙΣΗ ΠΛΗΡΟΦΟΡΙΑΣ – ΚΡΥΠΤΟΓΡΑΦΗΣΗ ..... 109**

**4.1 Συνάθροιση πληροφορίας ..... 110**

4.1.1 Εισαγωγικά ..... 110

4.1.2 Θεωρητικό υπόβαθρο ..... 111

4.1.3 Ο αλγόριθμος συνάθροισης ..... 112

**4.2 Κρυπτογράφηση ..... 125**

4.2.1 Γενικά για την Κρυπτογράφηση ..... 125

4.2.1.1 Ορολογία – Βασικές έννοιες ..... 126

4.2.1.2 Η διαδικασία της κρυπτογράφησης ..... 126

4.2.2 Είδη κρυπτοσυστημάτων ..... 129

4.2.2.1 Συμμετρική κρυπτογραφία ..... 130

4.2.2.1.1 Block αλγόριθμοι ..... 132

4.2.2.1.2 Stream Αλγόριθμοι ..... 133

4.2.2.1.3 Κωδικοί Πιστοποίησης Μηνύματος ..... 133

4.2.2.1.4 Χαρακτηριστικά παραδείγματα συμμετρικών αλγορίθμων ..... 134

4.2.2.1.5 Σύνοψη ..... 135

4.2.2.2 Ασύμμετρη Κρυπτογραφία ..... 136

4.2.2.2.1 Χαρακτηριστικά παραδείγματα ασύμμετρων αλγορίθμων ..... 137

4.2.2.2.2 Σύνοψη ..... 139

4.2.3 Εισαγωγή κρυπτογράφησης στην εφαρμογή ελέγχου ..... 140

4.2.3.1 Η επιλογή του κατάλληλου κρυπτοσυστήματος ..... 140

**5 ΠΡΑΓΜΑΤΟΠΟΙΗΣΗ ΜΕΤΡΗΣΕΩΝ – ΑΞΙΟΛΟΓΗΣΗ ..... 143**

**5.1 Κρυπτογράφηση ..... 144**

**5.2 Αποκρυπτογράφηση ..... 148**

**5.3 Αξιολόγηση μετρήσεων ..... 150**

**6 ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ ..... 153**

**7 ΒΙΒΛΙΟΓΡΑΦΙΑ ..... 157**

# Ευρετήριο Σχημάτων

*Σχήμα 1.1: Το βασικό BPL σύστημα.* ..... *21*
*Σχήμα 1.2: Η πρώτη αρχιτεκτονική BPL δικτύων.* ..... *22*
*Σχήμα 1.3 : Η δεύτερη αρχιτεκτονική BPL δικτύων.* ..... *24*
*Σχήμα 1.4: Η τρίτη αρχιτεκτονική BPL δικτύων.* ..... *25*
*Σχήμα 2.1: Ιδιότητες αυτόνομων συστημάτων.* ..... *31*
*Σχήμα 2.2: Βρόχος ελέγχου αυτόνομων συστημάτων.* ..... *33*
*Σχήμα 2.3: Το τρίγωνο των προκλήσεων που πρέπει να αντιμετωπίσουν τα έξυπνα δίκτυα.* ..... *47*
*Σχήμα 3.1: Συνηθισμένο σενάριο αλληλεπίδρασης σημείου ελέγχου – συσκευής.* ..... *71*
*Σχήμα 3.2: Διάγραμμα αρχιτεκτονικής του SDK για το πρωτόκολλο UPnP* ..... *74*
*Σχήμα 4.1: Το έγγραφο περιγραφής μιας συσκευής* ..... *110*
*Σχήμα 4.2: Η δόμηση του συστήματός ελέγχου μετά από την εισαγωγή των ενδιάμεσων σημείων συνάθροισης.* ..... *114*
*Σχήμα 4.3: Το έγγραφο περιγραφής XML μιας συσκευής (τροποποιημένο).* ..... *116*
*Σχήμα 4.4: Ο κώδικας της updateElement* ..... *118*
*Σχήμα 4.5: Εικονική αναπαράσταση της κατά DOM ιεραρχίας* ..... *119*
*Σχήμα 4.6: Τυπική DOM δομή ενός τυχαίου XML εγγράφου.* ..... *120*
*Σχήμα 4.7: Η ακριβής κατά DOM δομή του XML εγγράφου περιγραφής μιας συσκευής.* ..... *120*
*Σχήμα 4.8: Η κατά DOM αναπαράσταση του συναθροισμένου XML εγγράφου των συσκευών* ..... *121*
*Σχήμα 4.9: Συναθροισμένο έγγραφο τεσσάρων επιμέρους εγγράφων περιγραφής XML* ..... *122*
*Σχήμα 4.10: Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης.* ..... *127*
*Σχήμα 4.11: Τυπικό Μοντέλο Συστήματος Κρυπτογραφίας (κρυπτοσυστήματος)* ..... *128*
*Σχήμα 4.12: Είδη κρυπτοσυστημάτων* ..... *129*
*Σχήμα 5.1: Διάγραμμα περιγραφής της σχέσης συνολικού χρόνου εκτέλεσης – αριθμού συσκευών στο υπολογιστικό σύστημα 1.* ..... *144*
*Σχήμα 5.2: Διάγραμμα περιγραφής της σχέσης συνολικού χρόνου εκτέλεσης – αριθμού συσκευών στο υπολογιστικό σύστημα 2.* ..... *145*
*Σχήμα 5.3: Συγκεντρωτικό διάγραμμα απόδοσης για περιορισμένο αριθμό συσκευών.* ..... *145*
*Σχήμα 5.4: Χρόνος εκτέλεσης αλγορίθμου κρυπτογράφησης μετά από και χωρίς συνάθροιση.* ..... *146*
*Σχήμα 5.5: Σχέση του όγκου διακινούμενης πληροφορίας και του αριθμού συσκευών ελέγχου.* ..... *147*
*Σχήμα 5.6: Σχέση χρόνου – αριθμού συσκευών ελέγχου για την αντίστροφη διαδικασία της συνάθροισης.* ..... *149*
*Σχήμα 5.7: Διάγραμμα σύγκρισης χρόνου σύνθεσης και αποσύνθεσης του τελικού συναθροισμένου XML εγγράφου.* ..... *149*

# 1 Εισαγωγή στο BPL

## 1.1 Εισαγωγικά

Τα δίκτυα πρόσβαση υλοποιούν τη διασύνδεση μεταξύ των πελατών – συνδρομητών και των δικτύων κορμού. Επιτρέπουν σε ένα μεγάλο αριθμό συνδρομητών να κάνουν χρήση διάφορων τηλεπικοινωνιακών υπηρεσιών. Παρόλα αυτά, το κόστος υλοποίησης, εγκατάστασης και συντήρησης των δικτύων πρόσβασης είναι εξαιρετικά μεγάλο. Πολλές μάλιστα φορές αποτελούν περισσότερο από το 50% της επένδυσης στο δίκτυο. Έτσι, οι πάροχοι των δικτύων, προκειμένου να αυξήσουν την ανταγωνιστικότητά τους στην απελευθερωμένη αγορά των τηλεπικοινωνιών, επιδιώκουν την πραγματοποίησή τους με όσο το δυνατό χαμηλότερο κόστος. Στις περισσότερες των περιπτώσεων, τα δίκτυα πρόσβασης τελούν ακόμη υπό την ιδιοκτησία των κυρίων τηλεπικοινωνιακών φορέων των κρατών (για παράδειγμα των πρώην μονοπωλιακών τηλεφωνικών εταιριών). Εξ αιτίας αυτού, οι νέοι εναλλακτικοί πάροχοι τηλεπικοινωνιακών υπηρεσιών προσπαθούν να βρουν καινοτόμες λύσεις για τη δυναμική επανένταξή τους στην αγορά. Μια πολλά υποσχόμενη νέα τεχνολογία για την υλοποίηση των δικτύων πρόσβασης προσφέρεται μέσω των τεχνολογιών των Επικοινωνιών Πάνω από Γραμμές Μεταφοράς Ηλεκτρικής Ενέργειας (PowerLine Communication – PLC).

Η τεχνολογία PLC επιτρέπει τη χρήση των δικτύων μεταφοράς ηλεκτρικής ενέργειας για επικοινωνιακούς σκοπούς και πλέον γενικότερων ευρυζωνικών τηλεπικοινωνιακών υπηρεσιών. Η βασική ιδέα πίσω από το PLC είναι η μείωση του λειτουργικού κόστους και των εξόδων για την υλοποίηση νέων τηλεπικοινωνιακών δικτύων. Η χρήση των δικτύων μεταφοράς ηλεκτρικής ενέργειας για την παροχή τηλεπικοινωνιακών υπηρεσιών δεν είναι κάτι νέο. Υπάρχει μάλιστα από τις αρχές του προηγούμενου αιώνα. Έτσι, τα δίκτυα χαμηλής, μέσης και υψηλής τάσης (ΥΤ) χρησιμοποιήθηκαν για εσωτερικές επικοινωνίες ηλεκτρικών συσκευών και για την υλοποίηση απομακρυσμένων ελεγκτικών και διαγνωστικών σχημάτων. Τα PLC χρησιμοποιούνται επίσης σε εσωτερικές ηλεκτρικές εγκαταστάσεις σε κτίρια και κατοικίες (τα αποκαλούμενα PLC-homes) για διάφορες τηλεπικοινωνιακές εφαρμογές. Προς το παρόν, τα υπάρχοντα συστήματα PLC μπορούν να χωριστούν σε δύο μεγάλες κατηγορίες: τα συστήματα στενής ζώνης και τα συστήματα ευρείας ζώνης. Τα συστήματα στενής ζώνης επιτρέπουν τη λειτουργία υπηρεσιών επικοινωνιών χωρίς σημαντικές απαιτήσεις σε ρυθμούς μετάδοσης όπως επίσης και ορισμένων εφαρμογών φωνής, χαμηλού ρυθμού μετάδοσης έως και 100kbps. Τα ευρείας ζώνης συστήματα υποστηρίζουν πολύ μεγαλύτερες ταχύτητες και έτσι μπορούν να

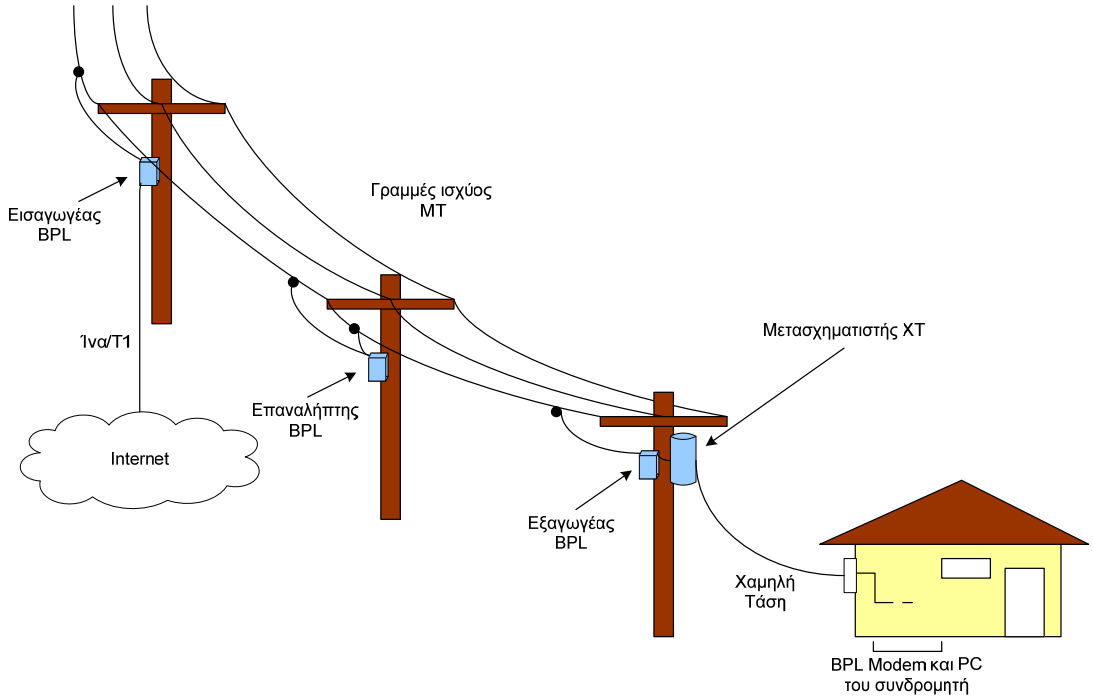
φιλοξενήσουν παράλληλα πολλαπλές τηλεπικοινωνιακές υπηρεσίες όπως είναι η τηλεφωνία και το internet.

Τα ευρυζωνικά PLC συστήματα ή αλλιώς BPL (Broadband Over PowerLine Networks), σε δίκτυα διανομής ΜΤ φαίνεται να είναι μια ευέλικτη και οικονομική λύση για τα τηλεπικοινωνιακά δίκτυα του «τελευταίου μιλίου» (Last Mile Communication Networks), τα λεγόμενα δίκτυα πρόσβασης PLC (1). Αυτό συμβαίνει διότι τα συστήματα BPL δεν υπάρχει ανάγκη για επιπλέον εφαρμογή καλωδίωσης: χρησιμοποιείται όπως έχει ήδη αναφερθεί το υπάρχον δίκτυο διανομής ενέργειας. Υπάρχουν πλέον πολλές δραστηριότητες που σχετίζονται με την ανάπτυξη και εφαρμογή των τεχνολογιών BPL στην περιοχή πρόσβασης. Έτσι, υπάρχει ένας αριθμός κατασκευαστών που προσφέρουν προϊόντα BPL που εξασφαλίζουν μεγάλες ταχύτητες μεταφοράς δεδομένων, ταχύτητες οι οποίες μάλιστα ολοένα και μεγαλώνουν. Υπάρχουν επίσης αρκετές σχετικές δοκιμές παγκοσμίως όπως και πολυάριθμα ήδη υλοποιημένα και εμπορικά συστήματα BPL. Ο αριθμός των συνδρομητών σε υπηρεσίες BPL είναι διαρκώς αυξανόμενος. Μια παρόμοια ανάπτυξη της τεχνολογίας αυτής σε ΜΤ και οικιακά BPL δίκτυα είναι επίσης υπό μελέτη και κατασκευή. Από την άλλη μεριά, δεν υπάρχουν δυστυχώς πρότυπα για τα BPL συστήματα, τα οποία υποτίθεται ότι πρέπει να χρησιμοποιούν ένα εύρος ζώνης μέχρι τα 30MHz. Συγκεκριμένα, το πρόβλημα είναι η ηλεκτρομαγνητική συμβατότητα των συστημάτων BPL σε περιπτώσεις παράλληλης συμβίωσής τους με άλλα τηλεπικοινωνιακά συστήματα, όπως είναι για παράδειγμα οι διάφορες ραδιοφωνικές υπηρεσίες, πρόβλημα το οποίο ακόμη και σήμερα δεν έχει επιλυθεί. Φυσικά όλα αυτά βρίσκονται υπό μελέτη από διάφορες ερευνητικές μονάδες ανά τον κόσμο, ενώ και η IEEE μελετά το θέμα με απώτερο στόχο την οριστική προτυποποίηση του BPL. Έτσι, η τεχνολογία BPL είναι πλέον σε μια πολύ κρίσιμη φάση ανάπτυξης που θα καθορίσει το μέλλον και την ύπαρξή της, τις περιοχές εφαρμογής της, και τη διείσδυσή της στον κόσμο των τηλεπικοινωνιών ως καίριος και ισχυρός ανταγωνιστής των υπαρχόντων δοκιμασμένων συστημάτων.

Ο εξοπλισμός πρόσβασης σε συστήματα Broadband Over PowerLine αποτελείται από εισαγωγείς (injectors), επαναλήπτες (repeaters) και εξαγωγείς (extractors). Ο διαχωρισμός του εξοπλισμού BPL είναι καταχρηστικός και χρησιμοποιείται μόνο για λόγους απλότητας. Ο εξοπλισμός παραμένει σταθερός, απλά αλλάζει η λειτουργία του. Η αναφορά σε αυτό θα γίνεται τελικά με βάση τη λειτουργία του, και όχι την ούτως ή άλλως ενιαία φύση του.

Οι εισαγωγείς BPL συνδέονται με το χώρο του διαδικτύου μέσω ινών ή γραμμών Τ1 και αλληλεπιδρούν με τις γραμμές Μέσης Τάσης (ΜΤ) του δικτύου ηλεκτροδότησης που

εξυπηρετούν την περιοχή εξυπηρέτησης των συστημάτων BPL. Οι γραμμές ΜΤ μπορεί να είναι υπέργειες ή υπόγειες. Στην περίπτωση των υπέργειων γραμμών ΜΤ, τα καλώδια που μεταφέρουν την τάση αναρτώνται σε κατάλληλους στύλους, οι οποίοι τυπικά πρέπει να βρίσκονται σε ύψος 10 μέτρων από την επιφάνεια του εδάφους.




**Σχήμα 1.1: Το βασικό BPL σύστημα.**

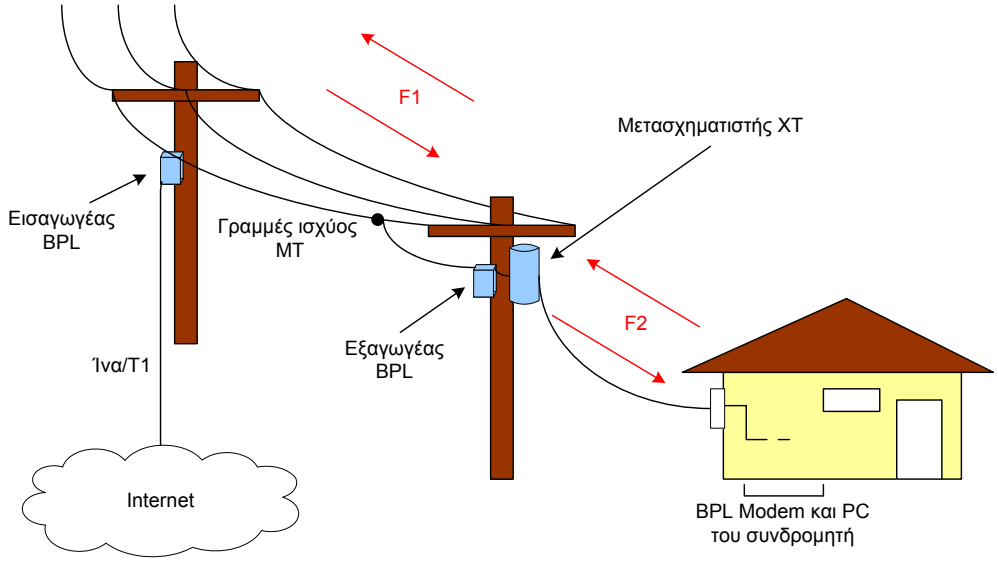
## 1.2 Αρχιτεκτονικές συστημάτων BPL

Η N.T.I.A. (National Telecommunications and Information Administration), η οποία είναι η ύπατη υπηρεσία τηλεπικοινωνιών των Ηνωμένων Πολιτειών Αμερικής, έχει διαχωρίσει τις πιθανές αρχιτεκτονικές των δικτύων BPL που χρησιμοποιούνται από τους περισσότερους παρόχους BPL σε τρεις βασικές αρχιτεκτονικές (2).

### 1.2.1 Αρχιτεκτονική #1

Η αρχιτεκτονική #1 (βλ. Σχήμα 1-2) κάνει χρήση της OFDM (Orthogonal Frequency Division Multiplexing) διαμόρφωσης για να μεταδώσει ευρυζωνικά σήματα BPL, χρησιμοποιώντας πολλαπλά φέροντα στενού εύρους. Ο BPL εισαγωγέας μετατρέπει δεδομένα που προέρχονται από το backbone δίκτυο του Internet, σε σήματα OFDM και κατόπιν εγχύει τα σήματα αυτά σε μία από τις τρείς φάσεις των γραμμών ΜΤ που εξυπηρετούν το δίκτυο BPL. Οι εισαγωγείς υλοποιούν επίσης όπως είναι φυσικό και την αντίστροφη διαδικασία, δηλαδή τη μετατροπή των σημάτων OFDM σε σήματα που είναι συμβατά με το backbone

Internet. Τα διαφορετικού τύπου αυτά δεδομένα μεταφέρονται από και προς τις γραμμές χαμηλής τάσης (ΧΤ), γραμμές οι οποίες τροφοδοτούν συστάδες οικιών, όπου γίνεται χρήση BPL εξαγωγέων προκειμένου να αποφευχθούν οι μετασχηματιστές ΧΤ, που τροφοδοτούν με ηλεκτρικό ρεύμα τις οικίες[1]. Οι εξαγωγείς εκτελούν διαδικασίες δρομολόγησης και ταυτόχρονα μετατρέπουν τα σήματα από τη μορφή που χρησιμοποιούνται για τη μεταφορά τους στα BPL συστήματα (στις γραμμές ΜΤ) σε μορφή που είναι κατάλληλη για χρήση από τους καταναλωτές των παρεχόμενων ευρυζωνικών υπηρεσιών. Οι καταναλωτές λοιπόν διατηρούν τη δυνατότητα πρόσβασης στα BPL δίκτυα με τη βοήθεια ειδικών BPL συσκευών (BPL modems). Προκειμένου να καταστεί δυνατή η σύνδεση μεταξύ των ακραίων (ή μη) εισαγωγέων και εξαγωγέων, είναι γίνεται χρήση επαναληπτών σε όλο το εύρος του δικτύου, όπως φαίνεται και στο Σχήμα 1-1.




**Σχήμα 1.2: Η πρώτη αρχιτεκτονική BPL δικτύων.**

Ο εισαγωγέας και ο εξαγωγέας στην πρώτη αυτή αρχιτεκτονική, μοιράζονται όπως φαίνεται και στο Σχήμα 1-2, ένα κοινό εύρος συχνοτήτων F1 σε όλο το εύρος των γραμμών ΜΤ, διαφορετικό από το εύρος συχνοτήτων F2 που χρησιμοποιείται στο δίκτυο ΧΤ, μετά από τους μετασχηματιστές ΧΤ, από τις οικιακές BPL συσκευές του συνδρομητή. Προκειμένου να μειωθούν οι παρεμβολές στο κανάλι, χρησιμοποιούνται πρωτόκολλα CSMA-CA (Carrier Sense Multiple Access - Collision Avoidance). Η πρώτη αυτή αρχιτεκτονική είναι σχεδιασμένη να δέχεται ένα μικρό ποσοστό ομοδιαυλικής παρεμβολής μεταξύ των

[1] Ο λόγος για τον οποίο οι μετασχηματιστές πρέπει να παρακαμφθούν είναι απλός. Ο ρόλος τους είναι να υποβαθμίζουν τη στάθμη της τάσης που φτάνει στο δίκτυο ΧΤ (καταναλωτές) για να αποφευχθούν κίνδυνοι που σχετίζονται με υψηλής στάθμης τάση. Μαζί όμως με την υποβάθμιση της τάσης, το BPL σήμα κόβεται, κάτι το οποίο είναι ανεπιθύμητο.

ημιανεξάρτητων κυψελών BPL χωρίς την περαιτέρω χρήση ειδικών φίλτρων στις γραμμές μεταφοράς ισχύος, καθώς όλες οι συσκευές στο δίκτυο ΜΤ λειτουργούν στο ίδιο εύρος συχνοτήτων. Τα σήματα BPL στην πρώτη αυτή προσέγγιση της αρχιτεκτονικής των δικτύων BPL είναι δυνατόν να παρέχουν αρκετά μικρά ποσοστά ομοδιαυλικής παρεμβολής ώστε να καθίσταται δυνατή η εφαρμογή δύο ή τριών παρόμοιων συστημάτων σε γειτονικές γραμμές ΜΤ, χωρίς τον κίνδυνο απώλειας πληροφορίας ή αποσυγχρονισμού. Κάτι τέτοιο είναι ιδιαίτερα κρίσιμο σε περιοχές όπου το δίκτυο ΜΤ είναι πυκνό, όπως στα μεγάλα αστικά κέντρα, περιοχές στις οποίες είναι δυνατόν να υπάρχουν περισσότερα από τρία «γειτονικά» δίκτυα ΜΤ. Τέλος, αξίζει να σημειωθεί ότι κατά την πρώτη αυτή αρχιτεκτονική, τα σήματα BPL διοχετεύονται μόνο στη μία φάση του δικτύου και όχι και στις τρεις. Αυτό ισχύει τόσο στο δίκτυο ΜΤ όσο και στο δίκτυο ΧΤ που φτάνει στους συνδρομητές, οπότε δεν είναι απαραίτητη η εγκατάσταση τριφασικών εγκαταστάσεων στις κατοικίες προκειμένου να καταστεί λειτουργική για κάποιον καταναλωτή η υπηρεσία του BPL που επιθυμεί.

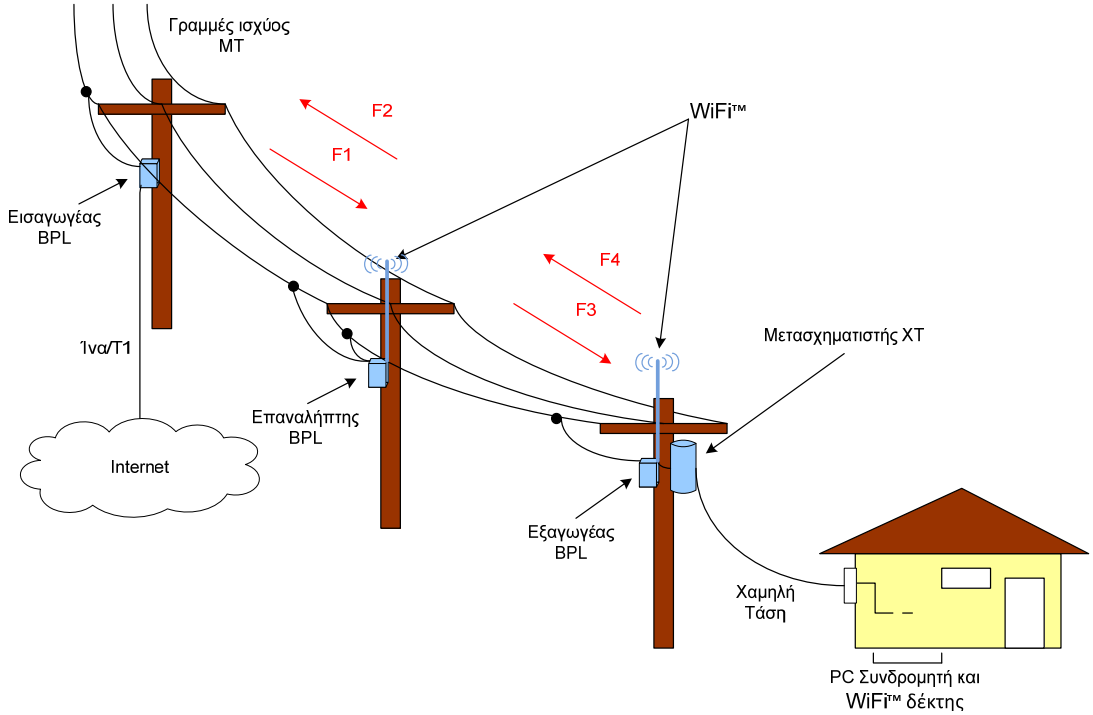
### 1.2.2 Αρχιτεκτονική #2

Η δεύτερη βασική αρχιτεκτονική των συστημάτων BPL είναι παρόμοια με την προαναφερθείσα υπό την έννοια ότι χρησιμοποιείται και πάλι OFDM διαμόρφωση των μεταφερόμενων σημάτων, αλλά διαφέρει ως προς τον τρόπο με τον οποίο μεταδίδει τα σήματα προς χρήση από τους συνδρομητές. Συγκεκριμένα, η δεύτερη αυτή αρχιτεκτονική εξάγει, με τη βοήθεια των εξαγωγέων, το BPL σήμα από τις γραμμές ΜΤ και το μετατρέπει σε IEEE 802.11b WiFi™ σήμα[2]. Οι συνδρομητές με τη σειρά τους πρέπει να διαθέτουν τον αντίστοιχο εξοπλισμό για να μπορέσουν να λάβουν το σήμα αυτό. Σε αυτό το σημείο πρέπει να τονισθεί το γεγονός ότι και άλλα ενδιαφέροντα πρωτόκολλα μπορούν να χρησιμοποιηθούν αντί του WiFi™, με το WiMAX να φαίνεται το επικρατέστερο από αυτά. Η μεγάλη διαφορά της δεύτερης αυτής αρχιτεκτονικής σε σχέση με την πρώτη είναι το γεγονός ότι δε χρησιμοποιείται BPL στις γραμμές ΧΤ προς τους τελικούς αποδέκτες. Το σήμα μεταφέρεται ασύρματα, παρακάμπτοντας έτσι αυτόματα τους μετασχηματιστές τάσης και εξασφαλίζοντας μεγαλύτερο βαθμό φορητότητας και ελευθερίας στους χρήστες που έχουν πρόσβαση στην υπηρεσία.

Μια σημαντική παράμετρος του συστήματος, που αποτελεί παράλληλα και σημαντική διαφορά με την προαναφερθείσα αρχιτεκτονική, είναι το γεγονός ότι το σύστημα

[2] Αυτή η τεχνική είναι η πλέον διαδεδομένη αλλά επί του παρόντος μελετώνται και διάφορες άλλες εναλλακτικές μετάδοσης όπως το νέο πρωτόκολλο IEEE 802.11n, το WiMAX κ.α. .

χρησιμοποιεί διαφορετικές συχνότητες για να ξεχωρίσει τα uplink από τα downlink BPL σήματα, όπως δείχνει και το Σχήμα 1-3 που ακολουθεί.



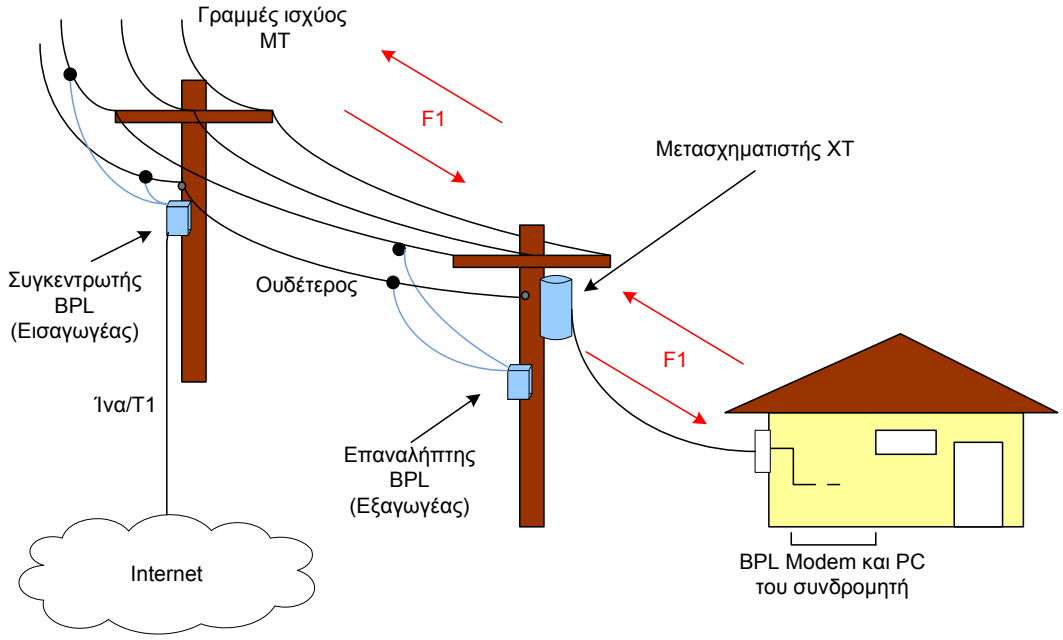

**Σχήμα 1.3 : Η δεύτερη αρχιτεκτονική BPL δικτύων.**

Αυτό γίνεται προκειμένου να περιορισθεί η ομοδιαυλική παρεμβολή μεταξύ γειτονικών καναλιών, εξασφαλίζοντας με αυτόν τον τρόπο πιθανοτικά μεγαλύτερη πυκνότητα δικτύου. Αυτό ιδιαίτερα σημαντικό σε μεγάλα αστικά κέντρα, στα οποία ο σχεδιασμός του συστήματος με στόχο τη μεγαλύτερη δυνατή πυκνότητα δικτύου, λόγω των αυξημένων αναγκών των κατοίκων, συχνά αποτελεί ένα ιδιαίτερα σύνθετο πρόβλημα. Σε ό,τι αφορά όμως τα δίκτυα εκτός πόλης, προκειμένου να εξασφαλισθεί η ελάχιστη δυνατή απώλεια σήματος στη μέγιστη δυνατή απόσταση, μπορεί να γίνει χρήση ειδικών BPL επαναληπτών και ενισχυτών σήματος. Ακριβώς όπως οι εισαγωγείς, έτσι και οι επαναλήπτες δέχονται και εκπέμπουν BPL σήματα σε διαφορετικά εύρη συχνοτήτων, εύρη τα οποία είναι διαφορετικά τόσο από τα αντίστοιχα των γειτονικών επαναληπτών (η εφαρμογή της τεχνικής επαναχρησιμοποίησης συχνότητας είναι ούτως ή άλλως ιδιαίτερα διαδεδομένη στα κυψελωτά συστήματα ασύρματων επικοινωνιών) όσο και από τα εύρη εκπομπής και αποδοχής των εισαγωγέων (βλ. Σχήμα 1-3). Ένα άλλο σημαντικό στοιχείο που σχετίζεται με την αυτονομία αυτής της αρχιτεκτονικής, είναι το γεγονός ότι εάν υπάρχει εξωτερική τροφοδοσία (για παράδειγμα μέσω ηλιακών συσσωρευτών) για τα λειτουργικά στοιχεία του συστήματος, τότε η μετάδοση του BPL σήματος είναι δυνατόν να γίνει και ασύρματα, χωρίς με αυτόν τον τρόπο να επηρεάζεται η σύνδεση των συνδρομητών με το διαδίκτυο

από τις τυχαίες διακοπές παροχής ηλεκτρικού ρεύματος. Τέλος, αξίζει να σημειωθεί ότι τα σήματα BPL εκπέμπονται σε μία μόνο φάση των γραμμών μεταφοράς ισχύος ΜΤ.

### 1.2.3 Αρχιτεκτονική #3

Σε αντίθεση με τις δύο προηγούμενες προτάσεις που παρουσιάστηκαν προηγουμένως οι οποίες έκαναν χρήση OFDM διαμόρφωση για τη μετάδοση των BPL σημάτων, η τρίτη αρχιτεκτονική που πρότεινε η NTIA χρησιμοποιεί την τεχνική DSSS (Direct Sequence Spread Spectrum), βάσει της οποίας όλοι οι χρήστες σε μία κυψέλη BPL χρησιμοποιούν όλο το εύρος συχνοτήτων. Προκειμένου λοιπόν να μειωθεί η ομοδιαυλική παρεμβολή, χρησιμοποιούνται τεχνικές CSMA. Η αρχιτεκτονική δε διαφέρει πολύ σε σχεδιασμό από την πρώτη που εξετάσθηκε, και η τοπολογική της διάταξη φαίνεται στο Σχήμα 1-4:




**Σχήμα 1.4: Η τρίτη αρχιτεκτονική BPL δικτύων.**

Όπως παρατηρείται και από το παραπάνω Σχήμα, κάθε BPL κυψέλη αποτελείται από ένα συγκεντρωτή (εισαγωγέα) ο οποίος όπως είπαμε και νωρίτερα προσφέρει μέσω Τ1 ή ίνας μια διεπαφή του BPL δικτύου με το διαδίκτυο, έναν αριθμό επαναληπτών (εξαγωγέων) οι οποίοι χρησιμοποιούνται για την ενίσχυση των εξασθενημένων σημάτων πάνω στις γραμμές ΜΤ, ενώ οι συνδρομητές προκειμένου να λάβουν το BPL σήμα και να το αξιοποιήσουν, πρέπει να έχουν τον αντίστοιχο εξοπλισμό (BPL modem). Στην αρχιτεκτονική αυτή παρουσιάζεται συχνά επικάλυψη γειτονικών BPL κυψελών. Για να διασφαλιστεί ότι

κάθε συνδρομητής συνδέεται σε μία μόνο κυψέλη, οι BPL επαναλήπτες έχουν τη δυνατότητα να συνδέονται με το συγκεντρωτή που παρουσιάζει τις λιγότερες απώλειες μεταφοράς προς αυτόν. Τέλος αξίζει να σημειωθεί ότι στην Τρίτη και τελευταία αυτή αρχιτεκτονική BPL δικτύων, και σε αντίθεση με τις δύο προηγούμενες, το BPL μεταφέρεται στις γραμμές ΜΤ μέσω τόσο μίας εκ των τριών φάσεων, όσο και από τον ουδέτερο αγωγό.

### 1.2.4 Πιθανά μελλοντικά συστήματα

Οι κατασκευαστές BPL συσκευών καθώς και οι πάροχοι BPL υπηρεσιών, περιμένουν ότι πληθώρα υπηρεσιών θα μπορέσουν να γίνουν προσιτές προς το κοινό μέσω του BPL. Διάφορες από αυτές τις υπηρεσίες όπως το υψηλής ποιότητας video και μουσική ή το VoIP έχουν ήδη δημιουργήσει και νέο ενδιαφέρον σχετικά με την αναζήτηση επιπλέον εύρους ζώνης. Για να μπορέσει να προσφέρει 1Mbps στο μέσο χρήστη (εύρος ζώνης ικανό να μεταφέρει την πιο απαιτητική από τις παραπάνω εφαρμογές που δεν είναι άλλο από το υψηλής ποιότητας video), τα BPL συστήματα δουλεύουν σε ταχύτητες κοντά στα 200Mbps.

Ένα πρόβλημα που έχει ανακύψει όμως και που θα οδηγήσει πιθανώς σε σχεδιασμό νέων συστημάτων διαμόρφωσης και μετάδοσης είναι το εύρος συχνοτήτων που θα χρησιμοποιείται στα BPL συστήματα για τη μετάδοση της πληροφορίας. Πολλοί έχουν προτείνει τις συχνότητες 4MHz – 130MHz, με παράλληλο αποκλεισμό των συχνοτήτων οι οποίες χρησιμοποιούνται από άλλες αδειοδοτημένες εφαρμογές. Στο μέλλον σκοπός είναι κάτι τέτοιο να γίνεται αυτόματα από το σύστημα χωρίς την παρέμβαση διαχειριστών. Για την εφαρμογή μιας τέτοιας λύσης με ταυτόχρονη μεγιστοποίηση του αξιοποιήσιμου εύρους ζώνης, αναμένεται να αναπτυχθούν νέες τεχνικές συμπίεσης, κωδικοποίησης και μετάδοσης σημάτων, με περισσότερα και καλύτερα κατανεμημένα φέροντα κύματα.

Ένα άλλο σημείο το οποίο χρήζει ιδιαίτερης προσοχής καθώς παρουσιάζει ιδιαίτερο τόσο επιστημονικό όσο και οικονομικό ενδιαφέρον είναι αυτό της χρησιμοποιούμενης ισχύος για τη μεταφορά των BPL σημάτων. Όπως είναι γνωστό, οι απώλειες που υφίστανται τα σήματα που μεταδίδονται σε αγωγούς στις προαναφερθείσες συχνότητες υπόκεινται σε υψηλές απώλειες, με αποτέλεσμα μια μελλοντική ανάγκη για περαιτέρω αύξηση του εύρους ζώνης να καθίσταται εξαιρετικά δύσκολη σε σχεδιασμό και υλοποίηση με τα υπάρχοντα μέσα και τεχνολογίες. Τα BPL συστήματα αναμένεται στο μέλλον όμως να λειτουργούν σε αυξημένο εύρος ζώνης, γεγονός που σημαίνει και αυξημένη εκπομπή ισχύος, αλλά όχι απαραίτητα και μεγαλύτερη πυκνότητα ισχύος από τη σημερινή. Μία πρόταση αρκετών BPL

κατασκευαστών είναι η εφαρμογή τεχνολογιών που μπορούν δυναμικά να επιτύχουν ελαχιστοποιημένο, συγκεκριμένο και σταθερό SNR καθ' όλη την έκταση του δικτύου, περιορίζοντας ταυτόχρονα τις ισχύς εκπομπής σε επίπεδα συμβατά με τη ρύθμιση του Part 15 (3) της FCC. Αυτό λοιπόν που παρουσιάζει ενδιαφέρον είναι η υλοποίηση τεχνικών με χρήση των οποίων θα μεγιστοποιείται η μεταδιδόμενη ισχύς με ταυτόχρονη όμως ελαχιστοποίηση της εκπομπής ραδιοσημάτων. Η εταιρία κατασκευής τηλεπικοινωνιακών συσκευών Nortel για παράδειγμα έχει ήδη παρουσιάσει ένα φίλτρο το οποίο καταφέρνει να φιλτράρει τα BPL σήματα, αφήνοντας ανεπηρέαστη τη μεταφορά των σημάτων ενέργειας ΜΤ. Μια τέτοια εξέλιξη είναι εξαιρετικά ελπιδοφόρα σε ότι αφορά την εύρεση νέων τεχνικών βέλτιστης κατάτμησης BPL δικτύων, με απώτερο στόχο την ελαχιστοποίηση **τ**ης ομοδιαυλικής παρεμβολής μεταξύ των γειτονικών BPL κυψελών, όπου όπως και νωρίτερα αναφέρθηκε και ιδιαίτερα στις αρχιτεκτονικές 1 και 3, το φαινόμενο είναι ιδιαίτερα έντονο[3]. Έτσι, όπως είναι λογικό κάτι τέτοιο θα οδηγήσει σε ευρύτερη εφαρμογή επαναχρησιμοποίησης συχνοτήτων, γεγονός ιδιαίτερα σημαντικό για την αύξηση του εύρους ζώνης που είναι δυνατό να εξυπηρετήσει το σύστημα.

[3] Τελικά το σύστημα λειτουργεί παρουσία ομοδιαυλικής παρεμβολής συγκεκριμένων – ανεκτών επιπέδων.

# 2 Αυτόνομα Συστήματα – Smart Grids

## 2.1 Αυτόνομα Συστήματα (Autonomic Systems)

### 2.1.1 Εισαγωγικά

Τα BPL συστήματα είναι κατά βάση κατανεμημένης φύσης και αποτελούνται από ηλεκτρικό εξοπλισμό ο οποίος χρήζει ελέγχου και προστασίας. Η αυτόματη διαχείριση τόσο του δικτύου όσο και του εξοπλισμού είναι αναγκαία για την αξιοπιστία και ορθή λειτουργία του συστήματος. Η ανάγκη για αυτόνομη λειτουργία οδήγησε στην εισαγωγή της έννοια του *αυτόνομου συστήματος* στο υπό μελέτη BPL σύστημα.

Ο όρος «Αυτόνομα Συστήματα» (Autonomic Systems) ή αλλιώς «Αυτόνομος Υπολογισμός» (Autonomic Computing) αποτελεί έννοια που παρουσιάστηκε για πρώτη φορά το 2001. Αναφέρεται στην ικανότητα διαφόρων συστημάτων υπολογισμού οποιασδήποτε μορφής να αντιλαμβάνονται τις αλλαγές στο περιβάλλον τους και να αντιδρούν αντίστοιχα, διαμορφώνοντας με αυτόν τον τρόπο τις κατάλληλες συνθήκες για τη βελτιστοποίηση της λειτουργίας τους, και τη μεγιστοποίηση της απόδοσής τους. Η ιδέα προέρχεται από τη λειτουργία του ανθρωπίνου σώματος, η λειτουργία του οποίου είναι σε πολλά μοντέλα βελτιστοποίησης απόδοσης υποδειγματική.

Το ανθρώπινο σώμα έχει την ικανότητα να προσαρμόζεται στις ανάγκες του εκάστοτε περιβάλλοντος στο οποίο βρίσκεται κάθε στιγμή. Παραδειγματικά, ως αντίδραση σε περίπτωση έντονης μυϊκής άσκησης, προκαλείται εφίδρωση με απώτερο στόχο την αποφυγή υπερθέρμανσης του μυϊκού συστήματος. Παρατηρείται ότι επειδή το ανθρώπινο σώμα λειτουργεί ως μέρος ενός γενικευμένου δυναμικού συστήματος, οι αλλαγές στο περιβάλλον είναι εκτεταμένες και πολλές φορές ακραίες ή και επικίνδυνες ενίοτε. Το παράδειγμα προσαρμογής του ανθρώπινου σώματος, αποτέλεσε και την αρχή της ιδέας του αυτόνομου υπολογισμού, ιδέα η οποία έχει ήδη γίνει αποδεκτή παγκοσμίως ως το πλέον κατάλληλο μοντέλο σχεδίασης αρχιτεκτονικών συστημάτων και λογισμικού που λειτουργούν σε δυναμικό περιβάλλον με αυξημένες ανάγκες αυτόματης και «έξυπνης» προσαρμογής σε διάφορες καταστάσεις που σχετίζονται τόσο με περιπτώσεις έκτακτης ανάγκης όπως πχ η κακόβουλη επίθεση στο λογισμικό, όσο και με συγχώνευση νέων συσκευών / λειτουργιών σε ήδη υπάρχον δίκτυο.

Ένα τέτοιο λοιπόν σύστημα αυτόματων αντιδράσεων παρουσιάζει σαφώς πολλαπλά πλεονεκτήματα σε σχέση με το παραδοσιακό μοντέλο σχεδίασης συστημάτων τόσο σε ό,τι αφορά το λογισμικό μιας πολύπλοκης εφαρμογής όσο και γενικότερα άλλα συστήματα τα οποία πρέπει να αλλάζουν δυναμικά προκειμένου να έχουν βελτιστοποιημένες αποδόσεις. Ειδικά για τα νεότερα συστήματα παντός τύπου που έχουν ως βάση τους εξαιρετικά πολύπλοκο λογισμικό, η συντήρησή τους είναι μια ιδιαίτερα επίπονη διαδικασία, σχετικά με την ανάνηψη του συστήματος από μία εσωτερική δυσλειτουργία, βλάβη ή επίθεση. Εκτός των άλλων, λαμβάνοντας υπόψη το δικτυωμένο περιβάλλον το οποίο υφίσταται, είναι εύκολα αντιληπτό ότι είναι κρίσιμο η δυνατότητα εισαγωγής νέων συσκευών ή λειτουργιών να γίνεται με τρόπο αυτόματο, χωρίς την ανθρώπινη παρέμβαση. Παρακάτω παρουσιάζονται διάφορα γενικευμένα χαρακτηριστικά που αφορούν τον αυτόνομο υπολογισμό, περιγράφοντας με λίγα λόγια την ιδιαιτερότητα αυτών των συστημάτων.

### 2.1.2 Γενικές Αρχές Αυτόνομων Συστημάτων

Η έννοια των αυτόνομων συστημάτων χαρακτηρίζεται από τέσσερα βασικά χαρακτηριστικά, τα οποία σημαντικά στον καθορισμό της έννοιας του αυτόνομου συστήματος και υπολογισμού. Έτσι, ένα αυτόνομο σύστημα, πρέπει να διαθέτει τα παρακάτω χαρακτηριστικά (4):

1. Να είναι αυτο–προσαρμοζόμενο (self–configuring), δηλαδή ικανό να προσαρμόζεται στις αλλαγές του περιβάλλοντός του.
2. Να είναι αυτο–ιάσιμο (self–healing), δηλαδή ικανό να ανανήψει από διάφορα τυχόν λάθη.
3. Να είναι αυτο–βελτιστοποιούμενο (self–optimizing), δηλαδή ικανό να βελτιστοποιεί την απόδοσή του χρησιμοποιώντας παράλληλα τους ελάχιστους δυνατούς υπολογιστικούς πόρους.
4. Να είναι αυτο–προστατευόμενο (self–protecting), δηλαδή ικανό να προλαμβάνει και να θεραπεύεται από τυχόν επιθέσεις.


**Σχήμα 2.1: Ιδιότητες αυτόνομων συστημάτων.**

Παρακάτω παρουσιάζονται αναλυτικότερα οι ιδιότητες αυτές.

### *2.1.2.1 Αυτο–προσαρμογή*

Με την ικανότητα να προσδιορίζει τον εαυτό του δυναμικά, ένα περιβάλλον πληροφορίας μπορεί να προσαρμοστεί αμέσως – με την ελάχιστη ανθρώπινη παρέμβαση όπου είναι απολύτως απαραίτητο – στην υλοποίηση νέων συστατικών ή οποιωνδήποτε αλλαγών στο περιβάλλον.

### *2.1.2.2 Αυτο–ίαση*

Τα αυτο–ιάσιμα περιβάλλοντα πληροφορίας έχουν την ικανότητα να αναγνωρίζουν προβληματικές λειτουργίες (είτε εκ των προτέρων μέσω διαφόρων ευρηστικών μεθόδων είτε με άλλες τεχνικές) και κατόπιν να επιλύουν ορθά τα προβλήματα χωρίς να επηρεάζονται με κανένα τρόπο οι υπόλοιπες διεργασίες του συστήματος. Υπό τον όρο επίλυση ενός προβλήματος εννοείται ότι το σύστημα αλλάζει την ίδια του την κατάσταση ή προκαλεί δραστικές και σημαντικές αλλαγές σε κρίσιμες παραμέτρους του συστήματος. Όσο περνάει ο καιρός, τόσο πιο ανθεκτικό και προσαρμόσιμο γίνεται τελικά το σύστημα, καθώς οι αλλαγές γίνονται με τέτοιο τρόπο ώστε να μειώνονται ή να βοηθούν να εξαλειφθούν οι επιδράσεις στο σύστημα και οι όποιες αστοχίες στα συστατικά του στοιχεία.

### *2.1.2.3 Αυτο–βελτιστοποίηση*

Η αυτο–βελτιστοποίηση αναφέρεται στην ικανότητα των αυτόνομων συστημάτων να μεγιστοποιούν με το βέλτιστο δυνατό τρόπο την κατανομή των πόρων στα διάφορα

συστατικά μέρη του συστήματος και τις υπηρεσίες αυτού προκειμένου να ικανοποιήσουν όσο το δυνατόν περισσότερες απαιτήσεις του τελικού χρήστη με τρόπο αυτόματο και με την ελάχιστη δυνατή ανθρώπινη παρέμβαση. Μικροσκοπικά, ο όρος αυτο – βελτιστοποίηση αφορά στη διαχείριση των πόρων του συστήματος. Μακροσκοπικά όμως τα αυτο–βελτιστοποιούμενα συστατικά μέρη μπορούν με τρόπο εμπειρικό να «μάθουν» το περιβάλλον τους και να συντονιστούν αυτόματα εκ των προτέρων, στα πλαίσια της μεγιστοποίησης της χρηστικότητας και της ευκολίας συντήρησης των αυτόνομων συστημάτων.

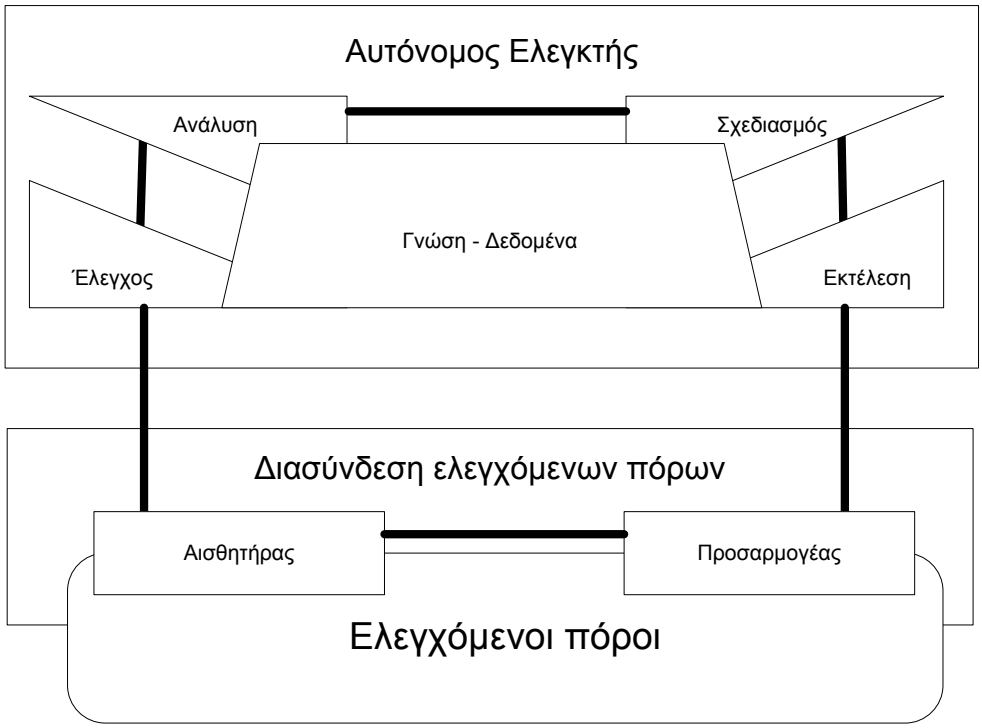
#### *2.1.2.4 Αυτο–προστασία*

Ένα αυτο–προστατευόμενο σύστημα επιτρέπει σε εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στα κατάλληλα δεδομένα την κατάλληλη χρονική στιγμή και μπορεί να δράσει με τέτοιο τρόπο ώστε να καταστήσει αυτόματα τον εαυτό του λιγότερο ευάλωτο σε επιθέσεις κάθε είδους. Ένα αυτο–προστατευόμενο σύστημα μπορεί να ανιχνεύσει εχθρική ή ανεπιθύμητη συμπεριφορά όταν αυτή προκύψει, και να λάβει άμεσα, αυτόνομα μέτρα με απώτερο στόχο να καταφέρει να επηρεάζεται λιγότερο από ιογενείς διεργασίες, επιθέσεις τύπου denial-of-service, και γενικώς κινδύνους και αστοχίες.

### 2.1.3 Βασικές Έννοιες των Αυτόνομων Συστημάτων

Σε ένα αυτόνομο περιβάλλον, τα διάφορα συστατικά μέρη λειτουργούν παράλληλα, με αμοιβαία συνεργασία και με υψηλού επιπέδου εργαλεία διαχείρισης. Μπορούν να ελέγξουν με επιτυχία τόσο τον εαυτό τους όσο και άλλα συστατικά μέρη.

Τα συστατικά αυτά μπορούν να ελέγξουν τον εαυτό τους. Όμως στη γενική περίπτωση και από την άποψη της συνολικής δομής του συστήματος, ορισμένες επιλογές πρέπει να γίνουν από συστατικά στοιχεία ανωτέρω επιπέδου που μπορούν να κάνουν τους απαραίτητους υπολογισμούς και ενίοτε συμβιβασμούς, προκειμένου να βελτιστοποιηθεί η απόδοση του συστήματος με βάση τόσο την στρατηγική όσο και την πολιτική του σχεδιασμού της εφαρμογής. Το παρακάτω σχήμα παρουσιάζει το βρόχο ελέγχου που είναι και ο κορμός της αρχιτεκτονικής αυτόνομων συστημάτων:




**Σχήμα 2.2: Βρόχος ελέγχου αυτόνομων συστημάτων.**

Στη συνέχεια ακολουθεί εκτενής παρουσίαση των στοιχείων που απαρτίζουν το βρόχο ελέγχου των αυτόνομων συστημάτων.

### *2.1.3.1 Αυτόνομος Ελεγκτής*

Ο αυτόνομος ελεγκτής είναι το βασικό στοιχείο του βρόχου ελέγχου. Η θεμελιώδης αρχιτεκτονική του βρόχου αυτού, τον χωρίζει σε τέσσερα βασικά τμήματα, όπως αυτά φαίνονται και στο Σχήμα 2-2:

- Το τμήμα του ελέγχου παρέχει τους μηχανισμούς οι οποίοι συλλέγουν, συναθροίζουν, φιλτράρουν, διαχειρίζονται και αναφέρουν πληροφορίες και λεπτομέρειες (μετρητικές και τοπολογικές) που συλλέγονται από κάθε συστατικό στοιχείο.
- Το τμήμα της ανάλυσης παρέχει τους μηχανισμούς που συσχετίζουν και μοντελοποιούν τις σύνθετες καταστάσεις που προκύπτουν. Αυτοί οι μηχανισμοί επιτρέπουν στον αυτόνομο ελεγκτή να μάθει για το πληροφοριακό περιβάλλον στο οποίο βρίσκεται, να καταφέρει να προβλέψει μελλοντικά γεγονότα, και, γενικά, να βελτιστοποιήσει το σύστημα.
- Το τμήμα του σχεδιασμού αφορά στους μηχανισμούς οι οποίοι δομούν τις κινήσεις που απαιτείται να γίνουν προκειμένου να επιτευχθούν οι στόχοι του αυτόνομου αυτού συστήματος. Η σχεδίαση αυτή χρησιμοποιεί πληροφοριακά δεδομένα που

σχετίζονται με την πολιτική διαχείρισης του συστήματος, έτσι ώστε να γίνει ο σωστότερος σχεδιασμός των επόμενων κινήσεων.

- Το τμήμα της εκτέλεσης είναι αυτό που ελέγχει την εκτέλεση ενός σχεδίου, συνυπολογίζοντας παράλληλα την πιθανότητα αλλαγής παραμέτρων του συστήματος, ενημερώσεων κτλ.

Τα τέσσερα αυτά τμήματα λειτουργούν σε περιβάλλον συνεργασίας και προσφέρουν τελικά τη λειτουργία του βρόχου ελέγχου. Το Σχήμα 2-2 παρουσιάζει μια δομημένη «τοπολογική» παρουσίαση της οριοθέτησης των στοιχείων και όχι κάποιο διάγραμμα ροής. Η έντονη γραμμή που συνδέει τις διάφορες οντότητες μεταξύ τους, θα μπορούσε καλύτερα να εννοηθεί ως μία αρτηρία πληροφορίας και μηνυμάτων. Με άλλα λόγια μπορεί να υπάρξουν καταστάσεις όπου το τμήμα σχεδιασμού πρέπει να επικοινωνήσει αρχικά με το τμήμα της ανάλυσης για να συλλέξει πληροφορίες σχετικά με το πρόβλημα. Θα μπορούσαν επίσης να υπάρξουν καταστάσεις όπου το τμήμα ελέγχου εξαναγκάζει απευθείας το τμήμα του σχεδιασμού να δημιουργήσει νέο σχέδιο δράσης, χωρίς να παρέμβει νωρίτερα το τμήμα ανάλυσης. Τα τέσσερα τμήματα επικοινωνούν μεταξύ τους ασύγχρονα χρησιμοποιώντας συνήθως κάποια αρτηρία μηνυμάτων, με απώτερο στόχο τη βέλτιστη και ταχύτερη επεξεργασία πληροφορίας και λήψη αποφάσεων.

Η αρχιτεκτονική που παρουσιάστηκε δεν προδιαγράφει κάποιο ιδιαίτερο ή μοναδικό πρωτόκολλο διαχείρισης και ελέγχου πληροφορίας. Αυτό που προδιαγράφει κατά κάποιο τρόπο είναι η συνεργασία μεταξύ των τεσσάρων συστατικών μελών του βρόχου ελέγχου, με οποιαδήποτε τεχνολογία υπολογισμού που διατίθεται σήμερα όπως πχ SNMP, Java Management Extensions (JME), Distributed Management Task Force (DMTF), Common Information Model (CIM) και διάφορα άλλα Application Programming Interfaces (API) ή εντολές, όπως και νέες τεχνολογίες που ενδεχομένως θα προκύψουν αργότερα. Στα παραπάνω πρωτόκολλα μπορεί να προστεθεί και το πρωτόκολλο στο οποίο βασίστηκε η παρούσα διπλωματική εργασία, δηλαδή το Universal Plug and Play Protocol (UPnP). Οι λόγοι για τους οποίους μια τέτοια επιλογή είναι δόκιμη θα αναλυθούν αργότερα στην αντίστοιχη παράγραφο.

### 2.1.3.2 Ελεγχόμενοι πόροι

Οι ελεγχόμενοι πόροι είναι τα ελεγχόμενα μέρη του συστήματος. Ένας ελεγχόμενος πόρος μπορεί να είναι ένας μεμονωμένος πόρος ή ένα σύνολο πόρων. Ο ελεγχόμενος πόρος ελέγχεται από τους Αισθητήρες και τους Προσαρμογείς του, όπως φαίνεται στο Σχήμα 2-2.

Οι Αισθητήρες προσφέρουν μηχανισμούς οι οποίοι συλλέγουν πληροφορίες σχετικές με την κατάσταση ή τις μεταβολές κατάστασης ενός στοιχείου. Οι Αισθητήρες μπορούν να υλοποιηθούν με κατάλληλες software συναρτήσεις τύπου *get* έτσι ώστε να είναι σε θέση να λαμβάνουν πληροφορίες σχετικές με την τρέχουσα κατάσταση ή ένα σύνολο από γεγονότα που χρήζουν ελέγχου και διαχείρισης (για παράδειγμα αυτόκλητα, ασύγχρονα μηνύματα ή ενημερώσεις) που προκύπτουν όταν η κατάσταση του αντικειμένου που εξετάζεται αλλάζει κατά συγκεκριμένο τρόπο.

Οι Προσαρμογείς είναι μηχανισμοί που αλλάζουν την κατάσταση (διαμόρφωση) ενός στοιχείου – αντικειμένου. Δηλαδή οι προσαρμογείς είναι μία συλλογή από συναρτήσεις *set* ή API που μεταβάλλουν την κατάσταση του ελεγχόμενου πόρου.

Ο συνδυασμός των Αισθητήρων με τους Προσαρμογείς συνιστά τη διεπαφή διαχείρισης (αναγράφεται ως Διασύνδεση Ελεγχόμενων Πόρων στο Σχήμα 2-2) που είναι διαθέσιμη στον Αυτόνομο Ελεγκτή. Η αρχιτεκτονική υποδεικνύει ότι οι Προσαρμογείς και οι Ελεγκτές είναι συνδεδεμένοι μεταξύ τους. Αυτό είναι πολύ σημαντικό καθώς η αλλαγή της κατάστασης ενός εκ των δύο, είναι αυτόματα ισοδύναμη με μία ισοδύναμη «κοινοποίηση» αλλαγής κατάστασης από τη διεπαφή του αντικειμένου αυτού (είτε πρόκειται για Αισθητήρα είτε για Προσαρμογέα), εξασφαλίζοντας έτσι ενοποιημένο τρόπο αναφοράς στις δύο αυτές οντότητες.

### 2.1.3.3 Πολλαπλά επίπεδα Αυτόνομων Ελεγκτών

Όπως έχει ήδη γίνει αντιληπτό, στα πλέον σύνθετα σενάρια (που όμως είναι και τα πλέον συνήθη), τα αυτόνομα συστήματα αποτελούνται από πολλούς Ελεγχόμενους Πόρους και πολλούς Αυτόνομους Ελεγκτές. Στην ιδεατή κατάσταση κάθε συστατικό ενός συστήματος πρέπει να αντιστοιχεί ένας Ελεγχόμενος Πόρος με το δικό του Αυτόνομο Ελεγκτή. Εντούτοις, και το ίδιο το σύστημα ως σύνολο μπορεί επίσης να θεωρηθεί ως Ελεγχόμενος Πόρος με το δικό του Αυτόνομο Ελεγκτή. Σε αυτήν την περίπτωση, μπορεί να θεωρηθεί ότι όλα τα συστατικά στοιχεία του συστήματος έχουν τους δικούς τους Αισθητήρες και Προσαρμογείς, οι οποίοι ελέγχονται από ένα κεντρικό Αυτόνομο Ελεγκτή, αυτόν του συστήματος. Έτσι είναι δυνατό ο κεντρικός Ελεγκτής να λάβει αποφάσεις, ανάλογα με τις αποκρίσεις των

επιμέρους Ελεγχόμενων Πόρων, επηρεάζοντας το σύστημα σε καθολικό επίπεδο, καθιστώντας έτσι πιο αποτελεσματική την διαχείριση των πόρων σε σχέση με την πολιτική και στρατηγική που απαιτεί η ορθή διαχείριση των πόρων του συστήματος. Έτσι, η πολιτική καταδεικνύει τις πληροφορίες ή πράξεις που πρέπει να αντιμετωπισθούν στο επίπεδο του συστατικού στοιχείου και τι πρέπει να ελεγχθεί από τον κεντρικό Αυτόνομο Ελεγκτή της εφαρμογής.

Παρόμοια, το σύστημα ενδέχεται να είναι και μέρος μιας επαγγελματικής λύσης που αποτελείται από ένα πλήθος άλλων συσχετιζόμενων συστημάτων. Η ικανότητα αυτής της αρχιτεκτονικής να κλιμακώνεται ανάμεσα σε πολλαπλά επίπεδα Αυτόνομων Ελεγκτών επιτρέπει τη σταδιακή υλοποίησή της με συσσωρευτικά ανά επίπεδο πλεονεκτήματα.

#### *2.1.3.4 Συνεργασία Αυτόνομων Ελεγκτών*

Οι πολυάριθμοι Αυτόνομοι ελεγκτές σε ένα πολύπλοκο σύστημα πληροφοριών πρέπει να συνεργάζονται για να μπορέσουν να εκπληρώσουν κάποιους κοινούς στόχους που έχουν τεθεί από την πολιτική του συστήματος. Για παράδειγμα, ένα σύστημα βάσεων δεδομένων πρέπει απαραίτητα να επικοινωνεί με το διακομιστή, το υποσύστημα αποθήκευσης, το λογισμικό διαχείρισης αποθήκευσης, τον Web Server, και άλλα στοιχεία στο σύστημα με σκοπό το σύστημα πληροφορίας να αποκτήσει την κατάλληλη υποδομή ώστε να αποτελέσει ένα αυτόνομο, αυτό – διαχειριζόμενο σύστημα. Οι Αισθητήρες και οι Προσαρμογείς που προσφέρονται από το αυτόνομο σύστημα διευκολύνουν τη συνεργατική αλληλεπίδραση με άλλους Αυτόνομους Ελεγκτές.

Επιπροσθέτως, οι Αυτόνομοι Ελεγκτές μπορούν να επικοινωνούν μεταξύ τους τόσο σε ομότιμες (peer–to–peer) όσο και σε ιεραρχικές δομές. Το ενδιαφέρον σε τέτοιες αρχιτεκτονικές είναι το γεγονός ότι εφόσον τα πλαίσια στα οποία οι Αυτόνομοι Ελεγκτές λαμβάνουν αποφάσεις ώστε να βελτιστοποιείται η απόδοση του συστήματος, πρέπει να μπορούν να συνεργαστούν με τρόπο ενιαίο, κοινό και αποδοτικό. Αυτό μπορεί να επιτευχθεί μέσω των Αισθητήρων και των Προσαρμογέων από τους Αυτόνομους Ελεγκτές, χρησιμοποιώντας αντίστοιχο κατάλληλο πρωτόκολλο διαχείρισης. Αυτό το πρωτόκολλο επιτυγχάνει να αναγνωρίσει καταστάσεις όπου οι απαιτήσεις πολλαπλών Ελεγκτών είναι φαινομενικά αντικρουόμενες. Σε αυτήν την περίπτωση, μπορεί να καταλήξει σε μια λύση βασισμένη σε μία ενιαία πολιτική βελτιστοποίησης της επιχειρηματικότητας και του κέρδους.

### 2.1.4 Πολιτικές για Αυτόνομους Ελεγκτές

Έχει γίνει ήδη εκτεταμένη αναφορά στο πώς επηρεάζουν γενικά το σύστημα οι πολιτικές τόσο των συστημάτων στο σύνολό τους, όσο και των εκάστοτε Αυτόνομων Ελεγκτών. Αν και η παρούσα εργασία δεν έχει ως σκοπό να περιγράψει ή να συγκρίνει πολιτικές μεταξύ τους, εν τούτοις θα γίνει μια πολύ μικρή αναφορά στο συγκεκριμένο θέμα.

Ένα αυτόνομο υπολογιστικό σύστημα απαιτεί μία ενιαία μέθοδο για να καθορίζει τις πολιτικές που ορίζουν τη λήψη αποφάσεων από τους Αυτόνομους Ελεγκτές. Μια πολιτική καθορίζει τα κριτήρια που ένας Αυτόνομος Ελεγκτής χρησιμοποιεί για να τελέσει ένα σύνολο διαδικασιών. Έτσι, οι πολιτικές είναι ένα μέρος – κλειδί της «γνώσης» που χρησιμοποιούν οι Αυτόνομοι Ελεγκτές για να λάβουν αποφάσεις, καθώς επηρεάζουν σε πολύ μεγάλο βαθμό τις αποφάσεις που λαμβάνονται από το τμήμα του σχεδιασμού στους Αυτόνομους Ελεγκτές. Καθορίζοντας τις πολιτικές με ένα συγκεκριμένο (standard) τρόπο, είναι δυνατό μέσω της διάδοσής τους σε όλους τους Αυτόνομους Ελεγκτές να ωθηθεί ένα ολόκληρο σύστημα σε λειτουργία βασισμένη σε ένα κοινό σύνολο πολιτικών.

Οι πολιτικές πρέπει να ορίζονται με τρόπο ενιαίο προκειμένου το αυτόνομο σύστημα να λειτουργεί και αυτό με τρόπο ενιαίο. Η IBM, μάλιστα, μέσω πλήθους σχετικών εγγράφων καθόρισε διάφορες προδιαγραφές και ικανότητες για Αυτόνομους Ελεγκτές με λειτουργία βασισμένη σε πολιτικές. Αυτός ο ορισμός περιέχει:

- Τον καθορισμό της κανονικής διευθέτησης των παραμέτρων των στοιχείων διαχείρισης.
- Τη διαμόρφωση που χρησιμοποιείται για να καθορισθούν οι ανάγκες ή τα κριτήρια απόφασης των χρηστών.
- Τους μηχανισμούς που χρησιμοποιούνται προκειμένου να καθορισθούν οι πολιτικές διαμοιρασμού και διακίνησης πολιτικών στους επιμέρους Αυτόνομους Ελεγκτές από τον κεντρικό Ελεγκτή.
- Τη δομή που χρησιμοποιείται ώστε να καθοριστεί και να μοιραστεί μια πολιτική μεταξύ των Αυτόνομων Ελεγκτών.

### 2.1.5 Η αξία των Αυτόνομων Συστημάτων

Με την κατάλληλη προσαρμογή ώστε τα υπολογιστικά συστήματα να έχουν ιδιότητες αυτό – προσαρμογής, αυτό – ίασης, αυτό – βελτιστοποίησης και αυτό – προστασίας, ο αυτόνομος υπολογισμός αναμένεται να προσφέρει πολλαπλά οφέλη για τα εμπορικά

συστήματα, όπως μειωμένα λειτουργικά έξοδα, μικρότερους ρυθμούς λαθών, μεγαλύτερη ασφάλεια και φυσικά την ικανότητα να αποκρίνονται ταχύτερα και ορθότερα στις ανάγκες της επιχείρησης μέσα στην αγορά την οποία λειτουργούν.

#### *2.1.5.1 Επιχειρήσεις*

Τα αυτόνομα συστήματα, αποτελώντας ένα καθολικό πρότυπο διαλειτουργικής συμπεριφοράς μεταξύ διαφόρων οντοτήτων, μπορούν να έχουν εφαρμογή και σε πολλές περιπτώσεις. Ειδικά για τις επιχειρήσεις που ασχολούνται με θέματα που απαιτούν ομαδική, κατανεμημένη και συνεργατική εργασία από τους υπαλλήλους τους, η εφαρμογή της θεωρίας των αυτόνομων συστημάτων στις διοικητικές πολιτικές εργασίας, μπορεί να έχει ευεργετικά αποτελέσματα. Οι πρωταρχικές επαγγελματικές δεσμεύσεις των σημερινών επιχειρήσεων εξάλλου περιλαμβάνουν τη σταδιακή μείωση του κόστους ιδιοκτησίας της υποδομής ενώ ταυτόχρονα πρέπει να αυξάνεται η παραγωγικότητα των χρηστών.

Ο Αυτόνομος Υπολογισμός αποτελεί βασικό μέρος της αυτονομίας, που είναι ένα από τα τρία κύρια χαρακτηριστικά της ηλεκτρονικής αγοράς. Τα άλλα δύο είναι:

- Τα ολοκληρωμένα, βασικά επιχειρηματικά συστήματα είναι συνδεδεμένα στα πλαίσια της επιχείρησης και προέρχονται από διαφορετικές εταιρίες.
- Εικονικά δεδομένα και εφαρμογές ελέγχονται κεντρικά, μέσω μιας δικτυακής υποδομής, η οποία βελτιστοποιεί τη χρήση της υπολογιστικής δυνατότητας και προσφέρει αυξημένη απόδοση.

Τα οφέλη από μία αυτόνομη επαγγελματική προσέγγιση είναι αμέσως ορατά: Οργανώνεται ένα δίκτυο, τα έξυπνα αυτόνομα στοιχεία μπορούν να προσφέρουν στους πελάτες ό,τι αυτοί ζητήσουν, όταν το χρειάζονται, χωρίς διαρκή πνευματικό ή σωματικό κόπο.

Όταν τα συστήματα και τα δίκτυα αρχίσουν να διαθέτουν τα χαρακτηριστικά των αυτόνομων συστημάτων, οι επαγγελματίες που αναπτύσσουν τα συστήματα αυτά θα μπορούν να επιτύχουν αυξημένη απόδοση. Οι επικεφαλείς θα μπορούν να θέτουν επιχειρηματικούς στόχους και οι υπολογιστές θα μπορούν να καθορίσουν τις ενέργειες που πρέπει να γίνουν προκειμένου οι στόχοι αυτοί να ικανοποιηθούν. Για παράδειγμα, σε ένα περιβάλλον οικονομικών συναλλαγών, οι επικεφαλείς είναι σε θέση να αποφασίσουν ότι οι συναλλαγές πρέπει να ολοκληρώνονται σε λιγότερο από ένα δευτερόλεπτο με απώτερο στόχο να επιτευχθούν συγκεκριμένοι στόχοι εξυπηρέτησης και κέρδους. Στα πλαίσια αυτά ευθύνη των διάφορων εργαλείων λογισμικού είναι να κατευθύνουν τα υπολογιστικά

συστήματα προς μία τέτοια λειτουργία ώστε να εξυπηρετηθεί ο στόχος που τέθηκε από τους επικεφαλής διευθυντές των οικονομικών τμημάτων της επιχείρησης.

Καθώς οι εταιρίες δημιουργούν υποδομές που υποστηρίζουν τις δυναμικές ανάγκες ενός υπολογιστικού συστήματος, τα προϊόντα λογισμικού που ικανοποιούν τις προδιαγραφές και υλοποιούν τεχνικές αυτόνομου υπολογισμού καθίστανται ελκυστικότερα στους υπεύθυνους λήψης αποφάσεων που σχετίζονται με την υπολογιστική υποδομή της επιχείρησης. Έτσι, στο μέλλον τα αυτόνομα συστήματα αναμένεται να διαδραματίσουν σημαντικότερο ρόλο στην αγορά και γενικότερα τα συστήματα υπολογισμού.

### *2.1.5.2 Επιχειρήσεις*

Στη συνέχεια παρατίθενται παραδείγματα θετικών επιπτώσεων που προκύπτουν από τη χρήση λειτουργιών αυτόνομου υπολογισμού με χαρακτηριστικά αυτο–ελέγχου και αυτό–διαχείρισης.

- Λειτουργική αποτελεσματικότητα

  Όσο η πληροφοριακή υποδομή γίνεται συγκριτικά αυτόνομη, τόσο σημαντικότερη γίνεται η εκτέλεση των διάφορων επιχειρηματικών πολιτικών από την πληροφοριακή διαχείριση. Η διαχείριση της επιχείρησης και του πληροφοριακού συστήματος θα είναι το ίδιο και το αυτό, χωρίς να υπάρχουν αντιτιθέμενες διεργασίες. Οι τεχνολογίες αυτό-προσαρμογής και αυτο-βελτιστοποίησης μας οδηγούν εκ του ασφαλούς στην υλοποίηση και εκτέλεσης νέων διεργασιών και δυνατοτήτων.
- Υποστήριξη εταιριών με πληροφοριακά συστήματα

  Η πραγματοποίηση αυτο–προσαρμοζόμενων συστημάτων επιταχύνει την υλοποίηση νέων λειτουργιών κι εφαρμογών που απαιτούνται για την υποστήριξη των νέων αναπτυσσόμενων αναγκών των επιχειρήσεων. Οι ιδιότητες αυτο–ίασης βοηθούν στην προσφορά υπηρεσιών 7x24 που είναι απαραίτητες ώστε η επιχείρηση να είναι σε λειτουργία το μέγιστο δυνατό χρόνο χωρίς δυσλειτουργίες.
- Παραγωγικότητα ανθρώπινου δυναμικού

  Η παραγωγικότητα του ανθρώπινου δυναμικού βελτιώνεται όταν δίνεται έμφαση στη διαχείριση των συστημάτων και των πολιτικών, με τρόπο ενιαίο για όλους τους τομείς εφαρμογής αυτών (5).

Τα συστήματα που είναι αυτο–διαχειριζόμενα απελευθερώνουν ανθρώπινους πόρους που μπορούν να διατεθούν για άλλους σκοπούς. Κάτι τέτοιο είναι ιδιαίτερα σημαντικό, καθώς με αυτόν τον τρόπο μπορούν με μεγαλύτερη άνεση να σχεδιαστούν και να αναπτυχτούν νέες τεχνολογίες και εφαρμογές για τη βελτιστοποίηση της απόδοσης των υπαρχόντων συστημάτων ή την επέκταση αυτών με σκοπό τη βέλτιστη χρηστικότητα, τη μέγιστη οικονομία και τον ελάχιστο επιχειρηματικό κίνδυνο, και, τέλος, μέγιστη δυνατή σταθερότητα του δικτύου με χαρακτηριστικά αυτόνομων συστημάτων.

## 2.2 Έξυπνα δίκτυα (Smart Grid)

### 2.2.1 Εισαγωγικά

Καθώς οι ανθρώπινες ανάγκες αυξάνονται, και η τεχνολογική πρόοδος απαιτεί ολοένα και μεγαλύτερα ποσά αδιάλειπτης, χωρίς αυξομειώσεις ισχύος ενέργειας, τα δίκτυα παραγωγής και διανομής ηλεκτρικής ενέργειας επιβαρύνονται σημαντικά. Οι αυξανόμενες ανάγκες για ισχύ και οι αναδιατάξεις στο χάρτη ζήτησης ενεργειακών υπηρεσιών και λύσεων φέρνουν συχνά τα διεθνή δίκτυα ηλεκτροδότησης σε αδιέξοδο, που μεταφράζεται σε χαμηλής ποιότητας προϊόν. Τα παρόντα δίκτυα παραγωγής και διανομής ενέργειας είναι παλαιωμένα ενώ συχνά επικρατεί αβεβαιότητα στις εκάστοτε ρυθμιστικές επιτροπές σχετικά με τον τρόπο οικονομικής ανταμοιβής των παρόχων ηλεκτρικής ενέργειας μετά την απελευθέρωση της αγοράς της ενέργειας. Όλα αυτά έχουν συμβάλει στην αισθητή μείωση των οικονομικών πόρων που διατίθενται για επενδύσεις στον τομέα της ενέργειας, ενώ παράλληλα υπάρχει μεγάλη ανάγκη για νέες υποδομές. Ένα θέμα που χρήζει επίσης ιδιαίτερης προσοχής είναι η μόλυνση του περιβάλλοντος και οι εναλλακτικές, «πράσινες» πηγές ενέργειας, σ τις οποίες θα γίνει ιδιαίτερη αναφορά παρακάτω.

Προς επίλυση των παραπάνω προβλημάτων, επινοήθηκαν νέες, έξυπνες συσκευές ενέργειας και συστήματα τα οποία βοηθούν στην εκτόνωση της πίεσης από τα υπερφορτωμένα δίκτυα παραγωγής και διανομής, στη μείωση του κόστους συντήρησης και λειτουργίας αυτών. Ταυτόχρονα βελτιώνουν σημαντικά την αξιοπιστία και ασφάλειά τους και αυξάνουν το ρυθμό ανάπτυξης και ενσωμάτωσης ανακυκλώσιμων πηγών ενέργειας στα ήδη υπάρχοντα δίκτυα.

Με τον όρο «έξυπνη ενέργεια» εννοείται η χρήση της τεχνολογίας ψηφιακών πληροφοριών προς βελτιστοποίηση της παραγωγής, διανομής και χρήσης ηλεκτρικής ενέργειας. Το smart

grid (SG, έξυπνο δίκτυο) είναι το αποτέλεσμα της εφαρμογής της τεχνολογίας της έξυπνης ενέργειας προς συστηματική βελτίωση τη διανομή και παραγωγή ηλεκτρικής ενέργειας.

Υπάρχουν πολλοί παράγοντες οι οποίοι είναι ανασταλτικοί αναφορικά με την εξέλιξη των έξυπνων δικτύων. Στο παρόν σημείο δεν κρίνεται απαραίτητο να γίνει εκτενής αναφορά αυτών, εντούτοις θα παρουσιασθούν συνοπτικά. Οι δύο κύριοι λόγοι που εμποδίζουν λοιπόν την εξέλιξη των έξυπνων δικτύων είναι:

- Οι νέες τεχνολογίες πρέπει να αποδεικνύουν σε κάθε περίπτωση ότι είναι αποτελεσματικότερες από τις ήδη υπάρχουσες. Το ισχύον ηλεκτρικό δίκτυο για πολλά χρόνια παρείχε αδιάλειπτη, καλής ποιότητας ενέργεια καθώς είχε αυτό ως μοναδικό του στόχο. Οι νέες τεχνολογίες πρέπει να ελεγχθούν εξαντλητικά πριν ενσωματωθούν μαζικά στα υπάρχοντα δίκτυα.
- Τα έξυπνα δίκτυα μπορούν να αποφέρουν φαινόμενα κέρδη και να είναι πιο αποδοτικά ενεργειακά, αλλά αυτό μπορεί να έχει δυσάρεστα αποτελέσματα στα ήδη υπάρχοντα επιχειρηματικά μοντέλα που εφαρμόζονται. Επίσης η μερική ή και σε κάποιες περιπτώσεις ολική αλλαγή εξοπλισμού είναι μια σημαντική παράμετρος.

Τα σημερινά δίκτυα αποτελούνται κατά κύριο λόγο από κεντρικούς σταθμούς παραγωγής και ηλεκτρομηχανικά συστήματα διανομής ηλεκτρικής ενέργειας. Όλα αυτά ελέγχονται από κατάλληλα κέντρα ελέγχου. Το ίδιο το δίκτυο όμως είναι παρόμοιο από τις αρχές σχεδίασής του, τον 19$^{ο}$ αιώνα. Τα έξυπνα δίκτυα μπορούν να αλλάξουν αυτά τα δεδομένα. Τα δίκτυα παραγωγής και διανομής ενέργειας είναι δυνατό να μετατραπούν σε έξυπνα δίκτυα, τα οποία μπορούν να ενσωματώσουν περισσότερα και πιο κατανεμημένα δίκτυα εναλλακτικών πηγών ενέργειας, να κάνουν χρήση ηλεκτρονικών μέσων για τη διαχείριση και μεταφορά ηλεκτρικής ενέργειας, και να χρησιμοποιούν προηγμένα ψηφιακά συστήματα για τη διαχείριση διαφόρων εργασιών επιτήρησης και συντήρησης του δικτύου. Τελικά η βιομηχανία της ενέργειας, η οποία προς το παρόν περιορίζει την αναπτυξιακή της προοπτική για οικονομικούς λόγους, έχει τη δυνατότητα τις επόμενες δεκαετίες να προσφέρει στο δίκτυο υψηλού επιπέδου και χαμηλού κόστους ευρυζωνικές υπηρεσίες μέσω της έγχυσης σε κάθε στοιχείο του δικτύου ψηφιακής υπολογιστικής νοημοσύνης. Εξάλλου πρέπει να επισημανθεί η υποστήριξη ενός τέτοιου σχεδίου από τις σημαντικότερες διεθνείς πολιτικές δυνάμεις όπως είναι η Ευρωπαϊκή Ένωση και οι Ηνωμένες Πολιτείες Αμερικής.

Συγκεκριμένα, η Ευρωπαϊκή Επιτροπή υποστηρίζει ότι η μετατροπή των υπαρχόντων δικτύων σε έξυπνα δίκτυα η Ευρώπη εισάγεται σε μια νέα ενεργειακή εποχή (6). Υποστηρίζει ότι τα έξυπνα δίκτυα καταστήσουν εφικτή μια νέα ενεργειακή πολιτική που θα συμβάλει στην επεκτασιμότητα, την επιβιωσιμότητα, την ανταγωνιστικότητα, και την ασφάλεια στην παροχή ηλεκτρικού ρεύματος. Όραμα της Ευρωπαϊκής Ένωσης αποτελεί ένα ευρύ πρόγραμμα έρευνας, ανάπτυξης και εφαρμογής που θα οδηγήσει στην ανάπλαση του ηλεκτρικού δικτύου με τρόπο ώστε να καλύπτει τις σύγχρονες ανάγκες του ευρωπαίου πολίτη. Στα ίδια πλαίσια κινούνται και οι Ηνωμένες Πολιτείες Αμερικής, οι οποίες έχουν τονίσει ότι η βασική αυτή έρευνα πρέπει να έχει τελειώσει μέσα σε δέκα το πολύ χρόνια ώστε να ακολουθήσουν αρκετά χρόνια δοκιμών και πειραματικών εφαρμογών, για τη βελτιστοποίηση και ωρίμαση της χρησιμοποιούμενης τεχνολογίας.

### 2.2.2 Η προέλευση των Έξυπνων Δικτύων

Σύμφωνα με τον αρμόδιο Ευρωπαϊκό φορέα (SmartGrids European Technology Platform), σκοπός των ερευνητικών ομάδων, που έχουν ως αντικείμενο την ανάπτυξη των έξυπνων δικτύων, είναι να διατυπωθεί και προωθηθεί το σχέδιο για την ανάπτυξη των δικτύων ενέργειας της Ευρώπης μετά το 2020 (6). Το σχέδιο αυτό αποσκοπεί να ικανοποιήσει στις αυξανόμενες ανάγκες αλλά και ευκαιρίες που παρουσιάζονται σχετικά με τα ηλεκτρικά δίκτυα. Αυτό θα γίνει μέσω μιας νέας προσέγγισης του προβλήματος, η οποία περιλαμβάνει τεχνικές, οικονομικές και κανονιστικές ρυθμίσεις.

Τα σημερινά ηλεκτρικά δίκτυα εξελίσσονται τα τελευταία από εκατό χρόνια. Εντούτοις, οι ανάγκες που προκύπτουν από την απελευθέρωση της αγοράς της ενέργειας και τις τεχνολογικές εξελίξεις απαιτούν το ριζικό ανασχεδιασμό τους. Τα σημερινά δίκτυα πρέπει να είναι σε θέση να ενσωματώσουν περαιτέρω χαρακτηριστικά και υπηρεσίες. Συγκεκριμένα, πρέπει να είναι σε θέση να εγγυηθούν ασφαλή και διατηρήσιμη παροχή ενέργειας, να εκμεταλλευτούν τις νέες τεχνολογίες και να συμμορφωθούν με τις δυναμικές επιταγές των μοντέρνων οικονομικών μοντέλων και πολιτικών των επιχειρήσεων, και να τηρήσουν τις επιταγές της νέας, ενιαίας και παγκόσμιας περιβαλλοντικής πολιτικής που συνέστησε το Πρωτόκολλο του Κιότο. Οι νέες προκλήσεις που αντιμετωπίζει ο κλάδος της ενέργειας παρατίθενται συνοπτικά κατωτέρω:

- **Ως προς τους τελικούς χρήστες**: Οι αυξημένες ανάγκες στον κλάδο της ενέργειας, οι νέες υπηρεσίες προστιθέμενης αξίας, η ελαστική ζήτηση ενέργειας, οι ανάγκη για χαμηλότερες τιμολογήσεις.
- **Ως προς τα δίκτυα ενέργειας**: Η αύξηση του βαθμού αυτοματοποίησης του δικτύου για καλύτερη ποιότητα υπηρεσιών, η χρήση απομακρυσμένου ελέγχου και διαχείρισης, η ανάπτυξη κατάλληλων επενδύσεων για την ανανέωση και τον εκσυγχρονισμό των γερασμένων υποδομών.
- **Ως προς την ασφάλεια**: Η ανάγκη περιορισμού της εκμετάλλευσης των πρωτογενών παραγωγών ενέργειας και η στροφή προς νέες εναλλακτικές πηγές ενέργειας, η ελαστική και δυναμική αποθήκευση ενέργειας, η ανάγκη για μεγαλύτερη αξιοπιστία και ποιότητα, η αυξημένη ανάγκη παραγωγής και διανομής ενέργειας.
- **Ως προς την απελευθερωμένη αγορά**: Η απάντηση στις ανάγκες και τις ευκαιρίες που δημιουργεί η απελευθέρωση αυτή μέσω της ανάπτυξης και αξιοποίησης τόσο των νέων προϊόντων όσο και των νέων υπηρεσιών, η αυξημένη ελαστικότητα της ζήτησης και ο ασταθής έλεγχος των τιμών, οι ανάγκη για ελαστικές και προβλέψιμες χρεώσεις.
- **Ως προς τη διαλειτουργικότητα των ηλεκτρικών δικτύων**: Η υποστήριξη μιας τέτοιας δυνατότητας στην εσωτερική αγορά σε χώρες όπως οι ΗΠΑ ή η ΕΕ, η αποτελεσματική διαχείριση των συνοριακών συμφορήσεων, η βελτιστοποίηση της μεταφοράς ηλεκτρικής ενέργειας και η εισαγωγή νέων εναλλακτικών πηγών ενέργειας στα ήδη υπάρχοντα ηλεκτρικά δίκτυα.
- **Ως προς την κατανεμημένη παραγωγή και τις εναλλακτικές πηγές ενέργειας**: Η τοπική παραγωγή ενέργειας, η μείωση των απωλειών και των εκπομπών, η ενσωμάτωση στα ήδη υπάρχοντα δίκτυα.
- **Ως προς την κεντρική παραγωγή**: Η ανανέωση των υπαρχόντων εργοστασίων παραγωγής ισχύος, η ανάπτυξη μεθόδων για μεγαλύτερη αποδοτικότητα, η αυξημένη ελαστικότητα ως προς τις υπηρεσίες του συστήματος, η ενσωμάτωση των κατανεμημένων σταθμών παραγωγής και των εναλλακτικών πηγών ενέργειας.
- **Ως προς το περιβάλλον**: Η ικανοποίηση των στόχων που τέθηκαν με το πρωτόκολλο του Κιότο, ο υπολογισμός του αντίκτυπου αυτών στη μεταφορά ενέργειας, η μείωση των απωλειών, η αύξηση της κοινωνικής υπευθυνότητας, η μείωση του χρόνου χορήγησης αδειών για νέες υποδομές.

### 2.2.3 Οι λόγοι που οδήγησαν στα Έξυπνα Δίκτυα

Οι κλιματικές αλλαγές απατούν αλλαγή στον τρόπο παραγωγής και διανομής της ηλεκτρικής ενέργειας. Τα φυσικά καύσιμα εξαντλούνται σταδιακά και η ασφάλεια της διανομής του ηλεκτρικού ρεύματος είναι υπό απειλή. Τα περιβαλλοντικά προβλήματα είναι γνωστά και οι χώρες πρέπει να συμμορφωθούν με τους στόχους που έχουν τεθεί. Το πρωτόκολλο του Κιότο ήταν η αρχή, και όλες οι χώρες έχουν τη δυνατότητα να συμβάλλουν ενεργά στην κοινή προσπάθεια για την περιβαλλοντική σωτηρία του πλανήτη. Τα έξυπνα δίκτυα αποτελούν έναν εξαίρετο βοηθό στον τομέα αυτό, καθώς επιτρέπουν την εκτεταμένη χρήση εναλλακτικών πηγών ενέργειας καθώς και τη βέλτιστη ενσωμάτωση αυτών στα υπάρχοντα δίκτυα. Τα περιβαλλοντικά προβλήματα δεν είναι όμως ο μοναδικός παράγοντας που οδηγεί στη χρήση των έξυπνων δικτύων. Υπάρχουν πολλοί λόγοι, τεχνικοί, οικονομικοί, τεχνολογικοί εκτός από τους περιβαλλοντικούς που οδηγούν στα έξυπνα δίκτυα. Στη συνέχεια παρατίθενται ορισμένοι από αυτούς:

- **Η ευρωπαϊκή και αμερικάνικη εσωτερική αγορά**: Οι εσωτερικές ενεργειακές αγορές τόσο των ΗΠΑ όσο και της Ευρωπαϊκής Ένωσης, δύο εκ των βασικότερων ενεργειακών δυνάμεων παγκοσμίως, παρουσιάζουν ιδιαιτερότητες. Αυτό συμβαίνει καθώς και οι δύο αποτελούνται από επιμέρους πολιτείες – κράτη, η διασυνεργασία των οποίων κρίνεται επιβεβλημένη για την ομαλή λειτουργία του συνόλου. Η ανάγκη λοιπόν για απελευθέρωση της διασυνοριακής διακίνησης ενέργειας, οδήγησε στην αναζήτηση δυναμικού ελέγχου και διαχείρισης της παραγόμενης ενέργειας. Αυτός είναι και ένας από τους κύριους λόγους ανάπτυξης και εφαρμογής των Έξυπνων Δικτύων.
- **Ασφάλεια και ποιότητα παροχής υπηρεσιών ενέργειας**: Η μοντέρνα κοινωνία εξαρτάται σε μεγάλο βαθμό από την ασφαλή παροχή ηλεκτρικής ενέργειας. Επιπλέον, οι τρέχουσες υποδομές των δικτύων διανομής είναι αναξιόπιστες ενώ αμφίβολη είναι και η ποιότητα παροχής ηλεκτρικού ρεύματος. Ο επανασχεδιασμός των δικτύων πρέπει να λάβει υπόψη του όλα τα παραπάνω προκειμένου να ανταποκριθεί στις νέες συνθήκες που δημιουργούνται. Απαιτούνται σημαντικές επενδύσεις για την ανανέωση των υποδομών και την ανάπτυξη νέων τεχνολογιών και αρχιτεκτονικών δικτύων.
- **Το περιβάλλον**: Εκτός από τα θέματα που σχετίζονται με τις πρωτογενείς πηγές ενέργειας, το μεγαλύτερο μειονέκτημα των φυσικών καυσίμων κατά την καύση τους, είναι ότι εκπέμπουν $CO_2$, $SO_2$, $NO_X$ και άλλους ρυπαντές. Τα αέρια του θερμοκηπίου συμβάλλουν αρνητικά στην κλιματική αλλαγή. Είναι απαραίτητη η

έρευνα για να βρεθούν οι οικονομικότερες λύσεις και τα μέτρα που θα επιτρέψουν στα διάφορα κράτη να ανταποκριθούν στους στόχους του πρωτοκόλλου του Κιότο, βοηθώντας με αυτόν τον τρόπο ενεργά στην επίλυση του προβλήματος της περιβαλλοντικής μόλυνσης.

#### *2.2.3.1 Τεχνολογίες νέας γενιάς*

Τα υδροηλεκτρικά και τα πυρηνικά εργοστάσια παραγωγής ενέργειας αποτελούν αξιόπιστες και δοκιμασμένες λύσεις για το πρόβλημα της παραγωγής ενέργειας, με ελάχιστες εκπομπές αερίων του θερμοκηπίου. Η επιτυχημένη εφαρμογή των έξυπνων δικτύων μπορεί να επιτευχθεί με την ενσωμάτωση νέων, εναλλακτικών πηγών ενέργειας. Ένα σχετικό παράδειγμα είναι τα αιολικά πάρκα, ενώ υπάρχουν και άλλες τεχνολογίες κατανεμημένης παραγωγής ενέργειας που είτε είναι ήδη εμπορικές είτε κοντά στην εμπορική τους αξιοποίηση. Αυτές πρέπει να εισαχθούν στα ήδη υπάρχοντα δίκτυα παραγωγής και διανομής ενέργειας, τα οποία όμως δεν ήταν αρχικά σχεδιασμένα για να ενσωματώσουν τέτοιες τεχνολογίες παραγωγής στην κλίμακα που απαιτείται σήμερα (7). Οι μορφές παραγωγής αυτές έχουν διαφορετικά χαρακτηριστικά από τις παραδοσιακές εργοστασιακές εγκαταστάσεις παραγωγής ενέργειας. Εκτός από τα μεγάλα αιολικά πάρκα και τα μεγάλα υδροηλεκτρικά εργοστάσια, αυτός ο τύπος παραγωγής έχει σε γενικές γραμμές μικρότερα ποσά παραγόμενης ενέργειας από ό,τι ο παραδοσιακός τύπος. Επιπλέον, μερικές από τις νέες τεχνολογίες παρουσιάζουν αυξημένη αστάθεια στην παροχή ενέργειας.

Είναι δύσκολο να παραβλεφθεί αντίκτυπος της κατανεμημένης παραγωγής στα μελλοντικά δίκτυα. Εντούτοις, αν οι ενεργειακές πολιτικές των διαφόρων κρατών ή ομοσπονδιών συνεχίζουν να προωθούν την αξιοποίηση κατανεμημένων τεχνολογιών, θα υπάρξει μεγάλη ανάγκη να μεταλλαχθούν τα υπάρχοντα δίκτυα με στόχο να καταστεί δυνατή η εφαρμογή των νέων αυτών τεχνολογιών σε ευρεία κλίμακα. Η κατανεμημένη παραγωγή μπορεί να έχει και υλικό αντίκτυπο στα τοπικά δίκτυα, εισάγοντας αντιστροφή της ροής ενέργειας, ποικιλία στην τοπική τάση του δικτύου καθώς και άλλες τεχνικές δυνατότητες απαραίτητες για την ασφαλή λειτουργία των δικτύων. Όμως, αποτελεσματικές και οικονομικές λύσεις σε αυτά και άλλα παρεμφερή προβλήματα δεν έχουν ακόμη δοθεί.

### *2.2.3.2 Οι στόχοι που έχουν τεθεί*

Η υπέρβαση των προαναφερθέντων δυσκολιών απαιτεί ευρεία και μακρόχρονια έρευνα. Ειδικά για την Ευρωπαϊκή Ένωση, η Στρατηγική της Λισσαβόνας[4] κατέδειξε την πρόθεσή της για προώθηση των επενδύσεων, τη δημιουργία θέσεων εργασίας, την κοινωνική συνοχή και την περιβαλλοντική συνείδηση σε όλη την ευρωπαϊκή επικράτεια.

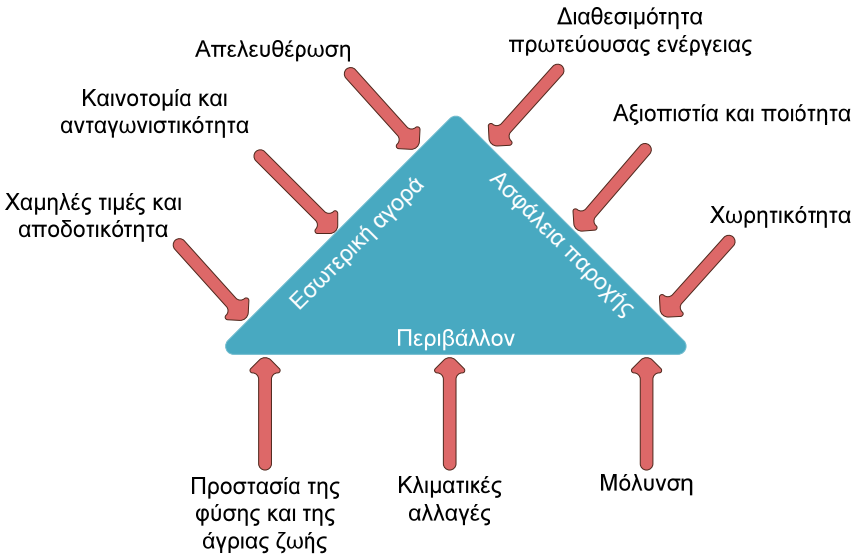
Παρά τα ευοίωνα προγνωστικά στοιχεία που υπάρχουν μέχρι τώρα, υπάρχει σχετική αβεβαιότητα σε αρκετούς τομείς των μελλοντικών δικτύων ενέργειας. Κάποιοι από αυτούς τους τομείς είναι η διαχείριση των ροών ενέργειας που θα προκύψουν από την ελεύθερη αγορά, η στιγμιαία απόδοση ισχύος από πολλούς σταθμούς κατανεμημένης παραγωγής ηλεκτρικού ρεύματος, και τα ρυθμιστικά πλαίσια και οι αποζημιώσεις των επιχειρήσεων που επενδύουν σε νέα και καινοτόμα προϊόντα και υπηρεσίες. Όλα αυτά αποτελούν προβλήματα που χρήζουν άμεσης αντιμετώπισης από τις αρμόδιες επιστημονικές, πολιτικές και ρυθμιστικές αρχές. Η καλύτερη στρατηγική για να αντιμετωπισθούν επιτυχώς αυτά τα σημεία αβεβαιότητας είναι να σχεδιαστούν ευέλικτα δίκτυα. Αυτό μπορεί να γίνει εφικτό μέσω ευρείας έρευνας και ανάπτυξης των έξυπνων δικτύων που, εκτός των άλλων, θα βοηθήσει στην ανάδειξη, καταγραφή και λύση οποιασδήποτε ρυθμιστικής αβεβαιότητας με συστηματικό και αυτοματοποιημένο τρόπο.

Είναι απαραίτητη η συνεργασία σε τοπικό και διεθνές επίπεδο προκειμένου να διαμορφωθεί και να ενδυναμωθεί η βασική έρευνα για την ανάπτυξη των έξυπνων δικτύων, να διευκολυνθούν οι συνεργασίες μεταξύ των κρατικών και των ιδιωτικών φορέων, να καταστεί δυνατό ένα ευνοϊκό ρυθμιστικό περιβάλλον, να αναπτυχθούν βοηθητικές οικονομικές αγορές και να δημιουργηθούν νέες εκπαιδευτικές και εργασιακές συνθήκες που θα έχουν ως αποτέλεσμα την ολοκλήρωση και τελειοποίηση των δικτύων.

Γενικότερα, η σχεδίαση των έξυπνων δικτύων μπορεί να θεωρηθεί ως ένα τυπικό πρόβλημα βελτιστοποίησης, όπου επιζητούνται βέλτιστα αποτελέσματα σε ό,τι αφορά την προστασία του περιβάλλοντος, τη μέγιστη εξυπηρέτηση των πολιτών μέσω καλής ποιότητας, σταθερή, αξιόπιστη, ελεύθερη, διαφανή παροχή ηλεκτρικού ρεύματος, ελαχιστοποιώντας παράλληλα

[4] Πρόκειται για τη λεγόμενη *Lisbon Strategy* (αλλιώς *Lisbon Agend* ή *Lisbon Process*) η οποία είναι μια πρωτοβουλία της Ευρωπαϊκής Ένωσης που έχει ως στόχο να γίνει η Ευρώπη ισχυρότερη οικονομικά. Παρά το γεγονός ότι τα θεμέλια αυτού του οράματος τέθηκαν κατά τη διάρκεια ενός συμβουλίου της Ευρωπαϊκής Επιτροπής στη Λισσαβόνα το Μάρτιο του 2000, ο σχετικός απολογισμός που έγινε από τον αρμόδιο φορέα το 2005 ήταν απογοητευτικός. Τα έξυπνα δίκτυα αναμένεται να διαδραματίσουν στο μέλλον ιδιαίτερα σημαντικό ρόλο στη μακροχρόνια επίτευξη του στόχου που έχει τεθεί, καθώς αποτελούν σημαντικό οικονομικό και αναπτυξιακό παράγοντα στα πλαίσια μιας ελεύθερης, ανοιχτής και διαφανούς αγοράς. Περισσότερες πληροφορίες μπορούν να βρεθούν στον ιστοχώρο της Ευρωπαϊκής Ένωσης http://europa.eu/scadplus/glossary/lisbon_strategy_en.htm.

το κόστος και επινοώντας νέες δραστικότερες, λύσεις στα διάφορα εμπόδια που παρουσιάζονται. Σχηματικά, η προσπάθεια όλων όσοι ασχολούνται με τα έξυπνα δίκτυα συμπυκνώνεται στο παρακάτω σχήμα:




**Σχήμα 2.3: Το τρίγωνο των προκλήσεων που πρέπει να αντιμετωπίσουν τα έξυπνα δίκτυα.**

Το παραπάνω διάγραμμα καταδεικνύει τη δυναμική που μπορεί να αποδώσουν στην παγκόσμια οικονομία τα έξυπνα δίκτυα. Μέσω σοβαρής έρευνας και της συντονισμένης προσπάθειας, μπορούν να λυθούν προβλήματα που μέχρι χθες έμοιαζαν άλυτα, όπως είναι η κατανεμημένη παραγωγή ενέργειας και η εισαγωγή της στο υπάρχον δίκτυο, η απελευθέρωση της αγοράς με δυνατότητα αντίστροφης της ροής ενέργειας από τους καταναλωτές προς το δίκτυο (negawatt) και η ενσωμάτωση εναλλακτικών πηγών ενέργειας σε μεγάλη κλίμακα μέσα στο δίκτυο. Είναι επίσης σημαντικό να τονιστεί ότι μια τέτοια εξέλιξη φαίνεται πλέον οικονομικά βιώσιμη και ανταγωνιστική, ενώ παράλληλα βοηθά και στην προώθηση νέων επενδύσεων και κατάλληλων ρυθμιστικών πλαισίων, τα οποία θα συμβάλουν στην απρόσκοπτη ανάπτυξη και εξέλιξη των έξυπνων δικτύων, χωρίς γραφειοκρατικές στενωπούς και καθυστερήσεις που βλάπτουν την εξελικτική πορεία του ενεργειακού τοπίου.

### 2.2.4 Οφέλη των έξυπνων δικτύων

Έχει ήδη γίνει αναφορά στα διάφορα οφέλη των έξυπνων δικτύων, αλλά δεν έχει αναλυθεί επαρκώς κανένα από αυτά. Στην παρούσα παράγραφο επιχειρείται μια εκτενέστερη ανάλυση των πλεονεκτημάτων που χαρακτηρίζουν τα έξυπνα δίκτυα σε σχέση με τα παραδοσιακά ηλεκτρικά δίκτυα. Στη συνέχεια θα παρουσιασθούν τρόποι με τη βοήθεια των οποίων τα έξυπνα δίκτυα μπορούν να επιταχύνουν τις νέες τεχνολογίες, να δημιουργήσουν

νέες θέσεις εργασίας, να μειώσουν τα έξοδα για τη μεταφορά και διανομή της ενέργειας, να μειώσουν τις διακυμάνσεις της τάσεις και τις τοπικές ή ολικές καταρρεύσεις του δικτύου, να βελτιώσουν την ενεργειακή αποδοτικότητα των δικτύων, να βοηθήσουν στην ελάττωση της περιβαλλοντικής μόλυνσης και να προωθήσουν την ανάπτυξη κατανεμημένων και ανακυκλώσιμων πηγών ενέργειας (8).

#### *2.2.4.1 Επιτάχυνση υιοθέτησης νέων τεχνολογιών*

Οι αναπτυσσόμενες τεχνολογίες των έξυπνων δικτύων δεν προσφέρουν μόνο υπηρεσίες στον τομέα στον οποίο εφαρμόζονται, αλλά παρέχουν οφέλη που αντικατοπτρίζονται σε όλη την έκταση του δικτύου. Για παράδειγμα, η αξία της παραγωγής ηλιακής ενέργειας μέσω φωτοβολταϊκών στοιχείων σε όρους μειωμένης λειτουργίας του δικτύου εκφράζεται σε πάνω από 20 cents/kWh (8). Οι τηλεπικοινωνιακές και διαχειριστικές δυνατότητες του έξυπνου δικτύου καθιστούν δυνατή την ενσωμάτωση νέων ενεργειακών συσκευών στο δίκτυο. Έτσι, το έξυπνο δίκτυο μπορεί να αξιοποιήσει τη συνολική επένδυση για μια συγκεκριμένη τεχνολογία που έχει για ολόκληρο το δίκτυο, ανεξάρτητα του τόπου εφαρμογής. Με αυτόν τον τρόπο, όταν μια επιχειρηματική δραστηριότητα έχει οφέλη τόσο για το δίκτυο στο σύνολό του όσο και τοπικά, θα υπάρχει δυνατότητα οικονομικής υποστήριξης και επιδότησης. Το δίκτυο θα επιτύχει έτσι να επιταχύνει την υιοθέτηση ενός μεγάλου εύρους τεχνολογιών έξυπνων δικτύων, συμβάλλοντας στη δημιουργία κλιμακούμενων, δομημένων οικονομικών αγορών, εξέλιξη που σημαίνει μείωση των τιμών και μεγαλύτερα περιθώρια επιλογής υπηρεσιών από τους τελικούς χρήστες. Αυτό ισχύει καθώς μέσω της κατανεμημένης παραγωγής ενέργειας από τους τοπικούς σταθμούς παραγωγής και διανομής ενέργειας, οι αγορές έχουν τη δυνατότητα να προσφέρουν υπηρεσίες που προσεγγίζουν το μοντέλο του διαδικτύου: η παροχή μπορεί να γίνει ολοκληρωτικά αναλογική με τη ζήτηση, ενώ παράλληλα, και λόγω του καλύτερου ελέγχου της ρέουσας ενέργειας, υπάρχει η δυνατότητα παροχής πρακτικά on demand υπηρεσιών στους τελικούς χρήστες.

#### *2.2.4.2 Μειωμένα κόστη υποδομών*

Τα σημερινά δίκτυα έχουν εξαιρετικά χαμηλό δείκτη χρησιμοποίησης συγκριτικά με τη χωρητικότητά τους. Έτσι, σύμφωνα με στοιχεία που έχουν δημοσιεύσει οι ΗΠΑ, προκύπτει ότι τα εργοστάσια παραγωγής που διατηρούν ανέρχονται σε 9000 συνολικής αξίας σε τιμές 2001 570.000.000.000 δολαρίων. Μπορούν να παράγουν μέχρι και 819 GW ενέργειας, όμως η ενέργεια που παράγουν δεν υπερβαίνει το 53% της ονομαστικής αυτής δυναμικότητας. Το αμερικάνικο δίκτυο γραμμών μεταφοράς ενέργειας αποτελείται από περισσότερα από

1.130.000 km γραμμών με συνολική αξία 64.000.000.000 δολαρίων, αλλά χρησιμοποιείται μέχρι στιγμής μόνο το 50% της χωρητικότητάς τους. Επίσης, σε ό,τι αφορά τη διανομή της ενέργειας, τα τοπικά δίκτυα που αποτελούνται από περισσότερα από 1.600.000 χιλιόμετρα γραμμών συνολικής αξίας 160.000.000.000 δολαρίων, έχουν βαθμούς χρησιμοποιήσης μικρότερους από 30% (9).

Οι τεχνολογίες έξυπνης ενέργειας προσφέρουν την προοπτική σημαντικής αύξησης του συστήματος παραγωγής και αντίστοιχης μείωσης των εξόδων αυτού. Για παράδειγμα, ειδικοί αισθητήρες στις γραμμές μεταφοράς μπορούν να δώσουν στους διαχειριστές των δικτύων πληροφορίες πραγματικού χρόνου σχετικά με τη θερμοκρασία των γραμμών ή να τους ενημερώσουν για διάφορες άλλες παραμέτρους, οι οποίες όμως μπορεί να είναι καθοριστικές για την απόδοση του δικτύου και την ελαχιστοποίηση των απωλειών.

Εκτός των άλλων και πάντα για τις ΗΠΑ (χωρίς αυτό να σημαίνει ότι τα στοιχεία δεν είναι ενδεικτικά και για την Ευρωπαϊκή Ένωση), το ηλεκτρικό δίκτυο αποτελείται από γερασμένες υποδομές, το 60% των οποίων χρήζει αλλαγής μέσα στα επόμενα 10-15 χρόνια, γεγονός που συνεπάγεται τεράστια οικονομικά κόστη (10). Εξαιτίας του γεγονότος αυτού, πρέπει να δοθούν κίνητρα ή και αντικίνητρα στην αγορά προς ανανέωση της υπάρχουσας υποδομής διαχείρισης και επίβλεψης της παραγωγής, της διανομής της και ποιότητας της ενέργειας.

Συγκεκριμένα, οι ψηφιακές τεχνολογίες μέσα σε ολόκληρη την έκταση του δικτύου μπορούν να ελέγχουν τη ζήτηση ενέργειας εκ μέρους των τελικών χρηστών και να συντονίζουν την τοπική, κατανεμημένη παραγωγή ενέργειας με το δίκτυο, μειώνοντας έτσι τα μέγιστα φορτία στους κεντρικους σταθμούς παραγωγής και προσφέροντας ελαστικότητα στην απόκριση για έκτακτες αυξήσεις ζήτησης ενέργειας. Όταν οι νέες ψηφιακές τεχνολογίες εγχυθούν στο δίκτυο, οι απαιτήσεις των τελικών χρηστών μπορούν να ικανοποιηθούν από τα διαθέσιμα ενεργειακά αποθέματα, και η τοπική παραγωγή να αναλάβει την υπόλοιπη ζήτηση, βοηθώντας στην αποφόρτιση των γραμμών μεταφοράς. Η ικανότητα ελέγχου και μείωσης των φορτίων αιχμής μειώνει την ανάγκη για δαπανηρές εφεδρικές υποδομές εκτόνωσης ενέργειας. Το πρόγραμμα εκσυγχρονισμού των αμερικάνικων γραμμών παραγωγής, μεταφοράς και διανομής ενέργειας GridWise, σε συνδυασμό με το Pacific Northwest National Laboratory (PNNL) διεξήγαγαν μία έρευνα σύμφωνα με την οποία μέσω της εγκατάστασης έξυπνων δικτύων τα επόμενα είκοσι χρόνια, θα καταστεί δυνατή η αποφυγή καταβολής σημαντικών ποσών για τον εκσυγχρονισμό και αντικατάσταση των υπαρχόντων ενεργειακών υποδομών. Αναλυτικότερα, υπολόγισαν ότι για την παραγωγή ενέργειας θα αποφευχθούν έξοδα της

τάξης των 19-49 δισεκατομμυρίων δολαρίων, για τη μεταφορά κόστη ύψους των 5-12 δισεκατομμυρίων δολαρίων και τέλος για τη διανομή θα εξοικονομηθούν από 22 μέχρι 56 δισεκατομμύρια δολάρια. Αθροιστικά, τα παραπάνω ποσά μεταφράζονται σε εξοικονόμηση 46-117 δισεκατομμυρίων δολαρίων (9), ποσό ιδιαίτερα σημαντικό για οποιαδήποτε εθνική οικονομία παγκοσμίως. Αυτά τα ποσά δε συμπεριλαμβάνουν τα κεφάλαια που απαιτούνται για την εφαρμογή νέων τεχνολογιών. Παρόλα αυτά, όπως τονίζουν και οι ερευνητές της PNNL, «τα bits είναι φθηνότερα από το σίδηρο». Ενδεικτικά τονίζουν ότι εφαρμογές και συσκευές έξυπνης ενέργειας συνολικού κόστους 600 εκατομμυρίων δολαρίων μπορούν να προσφέρουν την ίδια χωρητικότητα (χωρίς να συνυπολογίζονται τα υπόλοιπα οφέλη από τον έλεγχο και τη διαχείριση των γραμμών) που θα προσέφεραν υποδομές 6 δισεκατομμυρίων. Η διαφορά των δύο αυτών ενδεικτικών ποσών είναι τεράστια, και καταδεικνύει αυτά που υποστηρίχθηκαν προηγουμένως σχετικά με τα κόστη των υποδομών και τα αναμενόμενα κέρδη από την ψηφιοποίηση των δικτύων.

#### *2.2.4.3 Λιγότερα blackout και ενεργειακές διαταραχές*

Διάφορες μελέτες που πραγματοποιήθηκαν το 2003 καταδεικνύουν ότι το ετήσιο κόστος από τις διακοπές ρεύματος στις ΗΠΑ, κυμαίνεται σε ένα εύρος 30-120 δισεκατομμυρίων δολαρίων. Το εύρος αυτό αποδεικνύει ότι δεν είναι εύκολο να υπολογισθούν ακριβώς οι οικονομικές επιπτώσεις λόγω της αστάθειας παροχής ηλεκτρικής ενέργειας. Το βέβαιο είναι ότι τα έξυπνα δίκτυα μπορούν να αυξήσουν δραστικά την αξιοπιστία του δικτύου. Ένα πιθανό σενάριο που μελέτησε ο οργανισμός RAND[5] θεωρώντας ζημίες της τάξης των 50 δισεκατομμυρίων δολαρίων, είχε ως συμπέρασμα ότι η ζημία μπορεί να περιοριστεί στα 15 δισεκατομμύρια δολάρια, θεωρώντας μια διείσδυση των τεχνολογιών έξυπνων δικτύων της τάξης του 50% στα δίκτυα μεταφοράς και του 25% στα δίκτυα διανομής. Θεωρώντας μάλιστα αρχική ζημία της τάξης των 100 δισεκατομμυρίων δολαρίων, η χρήση τεχνολογιών έξυπνου δικτύου θα μείωνε τη ζημία κατά 51%, δηλαδή στα 49 δισεκατομμύρια δολάρια (11).

#### *2.2.4.4 Βελτιωμένη ενεργειακή απόδοση*

Η κατασκευή συστημάτων διαχείρισης και ελέγχου έξυπνου ενεργειακού εξοπλισμού, τα οποία παρακολουθούν αδιάκοπα και προσαρμόζουν αυτόν τον εξοπλισμό, προσφέρει σημαντικά ενεργειακά οφέλη. Σε μια από τις μελέτες της, η RAND υποστηρίζει ότι σε 20 χρόνια αυτά τα συστήματα θα είναι σε θέση να μειώσουν την ετήσια ενεργειακή ζήτηση

[5] Η RAND Corporation είναι ένας αμερικάνικος ανεξάρτητος, μη κερδοσκοπικός οργανισμός ο οποίος μελετά σενάρια προς βελτιστοποίηση σε θέματα οικονομικά και θέματα λήψης αποφάσεων.

κατά 52-106 δισεκατομμύρια κιλοβατώρες (11). Εκτεταμένη εφαρμογή των ψηφιακών τεχνολογιών στα δίκτυα μπορούν να αποφέρουν ακόμα μεγαλύτερη μείωση, αυξάνοντας έτσι τα ενεργειακά και οικονομικά οφέλη από μια τέτοια επιλογή.

#### *2.2.4.5 Μείωση εκπομπών αερίων του θερμοκηπίου*

Τα εργοστάσια παραγωγής ενέργειας υπό πλήρη παραγωγική ισχύ αποτελούν μια από τις κυριότερες πηγές περιβαλλοντικής ρύπανσης καθώς τότε τείνουν να έχουν τη μικρότερη απόδοση. Επιπλέον, όταν ένα εργοστάσιο λειτουργεί με αυξομειώσεις στην παραγωγή ενέργειας, παράγει πολύ μεγαλύτερες ποσότητες ρυπογόνων αποβλήτων (αερίων και μη) σε σχέση με τη λειτουργία του σε σταθερή παραγωγική κατάσταση. Η αυξομείωση αυτή δεσμεύει από την παραγωγή ένα ποσοστό 10-15% της ενέργειας που παράγεται, ενώ παράλληλα, τα εργοστάσια συνεχίζουν να λειτουργούν ακόμα και όταν η ενέργεια που παράγεται δεν είναι άμεσα απαιτούμενη. Το δίκτυο όμως χρειάζεται αυτό το περίσσευμα ενέργειας για να είναι σε θέση να αντιμετωπίσει τις εκρηκτικές μεταβολές ζήτησης ενέργειας που μπορεί να προκύψουν. Τα έξυπνα δίκτυα μπορούν να διαδραματίσουν σημαντικό ρόλο σε αυτό, καθώς μέσω της ενσωμάτωσης κατανεμημένων, τοπικών σταθμών παραγωγής με δυνατότητα αντιστροφής της ροής ενέργειας, έχουν τη δυνατότητα να εκτονώσουν την ενεργειακή ζήτηση από τα μεγάλα κεντρικά εργοστάσια, επιτυγχάνοντας με αυτόν τον τρόπο, εκτός από καλύτερη ενεργειακή απόδοση και μικρότερες ποσότητες εκπεμπόμενων ρύπων.

#### *2.2.4.6 Καθαρή ενεργειακή αγορά*

Αρκετοί σημερινοί τελικοί χρήστες έχουν τη δυνατότητα να καλύψουν τις ενεργειακές τους ανάγκες με «πράσινη» ενέργεια, πληρώνοντας ένα μικρό αντίτιμο. Επίσης στις μέρες μας, εν μέσω διαρκών προειδοποιήσεων σχετικά με τη μόλυνση του αέρα και γενικότερα του περιβάλλοντος, ορισμένα εργοστάσια παραγωγής και βαριές βιομηχανίες αναγκάζονται να διακόψουν τη λειτουργία τους. Τα έξυπνα δίκτυα θα μπορέσουν να βελτιώσουν αυτήν την κατάσταση, με χρήση αυτοματοποιημένων και προτυποποιημένων διαδικασιών. Έξυπνος εξοπλισμός, ειδικές συσκευές και κτίσματα, θα διαθέτουν τηλεπικοινωνιακές δυνατότητες να ειδοποιούν πχ για υπέρβαση των ορίων της στάθμης των ανεπιθύμητων αερίων σε συγκριμένους χώρους και ώρες, ή να δίνουν άλλες παρεμφερείς πληροφορίες στους διαχειριστές των δικτύων. Έτσι, θα είναι ανά πάσα στιγμή δυνατό να εντοπίζονται οι πλέον ρυπογόνες επιχειρήσεις και εργοστάσια παραγωγής, και να επιβάλλονται πρόστιμα, ή να αναστέλλεται η λειτουργία τους. Η προσφορά στους ιδιοκτήτες «καθαρών» εργοστασίων παραγωγής σε μια on demand αγορά όπου θα μπορούσαν να επενδύσουν, θα ανοίξει νέους

δρόμους για τις επιχειρήσεις αυτές και θα προωθήσει την εναλλακτική, καθαρή και κατανεμημένη παραγωγή προς το δίκτυο.

#### *2.2.4.7 Ευρείας κλίμακας αξιοποίηση ανανεώσιμων πηγών ενέργειας*

Η αιολική και η ηλιακή ενέργεια παρέχουν ενέργεια ασυνεχώς και εξαρτώνται από τυχαίους παράγοντες. Μέχρι στιγμής, σε Γερμανία, Δανία και Ισπανία οι εναλλακτικές πηγές ενέργειας έχουν επιτύχει να εισχωρήσουν σε ποσοστό 20% στα τυπικά δίκτυα. Εντούτοις, αν υλοποιηθούν οι δεσμεύσεις για τις πράσινες πηγές ενέργειας και τη μείωση των εκπεμπόμενων ρύποι, θα αυξηθεί ο βαθμός ενσωμάτωσης των εναλλακτικών πηγών ενέργειας στα ενεργειακά δίκτυα, με αποτέλεσμα την αύξηση της ασυνεχούς και διακοπτόμενης αυτής παραγωγής με όλα τα αποτελέσματα που αυτό συνεπάγεται. Οι τεχνολογίες έξυπνης ενέργειας προσφέρουν νέες δυνατότητες για την καλύτερη διαχείριση και αξιοποίηση των απρόβλεπτων αυτών πηγών ενέργειας:

- Η διασύνδεση όλων των στοιχείων του δικτύου μέσω τηλεπικοινωνιακών συστημάτων (όπως πχ το BPL) και αυτοματοποιημένων διεργασιών, το δίκτυο θα μπορεί άμεσα να αποκρίνεται σε αυξομειώσεις τάσης με διάφορους τρόπους. Με εξισορρόπηση των αποθεμάτων ενέργειας σε διαφορετικές γεωγραφικές περιοχές (για παράδειγμα όταν φυσάει σε μια γεωγραφική περιοχή αλλά όχι σε κάποια άλλη), μπορεί να γίνει επιτυχώς κάτι τέτοιο. Επίσης, ένας άλλος τρόπος είναι η ενεργοποίηση άλλων τοπικών σταθμών παραγωγής.
- Η προηγμένη υπολογιστική μοντελοποίηση επιτρέπει την ασφαλέστερη πρόβλεψη σε ό,τι αφορά τους ανέμους, την ηλιοφάνεια, ή τη ροή των υδάτων των ποταμών που χρησιμοποιούνται για την παραγωγή ενέργειας. Υπάρχουν ήδη αντίστοιχοι σταθμοί που πραγματοποιούν τέτοιες προβλέψεις. Ένας από αυτούς είναι ο 3 Tier Environmental Forecast Group. Ένας από τους υπεύθυνους του σταθμού αυτού, επισημαίνει ότι «μια αύξηση 10% στην ακρίβεια της πρόβλεψης μπορεί να έχει ως ισοδύναμο εξοικονόμηση ενός εκατομμυρίου δολαρίων ανά χρόνο, για ένα αιολικό πάρκο 100MW» (12).

Οι ειδικοί πάντως τονίζουν ότι για να έχουν όλα τα προηγούμενα νόημα και να επιτευχθούν οι στόχοι που έχουν τεθεί, πρέπει να γίνουν πολλές και ακριβές επενδύσεις, ενώ τα οφέλη, λόγω του απρόβλεπτου χαρακτήρα αυτών των πηγών ενέργειας, είναι προς το παρόν αμφίβολα, κάτι που αποτελεί ανασταλτικό παράγοντα για την ταχύτερη ενσωμάτωση των τεχνολογιών του έξυπνου δικτύου ενέργειας στα υπάρχοντα δίκτυα.

#### 2.2.4.8 Ενσωμάτωση κατανεμημένων σταθμών παραγωγής

Οι σημερινοί ιδιοκτήτες οικιών και επιχειρήσεων που θέλουν να εκμεταλλευτούν τα πλεονεκτήματα της ηλιακής ή γενικά της κατανεμημένη παραγωγής ενέργειας, πρέπει να υπερβούν πολλά εμπόδια που προβάλουν δικαιολογημένα οι εκάστοτε δημόσιες επιχειρήσεις ηλεκτρισμού. Η μεγάλη ροή ενέργειας από πολλούς κατανεμημένους σταθμούς παραγωγής εγκυμονεί τον κίνδυνο δημιουργίας ανισορροπίας στο δίκτυο. Επομένως, οι επιχειρήσεις ηλεκτρισμού επιθυμούν να υπάρχουν ελεγκτικοί μηχανισμοί και πρωτόκολλα ώστε να αποφευχθούν τέτοιες καταστάσεις. Το αποτέλεσμα είναι ότι τελικά, λόγω του μη συστηματικού χαρακτήρα των αιτημάτων των δημοσίων επιχειρήσεων ηλεκτρισμού, η εγκατάσταση ενός τοπικού, μικρού, περιφερειακού σταθμού παραγωγής καθίσταται εξαιρετικά σύνθετη και ακριβή, αποθαρρύνοντας τις σχετικές επενδύσεις. Η μοντελοποιημένη plug and play διασύνδεση των κατανεμημένων γεννητριών είτε είναι παλινδρομικοί κινητήρες είτε κυψέλες φυσικών καυσίμων, ηλιακές κυψέλες ή μικρές ανεμογεννήτριες, είναι βασικός στόχος της ανάπτυξης των έξυπνων δικτύων. Κάτι τέτοιο θα μειώσει σημαντικά τα κόστη εγκατάστασης του πρόσθετου εξοπλισμού, δημιουργώντας νέες προοπτικές στην κατανεμημένη παραγωγή.

#### 2.2.4.9 Μειωμένα κόστη για ενέργεια «ψηφιακής ποιότητας»

Η σημερινή ψηφιακή κοινωνία έχει ανάγκη  ηλεκτρικής ενέργειας που χαρακτηρίζεται από υψηλή ποιότητα, σταθερή ισχύ και αδιάκοπη λειτουργία. Το Ινστιτούτο Έρευνας Ηλεκτρικής Ενέργειας των ΗΠΑ μετά από σχετική έρευνα κατέληξε στο συμπέρασμα ότι μέχρι το 2020 το 10% της καταναλισκόμενης ενέργειας στις ΗΠΑ πρέπει να είναι εξαιρετικά υψηλής ποιότητας για το 99.99999% του χρόνου. Αρκετοί ερευνητές υποστηρίζουν ότι τα έξυπνα δίκτυα έχουν την ικανότητα να προσφέρουν τέτοιας ποιότητας υπηρεσίες. Ανεξάρτητα από το αν αυτό ισχύει ή όχι, η βελτιωμένη κατανεμημένη παραγωγή και η εύκολη διασύνδεση αυτής με το υπόλοιπο δίκτυο θα καταστήσουν αρκετά οικονομικότερη την υψηλής ποιότητας ενέργεια. Τα σημερινά συστήματα που απαιτούν υψηλής ποιότητας αδιάκοπη ενέργεια χρησιμοποιούν εφεδρικά συστήματα τροφοδοσίας τα οποία συντριπτικό ετήσιο ποσοστό μένουν εκτός δικτύου. Αν αυτά τα εφεδρικά συστήματα συνδεθούν στο δίκτυο και παρέχουν προς αυτό ενέργεια όταν είναι ανενεργά για την εγκατάσταση που προστατεύουν, η αυξημένη χρήση και η αντίστροφη ροή ενέργειας (προς το δίκτυο) σημαίνουν αυτόματα μειωμένα λειτουργικά κόστη καθώς και κόστη συντήρησης.

### 2.2.4.10 Μικροδίκτυα

Οι τεχνολογίες διαχείρισης έξυπνων δικτύων ανοίγουν το δρόμο για τη σύνδεση με το δίκτυο των μέχρι πρότινος μη συνδεδεμένων μικροδικτύων. Αυτά έχουν τη δυνατότητα να παράγουν ενέργεια σταθερής τάσης αντί για την κλασική εναλλασσόμενη, το οποίο είναι πολύ οικονομικό δεδομένου ότι οι ψηφιακές συσκευές που τυπικά χρησιμοποιούν σταθερή τάση φέρουν ακριβό και ενεργοβόρο εξοπλισμό μετατροπής του εναλλασσόμενου ρεύματος σε σταθερό. Συγκεκριμένα, τα μικροδίκτυα γενικά ορίζονται ως δίκτυα χαμηλής τάσης, με πηγές σταθερής τάσης, με παράλληλη συνύπαρξη τοπικών αποθηκευτικών σταθμών ενέργειας και ελεγχόμενων φορτίων. Το μοναδικό χαρακτηριστικό των μικροδικτύων είναι πως παρά το γεγονός ότι λειτουργούν σχεδόν μόνιμα σε σύνδεση με το κεντρικό δίκτυο, μπορούν να μετατρέψουν αυτόματα τον τρόπο λειτουργίας τους, ώστε να λειτουργούν απομονωμένα από αυτό. Αυτό είναι σημαντικό, σε περιπτώσεις όπου το κεντρικό δίκτυο καταρρέει, και στην περιοχή λειτουργίας του μικροδικτύου υπάρχουν συστήματα ευαίσθητα στην απώλεια ή τον κυματισμό της τάσης. Επίσης, η ηλεκτρονική ευφυΐα μπορεί σε αυτήν την περίπτωση να συνδέσει τα μικροδίκτυα κατάλληλα με κτίρια διαχείρισης ενέργειας ή έξυπνο ψηφιακό εξοπλισμό, μειώνοντας έτσι τα λειτουργικά κόστη.

### 2.2.4.11 Μειωμένες απώλειες γραμμών μεταφοράς

Καθιστώντας την τοπική παραγωγή περισσότερο αποδοτική οικονομικά, η τεχνολογία έξυπνης ενέργειας προσφέρει πολλά και διάφορα οφέλη σε σχέση με την αξιοπιστία, τη λειτουργικότητα και την αποδοτικότητα του συστήματος. Τυπικά το 9% της ενέργειας στις γραμμές μεταφοράς χάνεται μεταξύ των κέντρων παραγωγής και των τελικών χρηστών. Η κατανεμημένη παραγωγή μπορεί να μειώσει αυτό το μέγεθος στο 2% περίπου, επιτυγχάνοντας με άλλα λόγια θεαματική μείωση απωλειών. Άλλες τεχνολογίες έξυπνης ενέργειας, όπως για παράδειγμα ο έλεγχος τάσης και ρεύματος επί των γραμμών, μπορούν να μειώσουν ακόμη περισσότερο τις απώλειες αυτές (13).

### 2.2.4.12 Συνδυασμένη θερμότητα – ενέργεια

Η τοπική παραγωγή βοηθά την ανακύκλωση της θερμότητας στα συστήματα θέρμανσης και ψύξης των κτιρίων με χρήση διεργασιών Συνδυασμένης Θερμότητας και Ενέργειας (Combined Heat and Power, CHP). Ο Thomas R. Casten, πρόεδρος της Διεθνούς Συμμαχίας για την Αποκεντρωμένη Ενέργεια (World Alliance for Decentralized Energy), υπογραμμίζει ότι η αποδοτικότητα της ενεργειακής παραγωγής ήταν στο αποκορύφωμά της τη δεκαετία του 1910. Εκείνη τη χρονική περίοδο, η απόδοση των εργοστασίων παραγωγής ήταν μόλις στο 15%. Όμως, τα περισσότερα από αυτά ήταν εγκατεστημένα σε πυκνοκατοικημένες

περιοχές και οι απώλειες θερμότητας χρησιμοποιούνταν για τη θέρμανση των γύρω περιοχών, παρέχοντας συνολικά τελική απόδοση της τάξης του 65%. Έκτοτε, τα εργοστάσια παραγωγής έχουν μεγαλώσει σημαντικά σε έκταση και πολυπλοκότητα, και για περιβαλλοντικούς λόγους και λόγους υγιεινής μεταφέρθηκαν σε απομακρυσμένες περιοχές, καθιστώντας μη αξιοποιήσιμη την απώλεια θερμότητας. Έτσι, σήμερα, ακόμη και οι αρτιότεροι σταθμοί παραγωγής παγκοσμίως επιτυγχάνουν απλώς να φτάσουν απόδοση 50%, με το μέσο όρο απόδοσης των σταθμών παραγωγής να κυμαίνεται κοντά στο 33% (13).

#### *2.2.4.13 Δημιουργία θέσεων εργασίας*

Από όλα τα παραπάνω γίνεται εύκολα κατανοητό ότι η βασική έρευνα χρειάζεται πολλούς νέους επιστήμονες προκειμένου να στελεχωθούν ικανές επιστημονικές ομάδες για να ερευνήσουν τους τρόπους βελτιστοποίησης των δικτύων έξυπνης ενέργειας. Επίσης, δημιουργούνται νέες θέσεις εργασίας για μηχανικούς που θα αναλάβουν το σχεδιασμό, την ανάπτυξη και υλοποίηση των δικτύων. Εάν συνυπολογισθεί και το νομοθετικό, ρυθμιστικό και οικονομολογικό έργο που επιβάλλεται να παραχθεί, εύκολα προκύπτει ότι δημιουργούνται πολλές θέσεις εργασίας, ικανές να απορροφήσουν εκπαιδευμένο και εξειδικευμένο προσωπικό, γεγονός ιδιαίτερα σημαντικό για οποιαδήποτε οικονομία στον κόσμο.

### 2.2.5 Ποιοι επηρεάζονται από τα Έξυπνα Δίκτυα

Καθώς οι αγορές ενέργειας απελευθερώνονται σε ολοένα και μεγαλύτερο βαθμό και αναπτύσσονται, ένας αυξανόμενος αριθμός ανθρώπων εμπλέκεται στα μελλοντικά δίκτυα παροχής ενέργειας. Στη συνέχεια, αναφέρεται ποιοι επηρεάζονται από την τεχνολογία των έξυπνων δικτύων, και με ποιον τρόπο εμπλέκονται σε αυτή.

- **Οι χρήστες**: Οι ανάγκες των χρηστών περιλαμβάνουν ποιότητα υπηρεσιών και καλή σχέση αξίας προς κόστος. Στα επόμενα χρόνια, οι προσδοκίες των χρηστών θα διευρυνθούν και θα περιλαμβάνουν υπηρεσίες προστιθέμενης αξίας, ενεργειακές υπηρεσίες *κατ απαίτηση (on demand)*. Θα ζητούν κατανεμημένη οικιακή παραγωγή ενέργειας, τη δυνατότητα να εμπορεύονται το περισσεύμα της παραγόμενης αυτής ενέργειας, χρεώσεις πραγματικού χρόνου και την ελευθερία να επιλέγουν οι ίδιοι την εταιρία παροχής ηλεκτρικών υπηρεσιών.

- **Οι εταιρίες ηλεκτρικών δικτύων**: Οι ιδιοκτήτες δικτύων και οι πάροχοι καλούνται να ικανοποιήσουν τις απαιτήσεις των χρηστών με τρόπο αποτελεσματικό αλλά ταυτόχρονα και προσοδοφόρο (σε βιώσιμα επίπεδα δηλαδή). Καλούνται να πραγματοποιήσουν τις απαραίτητες επενδύσεις για να εγγυηθούν υψηλής ποιότητας ηλεκτρική ενέργεια και ασφάλεια, ενώ θα εγγυώνται παράλληλα υψηλές αποδόσεις στους μετόχους τους.
- **Οι εταιρίες ενεργειακών υπηρεσιών**: Οι εταιρίες πρέπει να ικανοποιήσουν τις αυξανόμενες ανάγκες των χρηστών. Κάποιοι χρήστες θα επιζητήσουν «ετοιμοπαράδοτες» υπηρεσίες. Τα κέρδη τόσο στην ποιότητα υπηρεσιών όσο και στις τιμές πρέπει να είναι σαφώς ορατά από τους χρήστες. Ενδεικτικά, αυτό μπορεί να συμβεί μέσω μιας αύξησης στις προσφερόμενες υπηρεσίες και μιας μείωσης σε ότι αφορά την ορατή επέμβαση, για παράδειγμα για εργασίες συντήρησης.
- **Πάροχοι τεχνολογίας**: Σημαντικές τεχνολογικές και επιχειρηματικές αλλαγές αναμένονται τα επόμενα χρόνια κι έτσι οι κατασκευαστές εξοπλισμών θα αποκτήσουν ρόλους – κλειδιά στην παραγωγική διαδικασία, καθώς θα αναπτύσσουν νέες καινοτόμες λύσεις και πρέπει να εναρμονίζονται με τις εταιρίες ηλεκτρικών δικτύων λόγω της απαραίτητης μεταξύ αυτών συνεργασίας. Όπως οι εταιρίες δικτύων, έτσι και οι τεχνολογικοί πάροχοι πρέπει να λάβουν σημαντικές αποφάσεις σε σχέση με ενδεχόμενες επενδύσεις. Ένα κοινό όραμα είναι ιδιαίτερα κρίσιμο για τη διασφάλιση κοινών στρατηγικών που θα έχουν ως αποτέλεσμα την παροχή στους τελικούς χρήστες ελεύθερης πρόσβασης. Ταυτόχρονα είναι σημαντική και η ενσωμάτωση με την υπάρχουσα υποδομή. Ολοκληρωμένες λύσεις θα ζητηθούν σε σχέση με τα δίκτυα, την κεντρική και αποκεντρωμένη παραγωγή ενέργειας, καθώς τα χαρακτηριστικά των δικτύων θα αλλάζουν συχνά και δυναμικά, ανάλογα με τις ισχύουσες συνθήκες ζήτησης, προσφοράς και διαθεσιμότητας ενέργειας και υποδομών.
- **Επιστήμονες**: Ο επιστημονικός κόσμος έχει να διαδραματίσει ένα ιδιαίτερα κρίσιμο ρόλο: χωρίς έρευνα δεν υπάρχει καινοτομία και χωρίς καινοτομία δεν υπάρχει ανάπτυξη. Η συνεργασία μεταξύ πανεπιστημιακών οργανισμών και ερευνητικών κέντρων, κατασκευαστών, ρυθμιστικών και νομοθετικών αρχών πρέπει να θεμελιωθεί, όχι μόνο για την πετυχημένη ανάπτυξη νέων τεχνολογιών αλλά και για την υπέρβαση διάφορων μη τεχνικών προβλημάτων.
- **Έμποροι**: Το ελεύθερο εμπόριο θα διευκολυνθεί μέσω των απελευθερωμένων αγορών, των εναρμονισμένων κανόνων και των διαφανών εμπορικών συναλλαγών.

Τα προβλήματα διαχείρισης των συμφορήσεων και της δέσμευσης ενέργειας πρέπει να επιλυθούν για να επιτευχθεί ενιαία αγορά ηλεκτρικής ενέργειας σε περιπτώσεις όπως οι ΗΠΑ ή η ΕΕ. Οι τελικοί χρήστες θα επωφεληθούν από την ευκαιρία να επιλέξουν τον πάροχο ενέργειας που ικανοποιεί τις προϋποθέσεις που οι ίδιοι κρίνουν ως σημαντικές.

- **Ρυθμιστικές αρχές:** Κάθε αγορά που σχετίζεται με ενέργεια και ανάλογες υπηρεσίες πρέπει να υποστηρίζεται από ένα απλό και σταθερό ρυθμιστικό πλαίσιο. Τα ρυθμιστικά πλαίσια πρέπει να διαθέτουν κανόνες που να εγγυώνται ένα ασφαλές δίκτυο με αυξανόμενα ελεύθερη πρόσβαση καθώς και ένα απλό σύστημα αποζημίωσης επενδύσεων. Τέλος πρέπει να διατηρούν τα κόστη διανομής όσο χαμηλότερα γίνεται, και να ανταμείβονται οι πρωτοβουλίες και οι καινοτομίες εκ μέρους των παρόχων και των παραγωγών ενέργειας.
- **Κυβερνητικές αρχές**: Οι κυβερνήσεις και οι νομοθέτες πρέπει να ετοιμάσουν νέα νομοθετικά πλαίσια για να λάβουν υπόψη διάφορους φαινομενικά αντίθετους στόχους. Ο αυξημένος ανταγωνισμός αναμένεται να δημιουργήσει μια πίεση των τιμών προς τα κάτω, και η χρήση εναλλακτικών ενεργειακών πηγών αναμένεται να επιφέρει νέες προκλήσεις σε αυτόν τον τομέα. Η νομοθεσία θα επηρεάζεται από τις ισχύουσες αλλά και τις νέες τεχνολογίες, την εξέλιξη των δικτυακών οργανισμών ενέργειας, την ανάγκη για μεγαλύτερη ελαστικότητα και αυξημένο διασυνοριακό εμπόριο και από την ανάγκη να διασφαλιστεί οικονομική ανάπτυξη, μεγαλύτερη ανταγωνιστικότητα και υψηλή ασφάλεια παροχής ρεύματος.
- **Προηγμένες ηλεκτρικές υπηρεσίες και πάροχοι**: Οι νέες υπηρεσίες θα δίνουν τη δυνατότητα στους τελικούς χρήστες να επιλέξουν την πηγή ενέργειας που επιθυμούν. Κατά τα γνωστά, οι εμπλεκόμενοι θα μπορούν είτε να παράγουν οι ίδιοι την ενέργεια που χρειάζονται, με τη δυνατότητα προφανώς να πουλήσουν το περίσσευμα ενέργειας πίσω στο δίκτυο, είτε να την αγοράζουν από τις εταιρίες παροχής ηλεκτρικής ενέργειας. Επίσης θα έχουν την ευκαιρία να προσφέρουν προϊόντα που ανταποκρίνονται στη ζήτηση των τελικών χρηστών και υπηρεσίες στο δίκτυο. Στην περίπτωση επιχειρήσεων που έχουν μεγάλες ενεργειακές ανάγκες, οι αποφάσεις τους θα εξαρτώνται από τις αλλαγές στις τιμές τις αγοράς. Ετσι πρέπει να αναζητήσουν λύση από ένα ευρύτερο σύνολο προτάσεων, που θα υφίστανται στην απελευθερωμένη πλέον αγορά, προκειμένου να καταλήξουν στη βέλτιστη γι' αυτές λύση.

- **Εργατικό δυναμικό**: Υπάρχει γενικά η θεώρηση ότι η μηχανική της ενέργειας είναι ένας κλάδος ξεπερασμένος και στατικός. Ιδιαίτερη προσοχή πρέπει να δοθεί για να καταρτιστεί κατάλληλα το τεχνικό προσωπικό και να λυθεί έτσι το πρόβλημα της έλλειψης εκπαιδευμένων εργατών από τους κατασκευαστές, τους παρόχους δικτύων, τις ρυθμιστικές αρχές κτλ. Νέες θέσεις εργασίας θα δημιουργηθούν, παρέχοντας ταυτόχρονα ευκαιρίες για εξειδίκευση σε τομείς οι οποίοι πριν από λίγα χρόνια δεν ήταν καν υπό σκέψη, όπως πχ η απομακρυσμένη διαχείριση των ενεργειακών δικτύων.

Η συνεργασία μεταξύ των διάφορων εμπλεκόμενων φορέων είναι προφανώς απαραίτητη για τη διατήρηση της ασφαλούς παροχής ηλεκτρικού ρεύματος σε μια διαφανή αγορά. Κοινοί τεχνικοί κανόνες και εργαλεία πρέπει να υιοθετηθούν από τους διαφορετικούς φορείς που αφορούν ανταλλαγή πληροφοριών, μοντελοποίηση δικτύων και διάφορες, βοηθητικές υπηρεσίες. Είναι ιδιαίτερα σημαντικό να υπάρξει συνεργασία μεταξύ όλων των ενδιαφερομένων που εμπλέκονται στην ανάπτυξη των δικτύων, προκειμένου να υπάρξει ταχεία και αποτελεσματική αντιμετώπιση των ενδεχόμενων μελλοντικών προβλημάτων.

### 2.2.6 Σύνοψη

Οι τεχνολογίες έξυπνων δικτύων και αυτόνομων συστημάτων είναι δύο διαφορετικές προσπάθειες, από φαινομενικά διαφορετικά επιστημονικά πεδία. Εντούτοις, έχουν κοινούς γενικούς στόχους: τη βελτιστοποίηση της απόδοσης και την αυτοματοποίηση βασικών διεργασιών κεντρικών συστημάτων, με χρήση και κατανεμημένων παραγωγών. Είναι προφανές ότι η τεχνολογία των αυτόνομων συστημάτων μπορεί σχεδόν αυτούσια να χρησιμοποιηθεί από τις τεχνολογίες έξυπνης ενέργειας, καθώς οι τελευταίες αποσκοπούν στην ένταξη στο γερασμένο ηλεκτρικό δίκτυο των αρχών του αυτόνομου υπολογισμού, όπως είναι η αυτο–προσαρμογή, η αυτο–ίαση, η αυτο–βελτιστοποίηση και η αυτο–προστασία. Εξάλλου, το γεγονός ότι το όραμα των έξυπνων δικτύων είναι η ψηφιοποίηση και η διαδικτύωση των δικτύων παραγωγής, μεταφοράς και διανομής ενέργειας, κάτι τέτοιο είναι επιθυμητό και αναμενόμενο.

Η ανάγκη για διαρκή έλεγχο και συλλογή πληροφοριών πραγματικού χρόνου, η εύκολη, ασφαλής και αυτόματη εισαγωγή νέων συσκευών δικτυακού ελέγχου, η σταθερότητα των ψηφιακών συστημάτων που απαιτούνται και η ανάγκη ελαχιστοποίησης του κόστους

αυτών των συσκευών, αποτελούν τις παραμέτρους που συνθέτουν το πρόβλημα της ανάπτυξης του αντίστοιχου λογισμικού.

Οι τεχνολογίες XML και ειδικότερα το πρωτόκολλο Universal Plug and Play επιτρέπουν την εύκολη ανάπτυξη κώδικα που υπόκειται στις αρχές του αυτόνομου υπολογισμού, ενώ κατασκευάζουν εύκολα λογισμικό που καθιστά τις συσκευές απλές στη διαχείριση και την προσαρμογή, ενώ ταυτόχρονα είναι τύπου plug and play. Στο κεφάλαιο που ακολουθεί θα μελετηθούν οι τεχνολογίες XML και ειδικότερα το πρωτόκολλο UPnP, το οποίο αποτελεί τη βάση για την παρούσα εφαρμογή, που είναι μια συσκευή ελέγχου του δικτύου MT. Εκτενέστερη ανάλυση θα γίνει στο επόμενο κεφάλαιο, ενώ η επεξήγηση του κώδικα της εφαρμογής ακολουθεί στα επόμενα κεφάλαια.

# 3 Η εφαρμογή ελέγχου– Το πρωτόκολλο UPnP

## 3.1 Εισαγωγικά

Οι τεχνολογίες XML (Extensible Mark-up Language) έχουν προταθεί ως μια εναλλακτική στα μέχρι τώρα πρότυπα δικτυακής διαχείρισης συσκευών. Το μεγάλο πλεονέκτημα της XML είναι ότι παρέχει στον προγραμματιστή μια άριστη δυνατότητα απλής αναπαράστασης πληροφοριών, σε σχετικά μικρό μέγεθος, ενώ ταυτόχρονα υπάρχουν πολλά άλλα πρωτόκολλα που βοηθούν στη δημιουργία δικτυακών εφαρμογών βασισμένων στις τεχνολογίες XML (χαρακτηριστικό παράδειγμα είναι το SOAP – Simple Object Access Protocol – το οποίο προσδίδει ένα μοντελοποιημένο τρόπο επικοινωνίας στις δικτυακές υπηρεσίες XML). Εκτός των άλλων, οι τεχνολογίες XML διαρκώς βελτιώνονται και εξελίσσονται με γοργούς ρυθμούς, σε αντίθεση με τα παραδοσιακά εργαλεία διαχείρισης δικτύων όπως για παράδειγμα το SNMP (Simple Network Management Protocol) τα οποία είναι σχετικά στατικά.

Το μεγάλο πλεονέκτημα των τεχνολογιών XML είναι η απλότητα των βασικών δομών αυτών των τεχνολογιών δηλαδή των εγγράφων XML. Η πολύ απλή, ιεραρχική δομή των αρχείων αυτών είναι εξαιρετικά σημαντική καθώς επιτρέπει την εύκολη δημιουργία νέων εφαρμογών, χωρίς προαπαιτούμενα και κόστος, σε αντίθεση με τα σχήματα διαχείρισης του SNMP, τα οποία είναι πιο δυσκίνητα.

Ακόμα και σήμερα, η απομακρυσμένη διαχείριση των δικτυακών συστατικών μιας υπηρεσίας (software και hardware) πραγματοποιείται με χρήση του πρωτοκόλλου SNMP. Το πρωτόκολλο αυτό, απαιτεί την ύπαρξη ενός κατάλληλου εξυπηρετητή (server) σε κάθε δικτυακό στοιχείο ελέγχου, ο οποίος θα έχει τη δυνατότητα πρόσβασης σε μια κατάλληλα διαρθρωμένη και ενημερωμένη βάση δεδομένων, η οποία περιγράφει πλήρως τις δυνατότητες και την κατάσταση της συσκευής. Τα δομικά στοιχεία του πρωτοκόλλου αυτού είναι σχετικά απλά, και διαρθρωμένα με τέτοιο τρόπο ώστε να διατηρείται η λογική ιεραρχία που διέπει τα χαρακτηριστικά αυτά. Αναλυτικότερα, μία κάρτα δικτύου μπορεί να έχει πολλές διεπαφές (interfaces), και κάθε διεπαφή μπορεί να έχει διαφορετική ονομαστική ταχύτητα ή ρυθμό λαθών. Επίσης κάποιες διεπαφές ενδέχεται να μην παρουσιάζον διαχειριστικό ενδιαφέρον, ενώ άλλες μπορεί να βρίσκονται σε κατάσταση αδράνειας (κλειστές). Όλα αυτά, πραγματοποιούνται με τρόπο εύκολο στο SNMP, το οποίο προσεγγίζει τον ανθρώπινο τρόπο οργάνωσης πληροφοριών. Αυτό είναι το κύριο

πλεονέκτημα της τεχνολογίας αυτής. Το κύριο μειονέκτημά της όμως είναι το γεγονός ότι δεν έχει δυνατότητα να αναγνωρίζει αυτόματα νέες συσκευές που εισάγονται στο δίκτυο, γεγονός ιδιαίτερα σημαντικό σε περιπτώσεις μεγάλων σε έκταση δικτύων (και γεωγραφικά όπως αποτελεί πχ ένα δίκτυο BPL).

Τα μεγάλα σε έκταση δίκτυα έχουν την ανάγκη αυτόματης εισαγωγής νέων συσκευών χωρίς την ανθρώπινη παρέμβαση για τη διαμόρφωση αυτών. Η ανάγκη για *αυτόνομα* δίκτυα συσκευών ελέγχου είναι μεγάλη. Σε προηγούμενο κεφάλαιο αναλύθηκε η αξία των αυτόνομων συστημάτων, και ο τρόπος με τον οποίο αυτά μπορούν να αποφέρουν οφέλη στη διαχειριστική αρχή ενέργειας. Έχοντας υπόψη τα παραπάνω, τα πρωτόκολλα του SNMP παρουσιάζονται μη επαρκή, καθώς απαιτούν εκτεταμένη ανθρώπινη παρουσία τόσο κατά την εγκατάσταση όσο και κατά τη συντήρηση των συσκευών (14). Οι τεχνολογίες XML και ειδικά το πρωτόκολλο UPnP (Universal Plug and Play) καταφέρνουν να συνδυάσουν όλα τα θετικά στοιχεία των τεχνολογιών του SNMP, ενώ παράλληλα προβαίνουν ένα ακόμη βήμα πιο κοντά στην αυτονόμηση του υπό διαχείριση συστήματος, καθώς το κύριο σχετικό χαρακτηριστικό τους είναι η εύκολη, αυτόνομη και διαφανής αναγνώριση νέων δικτυακών συσκευών που εισάγονται στο δίκτυο. Στα παρακάτω κεφάλαια θα παρουσιασθούν εκτενέστερα το πρωτόκολλο UPNP στο οποίο βασίζεται και η ιεραρχία ελέγχου που σχεδιάστηκε. Επίσης θα γίνει μια παρουσίαση της εφαρμογής που θα πραγματοποιεί τον έλεγχο των συσκευών του δικτύου.

## 3.2 Το πρωτόκολλο Universal Plug and Play

### 3.2.1 Εισαγωγικά

Η αρχιτεκτονική UPnP προσφέρει ένα διεισδυτικό τρόπο ομότιμης (peer-to-peer) επικοινωνίας μεταξύ διαφόρων ειδών υπολογιστικών συστημάτων σε ένα δίκτυο, είτε αυτά είναι απλές έξυπνες συσκευές (για παράδειγμα στην παρούσα εφαρμογή δεν υπάρχει ανάγκη για κάτι παραπάνω από απλούς microlinux stations) είτε πολύπλοκα συστήματα, τα οποία διασυνδέονται μεταξύ τους μέσω οποιουδήποτε φυσικού μέσου (ασύρματα ή ενσύρματα). Η αρχιτεκτονική UPnP είναι μια κατανεμημένη, ανοιχτού κώδικα, δικτυακή αρχιτεκτονική που εκμεταλλεύεται τις ιδιότητες του TCP/IP και του διαδικτύου προκειμένου να καταστήσει δυνατή την απρόσκοπτη μεταφορά δεδομένων ελέγχου και πληροφορίας μεταξύ των διασυνδεδεμένων στο ίδιο δίκτυο συσκευών (15).

Τα κύρια πλεονεκτήματα της τεχνολογίας UPnP είναι:

- **Ανεξαρτησία μέσου και συσκευής**: Το πρωτόκολλο UPnP μπορεί να τρέξει σε οποιαδήποτε δικτυακή τεχνολογία μετάδοσης όπως για παράδειγμα Wi-Fi, ομοαξονικά καλώδια, τηλεφωνικές γραμμές, γραμμές ενέργειας, Ethernet, IEEE 1394 κα.
- **Ανεξαρτησία πλατφόρμας**: Οι κατασκευαστές UPnP enabled συσκευών μπορούν να χρησιμοποιήσουν οποιαδήποτε γλώσσα προγραμματισμού και οποιοδήποτε λειτουργικό σύστημα προκειμένου να σχεδιάσουν την εφαρμογή τους. Αυτό είναι ιδιαίτερα σημαντικό καθώς σε ένα δικτυωμένο περιβάλλον είναι αναμενόμενη η ύπαρξη διαφορετικών λειτουργικών συστημάτων αλλά και ξεχωριστών αναγκών από συγκεκριμένα συστήματα, γεγονός που σημαίνει και διαφορετικές υλοποιήσεις του πρωτοκόλλου, ανάλογα με την περίσταση.
- **Τεχνολογίες βασισμένες στο διαδίκτυο**: Η τεχνολογία UPnP είναι βασισμένη μεταξύ των άλλων στα πρωτόκολλα IP, TCP, UDP, HTTP και XML.
- **Έλεγχος μέσω διεπαφών χρήστη**: Η αρχιτεκτονική UPnP επιτρέπει στους χρήστες να ελέγχουν τις συσκευές που επιθυμούν, απομακρυσμένα και εύκολα μέσω απλής χρήσης ενός οποιουδήποτε internet browser.
- **Προγραμματιστικός έλεγχος**: Το πρωτόκολλο UPnP καθιστά δυνατό τον έλεγχο μιας οποιαδήποτε UPnP enabled συσκευής προγραμματιστικά, υλοποιώντας όλες τις λειτουργίες που κρίνονται απαραίτητες.
- **Επεκτασιμότητα**: Κάθε UPnP enabled συσκευή μπορεί να εμπλουτιστεί με υπηρεσίες (services) προστιθέμενης αξίας, που τοποθετούνται ιεραρχικά πάνω στα ήδη υπάρχοντα πρότυπα, και προσφέρουν επιπλέον δυνατότητες διαχείρισης, χωρίς να υπάρχει ανάγκη πλήρους επαναπροσδιορισμού του ήδη υπάρχοντος κώδικα.

Άλλο ένα σημαντικό χαρακτηριστικό του πρωτοκόλλου UPnP είναι το γεγονός ότι βασίζεται σε τεχνολογίες ομότιμων δικτύων (peer-to-peer). Όπως θα εξηγηθεί και αναλυτικότερα στη συνέχεια, η διαχείριση των συσκευών που μας ενδιαφέρουν (devices) γίνεται μέσω (δυνητικά αντίστοιχων) σημείων ελέγχου (control points). Καμία από τις συσκευές παρόλα αυτά δεν διαδραματίζει το ρόλο του εξυπηρετητή ή του πελάτη στο κλασικό πλέον μοντέλο client – server. Αντίθετα, οι δύο συσκευές είναι εντελώς ομότιμες, ενώ είναι πολύ εύκολη με κατάλληλες τεχνικές να αντιστροφή των ρόλων τους. Κάτι τέτοιο είναι σημαντικό σε αρχιτεκτονικές BPL, όπου η πιθανή δυσλειτουργία ενός σημείου ελέγχου μπορεί να σημάνει την απώλεια ελέγχου μιας ολόκληρης περιοχής χρηστών, κάτι κρίσιμο ειδικά σε

περιπτώσεις εξυπηρέτησης πυκνοκατοικημένων αστικών κέντρων, ή περιοχών με αυξημένο φόρτο εξυπηρέτησης (σχετικά με την παροχή ρεύματος).

Τα σύγχρονα συστήματα ελέγχου οφείλουν να παρουσιάζουν τουλάχιστον κάποια από τα χαρακτηριστικά των αυτόνομων συστημάτων προκειμένου να επιτευχθεί αυξημένη αξιοπιστία, ταχύτητα, οικονομία, ευκολία διαχείρισης και ελέγχου, και προσθήκης νέων υπηρεσιών και συσκευών. Το πρωτόκολλο UPnP έχει τη δυνατότητα να προσφέρει αυτά τα χαρακτηριστικά στις εφαρμογές ελέγχου, καθώς υποστηρίζει μηδενικής διαμόρφωσης, αυτοματοποιημένη αναγνώριση και ενσωμάτωση συσκευών στο δικτυωμένο περιβάλλον. Έτσι, πολύ εύκολα και *αυτόματα* μία συσκευή έχει τη δυνατότητα:

- Να προστεθεί δυναμικά σε ένα δίκτυο,
- Να αποκτήσει μια διεύθυνση IP,
- Να ανακοινώσει την παρουσία και το όνομά της,
- Να ενημερώσει κατάλληλα τις συσκευές ελέγχου για τις υπηρεσίες που μπορεί να προσφέρει κατόπιν αιτήσεων των πρώτων,
- Να ενημερωθεί άμεσα για την παρουσία και τις δυνατότητες άλλων δικτυωμένων συσκευών,
- Να εξέλθει του δικτύου αυτόματα, ενημερώνοντας τα στοιχεία ελέγχου που πιθανώς την ελέγχουν, χωρίς ταυτόχρονα να αφήσει οποιαδήποτε ανεπιθύμητη ή περιττή πληροφορία (unwanted state information) στο δίκτυο.

Όπως γίνεται ήδη φανερό, η χρήση του πρωτοκόλλου UPnP επιτρέπει την ευκολότερη εισαγωγή, διαχείριση και μορφοποίηση νέων συσκευών σε και από τα εκάστοτε υπολογιστικά συστήματα ελέγχου. Το UPnP είναι κάτι παραπάνω από μία απλή επέκταση του μοντέλου Plug and Play. Είναι σχεδιασμένο ώστε να μπορεί να προσφέρει «αόρατο» τρόπο δικτύωσης, χωρίς ανθρώπινη παρέμβαση, καθώς και αυτόματη αναγνώριση νέων συσκευών για πολύ μεγάλο εύρος κατηγοριών συσκευών, για τεράστιο εύρος (πρακτικά άπειρων) υπηρεσιών (16). Στην επόμενη παράγραφο, θα εξεταστεί το σενάριο που παρουσιάζει ενδιαφέρον δηλαδή ο έλεγχος των δικτυακών συσκευών BPL που θα ευρίσκονται σε ένα κοινό δίκτυο. Σκοπός είναι αργότερα να επεκταθεί το πρωτόκολλο αυτό ώστε να εφαρμόζεται εν μέρει και σε άλλα, ανοιχτά δίκτυα, ενώ ανάλογα με τις ανάγκες του κάθε παρόχου ηλεκτρικής ενέργειας μπορούν να προστεθούν πολύ εύκολα και νέες υπηρεσίες προστιθέμενης αξίας, που θα ολοκληρώσουν το σύστημα ελέγχου του συστήματος (15).

### 3.2.2 Η λειτουργία του πρωτοκόλλου

Παρακάτω ακολουθεί μια συνοπτική περιγραφή της λειτουργίας του πρωτοκόλλου UPnP, που είναι σημαντική στην καλύτερη κατανόηση των δυνατοτήτων του πρωτοκόλλου, για τη δημιουργία των επιθυμητών εφαρμογών ελέγχου. Στους όρους που κρίνεται ότι είναι σημαντικοί, θα παρατίθεται και ο αγγλικός όρος την πρώτη φορά, για λόγους συμβατότητας με την ορολογία του πρωτοκόλλου.

Η λειτουργία του πρωτοκόλλου UPnP περιλαμβάνει τις ακόλουθες φάσεις (17):

1. ***Ανεύρεση (Discovery)***: Στην πρώτη αυτή φάση, τα σημεία ελέγχου (control points) ψάχνουν για συσκευές και υπηρεσίες. Παρόμοια, οι συσκευές αποστέλλουν μαζικά (μέσω multicast πακέτων) ανακοινώσεις (announcements) των υπηρεσιών που προσφέρουν.
2. ***Περιγραφή (Description)***: Μόλις ένα σημείο ελέγχου ανακαλύψει στη φάση Ανεύρεσης μια συσκευή με υπηρεσίες που το ενδιαφέρει, ζητά από τη συσκευή να του αποστείλει μια λεπτομερή περιγραφή των δυνατοτήτων, υπηρεσιών και εν γένει πληροφοριών που μπορεί η τελευταία να προσφέρει. Οι πληροφορίες αυτές, εκτός από υπηρεσίες, μπορεί να είναι και πληροφορίες για άλλες ενσωματωμένες συσκευές τις οποίες περιέχει ή άλλες πληροφορίες κατάστασης (state information).
3. ***Έλεγχος (Control)***: Κατά τη διάρκεια της φάσης ελέγχου, το σημείο ελέγχου καλείται να διαμορφώσει μία ή παραπάνω υπηρεσίες της συσκευής την οποία ελέγχει[6] προκαλώντας αλλαγές στην κατάσταση των υπηρεσιών αυτής.
4. ***Συγχρονισμός (Eventing)***: Αυτή η φάση επιτρέπει στο σημείο ελέγχου να διατηρείται σε συγχρονισμό με την κατάσταση των υπηρεσιών της συσκευής την οποία ελέγχει. Τα σημεία ελέγχου αιτούνται συνδρομής (subscribe) στον εξυπηρετητή συμβάντων (event server) για μια συγκεκριμένη υπηρεσία και λαμβάνουν κατόπιν ειδοποιήσεις όταν η κατάσταση της υπηρεσίας στη συσκευή αλλάζει.
5. ***Παρουσίαση (Presentation)***: Η φάση της παρουσίασης επιτρέπει σε μία συσκευή να λάβει ένα αρχείο, γραμμένο σε standard HTML, το οποίο μπορεί να λειτουργήσει ως διεπαφή χρήστη για τη συσκευή αυτή.

Οι παρακάτω παράγραφοι, περιγράφουν αναλυτικότερα (αρκετά συνοπτικά εντούτοις) τη λειτουργία και τη σημασία των παραπάνω φάσεων.

[6] Στη γενική περίπτωση φυσικά, ένα σημείο ελέγχου μπορεί να ελέγχει παραπάνω από μία συσκευή.

#### *3.2.2.1 Ανεύρεση (Discovery)*

Στη φάση της ανεύρεσης, το σημείο ελέγχου ανακαλύπτει συσκευές και υπηρεσίες αυτών, ενώ παράλληλα οι συσκευές ανακοινώνουν την παρουσία τους στα σημεία ελέγχου, χρησιμοποιώντας το πρωτόκολλο Simple Service Discovery (SSDP). Το πρωτόκολλο SSDP κάνει χρήση μιας παραλλαγής του πρωτοκόλλου HTTP πάνω από το πρωτόκολλο multicast UDP για ευρυεκπομπές (broadcast) και μια άλλη παραλλαγή του HTTP που λειτουργεί πάνω από unicast UDP για τις απαντήσεις.

Μία συσκευή μπορεί να αποτελείται από άλλες συσκευές, κάθε μία από τις οποίες μπορεί να παρέχει διαφορετικές υπηρεσίες. Οι συσκευές καθορίζονται τόσο από τον τύπο τους όσο και από ένα μοναδικό αναγνωριστικό (unique identifier). Οι υπηρεσίες αναγνωρίζονται από τον τύπο τους.

Προκειμένου να ψάξουν για συσκευές ή υπηρεσίες στο δίκτυο, τα σημεία ελέγχου χρησιμοποιούν μέσω πολυεκπομπής (multicast) την εντολή HTTP M-SEARCH στη διεύθυνση 239.255.255.250:1900 πάνω από πρωτόκολλο UDP. Οποιαδήποτε συσκευή στο δίκτυο πληροί όλα τα κριτήρια που αναζητά το σημείο ελέγχου, εκπέμπει μία απάντηση πάνω από unicast UDP που περιλαμβάνει εκτός των άλλων μία διεύθυνση URL υποδεικνύοντας το έγγραφο περιγραφής της (βλ. παράγραφο 3.2.2.2). Αν ένα σημείο ελέγχου λάβει μία ή παραπάνω αποδεκτές απαντήσεις, προχωρά στη φάση της περιγραφής.

Όταν ένα σημείο ελέγχου εκπέμψει ένα αίτημα αναζήτησης (search request), περιλαμβάνει το χρόνο τον οποίο είναι διαθέσιμο να περιμένει μέχρι να λάβει μία επικεφαλίδα SSDP. Οι συσκευές που πληρούν τα κριτήρια του σημείου ελέγχου περιμένουν για ένα τυχαίο χρονικό διάστημα μικρότερο από το χρόνο που ορίζει το σημείο ελέγχου και μετά απαντήσουν. Αν ένα σημείο ελέγχου δε λάβει απαντήσεις όταν το χρονικό διάστημα αναζήτησης τελειώσει, υποθέτει ότι δεν υπάρχουν αντίστοιχες συσκευές στο δίκτυο.

Οι συσκευές δε χρειάζεται να περιμένουν ένα σημείο ελέγχου να ψάξει για τις υπηρεσίες τους. Μπορούν να ανακοινώσουν τη διαθεσιμότητά τους μέσω μιας εντολής SSDP NOTIFY στην διεύθυνση πολυεκπομπής 239.255.255.250:1900. Όταν τα σημεία ελέγχου δουν αυτό το πακέτο πολυεκπομπής NOTIFY, μπορούν να ζητήσουν το έγγραφο περιγραφής της συσκευής χρησιμοποιώντας ένα τυπικό HTTP GET μήνυμα, στη διεύθυνση που καθορίζεται από το μήνυμα NOTIFY. Οι συσκευές πρέπει φυσικά να στείλουν και αντίστοιχη ειδοποίηση όταν οι υπηρεσίες τους δεν είναι πλέον διαθέσιμες.

### *3.2.2.2 Περιγραφή (Description)*

Όταν ένα σημείο ελέγχου εντοπίζει μία υπηρεσία για την οποία θέλει να μάθει περισσότερα, ζητά το έγγραφο περιγραφής της αντίστοιχης συσκευής. Το έγγραφο αυτό περιγραφής είναι ένα τυπικό XML αρχείο που περιγράφει τη συσκευή, περιλαμβάνοντας:

- Πληροφορίες σχετικές με τον κατασκευαστή κτλ,
- URL διευθύνσεις σχετικά με εικόνες που μπορούν να χρησιμοποιηθούν για τη συσκευή,
- Μια λίστα με τις ενσωματωμένες συσκευές και τέλος
- Μια λίστα με τις υπηρεσίες που υποστηρίζονται από τη συσκευή.

Για περισσότερες πληροφορίες σχετικά με το έγγραφο περιγραφής, ο αναγνώστης μπορεί να ανατρέξει στο έγγραφο *Universal Plug and Play Device Architecture* (15).

Το σημείο ελέγχου ζητά το έγγραφο περιγραφής μιας συσκευής χρησιμοποιώντας το πρωτόκολλο HTTP πάνω από TCP. Το σημείο ελέγχου εκδίδει μια εντολή HTTP GET (παρόμοια με αυτήν για τη μεταφόρτωση μιας ιστοσελίδας). Από την πλευρά του εξυπηρετητή (σε επόμενη παράγραφο θα παρουσιασθούν τα δομικά μέρη μιας UPnP enabled συσκευής) η συσκευή τρέχει έναν τυπικό HTTP server – είτε έναν πλήρη Web server όπως για παράδειγμα ο Apache, ή ένα miniserver. Πολλά από τα στοιχεία του εγγράφου περιγραφής είναι εξάλλου διευθύνσεις URL. Αυτά τα στοιχεία επίσης λαμβάνονται μέσω HTTP/TCP. Ακολουθεί ένα τυπικό παράδειγμα δόμησης ενός εγγράφου περιγραφής:

```
<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
 <specVersion>
  <major>1</major>
  <minor>0</minor>
 </specVersion>
 <device>
  <deviceType>urn:schemas-upnp-org:device:tvdevice:1</deviceType>
  <friendlyName>UPnP Television Emulator</friendlyName>
  <manufacturer>TV Manufacturer Name</manufacturer>
  <manufacturerURL>http://www.manufacturer.com</manufacturerURL>
  <modelDescription>UPnP Television Device Emulator 1.0</modelDescription>
  <modelName>TVEmulator</modelName>
  <modelNumber>1.0</modelNumber>
  <modelURL>http://www.manufacturer.com/TVEmulator/</modelURL>
  <serialNumber>123456789001</serialNumber>
  <UDN>uuid:Upnp-TVEmulator-1_0-1234567890001</UDN>
  <UPC>123456789</UPC>
  <serviceList>
   <service>
    <serviceType>urn:schemas-upnp-org:service:tvcontrol:1</serviceType>
    <serviceId>urn:upnp-org:serviceId:tvcontrol1</serviceId>
```

```
      <controlURL>/upnp/control/tvcontrol1</controlURL>
      <eventSubURL>/upnp/event/tvcontrol1</eventSubURL>
      <SCPDURL>/tvcontrolSCPD.xml</SCPDURL>
     </service>
     <service>
      <serviceType>urn:schemas-upnp-org:service:tvpicture:1</serviceType>
      <serviceId>urn:upnp-org:serviceId:tvpicture1</serviceId>
      <controlURL>/upnp/control/tvpicture1</controlURL>
      <eventSubURL>/upnp/event/tvpicture1</eventSubURL>
      <SCPDURL>/tvpictureSCPD.xml</SCPDURL>
     </service>
    </serviceList>
   <presentationURL>/tvdevicepres.html</presentationURL>
</device>
</root>
```

Παρατηρείται ότι υπάρχουν πολλές URL διευθύνσεις οι οποίες εν τέλει προσφέρουν τη δυνατότητα στο σημείο ελέγχου να μάθει τα πάντα σχετικά με τις δυνατότητες και τις υπηρεσίες της υπό διαχείριση συσκευής.

#### *3.2.2.3 Έλεγχος (Control)*

Μόλις ένα σημείο ελέγχου ανακαλύψει μια συσκευή και δεχθεί το έγγραφο περιγραφής της, μπορεί να ελέγξει μία ή παραπάνω από τις υπηρεσίες αυτής. Το πρωτόκολλο Simple Object Access Protocol (SOAP) επιτρέπει σε ένα σημείο ελέγχου να ερωτήσει ή να αλλάξει στοιχεία στον πίνακα κατάστασης υπηρεσιών της συσκευής. Το SOAP κάνει χρήση των εντολών POST και M-POST του πρωτοκόλλου HTTP που μεταφέρεται πάνω από TCP.

Το SOAP χρησιμοποιεί αποκλειστικά XML έγγραφα για να καθορίσει τις ενέργειες που επιθυμεί να διενεργηθούν. Το σημείο ελέγχου δημιουργεί το έγγραφο XML και κατόπιν το εκπέμπει στη διεύθυνση URL ελέγχου για τη συγκεκριμένη υπηρεσία, όπως αυτή περιγράφεται στο έγγραφο περιγραφής που έχει ήδη λάβει από τη συσκευή. Το σημείο ελέγχου μπορεί να ζητήσει τρέχουσες τιμές διαφόρων μεταβλητών και να προκαλέσει αλλαγές στον πίνακα κατάστασης υπηρεσιών τις συσκευής.

Από την πλευρά του εξυπηρετητή, το σημείο ελέγχου περιμένει για αναζητήσεις ελέγχου (control requests). Ο εξυπηρετητής ελέγχου (control server) είναι όμοιος με έναν εξυπηρετητή HTTP, ο οποίος τρέχει μια υλοποίηση του πρωτοκόλλου SOAP. Μία συσκευή μπορεί να λειτουργεί έναν ή παραπάνω εξυπηρετητές ελέγχου ανάλογα με το συνδυασμό των υπηρεσιών που επιθυμεί.

#### *3.2.2.4 Συγχρονισμός (Eventing)*

Αφότου ένα σημείο ελέγχου ανακαλύψει μία συσκευή και λάβει το έγγραφο περιγραφής της, μπορεί να παραμείνει ενημερωμένο σχετικά με την κατάσταση των υπηρεσιών που προσφέρονται από αυτή. Τα ενδιαφερόμενα σημεία ελέγχου μπορούν να εγγραφούν στην υπηρεσία ειδοποίησης γεγονότων (event notification service) της συσκευής, υπηρεσία της οποίας το URL λαμβάνουν από το έγγραφο περιγραφής της συσκευής (κατά τις φάσεις περιγραφής και του ελέγχου). Κάθε φορά που κάτι αλλάζει λοιπόν στον πίνακα κατάστασης της συσκευής, πραγματοποιείται μια αποστολή ειδοποίησης γεγονότος στο σημείο ελέγχου, ακόμα και αν την αλλαγή αυτήν την έχει προκαλέσει το ίδιο το σημείο ελέγχου, για λόγους επιβεβαίωσης.

Οι αιτήσεις εγγραφής / διαγραφής χρησιμοποιούν το πρωτόκολλο HTTP/TCP για να συγχρονιστούν με το αντίστοιχο URL που εμπεριέχεται στο έγγραφο περιγραφής της συσκευής[7]. Το σημείο ελέγχου καθορίζει ένα URL όπου θα καταγράφονται οι ειδοποιήσεις γεγονότων κατά την εγγραφή. Τα γεγονότα καταφθάνουν με τη βοήθεια του HTTP/TCP στο URL που έχει εγγραφεί με την υπηρεσία. Η ειδοποίηση γεγονότος περιλαμβάνει ένα μικρό XML αρχείο που περιγράφει το πραγματικό γεγονός, όπως για παράδειγμα μια αλλαγή στον πίνακα κατάστασης της συσκευής.

Από την πλευρά του εξυπηρετητή, ένας εξυπηρετητής γεγονότων περιμένει για αιτήσεις εγγραφής και διαγραφής. Ο εξυπηρετητής γεγονότων είναι βασισμένος στο πρωτόκολλο http και τρέχει μια υλοποίηση του πρωτοκόλλου General Event Notification Architecture (GENA). Μια συσκευή έχει τη δυνατότητα να διατηρεί παραπάνω από έναν εξυπηρετητή γεγονότων ανάλογα με το συνδυασμό των υπηρεσιών που προσφέρονται από τη συσκευή.

[7]Το έγγραφο περιγραφής είναι ιδιαίτερα κρίσιμο για την ορθή και υγιή λειτουργία του πρωτοκόλλου, γι αυτό το λόγο μεταφέρεται μέσω του πρωτοκόλλου HTTP/TCP. Επίσης, επειδή οι συσκευές ελέγχου ενός μεγάλου δικτύου είναι συνήθως ενός κατασκευαστή και παρόμοιας έκδοσης (λόγω παρουσίας συμβάσεων κτλ), υπάρχει πολύ μεγάλος όγκος πληροφορίας που επαναλαμβάνεται στο δίκτυο, καταναλώνοντας έτσι εύρος ζώνης που διαφορετικά θα μπορούσε να διατεθεί διαφορετικά πχ για κάποια άλλη λειτουργία ελέγχου, ή ακόμα και για εμπορική διάθεση. Όταν ο αριθμός των συσκευών και των σημείων ελέγχου γίνεται μεγάλος, τότε η ανάγκη για εξοικονόμηση αυτού του εύρους ζώνης γίνεται επιτακτική, κυρίως όπως αναφέρθηκε νωρίτερα για οικονομικούς σκοπούς. Στη συνέχεια της εργασίας θα επιχειρηθεί μια περιγραφή των τρόπων με τη βοήθεια των οποίων η επιθυμητή αυτή μείωση της πληροφορίας καθίσταται εφικτή. Επίσης θα μελετηθεί και η επίδρασή των τρόπων αυτών στη συνολική απόκριση του δικτύου, και το φόρτο αυτού.

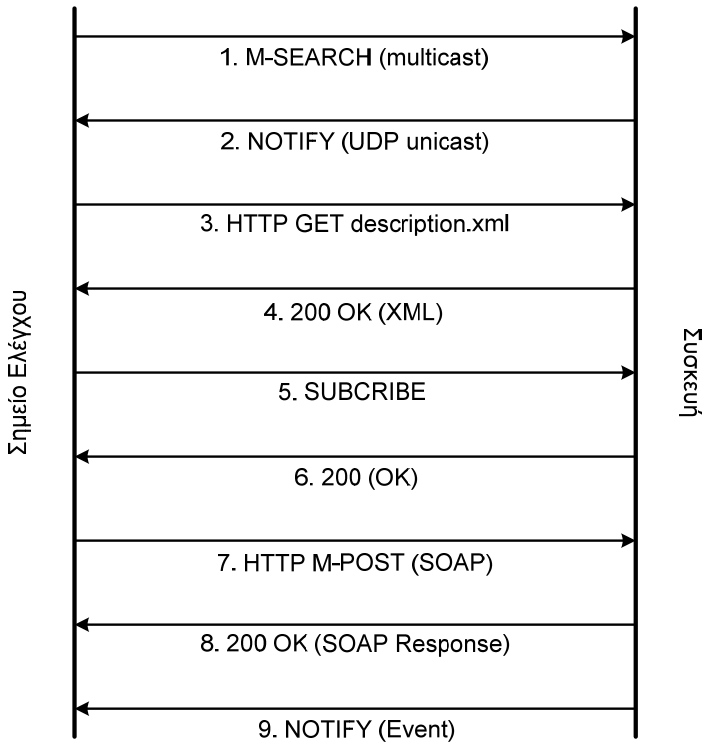
#### *3.2.2.5 Παρουσίαση (Presentation)*

Κάποιες συσκευές μπορούν να παρέχουν δυνατότητα γραφικής διεπαφής με το χρήστη (user interface). Στη φάση της παρουσίασης ένα σημείο ελέγχου μπορεί να μεταφορτώσει ένα έγγραφο HTML που παρουσιάζει τη γραφική διεπαφή του χρήστη με τη συσκευή. Αυτό είναι ένα τυπικό HTML αρχείο, που μπορεί να προσφέρει είτε μόνο οπτική παρατήρηση των γεγονότων και καταγραφή αυτών, είτε ακόμα και υπηρεσίες ελέγχου (υποτυπώδης γραφική υποστήριξη).

Το πρωτόκολλο για τη λήψη του εγγράφου παρουσίασης, όπως και στην περίπτωση του εγγράφου περιγραφής, είναι το HTTP/TCP. Το σημείο ελέγχου μπορεί να χρησιμοποιήσει τη διεύθυνση URL που εμπεριέχεται μέσα στο έγγραφο περιγραφής για να ζητήσει το έγγραφο παρουσίασης. Παρά τη φαινομενική χρησιμότητα αυτής της υπηρεσίας, δεν έχουν όλες οι συσκευές τη δυνατότητα να προσφέρουν κάτι τέτοιο, ενώ επίσης δεν έχουν όλα τα σημεία ελέγχου την ικανότητα να «διαβάσουν» περίπλοκες δομές HTML όπως frames, JAVA applets κτλ.

### 3.2.3 Το σημείο ελέγχου και η αλληλεπίδραση με τη συσκευή

Το Σχήμα 3.1 παρουσιάζει τη διαδοχή των αλληλεπιδράσεων μεταξύ ενός σημείου ελέγχου και μιας συσκευής κατά τη διάρκεια των διαδοχικών φάσεων του UPnP. Μετά το σχήμα ακολουθεί επεξήγηση αυτού. Οι περιγραφές που ακολουθούν περιλαμβάνουν επίσης βασικές προγραμματιστικές εντολές που βοηθάνε στην καλύτερη κατανόηση του κώδικα που θα ακολουθήσει αργότερα (βλ. κεφάλαιο 4). Σε αυτό το σημείο πρέπει να σημειωθεί ότι λόγω του ασύγχρονου χαρακτήρα της επικοινωνίας σημείου ελέγχου – συσκευής, οι αλληλεπιδράσεις δε συμβαίνουν απαραίτητα με τη σειρά που παρουσιάζονται παρακάτω: αυτό είναι απλά το πλέον συνηθισμένο σενάριο. Εντούτοις, οι φάσεις ελέγχου και συγχρονισμού μπορούν να συμβούν με οποιαδήποτε σειρά.




**Σχήμα 3.1: Συνηθισμένο σενάριο αλληλεπίδρασης σημείου ελέγχου – συσκευής.**

Σε σχέση λοιπόν με το παραπάνω σχήμα, κρίνεται σκόπιμο να γίνουν οι εξής παρατηρήσεις:

1. Το σημείο ελέγχου αποστέλλει μια αίτηση αναζήτησης χρησιμοποιώντας το API UpnpSearchAsync(). Το SDK για τη συσκευή UPnP εκδίδει ένα μήνυμα M-SEARCH SSDP στο δίκτυο.

2. Αν η συσκευή πληροί τις προϋποθέσεις που έχουν τεθεί από το σημείο ελέγχου, το SDK αποστέλλει μια unicast UDP NOTIFY απάντηση με το URL στο έγγραφο περιγραφής της συσκευής. Το SDK απαντά αυτόματα μέσω της πληροφορίας που ενυπάρχει στο έγγραφο περιγραφής της συσκευής που έχει εγγραφεί, χρησιμοποιώντας τα API UpnpRegisterRootDevice() ή UpnpRegisterRootDevice2().

3. Αν το σημείο ελέγχου επιθυμήσει περισσότερες πληροφορίες για τη συσκευή, καλεί τη συνάρτηση UpnpDownloadXmlDoc() και μεταφορτώνει το έγγραφο περιγραφής της συσκευής μέσω κλήσης μιας τυπικής HTTP GET εντολής. Η συνάρτηση αυτή, επιστρέφει ένα έγγραφο XML σε μορφή DOM που αποτελεί την περιγραφή της συσκευής. Αυτό το βήμα μπορεί να επαναληφθεί αρκετές φορές μέχρι να ληφθούν τα έγγραφα περιγραφής των υπηρεσιών που προσφέρει η υπηρεσία.

4. Ο εξυπηρετητής web που εδρεύει στη συσκευή απαντά στην αίτηση αυτή και επιστρέφει το έγγραφο περιγραφής XML.

5. Προκειμένου να μπορεί να λάβει αυτόματα ενημερώσεις για τυχόν αλλαγές στη συσκευή, το σημείο ελέγχου εγγράφεται (subscribe) στις υπηρεσίες της συσκευής που το ενδιαφέρουν. Αυτό γίνεται μέσω των API UpnpSubscribe() ή UpnpSubscribeAsync(). Το σημείο ελέγχου αποκτά τη διεύθυνση URL της εγγραφής από το έγγραφο περιγραφής της υπηρεσίας ή των υπηρεσιών που θέλει να εγγραφεί, και καλεί μία εκ των δύο συναρτήσεων εγγραφής. Για κάθε κλήση εγγραφής, το SDK στέλνει ένα μήνυμα SUBSCRIBE μέσω HTTP μαζί με μία URL το οποίο καταδεικνύει πού θα στέλνει η συσκευή την ειδοποίηση για τα γεγονότα.

6. Η συσκευή ερευνά την αίτηση εγγραφής και κατόπιν επιστρέφει ένα μοναδικό αναγνωριστικό εγγραφής (Subscription Identifier – SID).

7. Το σημείο ελέγχου δίνει εντολή στη συσκευή να πραγματοποιήσει μια αλλαγή στον πίνακα κατάστασής της, αλλάζοντας κάποια από τις μεταβλητές κατάστασης που καθορίζουν τη συσκευή. Η διεύθυνση URL στην οποία πρέπει να στέλνονται οι αιτήσεις του σημείου ελέγχου εμπεριέχεται μέσα στο έγγραφο περιγραφής της συσκευής. Το σημείο ελέγχου καλεί τη συνάρτηση UpnpSendAction() ή την UpnpSendActionAsync() για να αλλάξει την κατάσταση της συσκευής. Στην περίπτωση αυτή, το SDK εκδίδει μια δράση SOAP μέσω μιας απλής εντολής M-POST.

8. Η συσκευή αλλάζει την κατάσταση της εσωτερικής της μεταβλητής ανάλογα με την αίτηση που της έγινε, και εκδίδει μια απάντηση σε μορφή επίσης SOAP.

9. Η συσκευή μπορεί να ενημερώσει τους «πελάτες» της για αλλαγές στην κατάστασή της ή διάφορες άλλες αλλαγές, όπως στο βήμα 8 που περιγράφηκε νωρίτερα. Σε αυτήν την περίπτωση, η συσκευή κάνει χρήση των API UpnpNotify() ή UpnpNotifyExt() για να στείλει την αντίστοιχη ενημέρωση. Το SDK αυτόματα ενημερώνει όλα τα εγγεγραμμένα σημεία ελέγχου μέσω ενός unicast NOTIFY μηνύματος πάνω από HTTP.

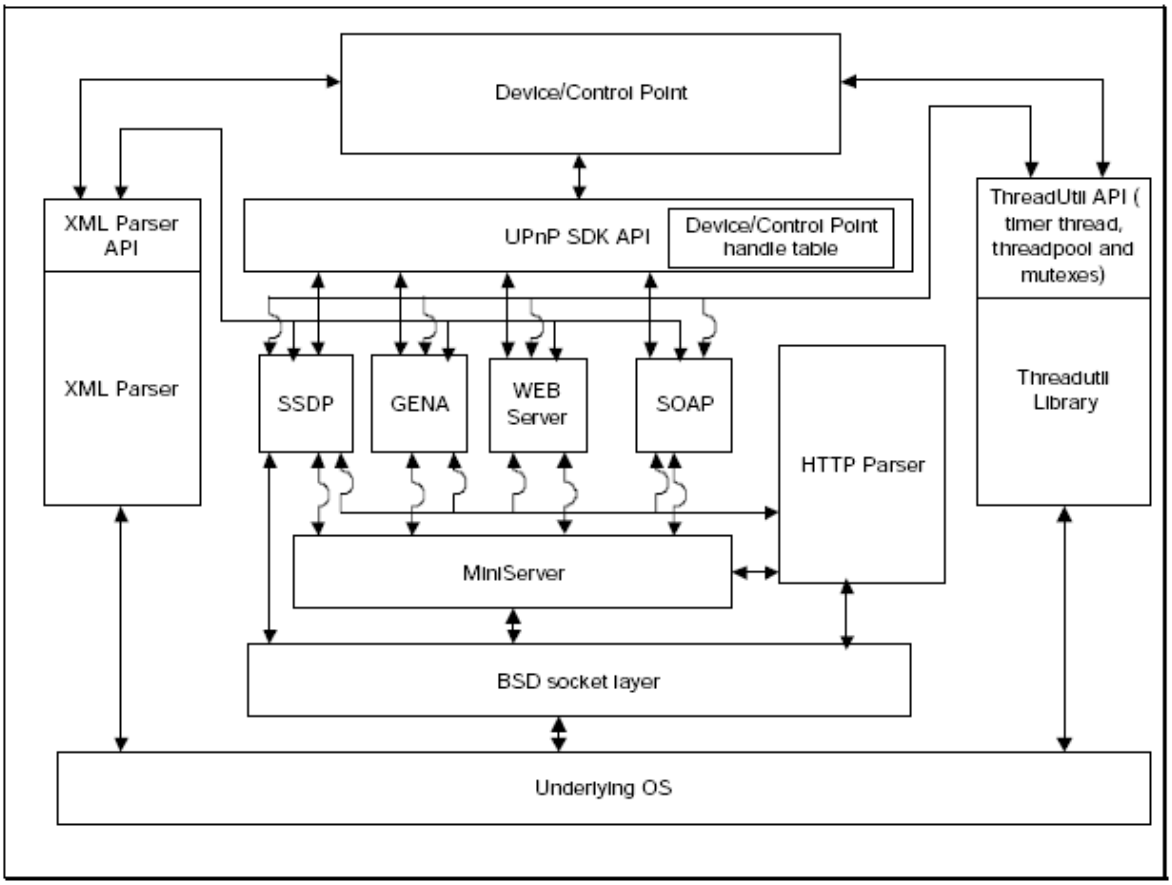
Σε όλα τα παραπάνω βήματα, παρατηρείται εκτεταμένη χρήση των εγγράφων XML, γεγονός που καθιστά το UPnP ένα πρωτόκολλο που εκμεταλλεύεται στο έπακρο τις τεχνολογίες XML. Από τον κώδικα του εγγράφου περιγραφής μιας συσκευής που παρουσιάστηκε

νωρίτερα, γίνεται αντιληπτό ότι η δομή του είναι καθαρά ιεραρχική. Το γεγονός αυτό, καθιστά την επεξεργασία και εξαγωγή των απαραίτητων πληροφοριών εύκολη, γρήγορη και αποτελεσματική. Επίσης, η εκτενής χρήση του πρωτοκόλλου SOAP για την περιγραφή των XML αντικειμένων, παρέχει μια στερεή, προτυποποιημένη βάση για την επικοινωνία μεταξύ των συσκευών και των στοιχείων ελέγχου.

Η ασύγχρονη φύση του πρωτοκόλλου όπως έχει ήδη προαναφερθεί, δίνει τη δυνατότητα δυναμικής αλλαγής της σειράς των παραπάνω βημάτων (εναλλαγή ανάμεσα στα βήματα ελέγχου και συγχρονισμού). Κάτι τέτοιο, λόγω της ασύγχρονης εισαγωγής νέων συσκευών στο δίκτυο (ή εξαγωγή αυτών πχ σε περίπτωση βλάβης) είναι ιδιαίτερα σημαντικό, και καταδεικνύει την ικανότητα του πρωτοκόλλου να συγχρονίζει αυτόματα με νέες συσκευές που εισάγονται στο δίκτυο.

### 3.2.4 Η αρχιτεκτονική του SDK

Το ακόλουθο διάγραμμα παρουσιάζει την αρχιτεκτονική του SDK του πρωτοκόλλου Universal Plug and Play:




Σχήμα 3.2: Διάγραμμα αρχιτεκτονικής του SDK για το πρωτόκολλο UPnP

Οι ακόλουθες παράγραφοι περιγράφουν κάθε μέρος του ανωτέρω διαγράμματος. Για περισσότερες πληροφορίες σχετικά με οποιοδήποτε από τα πρωτόκολλα, ο αναγνώστης μπορεί ανατρέξει στο έγγραφο *Universal Plug and Play Architecture* (16).

#### *3.2.4.1 Η εφαρμογή της συσκευής και του σημείου ελέγχου*

Στην ανώτατη βαθμίδα ιεραρχικά βρίσκονται οι εφαρμογές της συσκευής και του σημείου ελέγχου. Οι εφαρμογές αυτές υλοποιούν κάποιες συγκεκριμένες υπηρεσίες. Για παράδειγμα, αν πρέπει να υλοποιηθούν υπηρεσίες που συνήθως προσφέρονται από μια gateway ενός δικτύου, το λογισμικό του εξυπηρετητή υλοποιεί τη λειτουργία «Ενεργοποίηση δικτύου», υπηρεσία την οποία κάποιο σημείο ελέγχου μπορεί να ελέγξει μέσω του πρωτοκόλλου UPnP (19).

#### *3.2.4.2 SDK API*

Το SDK API αποκρύπτει την πληροφορία του πυρήνα των UPnP πρωτοκόλλων από τις εφαρμογές του σημείου ελέγχου και της συσκευής, ενώ παράλληλα καταφέρνει να δώσει στις εφαρμογές πρόσβαση στις εκάστοτε λειτουργίες μέσω ενός ενοποιημένου συστήματος

διεπαφών χρήστη και API. Κάτι τέτοιο ελευθερώνει τους μηχανικούς λογισμικού από την ανάγκη να γνωρίζουν και να λαμβάνουν υπόψη τους τις λεπτομέρειες των πρωτοκόλλων πυρήνα όπως είναι το SSDP, το GENA, και το SOAP. Κάτι τέτοιο βρίσκεται σε σύμπνοια με τις πλέον μοντέρνες αρχές δόμησης κώδικα λογισμικού, που υπαγορεύει τη χρήση δομών αφαίρεσης δεδομένων, τόσο για θέματα ασφαλείας όσο κυρίως για θέματα ευκολίας προς το μηχανικό λογισμικού που το αναπτύσσει.

Το στρώμα API συντηρεί επίσης και τον πίνακα των συσκευών και των σημείων ελέγχου που έχουν εγγραφεί στο SDK. Σε κάθε μία κλήση σε κάποια συνάρτηση του API, το SDK επαληθεύει αν η συσκευή/σημείο ελέγχου είναι γνωστή/ό ελέγχοντας κατάλληλα τον παραπάνω πίνακα. Προς το παρόν υπάρχει η δυνατότητα μόνο για ένα σημείο ελέγχου και μία συσκευή ταυτόχρονα από μία εφαρμογή. Αυτό σημαίνει ότι για μία εφαρμογή υπάρχει η δυνατότητα να εγγραφεί στο SDK μία φορά ως συσκευή και μία φορά ως συσκευή ελέγχου. Επιπλέον προσπάθειες εγγραφής (για παράδειγμα η ίδια εφαρμογή να συμπεριφέρεται και σαν σημείο ελέγχου αλλά και ως δύο διαφορετικές συσκευές) θα αποτύχουν. Για περισσότερες πληροφορίες σχετικά με το API, ο αναγνώστης μπορεί να ανατρέξει στο *Intel® SDK for UPnP™ Devices v1.2 Reference.*

#### *3.2.4.3 SSDP*

Η υπομονάδα του SSDP υλοποιεί το πρωτόκολλο Simple Service Discovery Protocol, δοθείσης της φάσης της ανεύρεσης του UPnP. Αυτή η υπομονάδα επιτρέπει στα σημεία ελέγχου να στέλνουν (μέσω πακέτων πολυεκπομπής) ερωτήματα για αναζήτηση υπηρεσιών ή και συσκευών στο δίκτυο, και λαμβάνει τις απαντήσεις επ' αυτών των ερωτημάτων. Εκτός των άλλων ενημερώνει όταν στο δίκτυο εισάγονται νέες υπηρεσίες. Τέλος, επιτρέπει στις συσκευές να στείλουν πακέτα πολυεκπομπής με ανακοινώσεις των υπηρεσιών τους στο δίκτυο.

#### *3.2.4.4 Mini Web Server*

Η υπομονάδα mini web server χειρίζεται τις κλασικές HTTP GET αιτήσεις. Πολλά μέρη του UPnP ζητούνται με χρήση αυτής της βασικής υπηρεσίας του πρωτοκόλλου HTTP. Αυτή η υπομονάδα χειρίζεται τις τοποθεσίες των εγγράφων που είναι διαθέσιμες με χρήση της εντολής GET και υλοποιεί τη ροή των δεδομένων χρησιμοποιώντας το πρωτόκολλο HTTP.

Εκτός των άλλων, ο mini web server υλοποιεί την επικεφαλίδα RANGE του πρωτοκόλλου HTTP/1.1. Αυτή η επικεφαλίδα επιτρέπει σε έναν απομακρυσμένο «πελάτη» (client) να ζητήσει ένα συγκεκριμένο κομμάτι (ή κομμάτια) από ένα έγγραφο αντί να ζητήσει ολόκληρο

το έγγραφο. Μια παραδειγματική εφαρμογή αυτής της δυνατότητας είναι η περίπτωση της αναζήτησης ενός συγκριμένου τραγουδιού σε μία λίστα αναπαραγωγής τραγουδιών, ή η αναζήτηση μιας λέξης σε ένα κείμενο μετά από μια ορισμένη σελίδα του εγγράφου κ.α.

Ο mini web server επίσης υποστηρίζει αιτήσεις HTTP POST για εικονικούς καταλόγους αρχείων, αλλά όχι για ο,τιδήποτε άλλο.

#### *3.2.4.5 GENA*

Η υπομονάδα GENA υλοποιεί την General Event Notification Architecture, η οποία προσφέρει τη φάση συγχρονισμού του UPnP. Τα σημεία ελέγχου χρησιμοποιούν αυτήν την υπομονάδα για να εγγραφούν ή να διαγραφούν από υπηρεσίες που τα ενδιαφέρουν. Οι εφαρμογές των υπηρεσιών λαμβάνουν κοινοποιήσεις εγγραφής ή διαγραφής και αναπαράγουν τις κατάλληλες ενέργειες που πρέπει να λάβουν χώρα.

#### *3.2.4.6 SOAP*

Η υπομονάδα SOAP υλοποιεί το Simple Object Access Protocol, το οποίο προσφέρει τη φάση του ελέγχου του UPnP. Τα σημεία ελέγχου χρησιμοποιούν το πρωτόκολλο αυτό για να μπορέσουν να σχηματίσουν τα κατάλληλα προτυποποιημένα έγγραφα XML τα οποία χρησιμοποιούνται για την επικοινωνία μεταξύ των σημείων ελέγχου και των συσκευών, σε όλες τις φάσεις του πρωτοκόλλου (π.χ. για την αλλαγή του πίνακα κατάστασης μιας υπηρεσίας). Ο εξυπηρετητής χρησιμοποιεί τη λειτουργία αυτή προκειμένου να αποκωδικοποιήσει τις εντολές ελέγχου και να αναπαράγει ορθές απαντήσεις.

#### *3.2.4.7 HTTP*

Η υπομονάδα HTTP επεξεργάζεται τις επικεφαλίδες για τα εισερχόμενα μηνύματα και βοηθά στην κατασκευή των κατάλληλων επικεφαλίδων για τα εξερχόμενα μηνύματα. Αντιλαμβάνεται πληθώρα επικεφαλίδων τόσο του πρωτοκόλλου HTTP/1.1 όσο και του HTTP/1.0, για να επιτύχει διαλειτουργικότητα μεταξύ συστημάτων νεότερης και παλαιότερης γενιάς. Επίσης παρέχει δυνατότητα για επεξεργασία για κωδικοποιημένων τεμαχισμένων πακέτων HTTP/1.1, γεγονός ιδιαίτερα χρήσιμο στην περίπτωση μεγάλων πακέτων που υπερβαίνουν την MTU που έχει οριστεί από το διαχειριστή του συστήματος (κυρίως λόγω μεγάλου μεγέθους του XML εγγράφου περιγραφής). Έτσι, ενώ το ίδιο το SDK δεν έχει τη δυνατότητα να παράγει τεμαχισμένα πακέτα, μπορεί εύκολα να τα χειριστεί, αν παρουσιαστεί ανάγκη για κάτι τέτοιο, και να αναπαράγει τις σωστές αποκρίσεις.

#### *3.2.4.8 Mini server*

Το υπόστρωμα του mini server παρέχει κοινή λειτουργικότητα μεταξύ των λειτουργικών μερών του UPnP, όπως είναι για παράδειγμα τα GENA, SOAP, SSDP και ο mini web server. Αυτό το στρώμα δέχεται όλες τις δικτυακές συνδέσεις, καθορίζει ποια αίτηση είναι εισερχόμενη και ποια όχι, μεταβιβάζει στο υπόστρωμα HTTP τις επικεφαλίδες των πακέτων που καταφτάνουν για περαιτέρω επεξεργασία, και εν γένει μεταφέρει τα πακέτα που αφικνούνται στο κατάλληλο υπόστρωμα, όπου θα υποβληθούν στις κατάλληλες μορφές επεξεργασίας, για την ομαλή λειτουργία του πρωτοκόλλου UPnP. Η πρώτη γραμμή της επικεφαλίδας HTTP περιέχει την αίτηση. Το στρώμα του mini server τυπικά χειρίζεται τις παρακάτω εντολές:

- **GET**: Τα σημεία ελέγχου κάνουν χρήση της εντολής GET για να μπορέσουν να λάβουν το έγγραφο περιγραφής και οποιοδήποτε υποστοιχείο αυτού συμπεριλαμβανομένου και του εγγράφου παρουσίασης (βλ. παράγραφο 3.2.2.5), τα έγγραφα περιγραφής των υπηρεσιών, και τις εικόνες που σχετίζονται με τη συσκευή. Χρησιμοποιώντας Εικονικούς Καταλόγους (οι οποίοι περιγράφονται στην παράγραφο 3.2.5) οι εφαρμογές των συσκευών μπορούν να ζητήσουν από το SDK να αναπαράγει αιτήσεις στην εφαρμογή προκειμένου η τελευταία να χειριστεί τις αιτήσεις GET για συγκεκριμένου καταλόγους αρχείων. Στην παράγραφο 3.2.5 υπάρχουν περισσότερες σχετικές λεπτομέρειες.
- **POST/M – POST**: Μια εντολή SOAP είναι σε μορφή M-POST ή POST εντολής. Όλες οι εντολές POST που εκδίδονται για μία από τις διευθύνσεις URL ελέγχου που αναγράφονται στο έγγραφο περιγραφής μεταφέρονται στην υπομονάδα SOAP για περαιτέρω επεξεργασία. Οι εντολές POST επιπλέον, επιτρέπονται στους Εικονικούς Καταλόγους (Virtual Directories), δημιουργώντας κατάλληλες αιτήσεις στην εφαρμογή της συσκευής.
- **SUBSCRIBE**: Οι εντολές SUBSCRIBE μεταφέρονται στην υπομονάδα GENA για επιπλέον επεξεργασία. Τα σημεία ελέγχου χρησιμοποιούν τις αιτήσεις SUBSCRIBE για να εγγραφούν ή να ανανεώσουν την εγγραφή τους στις ειδοποιήσεις γεγονότων μιας συγκεκριμένη υπηρεσίας.
- **UNSUBSCRIBE**: Οι εντολές UNSUBSCRIBE μεταφέρονται στην υπομονάδα GENA επίσης για περαιτέρω επεξεργασία. Τα σημεία ελέγχου χρησιμοποιούν τις αιτήσεις αυτές όταν θέλουν να ειδοποιήσουν έναν εξυπηρετητή ότι δεν ενδιαφέρονται πλέον για τη λήψη ειδοποιήσεων για τις αλλαγές στον πίνακα κατάστασης μιας υπηρεσίας της συσκευής.

- **NOTIFY**: Οι εντολές NOTIFY μεταφέρονται σε άλλα υποστρώματα για περαιτέρω επεξεργασία. Στην περίπτωση συνδέσεων TCP, μεταφέρονται στο στρώμα GENA. Στην περίπτωση UDP συνδέσεων, μεταφέρονται στο στρώμα SSDP. Ο εντολές NOTIFY μπορεί να είναι ειδοποιήσεις γεγονότων σταλμένες από εξυπηρετητές σε σημεία ελέγχου και περιέχουν περιγραφή του γεγονότος, ή ειδοποίηση σχετική με την εμφάνιση / εξαφάνιση κάποιας συσκευής ή υπηρεσίας στο / από δίκτυο.

#### *3.2.4.9 Η βιβλιοθήκη ThreadUtil*

Το *Intel SDK* για UPnP συσκευές χρησιμοποιεί εκτεταμένα threads (νήματα) για να καταστήσει όσο το δυνατόν πιο παράλληλη την επεξεργασία της UPnP κίνησης. Η βιβλιοθήκη ThreadUtil προσφέρει στο SDK μια «αφαίρεση» (abstraction) ενός API νημάτων παρόμοιο με του POSIX, εργαλεία διαχείρισης των νημάτων αυτών, καθώς και ευκολίες που σχετίζονται με χρήση ελευθέρων και διατεταγμένων λιστών. Η εφαρμογή διαχείρισης των νημάτων δημιουργεί ένα σωρό (heap) από νήματα που μπορούν να γίνουν αντικείμενα «δανεισμού» για τη διεκπεραίωση κάποιας εργασίας, τα οποία στη συνέχεια, και μετά την ολοκλήρωση του σκοπού του «δανεισμού», επιστρέφονται και πάλι στο σωρό όπου μπορούν κατόπιν να χρησιμοποιηθούν για άλλους σκοπούς. Διατηρείται επίσης ένας λόγος του αριθμού των εργασιών που έχουν μπει σε ουρά για επεξεργασία, προς το συνολικό αριθμό των νημάτων που βρίσκεται στο σωρό και είναι έτοιμα προς χρήση. Αν αυτός ο λόγος μεγαλώσει πολύ, θα αυξηθεί αυτόματα ο αριθμός των νημάτων στο σωρό αυτόματα. Παρόμοια, αν υπάρχουν νήματα που παραμένουν στο σωρό για πολύ ώρα ανεκμετάλλευτα, τότε θα μειωθεί ο συνολικός αριθμός των νημάτων στο σωρό για να μειώσει την κατασπατάληση πόρων αλλά ταυτόχρονα να εξασφαλίσει τη μέγιστη δυνατή λειτουργικότητα του συστήματος.

#### *3.2.4.10 XML Parser*

Η XML χρησιμοποιείται ευρέως στο πρωτόκολλο UPnP. Τα έγγραφα περιγραφής είναι αρχεία XML. Το GENA χρησιμοποιεί XML έγγραφα για να περιγράψει τις τυχόν αλλαγές στον πίνακα κατάστασης μιας υπηρεσίας. Το SOAP χρησιμοποιεί XML για να μορφοποιήσει τις αιτήσεις και τις απαντήσεις σχεδόν για κάθε φάση λειτουργίας του πρωτοκόλλου. Το SDK διατηρεί έναν XML parser ο οποίος χρησιμοποιείται τόσο από τα πρωτόκολλα πυρήνα του UPnP, αλλά και από τις εφαρμογές του σημείου ελέγχου και της συσκευής.

Η διεπαφή προς τον XML parser χρησιμοποιεί ένα υποσύνολο της σύστασης του World Wide Web Consortium (W3C) σχετικά με το Document Object Model (DOM) επιπέδου 2. Το SDK προσφέρει μία διεπαφή σε γλώσσα C (όπως θα διαπιστωθεί και αργότερα, αυτή είναι

και η γλώσσα που επιλέχθηκε για την ανάπτυξη της εφαρμογς, βλ. Παράγραφο 3.3.1). Οι διεπαφές που υλοποιούνται είναι οι Node, Attr, CDATASection, Document, Element, CharacterData, Text και Comment. Ο αναγνώστης μπορεί να ανατρέξει στη διεύθυνση http://w3c.org/DOM/ για περισσότερες πληροφορίες σχετικά με το DOM.

#### *3.2.4.11 Στρώμα BSD Socket*

Το SDK υποθέτει ότι το στρώμα BSD Socket (POSIX.1g) είναι στη διάθεση του λειτουργικού συστήματος. Παρά το γεγονός ότι δεν αποτελεί μέρος του SDK, συμπεριλαμβάνεται στο Σχήμα 3.2 για να καταδειχθεί η σχέση μεταξύ του SDK και του υποκείμενου λειτουργικού συστήματος.

### 3.2.5 Εικονικοί Κατάλογοι

Ο ενσωματωμένος Mini Web Server στο SDK υποστηρίζει μια δομή που ονομάζεται «Εικονικοί Κατάλογοι». Ένας Εικονικός Κατάλογος είναι ένα μονοπάτι (path) προσβάσιμο σε πελάτες HTTP που δεν συνάδει με τη φυσική δομή σε σχέση με το ριζικό κατάλογο (root directory) της δομής του Mini Web Server. Τυπικά, η διεύθυνση URL που στέλνεται σε έναν εξυπηρετητή web αντιστοιχεί στην πραγματική φυσική δομή των αρχείων που φιλοξενούνται από τον εξυπηρετητή. Ο εξυπηρετητής τότε προσθέτει στο URL που δέχεται από τον πελάτη το δικό του ριζικό κατάλογο και ανοίγει το αρχείο στο δικό του σύστημα αρχείων (filesystem), στέλνοντας μετά την κατάλληλη απάντηση στον πελάτη. Με τη βοήθεια ενός εικονικού καταλόγου, μια εφαρμογή κάποιας συσκευής μπορεί να καταχωρήσει ορισμένους καταλόγους στους οποίους επιθυμεί να δέχεται απαντήσεις ότι εκδίδει κάποια αίτηση. Για παράδειγμα, ας υποτεθεί ότι μια συσκευή έχει μια δομή καταλόγων όπως παρακάτω:

```
<webroot>
        index.html
        device.xml
        service.xml
```

Έστω ότι ένας πελάτης θέλει να λάβει το αρχείο index.html. Σε αυτήν την περίπτωση πρέπει να πραγματοποιήσει μια αίτηση GET της μορφής:

```
GET   /index.html      HTTP/1.0
```

Υποθέτοντας ότι η εφαρμογή έχει καταχωρήσει έναν Εικονικό Κατάλογο που ονομάζεται «docs», ένας πελάτης θα έκανε μια αντίστοιχη αίτηση ως εξής:

```
GET   /docs/current_counterdescr.xml        HTTP/1.0
```

Η εφαρμογή της συσκευής λαμβάνει μια αίτηση από το Mini Web Server ζητώντας από την εφαρμογή της συσκευής να προσφέρει την πληροφορία πίσω στον πελάτη. Η προέλευση και μεταφορά της λαμβανόμενης πληροφορίας δεν αφορά τη λειτουργία του Mini Web Server. Θα μπορούσε να έχει γίνει μέσω απευθείας ροής (streaming) από το διαδίκτυο, να έχει διαβαστεί από ένα κατάλογο που βρίσκεται εκτός του ριζικού καταλόγου του Mini Web Server, ή ακόμα και να είχε παραχθεί δυναμικά.

Το API που χρησιμοποιεί η εφαρμογή μιας συσκευής για να λάβει αυτές τις κλήσεις, είναι παρόμοιο με μια τυπική ιεράρχηση αρχείων που αποτελείται από μια δομή με έξι δείκτες συναρτήσεων:

- `get_info()`: Είναι η πρώτη κλήση για μια αίτηση. Περνά μια δομή στην εφαρμογή με πληροφορίες σχετικές με τη διεύθυνση URL που ζητά ο πελάτης. Η εφαρμογή επιστρέφει πληροφορίες σχετικές με το αρχείο, όπως για παράδειγμα το μέγεθος αυτού, στο Mini Web Server. Η πληροφορία αυτή γίνεται η βάση για την επικεφαλίδα του HTTP μηνύματος απάντησης.
- `open()`: Επιστρέφει ένα σύνδεσμο πίσω στο Mini Web Server για τις επικείμενες εργασίες. Αυτό που στην πραγματικότητα κάνει είναι εντελώς ανεξάρτητο του Mini Web Server. Απλά περνά ως παράμετρο αυτόν το σύνδεσμο σε οποιεσδήποτε κλήσεις που θα γίνουν στη συνέχεια.
- `read()`: Λαμβάνει ένα πακέτο πληροφοριών. Ο Mini Web Server καλεί αυτή τη συνάρτηση επαναληπτικά μέσω HTTP GET αιτήσεων, μέχρις ότου να μη λαμβάνει κάποια πληροφορία.
- `write()`: Καταγράφει ένα πακέτο πληροφοριών. Ο Mini Web Server καλεί αυτήν τη συνάρτηση επαναληπτικά μέσω HTTP POST αιτήσεων προς έναν Εικονικό Κατάλογο.
- `seek()`: Αλλάζει τη θέση ενός αρχείου. Ο Mini Web Server χρησιμοποιεί αυτή τη συνάρτηση κυρίως για να ικανοποιήσει τις αιτήσεις HTTP RANGE που ζητούν συγκεκριμένη θέση στα αρχεία ενδιαφέροντος.
- `close()`: Κλείνει το σύνδεσμο που έχει δημιουργηθεί νωρίτερα με τη συνάρτηση open().

Μια συσκευή καλεί αυτές τις συναρτήσεις έμμεσα μέσω της συνάρτησης UpnpSetVirtualDirCallbacks(). Η συνάρτηση UpnpAddVirtualDir() προσθέτει μια νέα καταχώρηση στη λίστα με τους Εικονικούς Καταλόγους. Στο σημείο αυτό πρέπει να σημειωθεί ότι ο κατάλογος που περνά ως είσοδος στην UpnpAddVirtualDir() γίνεται το πρόθεμα το οποίο ο Mini Web Server χρησιμοποιεί για να καθορίσει εάν πρέπει να επιστρέψει κάποια άλλη κλήση. Η συνάρτηση UpnpRemoveVirtualDir() αφαιρεί τον Εικονικό Κατάλογο τη διεύθυνση του οποίου δέχεται ως όρισμα από τη λίστα των Εικονικών Καταλόγων. Αντίστοιχα, η UpnpRemoveAllVirtualDirs() αφαιρεί όλους τους Εικονικούς Καταλόγους. Για περισσότερες πληροφορίες ο αναγνώστης μπορεί να ανατρέξει στο *Intel® SDK for UPnP™ Devices v1.2 API Reference.*

## 3.3 Η εφαρμογή ελέγχου

### 3.3.1 Εισαγωγικά

Ο σκοπός αυτής της διπλωματικής εργασίας είναι η ανάπτυξη ενός περιβάλλοντος ασφαλούς διαχείρισης των BPL συσκευών ενός δικτύου BPL. Σε πρώτη προσέγγιση του προβλήματος, το ενδιαφέρον εστιάζεται στην καταγραφή απλά της έντασης του ρεύματος που διαρρέει κάθε συσκευή, καθώς και στην κατάστασή της (αν βρίσκεται σε λειτουργία ή όχι). Η απαίτηση για τον έλεγχο των συσκευών είναι να μην υπάρχουν δομές τύπου πελάτη – εξυπηρετητή, αλλά καλύτερα δομές ομότιμων στοιχείων, καθώς ο κίνδυνος μια συσκευή να τεθεί εκτός λειτουργίας είναι σχετικά μεγάλος, και μια κλασική, στατική προσέγγιση θα μπορούσε να δημιουργήσει προβλήματα. Εξ άλλου, η φιλοσοφία τόσο των BPL συστημάτων όσο και των Αυτόνομων δικτύων και των Έξυπνων Δικτύων ενέργειας, είναι περισσότερο κατανεμημένη παρά συγκεντρωτική. Εκτός των άλλων, η συντήρηση του δικτύου, ειδικά σε περιόδους έντονων καιρικών φαινομένων ή έντονης ζήτησης ηλεκτρικής ενέργειας, είναι ιδιαίτερα δύσκολη, και όταν λαμβάνει χώρα απαιτείται η διαρκής απενεργοποίηση και ενεργοποίηση των συσκευών του δικτύου. Η χρήση ενός πρωτοκόλλου που δε θα είχε την ικανότητα να ανιχνεύει εύκολα, γρήγορα, πλήρως και ιεραρχικά τις συσκευές που εισέρχονται ή εξέρχονται του δικτύου, θα ήταν απαγορευτική, καθώς η υποβάθμιση της παρεχόμενης υπηρεσίας θα ήταν κρίσιμη. Η πλήρης εκ νέου μορφοποίηση των σημείων ελέγχου και των συσκευών (σύμφωνα με την ορολογία που αναπτύχθηκε νωρίτερα κατά την περιγραφή του πρωτοκόλλου UPnP) θα ήταν εκτός από εξαιρετικά χρονοβόρα και ιδιαίτερα επικίνδυνη, με σημαντικότατες επιδράσεις και στους καταναλωτές αλλά και στους διαχειριστές των δικτύων ενέργειας. Στο υποθετικό σενάριο όπου μια μεγάλη γεωγραφική

περιοχή βρισκόταν σε μη λειτουργική κατάσταση, τότε μια στατική δόμηση του δικτύου από την πλευρά της διοίκησης και του ελέγχου του, θα άφηνε τους διαχειριστές του συστήματος ανήμπορους να αντιδράσουν, ενώ η χρονική διάρκεια της επιδιόρθωσης θα ήταν τεράστια (συγκριτικά με τα περιθώρια ποιότητας που έχουν τεθεί ήδη από τις κατά τόπους επιτροπές Δικτύων Ενέργειας). Το πρωτόκολλο UPnP καταφέρνει να συγκεντρώσει όλα τα θετικά προαπαιτούμενα για την ομαλή διαχείριση του δικτύου, χωρίς να παρουσιάζει κάποια ανεπιθύμητα χαρακτηριστικά.

Το πρωτόκολλο UPnP είναι ένα πρωτόκολλο εξαιρετικά διαδεδομένο, με χρήση σε διάφορα συστήματα και εφαρμογές. Είναι λοιπόν φυσιολογικό να υπάρχουν γι αυτό διαφορετικές υλοποιήσεις, σε πολλά λειτουργικά συστήματα. Προφανώς κάθε υλοποίηση πρέπει να είναι λειτουργική, και σύμφωνη με τις προδιαγραφές που αναφέρθηκαν στις προηγούμενες παραγράφους αυτού του κεφαλαίου. Το λειτουργικό σύστημα που θα φιλοξενεί τις εφαρμογές των συσκευών και των σημείων ελέγχου πρέπει να χαρακτηρίζεται από τη μέγιστη δυνατή σταθερότητα, ενώ πρέπει για λόγους οικονομικούς να έχει κατά το δυνατόν το μικρότερο κόστος. Επίσης πρέπει να είναι ικανό να λειτουργήσει σε πληθώρα επεξεργαστικών μονάδων και αρχιτεκτονικών, με υποτυπώδες hardware και μικρή (ίσως τύπου flash μνήμη). Λαμβάνοντας υπόψη όλα τα προηγούμενα, επιλέχθηκε ως καταλληλότερο λειτουργικό σύστημα το Linux, ένα διαδεδομένο λειτουργικό σύστημα βασισμένο (και πολύ κοντά) στο UNIX, το οποίο είναι γνωστό για τη σταθερότητά και την ασφάλειά του. Παρέχεται δωρεάν, είναι αποκρίσιμο, μοντέρνο και με μικρές απαιτήσεις μνήμης, ενώ παράλληλα υποστηρίζει πληθώρα αρχιτεκτονικών.

Αναλογικά με τη γλώσσα προγραμματισμού του συστήματος, αποφασίστηκε να είναι η C, η οποία υποστηρίζεται πλήρως από το λειτουργικό σύστημα που επιλέχθηκε (εξάλλου τόσο το UNIX όσο και το Linux είναι γραμμένα σε C), έχει επίσης μικρές απαιτήσεις μνήμης, ενώ ταυτόχρονα, υπάρχουν έτοιμες υλοποιήσεις του πρωτοκόλλου UPnP στη γλώσσα αυτή.

Στις επόμενες παραγράφους του κεφαλαίου, θα παρουσιασθεί ο τρόπος με τον οποίο σχεδιάστηκαν οι εφαρμογές των συσκευών (που ελέγχονται) και των σημείων ελέγχου, με τη βοήθεια παραδειγματικών τμημάτων κώδικα.

### 3.3.2 Η εφαρμογή της UPnP συσκευής

Υπάρχουν πολλοί τρόποι για να υλοποιηθεί μια UPnP συσκευή χρησιμοποιώντας το SDK για τις UPnP συσκευές. Παρόλα αυτά, κάθε υλοποίηση απαιτεί ορισμένα βασικά βήματα για να μπορέσει να είναι λειτουργική και αποτελεσματική. Συγκεκριμένα, η εφαρμογή πρέπει:

1. Να διαμορφώσει και να αρχικοποιήσει τη συσκευή με τα ακόλουθα βήματα:
    a. Να αρχικοποιήσει το SDK με τη βοήθεια της συνάρτησης UpnpInit().
    b. Να καθορίσει έναν Εικονικό Κατάλογο για το Mini Web Server με την κλήση της συνάρτησης UpnpSetWebServerRootDir().
    c. Να αρχικοποιήσει το έγγραφο περιγραφής της συσκευής χρησιμοποιώντας τη UpnpRegisterRootDevice() ή την UpnpRegisterRootDevice2().
    d. Να πραγματοποιήσει οποιαδήποτε αρχικοποίηση που απαιτεί αυτή καθ' εαυτή η συσκευή.
    e. Να «διαφημίσει» τη συσκευή στο δίκτυο με τη χρήση της εντολής UpnpSendAdvertisement().
2. Να χειριστεί οποιεσδήποτε ασύγχρονες αιτήσεις. Η συσκευή πρέπει είναι σε θέση να χειριστεί τρεις, διαφορετικού τύπου αιτήσεις:
    a. Αιτήσεις για εγγραφές σε υπηρεσίες ειδοποιήσεων για αλλαγές στους πίνακες κατάστασης υπηρεσιών.
    b. Αιτήσεις για απόδοση της τρέχουσας τιμής κάποιας παραμέτρου μιας υπηρεσίας που παρέχεται από τη συσκευή.
    c. Αιτήσεις για αλλαγή της τρέχουσας τιμής κάποιας παραμέτρου μιας υπηρεσίας που παρέχει η συσκευή.
3. Να κρατήσει ενήμερα τα σημεία ελέγχου χρησιμοποιώντας τις εντολές UpnpNotify() ή UpnpNotifyExt(), όταν πραγματοποιείται κάποια αλλαγή στις μεταβλητές κατάστασής των υπηρεσιών της.
4. Να θέσει εκτός λειτουργίας (shutdown) τη συσκευή με χρήση των παρακάτω διαδικασιών:
    a. Να αποστείλει μηνύματα SSDP τύπου «bye bye» στα σημεία ελέγχου και να διαγράψει τη συσκευή από το SDK χρησιμοποιώντας την εντολή UpnpUnregisterRootDevice().
    b. Να σταματήσει τη λειτουργία του SDK χρησιμοποιώντας την UpnpFinish().

Στις παραγράφους που ακολουθούν, θα παρουσιασθεί η εφαρμογή που σχεδιάστηκε. Ορισμένα σημεία του κώδικα, που έχουν μικρότερη σημασία στην κατανόηση, έχουν αφαιρεθεί από την παρουσίαση αυτή, για λόγους απλότητας.

#### *3.3.2.1 Διαμόρφωση και αρχικοποίηση*

##### 3.3.2.1.1 Η αρχικοποίηση του SDK

Προτού ξεκινήσει η λειτουργία μιας συσκευής, είναι πολύ σημαντικό να καταγραφούν ή να αποκτηθούν τα έγγραφα περιγραφής της συσκευής και των υπηρεσιών τις οποίες αυτή παρέχει και που θα χρησιμοποιηθούν. Αυτές καθορίζουν τον τύπο και τον αριθμό των υπηρεσιών που υποστηρίζει η συσκευή, όπως επίσης και τις ενέργειες, παραμέτρους και μεταβλητές που η κάθε υπηρεσία υποστηρίζει.

Κατ αρχήν, η εφαρμογή πρέπει να αρχικοποιήσει το SDK προκειμένου να μπορέσει στη συνέχεια να χρησιμοποιήσει τα API που προσφέρονται. Αυτό γίνεται μέσω του παρακάτω block εντολών:

```
if( ( ret = UpnpInit( ip_address, port ) ) != UPNP_E_SUCCESS ) {
      SampleUtil_Print( "Error with UpnpInit -- %d\n", ret );
      UpnpFinish(  );
      return ret;
   }
```

Η εφαρμογή μπορεί να ορίσει μόνη της τη διεύθυνση IP και τη θύρα κατά τη διάρκεια της αρχικοποίησης. Αυτές χρησιμοποιούνται για να οριστεί η διεύθυνση και ο αριθμός θύρας στις οποίες ακούει ο εξυπηρετητής για αιτήσεις UPnP και HTTP. Αν η διεύθυνση IP είναι NULL, τότε χρησιμοποιείται η πρώτη μη NULL, μη loopback IP που ορίζεται στη συσκευή. Αν ο αριθμός θύρας είναι 0, τότε ως θύρα τίθεται ένας τυχαίος αριθμός[8]. Η εφαρμογή μπορεί στη συνέχεια να λάβει τη διεύθυνση IP και τη θύρα αρχικοποίησης του SDK μέσω των εντολών UpnpGetServerIpAddress() και UpnpGetServerPort() αντίστοιχα.

[8]Στην παρούσα υλοποίησή μας, η εφαρμογή ακούει σε όλες τις διεπαφές. Αυτό σημαίνει ότι η διεύθυνση IP και ο αριθμός θύρας που ορίζονται στην αρχικοποίηση, θα επηρεάσουν μόνο τη διεύθυνση IP που θα αποσταλεί ως διαφήμιση κατά τη διάρκεια των SSDP διαφημίσεων και απαντήσεων ερωτημάτων.

#### 3.3.2.1.2 Ορισμός ριζικού καταλόγου

Αμέσως μετά την αρχικοποίηση του SDK, η εφαρμογή της συσκευής μπορεί να προσδιορίσει το ριζικό κατάλογο του εξυπηρετητή web. Αυτός είναι ο τοπικός κατάλογος τον οποίο ο εξυπηρετητής web ψάχνει προκειμένου να προσφέρει αρχεία ως απάντηση σε αιτήσεις HTTP. Ο προσδιορισμός του ριζικού καταλόγου είναι προαιρετικός. Σε περίπτωση που δεν οριστεί, τότε προσφέρονται μόνο αιτήσεις για αντικείμενα που βρίσκονται στον εικονικό κατάλογο μέσω των εγγεγραμμένων κλήσεων. Αφήνεται στην εφαρμογή να διασφαλίσει ότι ο συγκεκριμένος κατάλογος περιέχει τα κατάλληλα αρχεία (όπως για παράδειγμα τα έγγραφα περιγραφής για τη συσκευή και τις υπηρεσίες αυτής). Ο κώδικας που ακολουθεί, παρουσιάζει εν τάχει αυτά που αναφέρθηκαν στην παράγραφο αυτή:

```
if( ip_address == NULL ) {
      ip_address = UpnpGetServerIpAddress(  );
}
if( port == 0 ) {
      port = UpnpGetServerPort(  );
}
if( desc_doc_name == NULL )
   desc_doc_name = "CURRENT_COUNTERdevicedesc.xml";
if( web_dir_path == NULL )
   web_dir_path = DEFAULT_WEB_DIR;
if((ret=UpnpSetWebServerRootDir(web_dir_path)) != UPNP_E_SUCCESS) {
   UpnpFinish(  );
   return ret;
}
```

Παρατηρείται ότι η εφαρμογή είναι αυτή που ελέγχει την ύπαρξη των απαραίτητων εγγράφων περιγραφής, όπως και τη διεύθυνση IP και τον αριθμό θύρας του εξυπηρετητή web.

Επίσης, πρέπει να τονισθεί ότι αφού η UpnpInit() έχει επιτύχει, είναι πολύ σημαντικό να κληθεί η UpnpFinish() εάν η συσκευή πρέπει να τεθεί εκτός λειτουργίας για κάποιο λόγο. Αυτό δίνει την ευκαιρία στο SDK να αποδεσμεύσει τους πόρους που είχε εξ αρχής δεσμεύσει.

#### 3.3.2.1.3 Εγγραφή ριζικής συσκευής

Το επόμενο βήμα στο «στήσιμο» της συσκευής, είναι η εγγραφή με το SDK. Υπάρχουν δύο διαφορετικές συναρτήσεις για την εγγραφή αυτή της συσκευής, η UpnpRegisterRootDevice() και η UpnpRegisterRootDevice2(). Η πρώτη συνάρτηση λαμβάνει μια πλήρη διεύθυνση URL περιγραφής για είσοδο και η δεύτερη μπορεί να λάβει ένα έγγραφο παρουσίασης σε πληθώρα μορφών. Το παρακάτω παράδειγμά μας υλοποιεί την πρώτη από τις δύο περιπτώσεις:

```
if( ( ret = UpnpRegisterRootDevice( desc_doc_url,
                                    CURRENT_COUNTERDeviceCallbackEventHandler,
                                    &device_handle, &device_handle ) )
                                    != UPNP_E_SUCCESS )
{
    SampleUtil_Print( "Error registering the rootdevice : %d\n", ret );
    UpnpFinish(  );
    return ret;
  }
```

Η πρώτη παράμετρος της συνάρτησης είναι η διεύθυνση URL του εγγράφου περιγραφής και πρέπει να δείχνει προς ένα έγκυρο έγγραφο περιγραφής της συσκευής. Αν το έγγραφο περιγραφής είναι ένα αρχείο που προσφέρεται από τον εξυπηρετητή web, πρέπει να βρίσκεται σε κάποιον κατάλογο εκτός αυτού που ορίστηκε νωρίτερα μέσω της κλήσης της συνάρτησης UpnpSetWebServerRootDir(). Η δεύτερη παράμετρος καταχωρεί μια κλήση στο SDK. Το πρωτότυπο αυτής της κλήσης της γενικευμένης αυτής συνάρτησης είναι:

```
int CallbackFxn ( Upnp_EventType EventType, void * Event, void * Cookie ) ;
```

Όποτε μια αίτηση λαμβάνεται για τη συσκευή από το δίκτυο, όπως για παράδειγμα μια εντολή εγγραφής (subscription), μια παράμετρος εντολής get, ή μια αίτηση για κάποια ενέργεια, αυτή η εντολή καλείται σε ένα ανεξάρτητο νήμα με τις αντίστοιχες κατάλληλες παραμέτρους. Η παράμετρος EventType καθορίζει τον τύπο της αίτησης που λήφθηκε, ενώ η παράμετρος Event είναι μια δομή της οποίας ο πραγματικός τύπος διαφέρει, βασισμένος στο EventType. Τέλος η παράμετρος Cookie είναι μια δομή που περιέχει πληροφορία σχετική με την εκάστοτε εφαρμογή, και εξαρτάται από την επιστροφή της κλήσης της συνάρτησης UpnpRegisterRootDevice(). Για τη δική μας εφαρμογή, η καταχωρημένη κλήση είναι η παρακάτω:

```
int CURRENT_COUNTERDeviceCallbackEventHandler( Upnp_EventType EventType, void *Event, void *Cookie )
```

Επιστρέφοντας στην κλήση της συνάρτησης UpnpRegisterRootDevice(), η τρίτη παράμετρος αυτής είναι ένας κατάλληλα ορισμένος από το χρήστη δείκτης. Το μέγεθος του δείκτη μπορεί να είναι οτιδήποτε και μπορεί να χρησιμοποιηθεί για εργασίες σχετικές με την εφαρμογή. Επίσης μπορεί να είναι και κενός (NULL). Η εφαρμογή είναι υπεύθυνη για τη δέσμευση της μνήμης που απαιτείται κάθε φορά καθώς επίσης και για την αποδέσμευση αυτής (φυσικά σε περίπτωση χρήσης του δείκτη). Η τελευταία παράμετρος της UpnpRegisterRootDevice() είναι ένας δείκτης στο χώρο που έχει δεσμεύσει η εφαρμογή για την αποθήκευση του δείκτη αυτού, ο οποίος χρησιμοποιείται σαν παράμετρος και σε διάφορες άλλες συναρτήσεις του API.

#### 3.3.2.1.4 Αρχικοποίηση συσκευής

Προτού η συσκευή ανακοινώσει την παρουσία της στο δίκτυο, πρέπει να λάβουν χώρα όλες οι απαραίτητες αρχικοποιήσεις της συσκευής και των υπηρεσιών αυτής. Μόλις η συσκευή ανακοινωθεί, μπορεί να αρχίσει αμέσως να λαμβάνει αιτήσεις. Η συσκευή είναι υπεύθυνη για τη διατήρηση των τιμών των μεταβλητών του πίνακα κατάστασης των υπηρεσιών που φιλοξενεί, όπως επίσης και για την ορθή διαχείριση των τελευταίων στις περιπτώσεις που υπάρχει απάντηση (ενέργεια) στις εισερχόμενες αιτήσεις. Στον κώδικά που υλοποιεί ένα μετρητή ρεύματος, η συνάρτηση CURRENT_COUNTERDeviceStateTableInit( IN char *DescDocURL ) πραγματοποιεί αυτήν την αρχικοποίηση, καθώς μεταφορτώνει το έγγραφο περιγραφής της συσκευής, και αρχικοποιεί τον πίνακα μεταβλητών κατάστασης των υπηρεσιών της συσκευής.

#### 3.3.2.1.5 Διαφήμιση της συσκευής

Το τελικό βήμα στο αρχικό στήσιμο της συσκευής είναι η ανακοίνωσή της στο δίκτυο, καθώς όπως έχει ήδη προαναφερθεί μετά από το βήμα αυτό η συσκευή μπορεί να αρχίσει να λαμβάνει αιτήσεις και να τις ικανοποιεί– είναι δηλαδή πλήρως λειτουργική. Στον κώδικα, αυτό γίνεται εύκολα μέσω του block εντολών:

```
if( ( ret = UpnpSendAdvertisement( device_handle, default_advr_expire ) )
        != UPNP_E_SUCCESS ) {
                SampleUtil_Print( "Error sending advertisements : %d\n", ret );
                UpnpFinish(  );
                return ret;
    }
```

Η πρώτη παράμετρος της βασικής συνάρτησης UpnpSendAdvertisement είναι ο δείκτης που επεστράφη κατά τη διάρκεια της εγγραφής που παρουσιάστηκε στην παράγραφο 3.3.2.1.3. Η δεύτερη παράμετρος καθορίζει το χρόνο λήξης της διαφήμισης. Όσο η συσκευή είναι σε λειτουργία, μπορεί να ανακοινώνει τον εαυτό της πριν λήξει το προκαθορισμένο αυτό διάστημα, προκειμένου να είναι ορατή ως λειτουργική στις υπόλοιπες συσκευές του συστήματος (και φυσικά στα σημεία ελέγχου).

Μετά το πέρας και αυτού του βήματος, η συσκευή πρέπει να θέσει τον εαυτό της σε ένα διαρκή βρόχο, ή να περιμένει σε κάθε περίπτωση μια εντολή ή την επαλήθευση μιας συνθήκης προκειμένου να τεθεί εκτός λειτουργίας.

#### *3.3.2.2 Διαχείριση αιτήσεων*

Κατά τη διάρκεια λειτουργίας της συσκευής, ο κύριος σκοπός της είναι να διαχειρίζεται τις αιτήσεις που δέχεται από τα διάφορα σημεία ελέγχου. Όταν λαμβάνονται από το SDK αιτήσεις, προωθούνται στην εφαρμογή μέσω της κατάλληλης κλήσης συναρτήσεων που καθορίζονται όταν εγγράφεται η συσκευή (βλ. παράγραφο 3.3.2.1.3). Η κλήση γίνεται μέσω ενός ανεξάρτητου νήματος με τις κατάλληλες παραμέτρους, ανάλογα με τον τύπο της κλήσης. Υπάρχουν τρεις (3) βασικοί τύποι αιτήσεων:

- Αιτήσεις εγγραφής (subscription requests)
- Αιτήσεις λήψης παραμέτρων (get variable requests)
- Αιτήσεις ενεργειών

Σε αυτό το σημείο αξίζει να σημειωθεί ότι η συσκευή δε χρειάζεται να χειρίζεται καμία αίτηση ανακάλυψης (discovery request). Από το στιγμή που το SDK αποκτήσει το έγγραφο περιγραφής για τη συσκευή (έχει δοθεί μέσω της κλήσης της UpnpRegisterRootDevice()), μπορεί αυτόματα να αποφασίσει αν τα κριτήρια αναζήτησης ταιριάζουν με τη συσκευή. Αν κάτι τέτοιο ισχύει, τότε απαντά με τη διεύθυνση URL του εγγράφου περιγραφής της συσκευής. Ο τύπος της αίτησης προσδιορίζεται στην κλήση μέσω της μεταβλητής εισόδου

EventType στην οποία έγινε και νωρίτερα αναφορά. Η κλήση για τη συσκευή που υλοποιήθηκε χρησιμοποιεί μια απλή δομή επιλογής όπως παρακάτω[9]:

```
switch ( EventType ) {
     case UPNP_EVENT_SUBSCRIPTION_REQUEST:
      CURRENT_COUNTERDeviceHandleSubscriptionRequest( ( struct Upnp_Subscription_Request * ) Event );
        break;
      case UPNP_CONTROL_GET_VAR_REQUEST:
        CURRENT_COUNTERDeviceHandleGetVarRequest( ( struct Upnp_State_Var_Request * ) Event );
        break;
      case UPNP_CONTROL_ACTION_REQUEST:
        CURRENT_COUNTERDeviceHandleActionRequest( ( struct Upnp_Action_Request * ) Event );
        break;
}
```

#### 3.3.2.2.1 Αιτήσεις εγγραφής

Όταν ένα σημείο ελέγχου εκπέμπει μια αίτηση εγγραφής, το SDK καλεί την αντίστοιχη εγγεγραμμένη συνάρτηση με τη μεταβλητή EventType να έχει τύπο UPnP_EVENT_SUBSCRIPTION_REQUEST. Η συσκευή είναι υπεύθυνη για την αποδοχή της εγγραφής (συνδρομής) καλώντας είτε την UpnpAcceptSubscription() ή την UpnpAcceptSubscriptionExt(), στέλνοντας παράλληλα τον τρέχον πίνακα κατάστασης στο σημείο ελέγχου. Η διαφορά μεταξύ των δύο συναρτήσεων είναι ο τρόπος με τον οποίο η εφαρμογή περνά τον πίνακα κατάστασης στο SDK για αποστολή στο κατάλληλο σημείο ελέγχου. Η UpnpAcceptSubscription() δέχεται μερικούς πίνακες συμβολοσειρών για τα ζεύγη μεταβλητών/τιμής. Η UpnpAcceptSubscriptionExt() δέχεται ένα έγγραφο τύπου DOM για τις τρέχουσες τιμές των μεταβλητών. Η δόμηση του εγγράφου DOM δίνεται στην παράγραφο 4.3 του εγγράφου *Universal Plug and Play Device Architecture*. Στην εφαρμογή μας κάναμε χρήση της UpnpAcceptSubscription(), όπως παρακάτω:

```
int CURRENT_COUNTERDeviceHandleSubscriptionRequest( IN struct Upnp_Subscription_Request *sr_event )
{
   unsigned int i = 0;
   ithread_mutex_lock( &CURRENT_COUNTERDevMutex );
   for( i = 0; i < CURRENT_COUNTER_SERVCOUNT; i++ ) {
      if( ( strcmp( sr_event->UDN, CURRENT_COUNTER_service_table[i].UDN ) == 0 ) &&
         ( strcmp( sr_event->ServiceId, CURRENT_COUNTER_service_table[i].ServiceId ) == 0 ) ) {
         UpnpAcceptSubscription( device_handle, sr_event->UDN,  sr_event->ServiceId,
                                 ( const char ** )CURRENT_COUNTER_service_table[i].VariableName,
                                 ( const char ** )CURRENT_COUNTER_service_table[i].VariableStrVal,
                                 CURRENT_COUNTER_service_table[i].VariableCount,
                                 sr_event->Sid );
```

[9] Όπως και τις προηγούμενες φορές έτσι και τώρα έχουν αφαιρεθεί κομμάτια κώδικα και παρουσιάζονται μόνο αυτά που συμβάλλουν στην κατανόηση της λειτουργίας του μηχανισμού του πρωτοκόλλου και της εφαρμογής.

```
      }
    }
    ithread_mutex_unlock( &CURRENT_COUNTERDevMutex );
    return ( 1 );
}
```

Σε αυτήν την περίπτωση, η παράμετρος Event που περνά στη συνάρτηση είναι ένας δείκτης σε μια δομή τύπου struct Upnp_Subscription_Request. Η δομή της αίτησης εγγραφής καθορίζει το UDN και το ServiceID της συσκευής για την οποία η εγγραφή ζητείται, ενώ ορίζεται επίσης και ένα μοναδικό αναγνωριστικό εγγραφής SID για τη μετέπειτα ταυτοποίηση της συσκευής. Στο παραπάνω block κώδικα που παρουσιάστηκε, μόλις η συσκευή αναγνωριστεί και ταυτοποιηθεί, οι μεταβλητές κατάστασης, που έχουν ήδη αποθηκευτεί στον πίνακα CURRENT_COUNTER_service_table[i], στέλνονται στο σημείο ελέγχου με τη χρήση της UpnpAcceptSubscription(). Η τελευταία, δέχεται ως είσοδο τα εξής:

- Το δείκτη που «δείχνει» τη συσκευή
- Το UDN της συσκευής
- Το ServiceID της συσκευής
- Τα ονόματα των μεταβλητών (CURRENT_COUNTER_service_table[i].VariableName)
- Τις τιμές των μεταβλητών (CURRENT_COUNTER_service_table[i].VariableStrVal)
- Το SID της συσκευής

Μόλις η εγγραφή γίνει αποδεκτή, το σημείο ελέγχου λαμβάνει ανακοινώσεις για τις αλλαγές κατάστασης που λαμβάνουν χώρα στη συσκευή. Προκειμένου να αποφευχθούν ταυτόχρονες αλλαγές κατάστασης από διαφορετικά σημεία ελέγχου ή άλλες τέτοιες δυσάρεστες παρενέργειες απόρροια του δικτυακού χαρακτήρα της εφαρμογής, γίνεται χρήση μιας μεταβλητής αμοιβαίου αποκλεισμού CURRENT_COUNTERDevMutex. Με αυτόν τον τρόπο, προστατεύεται η ακεραιότητα των δεδομένων της συσκευής. Οι κλήσεις του SDK είναι ούτως ή άλλως πολυνηματικές και αφήνεται στη συσκευή η ορθή χρήση και πρόσβαση των δεδομένων (μεταβλητών) της συσκευής από άλλα σημεία ελέγχου.

#### 3.3.2.2.2 Αιτήσεις λήψης παραμέτρων

Όταν ένα σημείο ελέγχου επιθυμεί να λάβει την κατάσταση μιας μεταβλητής, το SDK καλεί την αντίστοιχη καταχωρημένη συνάρτηση με τη μεταβλητή EventType να έχει τεθεί στην τιμή UPNP_CONTROL_GET_VAR_REQUEST.

Σε αυτό το σημείο αξίζει να σημειωθεί ότι το UPnP Forum έχει αποδοκιμάσει αυτή τη δυνατότητα. Έτσι, ο προτιμότερος πλέον τρόπος για τη λήψη της κατάστασης μιας μεταβλητής από ένα σημείο ελέγχου είναι να έχει έναν ειδικευμένο τρόπο να λάβει τη μεταβλητή. Το να έχει μια συσκευή αυτή τη δυνατότητα φυσικά δεν είναι απαραίτητο, απλά ενδείκνυται για λόγους αξιοπιστίας, και σύμπνοιας με της οδηγίες του UPnP Forum, που είναι άλλωστε και αρμόδιος οργανισμός για τη διαχείριση και συντήρηση του πρωτοκόλλου. Παρακάτω παρουσιάζεται συνοπτικά ο τρόπος αξιοποίησης αυτής της δυνατότητας πάνω από το SDK του UPnP πρωτοκόλλου για να καταστεί δυνατή η επικοινωνία μεταξύ συσκευής και σημείου ελέγχου σε επίπεδο λήψης παραμέτρων:

```
int CURRENT_COUNTERDeviceHandleGetVarRequest( INOUT struct Upnp_State_Var_Request *cgv_event )
{
   ithread_mutex_lock( &CURRENT_COUNTERDevMutex );
   for( i = 0; i < CURRENT_COUNTER_SERVCOUNT; i++ ) {
      if( ( strcmp( cgv_event->DevUDN, CURRENT_COUNTER_service_table[i].UDN ) == 0 ) &&
         ( strcmp( cgv_event->ServiceID, CURRENT_COUNTER_service_table[i].ServiceId ) == 0 ) ) {
         for( j = 0; j < CURRENT_COUNTER_service_table[i].VariableCount; j++ ) {
            if( strcmp( cgv_event->StateVarName,CURRENT_COUNTER_service_table[i].VariableName[j] ) == 0 ) {
               getVar_succeeded = 1;
               cgv_event->CurrentVal=ixmlCloneDOMString(CURRENT_COUNTER_service_table[i].VariableStrVal[j]);
               break;
            }
         }
      }
   }
   ithread_mutex_unlock( &CURRENT_COUNTERDevMutex );
   return ( cgv_event->ErrCode == UPNP_E_SUCCESS );
}
```

Η μεταβλητή CurrentVal της δομής cgv_event (που είναι τύπου Upnp_State_Var_Request) πρέπει να έχει πάρει ως τιμή μια συμβολοσειρά δημιουργημένη από τη συνάρτηση, της βιβλιοθήκης ixml, ixmlCloneDomString(). Η μνήμη που χρησιμοποιεί αυτή η μεταβλητή απελευθερώνεται από το SDK μόλις η τιμή σταλθεί στο σημείο ελέγχου, ενώ και πάλι έχει γίνει χρήση της μεταβλητής αμοιβαίου αποκλεισμού για να διασφαλισθεί η ακεραιότητα της πληροφορίας της συσκευής (σε ότι έχει φυσικά να κάνει με την ταυτόχρονη προσπέλαση των δεδομένων από πολλαπλά σημεία ελέγχου).

#### 3.3.2.2.3 Αιτήσεις ενεργειών

Όταν ένα σημείο ελέγχου αποστέλλει μια αίτηση για την πραγματοποίηση κάποιας ενέργειας στη συσκευή, το SDK καλεί την αντίστοιχη συνάρτηση με τον τύπο της μεταβλητής EventType να είναι UPNP_CONTROL_ACTION_REQUEST.

Η παράμετρος Event που περνά στη συνάρτηση είναι ένας δείκτης σε μια δομή τύπου struct Upnp_Action_Request. Η δομή αίτησης καθορίζει το UDN, το ServiceID, το όνομα της ενέργειας που πρέπει να διενεργηθεί, καθώς επίσης και το έγγραφο αίτησης δράσης το οποίο είναι φυσικά σε μορφή XML εγγράφου. Η συσκευή είναι υπεύθυνη για την εύρεση του εγγράφου και την προσπέλασή του, την ανεύρεση των σχετικών παραμέτρων και τέλος για την εκτέλεση της ενέργειας που απαιτεί το σημείο ελέγχου. Επίσης πρέπει να λάβει μέριμνα για τη δημιουργία του εγγράφου απάντησης και την αποστολή τόσο αυτού όσο και των γενικότερων ανακοινώσεων αλλαγής κατάστασης στις υπόλοιπες συσκευές που έχουν εγγραφεί στην αντίστοιχη υπηρεσία ενημέρωσης της συσκευής. Στον κώδικά, ο χειρισμός της αιτήσεως αλλαγής κατάστασης γίνεται μέσω της κλήσης της συνάρτησης CURRENT_COUNTERHandleActionRequest(). Αυτή η συνάρτηση με τη σειρά της εξετάζει την εισερχόμενη αίτηση, ελέγχοντας το όνομα της ενέργειας που πρέπει να ληφθεί, από έναν κατάλληλο πίνακα, και χρησιμοποιεί την κατάλληλη συνάρτηση για το σκοπό αυτό. Για κάθε ενέργεια UPnP αντιστοιχεί μία αντίστοιχη συνάρτηση. Το πρωτότυπο της συνάρτησης σε αυτήν την περίπτωση είναι:

```
int upnp_action( IN Document *in, OUT Document **out,OUT char **errorString )
```

Η συνάρτηση αυτή δέχεται ένα όρισμα εισόδου ενώ παρέχει και δύο ορίσματα εξόδου. Η είσοδος που δέχεται είναι το έγγραφο XML που περιέχει τις παραμέτρους για την ενέργεια και είναι σαφώς απαραίτητη για τη δημιουργία του εγγράφου απάντησης που αποτελεί και τη μία εκ των εξόδων. Η άλλη έξοδος που παρέχει η συνάρτηση αφορά μια συμβολοσειρά που καταδεικνύει αν η απαιτούμενη ενέργεια ολοκληρώθηκε με επιτυχία ή όχι. Η εφαρμογή αρχικά αναγνωρίζει ποια υπηρεσία αφορά η ενέργεια που πρέπει να πραγματοποιηθεί. Έχοντας αυτό υπόψη, βρίσκει την αντίστοιχη ενέργεια και ενημερώνει κατάλληλα τη συνάρτηση διαχείρισης για περαιτέρω επεξεργασία. Παραδειγματικά, παρατίθεται παρακάτω πώς υλοποιείται η ενέργεια αλλαγής της τρέχουσας τιμής του ρεύματος:

```
int CURRENT_COUNTERDeviceSetCurrent( IN IXML_Document * in, OUT IXML_Document ** out,
                                     OUT char **errorString )
{

   char *value = NULL;

   int current = 0;

   ( *out ) = NULL;
   ( *errorString ) = NULL;

   if( !( value = SampleUtil_GetFirstDocumentItem( in, "Current" ) ) ) {
      ( *errorString ) = "Invalid Current";
      return UPNP_E_INVALID_PARAM;
   }

   current = atoi( value );

   if( current < MIN_CURRENT || current > MAX_CURRENT ) {

      free( value );
      SampleUtil_Print( "error: can't change to current %d\n", current );
      ( *errorString ) = "Invalid Current";
      return UPNP_E_INVALID_PARAM;
   }

   if( CURRENT_COUNTERDeviceSetServiceTableVar( CURRENT_COUNTER_CONTROL,
                                                CURRENT_COUNTER_CURRENT, value ) ) {
      if( UpnpAddToActionResponse( out, "SetCurrent",
                                   CURRENT_COUNTERServiceType[CURRENT_COUNTER_CONTROL],
                                   "NewCurrent", value )
                                   != UPNP_E_SUCCESS ) {
         ( *out ) = NULL;
         ( *errorString ) = "Internal Error";
         free( value );
         return UPNP_E_INTERNAL_ERROR;
      }
      free( value );
      return UPNP_E_SUCCESS;
   } else {
      free( value );
      ( *errorString ) = "Internal Error";
      return UPNP_E_INTERNAL_ERROR;
   }
}
```

Η συνάρτηση κάνει χρήση της UpnpAddToActionResponse() η οποία είναι υπεύθυνη για το χτίσιμο της απόκρισης της συσκευής.

#### *3.3.2.3 Αποστολή Γεγονότων*

Κάθε φορά που μια μεταβλητή κατάστασης μεταβάλλεται, η συσκευή είναι υποχρεωμένη (αν της έχει ζητηθεί φυσικά νωρίτερα, στη διάρκεια της εγγραφής των σημείων ελέγχου) να

αποστείλει μια ανακοίνωση γεγονότος ανακοινώνοντας ότι άλλαξε ο πίνακας κατάστασης μεταβλητών της (eventing). Φυσικά μια τέτοια αλλαγή μπορεί να προέκυψε ως απάντηση σε μια αίτηση ενέργειας, ένα εξωτερικό γεγονός κτλ. Η εφαρμογή της συσκευής είναι υπεύθυνη για τον καθορισμό πότε πρέπει να σταλεί μια τέτοια ειδοποίηση. Το SDK στέλνει το γεγονός (event) σε όλα τα εγγεγραμμένα σημεία ελέγχου. Συγκεκριμένα, στέλνονται γεγονότα ως απάντηση σε αιτήσεις ενεργειών προκειμένου να ενημερωθούν όλα τα εγγεγραμμένα σημεία ελέγχου για την αλλαγή της κατάστασης του ρεύματος ή της λειτουργικής κατάστασης της συσκευής. Η διαχείριση της αποστολής γεγονότων γίνεται από την CURRENT_COUNTERDeviceSetServiceTableVar(), η δομή της οποίας φαίνεται παρακάτω:

```
Int CURRENT_COUNTERDeviceSetServiceTableVar( IN unsigned int service,
                                             IN unsigned int variable,
                                             IN char *value )
{
   if( ( service >= CURRENT_COUNTER_SERVCOUNT ) ||
       ( variable >= CURRENT_COUNTER_service_table[service].VariableCount ) ||
       ( strlen( value ) >= CURRENT_COUNTER_MAX_VAL_LEN ) ) {
      return ( 0 );
   }

   ithread_mutex_lock( &CURRENT_COUNTERDevMutex );

   strcpy( CURRENT_COUNTER_service_table[service].VariableStrVal[variable], value );

   UpnpNotify( device_handle,
           CURRENT_COUNTER_service_table[service].UDN,
           CURRENT_COUNTER_service_table[service].ServiceId,
           ( const char ** )&CURRENT_COUNTER_service_table[service].VariableName[variable],
           ( const char ** )&CURRENT_COUNTER_service_table[service].VariableStrVal[variable], 1 );

   ithread_mutex_unlock( &CURRENT_COUNTERDevMutex );

   return ( 1 );

}
```

Η συνάρτηση ενημερώνει τον εσωτερικό πίνακα μεταβλητών κατάστασης της συσκευής και αποστέλλει ένα γεγονός κάνοντας χρήση της (εξαιρετικά σημαντικής) συνάρτησης UpnpNotify(). Η τελευταία δέχεται τα παρακάτω ορίσματα:

- Το δείκτη στη συσκευή
- Το UDN της συσκευής
- Το ServiceID της υπηρεσίας που επηρεάστηκε και προκάλεσε την αποστολή του γεγονότος

- Τα ονόματα των αλλαγμένων μεταβλητών που αποθηκεύονται στη δομή CURRENT_COUNTER_service_table[service].VariableName[variable]
- Τις τιμές των αλλαγμένων μεταβλητών που αποθηκεύονται στη δομή CURRENT_COUNTER_service_table[service].VariableStrVal[variable]
- Τον αριθμό των επηρεασμένων μεταβλητών (στη συγκεκριμένη περίπτωση 1).

#### *3.3.2.4 Διακοπή λειτουργίας*

Όταν μια συσκευή βρίσκεται εκτός λειτουργίας, το SDK πρέπει να από-αρχικοποιηθεί. Αυτό γίνεται καλώντας τις συναρτήσεις UpnpUnRegisterRootDevice() και UpnpFinish(). Ο κώδικάς που σχεδιάστηκε, λαμβάνει μέριμνα για τη λειτουργία αυτή μέσω της κλήσης της CURRENT_COUNTERDeviceStop() που καταγράφεται κάτωθι:

```
Int CURRENT_COUNTERDeviceStop( )
{
   UpnpUnRegisterRootDevice( device_handle );
   UpnpFinish( );
   SampleUtil_Finish( );
   ithread_mutex_destroy( &CURRENT_COUNTERDevMutex );
   return UPNP_E_SUCCESS;
}
```

Μετά από την κλήση αυτής της συνάρτησης, η συσκευή μπορεί να κλείσει χωρίς να αφήνει παρενέργειες στο SDK ή στις άλλες συσκευές του δικτύου.

### 3.3.3 Η εφαρμογή του σημείου ελέγχου

Το *Intel® SDK for UPnP™ Devices* (17) που χρησιμοποιήθηκε υποστηρίζει τόσο συσκευές όσο και σημεία ελέγχου. Τα βασικά βήματα που απαιτούνται για την υλοποίηση των εφαρμογών των σημείων ελέγχου είναι τα ακόλουθα:

1. Η διαμόρφωση και αρχικοποίηση του σημείου ελέγχου με τα ακόλουθα βήματα:
   a. Αρχικοποίηση του SDK μέσω της UpnpInit().
   b. Εγγραφή μιας γενικευμένης συνάρτησης του σημείου ελέγχου (αλλιώς πελάτη) κάνοντας χρήση της συνάρτησης UpnpRegisterClient().
2. Η εύρεση συσκευών με ενδιαφέρον από την πλευρά του σημείου ελέγχου μέσω της UpnpSearchAsynch().

3. Η μεταφόρτωση των εγγράφων περιγραφής των συσκευών που το ενδιαφέρουν με χρήση των συναρτήσεων UpnpDownloadXmlDoc() ή σε κάθε περίπτωση της οικογένειας συναρτήσεων UpnpHttp().
4. Η εγγραφή (subscription) σε υπηρεσίες ενδιαφέροντος χρησιμοποιώντας τη συνάρτηση UpnpSubscribe() ή την UpnpSubscribeAsync().
5. Η διαχείριση των υπηρεσιών των συσκευών μέσω κλήσης των συναρτήσεων UpnpSendAction() ή UpnpSendActionAsync().
6. Τη διακοπή λειτουργίας του σημείου ελέγχου ακλουθώντας τα βήματα:
   a. Διαγραφή του σημείου ελέγχου από το SDK χρησιμοποιώντας τη UpnpUnRegisterClient().
   b. Να τερματίσει το SDK μέσω της UpnpFinish().

Στις παραγράφους που ακολουθούν θα αναλυθεί εν τάχει η λειτουργία της υλοποίησης σε επίπεδο σημείου ελέγχου, ενώ θα παρατίθενται και τμήματα κώδικα που κρίνεται ότι συμβάλουν στη βέλτιστη κατανόηση του μηχανισμού του σημείου ελέγχου.

### *3.3.3.1 Διαμόρφωση και αρχικοποίηση*

#### 3.3.3.1.1 Αρχικοποίηση του SDK

Ακριβώς όπως και μια συσκευή, έτσι και ένα σημείο ελέγχου πρέπει να αρχικοποιήσει το SDK προκειμένου να μπορέσει στη συνέχεια να είναι λειτουργικό. Για το σκοπό αυτό, χρησιμοποιεί το παρακάτω τμήμα κώδικα:

```
short int port = 0;
char *ip_address = NULL;

ithread_mutex_init( &DeviceListMutex, 0 );
rc = UpnpInit( ip_address, port );
if( UPNP_E_SUCCESS != rc ) {
   SampleUtil_Print( "WinCEStart: UpnpInit() Error: %d", rc );
   UpnpFinish(  );
   return CURRENT_COUNTER_ERROR;
}
```

Η εφαρμογή καθορίζει μια συγκεκριμένη IP διεύθυνση και αριθμό θύρας κατά τη διάρκεια της αρχικοποίησης. Για τα σημεία ελέγχου, κάτι τέτοιο θα θέσει την προκαθορισμένη διεύθυνση IP και αριθμό θύρας που θα χρησιμοποιήσουν προκειμένου να προσέχουν για ενδεχόμενη αποστολή γεγονότων από τις συσκευές. Αν η διεύθυνση IP είναι NULL, τότε

χρησιμοποιείται η πρώτη μη NULL, μη loopback διεύθυνση που είναι διαθέσιμη. Αν ο αριθμός θύρας είναι 0, τότε χρησιμοποιείται ένας τυχαίος αριθμός θύρας. Η διεύθυνση IP και ο αριθμός θύρας που επιλέχθηκαν μπορούν πολύ εύκολα αργότερα να μαθευτούν με χρήση των συναρτήσεων του SDK UpnpGetServerIpAddress() και UpnpGetServerPort(). Ο μοναδικός λόγος για τον οποίο τα σημεία ελέγχου θα επιθυμούσαν[10] να θέσουν απευθείας τη διεύθυνση IP που ακούν θα ήταν στην περίπτωση ύπαρξης πολυδιεπαφικής διαμόρφωσης. Η επιλογή συγκεκριμένου αριθμού θύρας στην πραγματικότητα δεν παρουσιάζει κανένα συγκεκριμένο πλεονέκτημα.

#### 3.3.3.1.2 Αρχικοποίηση σχετική με το σημείο ελέγχου

Πριν ξεκινήσει η διαδικασία εγγραφής της γενικευμένης συνάρτησης (callback) του σημείου ελέγχου με το SDK (βλ. επόμενη παράγραφο), η εφαρμογή πρέπει να πραγματοποιήσει οποιαδήποτε αρχικοποίηση χρειάζεται για να λειτουργήσει. Κάτι τέτοιο είναι σημαντικό καθώς μόλις ολοκληρωθεί η εγγραφή της γενικευμένης συνάρτησης, πρέπει να έχει τη δυνατότητα να δεχθεί κλήσεις. Στην παρούσα εφαρμογή καμία τέτοια αρχικοποίηση δεν ήταν απαραίτητη.

#### 3.3.3.1.3 Εγγραφή σημείου ελέγχου

Το επόμενο βήμα είναι η εγγραφή (registration) της γενικευμένης συνάρτησης με το SDK. Αυτή αποτελεί και την προκαθορισμένη μέθοδο κοινοποιήσεων του SDK. Ορισμένες συναρτήσεις όπως η UpnpSendActionAsync() που θα παρουσιασθούν αργότερα επιτρέπουν διαφορετική γενικευμένη συνάρτηση ανάλογα με την περίπτωση. Αντίστοιχα με τις συσκευές, η συνάρτηση αυτή έχει πρωτότυπο όπως παρακάτω:

```
int CallbackFxn ( Upnp_EventType EventType, void * Event, void * Cookie ) ;
```

Όλες οι διεργασίες αναζήτησης παρόλα αυτά χρησιμοποιούν την προεπιλεγμένη γενικευμένη συνάρτηση μέσω της UpnpRegiserClient(), όπως παρακάτω:

[10] Υπό την έννοια ότι θα υπήρχε κάποιο πρακτικό πλεονέκτημα φυσικά.

```
rc = UpnpRegisterClient( CURRENT_COUNTERCtrlPointCallbackEventHandler, &ctrlpt_handle, &ctrlpt_handle );
  if( UPNP_E_SUCCESS != rc ) {
    SampleUtil_Print( "Error registering CP: %d", rc );
    UpnpFinish(  );
    return CURRENT_COUNTER_ERROR;
  }
```

Η πρώτη παράμετρος της συνάρτησης είναι η συνάρτηση διαχείρισης γεγονότων που θέλει να χρησιμοποιήσει το SDK. Στον κώδικα που μόλις παρατέθηκε, είναι φανερό ότι χρησιμοποιείται η CURRENT_COUNTERCtrlPointCallbackEventHandler() γι αυτό το σκοπό. Η δεύτερη παράμετρος εισόδου είναι ένας δείκτης σε ένα cookie που θα περάσει στη γενικευμένη συνάρτηση όταν αυτή κληθεί. Η τελευταία παράμετρος είναι ένας δείκτης προς το ίδιο το σημείο ελέγχου. Αυτό είναι ιδιαίτερα σημαντικό για τη μετέπειτα κλήση συναρτήσεων του SDK.

Στον κώδικά καλείται η CURRENT_COUNTERCtrlPointCallbackEventHandler() για όλες τις ασύγχρονες ενέργειες. Εξ αιτίας αυτού η συνάρτηση είναι αρκετά μεγάλη σε μέγεθος γι αυτό και δε θα σχολιασθεί εδώ εξ ολοκλήρου. Αργότερα, διάφορα μέρη αυτής της συνάρτησης θα περιληφθούν στην ανάλυσή του κώδικα προκειμένου να καταστεί σαφής ο τρόπος με τον οποίο γίνεται η χρήση και διαχείριση των εκάστοτε κλήσεων συναρτήσεων που παράγει το SDK. Εκεί θα τονισθεί και η τεράστια σημασία που έχει αυτή η συνάρτηση για την εφαρμογή του σημείου ελέγχου.

Μόλις η εφαρμογή λοιπόν καλέσει και τη συνάρτηση UpnpRegisterClient(), κάθε κίνηση από «διαφημίσεις» συσκευών, θα προκαλέσουν τη δημιουργία κλήσεων προς την εφαρμογή. Η τελευταία πρέπει προφανώς να είναι σε θέση να ανταπεξέλθει σε αυτές άμεσα, όπως έχει ήδη εξάλλου αναφερθεί.

#### *3.3.3.2 Αναζήτηση για υπηρεσίες ενδιαφέροντος*

Μόλις το σημείο ελέγχου είναι πλήρως αρχικοποιημένο, μπορεί αυτόματα να αρχίσει να ψάχνει για συσκευές ενδιαφέροντος στο δικτυωμένο περιβάλλον που βρίσκεται. Στην παρούσα υλοποίηση, λόγω του σκοπού για τον οποίο αυτό δημιουργήθηκε, το σημείο ελέγχου ψάχνει αποκλειστικά για μία συσκευή: τη συσκευή μέτρησης ρεύματος που αναλύθηκε νωρίτερα.

```
rc = UpnpSearchAsync( ctrlpt_handle, 5, CURRENT_COUNTERDeviceType, NULL );
   if( UPNP_E_SUCCESS != rc ) {
      SampleUtil_Print( "Error sending search request %d", rc );
      return CURRENT_COUNTER_ERROR;
   }
```

Το σημείο ελέγχου ξεκινά ψάχνοντας για συσκευές μέτρησης ρεύματος με τη χρήση της CURRENT_COUNTERCtrlPointRefresh() η οποία και περιλαμβάνει το παραπάνω τμήμα κώδικα. Η βασική συνάρτηση που καλείται μέσω της τελευταίας δεν είναι η UpnpSearchAsync(), η οποία ουσιαστικά ξεκινά τη διαδικασία εύρεσης συσκευών. Η συνάρτηση αυτή λαμβάνει τα εξής ορίσματα:

- Ένα δείκτη προς το ίδιο το σημείο ελέγχου
- Τον αριθμό των δευτερολέπτων κατά τη διάρκεια των οποίων το σημείο ελέγχου είναι διατεθειμένο να περιμένει για απαντήσεις
- Το στόχο της αναζήτησης
- Ένα προαιρετικό cookie για να περασθεί στη γενικευμένη συνάρτηση όταν αυτή κληθεί (στην περίπτωσή μας είναι NULL)

Ο στόχος αναζήτησης μπορεί να εμπεριέχει ανάλογα με τη διατύπωσή του είτε μόνο μια συγκεκριμένη συσκευή, είτε μια οικογένεια συσκευών (και αντίστοιχα φυσικά υπηρεσιών). Γενικότερα, ένας στόχος αναζήτησης πρέπει να περιέχει ένα από τα ακόλουθα χαρακτηριστικά:

- ssdp:all – ψάχνει για όλες τις UPnP συσκευές και υπηρεσίες στο δίκτυο
- upnp:rootdevice – ψάχνει μόνο για ριζικές συσκευές στο δίκτυο
- uuid:device-UUID – ψάχνει για μια συγκεκριμένη συσκευή στο δίκτυο που να έχει UUID ίδιο με αυτό που αναζητείται
- urn:schemas-upnp-org:device:deviceType:v – ψάχνει για ένα συγκεκριμένο τύπο συσκευής, deviceType, σε μια συγκεκριμένη έκδοση, v
- urn:schemas-UPnP-org:service:serviceType:v – ψάχνει για ένα συγκεκριμένο τύπο υπηρεσίας, serviceType, μιας συγκεκριμένης έκδοσης, v.

Για μια συσκευή μετρήσεως ρεύματος όπως η δικιά μας, ο στόχος αναζήτησης ορίζεται ως εξής:

```
char CURRENT_COUNTERDeviceType[] = "urn:schemas-upnp-org:device:CURRENT_COUNTERdevice:1";
```

Ο χρόνος αναμονής (MX) καθορίζει το μέγιστο χρόνο που ένα σημείο ελέγχου είναι διατεθειμένο να περιμένει για απαντήσεις συσκευών που ταιριάζουν με την αναζήτησή του. Οι συσκευές θα περιμένουν ένα τυχαίο χρονικό διάστημα μεταξύ 0 και της τιμής MX που καθορίζεται από το σημείο ελέγχου πριν απαντήσει, με απώτερο στόχο την ελαχιστοποίηση κατά το δυνατό της συμφόρησης στο δίκτυο. Το SDK παράγει ένα γεγονός, UPnP_DISCOVERY_SEARCH_TIMEOUT, όταν το χρονικό διάστημα MX παρέλθει. Σε αυτήν την περίπτωση, το SDK δε θα παράγει άλλα γεγονότα για την συγκεκριμένη αναζήτηση, παρά το γεγονός ότι οι διαφημίσεις των συσκευών θα συνεχίσουν να παράγουν γεγονότα.

Στην εφαρμογή που υλοποιήθηκε, όλα αυτά τα μηνύματα ανεύρεσης είναι αντικείμενα διαχείρισης από τη συνάρτηση CURRENT_COUNTER CtrlPointCallbackEventHandler:

```
int CURRENT_COUNTERCtrlPointCallbackEventHandler( Upnp_EventType EventType, void *Event, void *Cookie )
{
   switch ( EventType ) {
      case UPNP_DISCOVERY_ADVERTISEMENT_ALIVE:
      case UPNP_DISCOVERY_SEARCH_RESULT:
         {
            struct Upnp_Discovery *d_event = ( struct Upnp_Discovery * )Event;
            IXML_Document *DescDoc = NULL;
            int ret;
            if( ( ret = UpnpDownloadXmlDoc( d_event->Location,  &DescDoc ) ) != UPNP_E_SUCCESS ) {
               /*…*/
            } else {
               CURRENT_COUNTERCtrlPointAddDevice( DescDoc, d_event->Location, d_event->Expires );
            }
            if( DescDoc )
               ixmlDocument_free( DescDoc );
            CURRENT_COUNTERCtrlPointPrintList(  );
            break;
         }

      case UPNP_DISCOVERY_SEARCH_TIMEOUT:
         break;

      case UPNP_DISCOVERY_ADVERTISEMENT_BYEBYE:
         {
            struct Upnp_Discovery *d_event = ( struct Upnp_Discovery * )Event;
            CURRENT_COUNTERCtrlPointRemoveDevice( d_event->DeviceId );
            CURRENT_COUNTERCtrlPointPrintList(  );
            break;
         }
```

Στο παραπάνω block κώδικα έχουν παραληφθεί πολλές, δευτερεύουσας σημασίας εντολές, σε μια προσπάθεια απόκρυψης της πολυπλοκότητας, προς όφελος της απλότητας και κατανόησης από την πλευρά του αναγνώστη.

Όταν η διαφήμιση μιας συσκευής φτάσει στη χρονική της λήξη, ή όταν κάποια συσκευή απλά αποστείλει ένα μήνυμα «bye-bye», τότε η συσκευή αυτή πρέπει να διαγραφεί από τη λίστα με τις γνωστές συσκευές. Τα μηνύματα «bye-bye» χειρίζονται πολύ απλά όπως φαίνεται στον κώδικα νωρίτερα. Η συνάρτηση CURRENT_COUNTERCtrlPointTimerLoop () διαχειρίζεται τις λήξεις των διαφημίσεων κάθε 30 δευτερόλεπτα, καλώντας με τη σειρά της την CURRENT_COUNTERCtrlPointVerifyTimeouts() η οποία ελέγχει για διαφημίσεις που έχουν παρέλθει χρονικά. Η εφαρμογή πραγματοποιεί μια αυτόματη αναζήτηση για συσκευές οι οποίες είναι έτοιμες να λήξουν ψάχνοντας για το UDN της υπό απειλή χρονικής λήξεως συσκευής. Τυπικά αυτό δεν απαιτείται, καθώς στη συνήθη περίπτωση η συσκευή έχει προλάβει και έχει ανανεώσει την διαφήμισή της πριν τη λήξη αυτού του χρονικού διαστήματος MX.

#### *3.3.3.3 Λήψη περιγραφών*

Ο κώδικάς που σχεδιάστηκε χειρίζεται τις διαφημίσεις των συσκευών και τα αποτελέσματα των αναζητήσεων με τον ίδιο ενιαίο τρόπο. Χρησιμοποιεί την UpnpDownloadXmlDoc() για να λάβει το έγγραφο περιγραφής και προσθέτει τη συγκεκριμένη συσκευή στη λίστα γνωστών συσκευών που διατηρεί. Είναι ιδιαίτερα σημαντικό να καταστραφεί το έγγραφο περιγραφής αυτό όταν δεν είναι πλέον χρήσιμο, τόσο για λόγους χωρητικότητας, όσο και ασφαλείας. Στον κώδικά μας, το έγγραφο περιγραφής προς το παρόν δεν αποθηκεύεται κάπου στο σημείο ελέγχου, και σβήνεται μόλις η χρησιμότητά του είναι πλέον μηδαμινή. Αναφορικά με την UpnpDownloadXmlDoc(), αυτή επιστρέφει ένα καθόλα δομημένο έγγραφο DOM του εγγράφου περιγραφής, έτοιμο για χρήση από την εφαρμογή του σημείου ελέγχου. Η συνάρτηση αυτή μπορεί να αποδειχθεί αρκετά απαιτητική σε θέματα μνήμης, ειδικά αν το έγγραφο περιγραφής είναι μεγάλο, καθώς αυτό μεταφορτώνεται, αναλύεται και επιστρέφεται σε ένα μόλις block. Ένα εναλλακτικό API που επιτρέπει το SDK επιτρέπει πολύ μεγαλύτερες μεταφορές HTTP τεμαχίζοντας το αρχείο σε περισσότερα κομμάτια. Αντίθετα από την UpnpDownloadXmlDoc(), κάτι τέτοιο έχει ανάγκη από πολλαπλές κλήσεις κατάλληλων συναρτήσεων. Έτσι, με χρήση της UpnpOpenHttpGet() δημιουργείται μια νέα HTTP σύνδεση, η UpnpReadHttpGet() μεταφέρει ένα ένα τα κομμάτια του αρχείου και τέλος η UpnpCloseHttpGet() ολοκληρώνει και κλείνει τη σύνδεση

που έχει δημιουργηθεί. Αυτή η μέθοδος μπορεί να φαίνεται ελαφρώς πιο πολύπλοκη, αλλά το γεγονός ότι η εφαρμογή μπορεί να λειτουργήσει ακριβώς όπως ο δημιουργός της θέλει, προσδίδει μεγάλη δύναμη στον τελευταίο, ο οποίος τελικά μπορεί να διαχειριστεί την κίνηση στο δίκτυο όπως αυτός κρίνει καλύτερα.

#### *3.3.3.4 Αναμονή γεγονότων*

Όταν μια μεταβλητή κατάστασης σε μια συσκευή αλλάξει τιμή, τότε η συσκευή αποστέλλει ειδοποιήσεις σε όλα τα σημεία ελέγχου που έχουν εγγραφεί ως συνδρομητές σε αυτή, προκειμένου να λαμβάνουν αυτές τις ειδοποιήσεις – γεγονότα. Το SDK έχει δυο τρόπους για τη συνδρομή σε μια υπηρεσία: μέσω χρήσης των συναρτήσεων UpnpSubscribe() και UpnpSubscribeAsync(). Και οι δύο συναρτήσεις εκτελούν τις ίδιες λειτουργίες, μόνο που η δεύτερη από αυτές παράγει και ένα γεγονός (callback) όταν η αίτηση συνδρομής ολοκληρωθεί. Είναι σημαντικό να σημειωθεί ότι όταν γίνεται η εγγραφή, το σημείο ελέγχου γίνεται συνδρομητής για όλα τα γεγονότα μιας συγκεκριμένης υπηρεσίας.

Στην παρούσα εφαρμογή, το σημείο ελέγχου εγγράφεται στην υπηρεσία μέτρησης ρεύματος με τη συνάρτηση CURRENT_COUNTERCtrlPointAddDevice() ως απάντηση σε μια αίτηση αναζήτησης ή όταν μια συσκευή αποστέλλει κάποια διαφήμιση όπως παρακάτω:

```
ret = UpnpSubscribe( ctrlpt_handle, eventURL[service], &TimeOut[service], eventSID[service] );

            if( ret == UPNP_E_SUCCESS ) {
               /****/
            } else {
               SampleUtil_Print ( "Error Subscribing to EventURL -- %d", ret );
               strcpy( eventSID[service], "" );
            }
```

Η UpnpSubscribe() δέχεται τις ακόλουθες παραμέτρους:

- Ένα δείκτη προς το σημείο ελέγχου
- Τη διεύθυνση URL της υπηρεσίας που το σημείο ελέγχου θέλει να εγγραφεί
- Ένα δείκτη προς μια ζητούμενη τιμή αναμονής. Μόλις επιστρέψει η συνάρτηση, ο δείκτης αυτός θα περιέχει την πραγματική διάρκεια ζωής της συνδρομής αν η συσκευή δε συμφώνησε με την εκδοχή που πρότεινε το σημείο ελέγχου
- Ένα δείκτη στον οποίο θα αποθηκευθεί το SID

Η UpnpSubscribeAsync() δέχεται παρόμοιες τιμές εισόδου, αλλά το SID και η πραγματική διάρκεια διαφήμισης δίνονται στην εφαρμογή κατά τη διάρκεια του γεγονότος που εκπέμπεται και όχι κατά την επιστροφή της συνάρτησης.

Το SDK αποστέλλει γεγονότα στη γενικευμένη συνάρτηση που έχει εγγραφεί, μέσω της UpnpRegisterClient() όπως έχει ήδη αναφερθεί. Για τη συσκευή ελέγχου, αυτή η συνάρτηση είναι η CURRENT_COUNTERCtrlPointCallbackEventHandler():

```
int CURRENT_COUNTERCtrlPointCallbackEventHandler( Upnp_EventType EventType,
                                                  void *Event, void *Cookie )
{
   /*....*/
   switch ( EventType ) {
  /*....*/
      case UPNP_EVENT_RECEIVED:
         {
            struct Upnp_Event *e_event = ( struct Upnp_Event * )Event;
            CURRENT_COUNTERCtrlPointHandleEvent( e_event->Sid,
                                                 e_event->EventKey,
                                                 e_event->ChangedVariables );
            break;
         }
    /*....*/
  return 0;
}
```

Το γεγονός UPNP_EVENT_RECEIVED που αναγράφεται, είναι στην ουσία ένα γεγονός που έχει ληφθεί από μια συσκευή. Η παράμετρος Event περιέχει μια δομή UPnP_Event, η οποία περιγράφει το πραγματικό γεγονός που προξένησε και την αποστολή της ανακοίνωσης γεγονότος. Αυτά τα γεγονότα γίνονται αντικείμενα διαχείρισης από τη συνάρτηση CURRENT_COUNTERCtrlPointHandleEvent().

Μόλις ένα σημείο ελέγχου γίνει συνδρομητής σε μια συγκεκριμένη υπηρεσία, το SDK θα αρχίσει αυτόματα να ανανεώνει τη συνδρομή αυτή μέχρι η συσκευή απλά να τη διακόψει.

#### *3.3.3.5 Πρόκληση ενεργειών*

Τα σημεία ελέγχου έχουν τη δυνατότητα να προκαλέσουν αλλαγές στις μεταβλητές κατάστασης της συσκευής, ελέγχοντας με αυτόν τον τρόπο την κατάσταση και την ποιότητα του δικτύου. Κάτι τέτοιο γίνεται με την αποστολή αιτήσεων γεγονότων στη συσκευή. Το SDK έχει δύο συναρτήσεις για τη διαχείριση των γεγονότων αυτών: την UpnpSendAction() και την UpnpSendActionAsync(). Και οι δύο συναρτήσεις πραγματοποιούν τις ίδιες ενέργειες,

με μόνη διαφορά ότι η δεύτερη λειτουργεί εντελώς ασύγχρονα. Κάθε μία από αυτές τις συναρτήσεις λαμβάνει ένα έγγραφο DOM που περιγράφει την ενέργεια που το σημείο ελέγχου επιθυμεί να διενεργηθεί από πλευράς συσκευής. Η δομή αυτών DOM εγγράφων μπορεί να βρεθεί στην παράγραφο 3.2.1 του *Universal Plug and Play Device Architecture*. Το SDK έχει διάφορες χρήσιμες συναρτήσεις για τη δόμηση τέτοιων μηνυμάτων, και κυρίως τις UpnpMakeAction() και UpnpAddToAction(). Η εφαρμογή που υλοποιήθηκε επωφελείται στο έπακρο των πλεονεκτημάτων αυτών των δύο συναρτήσεων μέσω της συνάρτησης CURRENT_COUNTERCtrlPointSendAction() που περιγράφεται κάτωθι:

```
IXML_Document *actionNode = NULL;

if( 0 == param_count ) {
        actionNode = UpnpMakeAction( actionname,
                                     CURRENT_COUNTERServiceType[service],
                                      0, NULL );
    } else {
      for( param = 0; param < param_count; param++ ) {
        if( UpnpAddToAction( &actionNode, actionname,
                             CURRENT_COUNTERServiceType[service],
                             param_name[param], param_val[param] )
                             != UPNP_E_SUCCESS ) {
          /*....*/
        }
      }

rc = UpnpSendActionAsync( ctrlpt_handle,
                          devnode->device.CURRENT_COUNTERService[service].ControlURL,
                          CURRENT_COUNTERServiceType[service], NULL, actionNode,
                          CURRENT_COUNTERCtrlPointCallbackEventHandler, NULL );

if( rc != UPNP_E_SUCCESS ) {
        SampleUtil_Print( "Error in UpnpSendActionAsync -- %d", rc );
        rc = CURRENT_COUNTER_ERROR;
    }
```

Αν μια ενέργεια δεν απαιτεί καμία παράμετρο, η UpnpMakeAction() είναι αρκετή για να δομήσει το σωστό actionNode (το έγγραφο DOM περιγραφής της ενέργειας) για την ενέργεια. Σε κάθε άλλη περίπτωση, η εφαρμογή καλεί την UpnpAddToAction() επαναληπτικά μέχρι να προστεθούν όλες οι παράμετροι και οι τιμές αυτών στο έγγραφο actionNode. Τελικά, καλείται η UpnpSendActionAsync() για να σταλεί το μήνυμα ενέργειας στη συσκευή.

Μια συνάρτηση που αξίζει σχολιασμού, είναι η CURRENT_COUNTERCtrlPointSendAction(). Αυτή είναι μια γενική συνάρτηση που χρησιμοποιήθηκε για την αποστολή των γεγονότων

που απαιτούνται. Παραδειγματικά, ένα σημείο ελέγχου ζητά από μια συσκευή να διακόψει τη λειτουργία της όπως παρακάτω:

```
int CURRENT_COUNTERCtrlPointSendPowerOff( int devnum )
{
   return CURRENT_COUNTERCtrlPointSendAction( CURRENT_COUNTER_SERVICE_CONTROL,
                                              devnum, "PowerOff", NULL, NULL, 0 );
}
```

Μόλις η ασύγχρονη ενέργεια πραγματοποιηθεί και ολοκληρωθεί, το γεγονός που δημιουργείται περνά διαχειριστή γεγονότων που ορίστηκε νωρίτερα μέσω των UpnpSendActionAsync() ή που εγγράφηκε μέσω της UpnpRegisterClient(). Η εφαρμογή που υλοποιήθηκε κάνει χρήση ενός κοινού διαχειριστή γεγονότων για όλα τα γεγονότα, οπότε το μήνυμα του γεγονότος ολοκλήρωσης της ενέργειας τυγχάνει ειδικής μέριμνας στην CURRENT_COUNTERCtrlPointHandleEvent():

```
case UPNP_CONTROL_ACTION_COMPLETE:
        {
           struct Upnp_Action_Complete *a_event = ( struct Upnp_Action_Complete * )Event;
           if( a_event->ErrCode != UPNP_E_SUCCESS ) {
              SampleUtil_Print ( "Error in  Action Complete Callback -- %d", a_event->ErrCode );
           }
           break;
        }
```

### *3.3.3.6 Διακοπή λειτουργίας*

Όταν το σημείο ελέγχου θέλει να διακόψει για κάποιο λόγο (πχ για λόγους συντήρησης) τη λειτουργία του, πρέπει να διαγράψει τον εαυτό του από το SDK, χρησιμοποιώντας τη συνάρτηση UpnpUnregisterClient() και να κλείσει και το ίδιο το SDK με χρήση της UpnpFinish() όπως παρουσιάζεται παρακάτω:

```
Int CURRENT_COUNTERCtrlPointStop( void )
{
   CURRENT_COUNTERCtrlPointRemoveAll(  );
   UpnpUnRegisterClient( ctrlpt_handle );
   UpnpFinish(  );
   SampleUtil_Finish(  );

   return CURRENT_COUNTER_SUCCESS;
}
```

## 3.4 Σύνοψη

Στο κεφάλαιο αυτό, παρουσιάσθηκαν τα πλεονεκτήματα των τεχνολογιών XML σε σχέση με τις παλαιότερες τεχνικές ελέγχου δικτύων (όπως πχ το SNMP), ενώ στη συνέχεια πραγματοποιήθηκε και μια συνοπτική παρουσίαση του πρωτοκόλλου Universal Plug and Play, ενός από τα βασικότερα σήμερα παραδείγματα εφαρμογής των XML τεχνολογιών, με καθημερινή εφαρμογή σε πάρα πολλούς τομείς της ανθρώπινης δραστηριότητας σε δικτυωμένα περιβάλλοντα. Στη συνέχεια παρατέθηκε μια μικρή περιγραφή της εφαρμογής που υλοποιήθηκε, η οποία είναι ένα σημείο ελέγχου, το οποίο ελέγχει μια συσκευή (στην πραγματικότητα μια οικογένεια συσκευών) που μετρά το ρεύμα που τη διαρρέει. Η εφαρμογή αυτή, όσο απλοϊκή και αν φαίνεται, μπορεί να βοηθήσει σημαντικά στην παρακολούθηση της μεταφοράς ισχύος ενός δικτύου ενέργειας, γεγονός ιδιαίτερα σημαντικό καθώς μπορεί να συμβάλει αποτελεσματικά στην πρόληψη βλαβών ή άλλων διαχειριστικών ατοπημάτων από πλευράς διαχείρισης του δικτύου. Το πρωτόκολλο UPnP παρέχει ένα εύκολο και επιβεβαιωμένα λειτουργικό περιβάλλον παρακολούθησης, ενώ η κατανεμημένη αρχιτεκτονική του βοηθά στην εύκολη ανάκαμψη των όποιων προβλημάτων μπορεί να συμβούν σε ένα δίκτυο. Το μεγαλύτερο πλεονέκτημά του όμως είναι η δυνατότητα εύκολης και γρήγορης παραμετροποίησης αυτού, η προσθήκη νέων λειτουργιών και χαρακτηριστικών (όπως για παράδειγμα η αποστολή επιπλέον στοιχείων για τον κυματισμό της τάσης, την ένταση του σήματος BPL στο δίκτυο και τον κυματισμό αυτής, η αποστολή γεωγραφικών στοιχείων από τις συσκευές για τη δημιουργία διασυνδεδεμένων χαρτών σταθμών ΜΤ για οπτική παρατήρηση ή επεξεργασία κοκ). Με την κατάλληλη προσθήκη ορισμένων απλών αυτοματισμών στον παρόντα κώδικά, η εφαρμογή αυτή θα μπορούσε εύκολα να αποτελέσει ένα αυτόνομο σύστημα στην ιδανική του μορφή. Το μόνο το οποίο λείπει αυτή τη στιγμή από την εφαρμογή (και ίσως το πρωτόκολλο αυτό καθ εαυτό) είναι η ασφάλεια και διατήρηση της ακεραιότητας από πιθανές επιθέσεις στο δίκτυο. Η εισαγωγή κρυπτογράφησης μπορεί να διαγράψει αυτήν την έλλειψη, καθώς με την εφαρμογή ισχυρών κρυπτογραφικών μεθόδων στα πακέτα που κινούνται στο δίκτυο, η οποιαδήποτε απειλή μπορεί να αντιμετωπιστεί αποτελεσματικά. Όλα αυτά θα αναπτυχθούν σε ειδικό κεφάλαιο της παρούσας διπλωματικής εργασίας.

Το κύριο μέρος της εφαρμογής έχει πλέον παρουσιαστεί. Στα επόμενα κεφάλαια θα ακολουθήσουν διάφορες μέθοδοι ελαχιστοποίησης της πληροφορίας που αποστέλλεται στο δίκτυο, ενώ θα γίνει αναφορά στην περίπτωση κρυπτογράφησης των μηνυμάτων που στέλνονται δικτυακά από τις συσκευές στα σημεία ελέγχου και το αντίστροφο.

# 4 Συνάθροιση πληροφορίας – Κρυπτογράφηση

Στην προηγούμενη παράγραφο, παρουσιάστηκαν εν τάχει τα χαρακτηριστικά του πρωτοκόλλου UPnP που χρησιμοποιήθηκε για την υλοποίηση της εφαρμογής. Καταδείχθηκε η δυνατότητα αποτελεσματικού ελέγχου των συσκευών μέτρησης ρεύματος του δικτύου μας, και η δυνατότητα εύκολης προσθαφαίρεσης χαρακτηριστικών και υπηρεσιών. Επίσης, το UPnP προσομοιάζει επιτυχώς τη λειτουργία των αυτόνομων συστημάτων καθώς διαθέτει τις βασικές ιδιότητες αυτών: είναι αυτο–προσαρμόσιμο, αυτο–ιάσιμο και αυτο-βελτιστοποιούμενο. Το μόνο σημείο που πρακτικά υστερεί των αυτόνομων συστημάτων είναι η αυτο–προστασία. Σε αυτό το κεφάλαιο, παρατίθενται διάφορες λύσεις κρυπτογράφησης που εγγυώνται την ορθή και ασφαλή λειτουργία του υπό σχεδίαση συστήματός. Θα περιγραφθεί η λειτουργία διάφορων μεθόδων κρυπτογράφησης, ενώ παράλληλα θα εξετασθεί και τη σχετική δυνατότητα εφαρμογής τους στην εφαρμογή του μετρητή ρεύματος.

Ένα άλλο σημαντικό σημείο που δεν εξετάστηκε νωρίτερα είναι η παραγόμενη από τις συσκευές και τα σημεία ελέγχου κίνηση λόγω της κυκλοφορίας των XML μηνυμάτων στο δίκτυο. Η κίνηση αυτή μπορεί να προκαλέσει διάφορα προβλήματα συμφόρησης στο δίκτυο. Επίσης, πρέπει πλέον να συνυπολογισθεί και η επιπλέον καθυστέρηση που εισάγεται από την (απο)κρυπτογράφηση των μηνυμάτων που στέλνονται, και να βρεθεί ένας τρόπος μείωσης αυτής. Η εφαρμογή σχήματος συνάθροισης πληροφορίας, μπορεί να λύσει κάποια από αυτά τα προβλήματα, δημιουργεί όμως νέα πεδία έρευνας που σχετίζονται τόσο με τη βελτιστοποίηση του εφαρμοζόμενου αλγορίθμου συνάθροισης, όσο και τη σειρά εφαρμογής των τεχνικών συνάθροισης και κρυπτογράφησης, για να επιτευχθεί βέλτιστη λειτουργία του δικτύου, δεδομένου ότι τόσο οι συσκευές όσο και τα σημεία ελέγχου δεν αποτελούν ισχυρούς σταθμούς επεξεργασίας δεδομένων, αλλά μάλλον συστήματα περιορισμένης επεξεργαστικής ισχύος και φυσικής μνήμης, γεγονός που εισάγει επιπλέον περιορισμούς και δυσκολίες. Σε κάθε περίπτωση, η εφαρμογή τεχνικών συνάθροισης θα βοηθήσει το σύστημα να μειώσει αισθητά την παραγόμενη κίνηση, ενώ η δημιουργία μιας μορφής ιεραρχίας στο σύστημά θα επιτρέψει τον πιο κατανεμημένο έλεγχο των περιοχών ελέγχου, αυξάνοντας τη δυναμική των δυνατοτήτων της εφαρμογής που σχεδιάσθηκε.

## 4.1 Συνάθροιση πληροφορίας

### 4.1.1 Εισαγωγικά

Σε προηγούμενη παράγραφο μελετήθηκε η δομή ενός XML εγγράφου περιγραφής συσκευών του δικτύου BPL. Διαπιστώθηκε ότι δίνει επαρκείς πληροφορίες για την περιγραφή της ίδιας της συσκευής και των υπηρεσιών της, ενώ παράλληλα διαχώριζε εντελώς μια συγκεκριμένη συσκευή από όλες τις άλλες. Η δομή του εγγράφου περιγραφής είναι ως γνωστόν πλέον:

```
<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
 <specVersion>
  <major>1</major>
  <minor>0</minor>
 </specVersion>
 <device>
  <deviceType>urn:schemas-upnp-org:device:CURRENT_COUNTERdevice:1</deviceType>
  <friendlyName>UPnP Current Counter Emulator</friendlyName>
  <manufacturer>Artemis Voulkidis by Intel's Sample</manufacturer>
  <manufacturerURL>http://users.ntua.gr/el02045/</manufacturerURL>
  <modelDescription>UPnP Current Counter Device Emulator 1.0</modelDescription>
  <modelName>CurrentCounterEmulator</modelName>
  <modelNumber>1.0</modelNumber>
  <modelURL>http://users.ntua.gr/el02045/Current_Counter/</modelURL>
  <serialNumber>123456789001</serialNumber>
  <UDN>uuid:Upnp-Current_CounterEmulator-1_0-1234567890001</UDN>
  <UPC>123456789</UPC>
  <serviceList>
   <service>
    <serviceType>urn:schemas-upnp-org:service:CURRENT_COUNTERcontrol:1</serviceType>
    <serviceId>urn:upnp-org:serviceId:CURRENT_COUNTERcontrol:1</serviceId>
    <controlURL>/upnp/control/CURRENT_COUNTERcontrol1</controlURL>
    <eventSubURL>/upnp/event/CURRENT_COUNTERcontrol1</eventSubURL>
    <SCPDURL>/CURRENT_COUNTERcontrolSCPD.xml</SCPDURL>
   </service>
  </serviceList>
 <presentationURL>CURRENT_COUNTERdevicepres.html</presentationURL>
</device>
</root>
```

**Σχήμα 4.1: Το έγγραφο περιγραφής μιας συσκευής**

Μια προσεκτική ματιά στο τυπικό αυτό έγγραφο περιγραφής μιας συσκευής μπορεί να βοηθήσει στην εξαγωγή ορισμένων αρκετά σημαντικών συμπερασμάτων. Το πρώτο και βασικότερο που αναφέρθηκε ήδη, είναι ότι παρέχονται πάρα πολλές πληροφορίες για τη συσκευή, από το σειριακό αριθμό παραγωγής που τη χαρακτηρίζει μέχρι τη διεύθυνση URL του παραγωγού της εφαρμογής. Ένα δεύτερο συμπέρασμα που εξάγεται είναι ότι σε ένα δίκτυο με πολλές συσκευές ιδίου τύπου (όπως εξ άλλου γίνεται στη συνήθη περίπτωση)

ορισμένα από αυτά τα χαρακτηριστικά που αναγράφονται στο έγγραφο αυτό επαναλαμβάνονται. Σε ένα μικρού μεγέθους δίκτυο με λίγες συσκευές κάτι τέτοιο δεν αποτελεί πρόβλημα. Σε ένα μεγάλο δίκτυο εκατοντάδων ή και χιλιάδων συσκευών όμως, αυτή η επαναλαμβανόμενη πληροφορία μπορεί να δημιουργήσει φαινόμενα συμφόρησης κίνησης, κίνηση η οποία δε θα έχει κάποιο ιδιαίτερο αντίκτυπο σε όρους επιπλέον πληροφορίας. Η ελαχιστοποίηση της κίνησης αυτής, με ταυτόχρονη μεγιστοποίηση της πυκνότητας πληροφορίας που μεταφέρεται, αποτελεί λοιπόν ένα σημείο ιδιαίτερης προσοχής για την εφαρμογή. Η ιδέα προέρχεται από τη μελέτη των ασύρματων δικτύων αισθητήρων, τα οποία κατά παρόμοιο τρόπο με την περίπτωσή μας, αποτελούνται από συσκευές περιορισμένης δυνατότητας κατανάλωσης ενέργειας, επεξεργαστικής ισχύος και φυσικής μνήμης, ενώ παρόλα αυτά καλούνται να είναι διαρκώς σε λειτουργία, διατηρώντας παράλληλα το σύστημα πλήρως λειτουργικό, χωρίς να προκαλούν παρενέργειες στη φυσική κίνηση δεδομένων του δικτύου.

### 4.1.2 Θεωρητικό υπόβαθρο

Η ιδέα για την εφαρμογή ενός τέτοιου γενικευμένου, κατανεμημένου αλγόριθμου συμπίεσης πληροφορίας, προέρχεται από τη μελέτη των ασύρματων δικτύων αισθητήρων (Wireless Sensor Networks - WSN). Τα δίκτυα αυτά, παρουσιάζουν αρκετές ομοιότητες με τα ισχύοντα BPL δίκτυα, ενώ έχει παράλληλα διενεργηθεί σοβαρή και σε βάθος έρευνα τα τελευταία χρόνια.

Τα WSN είναι δίκτυα ευρέως κατανεμημένα, κατάλληλα για λήψη και *in situs* επεξεργασία δεδομένων γενικά αραιής ή και κατά τόπους και περιόδους πυκνής δόμησης. Αποτελούνται από μεγάλο αριθμό αυτόνομων, διασυνδεδεμένων κόμβων ελέγχου (αισθητήρων), οι οποίοι διαρκώς ελέγχουν και αποθηκεύουν δεδομένα σχετικά με τοπικά φαινόμενα, και μπορούν να υλοποιηθούν σε μεγάλη κλίμακα σε περιοχές με περιορισμούς σε πόρους (σε ό,τι έχει να κάνει με χρήση ενέργειας κτλ) και σκληρά περιβάλλοντα, όπως για παράδειγμα σεισμικές ζώνες, περιοχές με μη ομογενή γεωλογικά χαρακτηριστικά, ή πεδία μαχών (18). Οι διαδικτυακές διαδικασίες που πρέπει να πραγματοποιηθούν, γίνονται πράξη μέσω δρομολόγησης και συνεργατικής επεξεργασίας των δεδομένων που έχουν αναγνωρίσει οι κόμβοι.

Η τυχαία και μη παρακολουθούμενη φύση των κόμβων στα ασύρματα δίκτυα αισθητήρων περιορίζει σημαντικά τον αριθμό των υλοποιήσιμων αλγορίθμων δρομολόγησης της

πληροφορίας που προκύπτει από αυτά. Στις περιπτώσεις κεντρικής δρομολόγησης πληροφορίας, οι ερωτήσεις ενδιαφέροντος διασπείρονται στο δίκτυο λαμβάνοντας συγκεκριμένες πληροφορίες, όπως για παράδειγμα δεδομένα τα οποία ταιριάζουν σε κάποια περιγραφή. Επιπλέον, τα δεδομένα μπορούν να συναθροισθούν ή να συνδυασθούν σε καθορισμένους κόμβους ενδιαφέροντος κατά μήκος του δέντρου δρομολόγησης προκειμένου να μειωθεί η εκρηκτικότητα της κίνησης που παράγεται από τέτοιες αναζητήσεις. Τα πακέτα πληροφορίας πρέπει επίσης να προωθούνται μέσω μονοπατιών κατά το δυνατό ελαχιστοποιημένου κόστους. Μια άλλη εναλλακτική μέτρησης θα ήταν η δρομολόγηση των πακέτων μέσω διαδρομών οι οποίες θα ικανοποιούσαν την ανάγκη ελαχιστοποίησης κατανάλωσης ρεύματος. Παρόλα αυτά, τέτοιες τεχνικές δρομολόγησης θα μπορούσαν να έχουν ως αποτέλεσμα την μη ομοιόμορφη κατανομή της κίνησης, ή ακόμα και την υπερχρησιμοποίηση κάποιων κόμβων με ταυτόχρονο παραγκωνισμό κάποιων άλλων κόμβων που θα τίθονταν πρακτικά εκτός λειτουργίας δρομολόγησης (πχ λόγω του δύσβατου της περιοχής που βρίσκονται). Έτσι, φαίνεται πιο λογική η χρήση σχημάτων δρομολόγησης, βασισμένων στα διάφορα τηλεπικοινωνιακά κόστη.

Με βάση τα παραπάνω, έχει αποδειχθεί (18), ότι η εισαγωγή σχημάτων συνάθροισης σε δίκτυα τέτοιου τύπου μπορεί να προσφέρει μεγάλη οικονομία τόσο σε εύρος ζώνης όσο και σε ενέργεια που απαιτούνται για την αποτελεσματική υλοποίηση των WSN. Μάλιστα με κατάλληλη χρήση και εφαρμογή της θεωρίας παιγνίων, μπορεί να προκύψει μια πλήρης και σχετικά αξιόπιστη πλατφόρμα υπολογισμού της αποτελεσματικότητας της εφαρμογής της συνάθροισης, όσο και άλλων σχημάτων βελτιστοποίησης.

### 4.1.3 Ο αλγόριθμος συνάθροισης

Αναφέραμε νωρίτερα ότι πολλά τμήματα του εγγράφου περιγραφής μιας συσκευής είναι κοινά μεταξύ διαφορετικών συσκευών. Μικρή μελέτη του εγγράφου αυτού μας δείχνει ότι τα κοινά τμήματα αυτά είναι τα εξής πεδία[11]:

- deviceType
- friendlyName
- manufacturer
- manufacturerURL
- modelDescription

[11] Φυσικά γίνεται αναφορά για την πλειοψηφία και όχι για το σύνολο των συσκευών, και εφόσον μιλάμε για ομαδική υλοποίηση. Σε κάθε περίπτωση θα γίνεται έλεγχος και γι αυτά τα πεδία, αλλά σε διαφορετικό επίπεδο.

- modelName
- modelNumber
- modelURL
- presentationURL

Αν επίσης υποτεθεί ότι όλες οι συσκευές του δικτύου θα έχουν και κοινές υπηρεσίες, σενάριο που φαντάζει ως αρκετά πιθανό, τότε σε αυτά πρέπει να προστεθούν και τα:

- serviceType
- serviceId
- controlURL
- eventSubURL
- SCPDURL

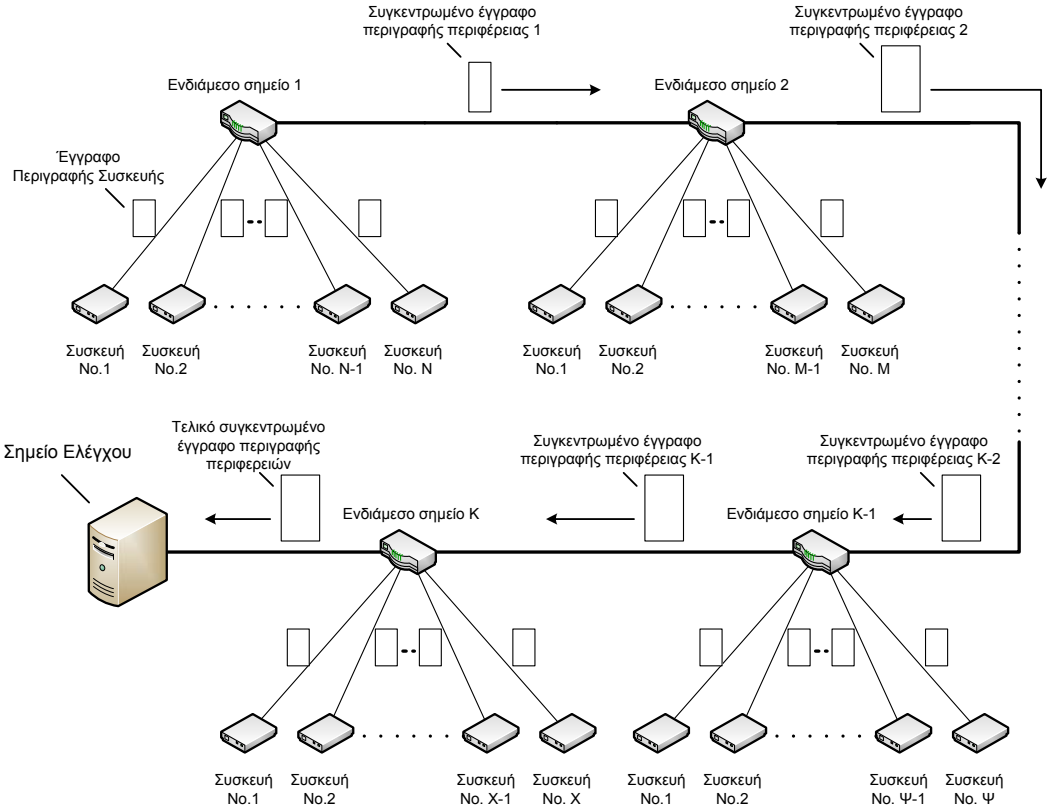
Παρατηρείται εύκολα αυτό που αναφέραμε και νωρίτερα, το γεγονός δηλαδή ότι πολλά τμήματα του XML εγγράφου περιγραφής επαναλαμβάνονται.

Αφού εντοπίσθηκαν επιτυχώς τα σημεία επανάληψης της πληροφορίας, μπορεί πλέον να αναπτυχθεί ένας απλός αλγόριθμος συνάθροισης πληροφορίας, ο οποίος, δεδομένων n ($n \geq 2$) διαφορετικών εγγράφων, θα μπορεί να «συμπιέσει» την πληροφορία, παρέχοντας ένα ενοποιημένο XML αρχείο, με διαδικασία όμως πλήρως αντιστρέψιμη ώστε στα σημεία ελέγχου να είναι δυνατή η πλήρης αποσυμπίεση του ενοποιημένου εγγράφου, και η ανάκτηση των επιμέρους προς επεξεργασία XML αρχείων, ώστε να μην απαιτείται ο επανασχεδιασμός του πρωτοκόλλου UPnP.

Για να έχει νόημα η εφαρμογή της συνάθροισης στην εφαρμογή που σχεδιάστηκε, πρέπει να υλοποιηθεί με τέτοιο τρόπο ώστε να καθιστά πραγματικότητα όλα τα πλεονεκτήματα που συνεπάγεται μια τέτοια κίνηση, πλεονεκτήματα που αναφέρθηκαν και νωρίτερα. Για το σκοπό αυτό, θεωρήθηκε σωστό, όπως συμβαίνει και με τα ασύρματα δίκτυα αισθητήρων, να εισαχθεί η παρουσία νέων συσκευών που θα εφαρμόζουν τη συνάθροιση στα έγγραφα μιας «περιφέρειας» συσκευών, ενώ κατά τα άλλα θα λειτουργούν περίπου ως απλοί δρομολογητές. Από εδώ και στο εξής, γίνεται αναφορά σε αυτές τις συσκευές ως «ενδιάμεσα σημεία». Τα *ενδιάμεσα σημεία* θα μπορούν να βρίσκονται σε σειρά με άλλα ενδιάμεσα σημεία, ενώ τελικά θα επικοινωνούν με ένα σημείο ελέγχου. Με αυτόν τον τρόπο, θα δημιουργηθεί μια δομή ιεραρχίας, η οποία θα εξασφαλίζει τη βελτιστοποίηση της δικτυακής κίνησης. Σε αυτό το σημείο αξίζει να αναφερθεί ένας άλλος περιορισμός που υπεισέρχεται στην παρούσα ανάλυση. Σε περίπτωση που τα ενδιάμεσα σημεία (ή κάποια ενδιάμεσα σημεία) τεθούν εκτός λειτουργίας, το σύστημα πρέπει έχει τη δυνατότητα να συνεχίσει να συμπεριφέρεται ορθά, με μόνη διαφορά την έλλειψη βελτιστοποίησης που τα

ενδιάμεσα σημεία προσέφεραν. Σε αυτήν την περίπτωση, το σύστημα πρέπει να μην αντιλαμβάνεται διαφορά, και να συνεχίσει να λειτουργεί ορθά, χωρίς παρενέργειες.

Με βάση τα προηγούμενα, η σχηματική πλέον δομή του υπό μελέτη και σχεδιασμό συστήματός πρέπει να είναι περίπου όπως φαίνεται παρακάτω στο Σχήμα 4.2.




**Σχήμα 4.2: Η δόμηση του συστήματός ελέγχου μετά από την εισαγωγή των ενδιάμεσων σημείων συνάθροισης.**

Σύμφωνα με το παραπάνω σχήμα, τα *ενδιάμεσα σημεία* λαμβάνουν τα έγγραφα περιγραφής αντικειμένων εκτελούν τη συναθροιστική συμπίεση πληροφορίας και κατόπιν τα προωθούν στο επόμενο κάθε φορά ενδιάμεσο σημείο, το οποίο εκτελεί την ίδια διαδικασία, λαμβάνοντας όμως και το συγκεντρωμένο έγγραφο περιγραφής του προηγούμενου ενδιάμεσου σημείου, το οποίο και χειρίζονται παρόμοια με μια απλή συσκευή. Τελικά, στο σημείο ελέγχου, θα φθάσει ένα τελικό συγκεντρωτικό έγγραφο, το οποίο θα περιέχει όλη την απαιτούμενη πληροφορία, συμπιεσμένη σε ένα μόλις (θεωρητικά αρκετά μικρότερο από ότι θα ήταν όλα τα αρχεία χωριστά) αρχείο XML (19). Φυσικά είναι εξαιρετικά σημαντικό το τελικό κείμενο να υπάρχει σε μορφή που να είναι

εύκολα αντιστρέψιμη, να είναι εύκολα δυνατή με άλλα λόγια η εξαγωγή της αρχικής μορφής των αρχείων, πριν τη διαδικασία της συνάθροισης.

Προτού αναλυθεί ο αλγόριθμος που χρησιμοποιήθηκε για την υλοποίηση του σχήματος συνάθροισης, κρίνεται απαραίτητο να τονισθούν κάποια σημεία που έχουν σχέση κυρίως με τη δυνατότητα του αλγορίθμου σε θέματα αποσυμπίεσης των συστατικών εγγράφων περιγραφής XML των συσκευών που ελέγχονται.

- Όπως είναι λογικό, το κύριο χαρακτηριστικό του αλγορίθμου πρέπει να είναι η λειτουργικότητά του, με άλλα λόγια η ικανότητά του να είναι πλήρως αντιστρέψιμος. Η συνένωση αρκετών χιλιάδων εγγράφων, πρέπει να είναι εφικτή με τον πλέον αποδοτικό και αντιστρέψιμο τρόπο, δεδομένων ορισμένων σημαντικών περιορισμών όπως είναι για παράδειγμα η περιορισμένη επεξεργαστική ισχύς[12] των ενδιάμεσων συναθροιστικών συστημάτων που εισήχθησαν στο δίκτυο καθώς και η προσπάθεια ελαχιστοποίησης της μεταδιδόμενης για σκοπούς ελέγχου κίνησης του δικτύου.
- Πρέπει η κρυπτογράφηση που θα εφαρμοσθεί (βλ. παράγραφο 4.2.3) να είναι αντιστρέψιμη στους τελικούς κόμβους ελέγχου (τα σημεία ελέγχου), εξασφαλίζοντας με αυτόν τον τρόπο την ορθότητα της πληροφορίας που καταφθάνει σε αυτούς.

Η δομή ενός τυπικού εγγράφου XML είναι αυτή που φαίνεται στο Σχήμα 4.1.

Έστω επίσης ότι υπάρχουν διάφορα άλλα έγγραφα XML της μορφής:

```
<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
 <specVersion>
  <major>1</major>
  <minor>0</minor>
 </specVersion>
 <device>
  <deviceType>urn:schemas-upnp-org:device:CURRENT_COUNTERdevice:1</deviceType>
  <friendlyName>UPnP Current Counter Emulator</friendlyName>
```

[12] Στην πραγματικότητα οι γενικότεροι περιορισμοί σε πόρους, όχι μόνο υπολογιστικής ισχύος.

```
  <manufacturer>Artemis Voulkidis by Intel Sample -- Update 1</manufacturer>
  <manufacturerURL>http://users.ntua.gr/el02045/ -- Update 1</manufacturerURL>
  <modelDescription>UPnP Current Counter Device Emulator 1.0</modelDescription>
  <modelName>CurrentCounterEmulator</modelName>
  <modelNumber>1.0</modelNumber>
  <modelURL>http://users.ntua.gr/el02045/Current_Counter/</modelURL>
  <serialNumber>123456789000 -- Update 1</serialNumber>
  <UDN>uuid:Upnp-Current_CounterEmulator-1_0-1234567890000 -- Update 1</UDN>
  <UPC>123456780 -- Update 1</UPC>
  <serviceList>
   <service>
    <serviceType>urn:schemas-upnp-org:service:CURRENT_COUNTERcontrol:1</serviceType>
    <serviceId>urn:upnp-org:serviceId:CURRENT_COUNTERcontrol:1</serviceId>
    <controlURL>/upnp/control/CURRENT_COUNTERcontrol1</controlURL>
    <eventSubURL>/upnp/event/CURRENT_COUNTERcontrol1</eventSubURL>
    <SCPDURL>/CURRENT_COUNTERcontrolSCPD.xml</SCPDURL>
   </service>
  </serviceList>
 <presentationURL>CURRENT_COUNTERdevicepres.html</presentationURL>
</device>
</root>
```

**Σχήμα 4.3: Το έγγραφο περιγραφής XML μιας συσκευής (τροποποιημένο).**

Δηλαδή έχει τη μορφή του εγγράφου του Σχήματος 4.1 με ανανεωμένες τις τιμές manufacturer, manufacturerURL, serialNumber, UDN και UPC. Η επιθυμητή λειτουργία της διαδικασίας της συνάθροισης είναι να αναγνωρίζει τα διαφορετικά πεδία στα διαφορετικά έγγραφα, και να ενοποιεί τις διαφορές σε ένα ενιαίο αρχείο, καταγράφοντας φυσικά και τον αύξοντα αριθμό του αρχείου, προκειμένου να υπάρχει ταυτοποίηση σε περίπτωση που συναθροίζονται παραπάνω από ένα αρχεία, περίπτωση που είναι και η πλέον πιθανή. Ειδικότερα, τα βήματα που ακολουθεί ο αλγόριθμος συνάθροισης (όταν εκτελεί συμπίεση πληροφορίας) είναι τα ακόλουθα:

1. Λήψη του αρχικού XML αρχείου περιγραφής, αναγνώριση του αριθμού των εγγράφων που αποτελούν το τρέχον συναθροισμένο έγγραφο περιγραφής και αντιγραφή του τελευταίου για περαιτέρω επεξεργασία.

2. Αντιγραφή των αρχικών τιμών ενδιαφέροντος του εγγράφου, και αποθήκευση αυτών.

3. Έλεγχος της τρέχουσας τιμής ενδιαφέροντος (πχ UDN) και στη συνέχεια ενημέρωση του συναθροισμένου εγγράφου περιγραφής. Μια πολύ βασική συνάρτηση που ορίσθηκε και η οποία εκτελεί τις λειτουργίες που απαιτούνται σε περίπτωση που ανιχνευθεί διαφορά μεταξύ της τιμής των υπαρχόντων και του τρέχοντος εγγράφου περιγραφής, είναι η updateElement, με ορισμό όπως παρακάτω:

```
void updateElement ( IXML_Document *doc, char *elementName,
                     char *elementValue, int docNumber );
```

   Η συνάρτηση αυτή είναι ιδιαίτερα κρίσιμη, εντούτοις, θα αναλυθεί λίγο αργότερα, εξηγώντας παράλληλα διάφορα κρίσιμα σημεία που σχετίζονται με την αναπαράσταση κατά DOM ενός εγγράφου XML.

4. Ενημέρωση του εγγράφου σχετικά με τον τρέχοντα αριθμό εγγράφων περιγραφής που το απαρτίζουν.

5. Προώθηση του συναθροισμένου εγγράφου περιγραφής, μετά την ενημέρωσή του, στον επόμενο ακολουθιακά κόμβο συνάθροισης για περαιτέρω επεξεργασία[13].

Η πολύ βασική συνάρτηση updateElement λαμβάνει ως όρισμα ένα έγγραφο τύπου IXML_Document (που είναι η DOM αναπαράσταση ενός XML εγγράφου, σύμφωνα με τις βιβλιοθήκες επεξεργασίας XML εγγράφων που καθορίζει η DOM αναπαράσταση, οι οποίες υλοποιούνται μέσω του συνόλου βιβλιοθηκών ixml στην παρούσα εφαρμογή), το όνομα και την τιμή της τιμής που μας ενδιαφέρει, καθώς επίσης και τον αύξων αριθμό της προς έλεγχο συσκευής, ο οποίος φυσικά νοείται ως μοναδικός. Ο κώδικας που αναλαμβάνει την ανανέωση των υπαρχόντων τιμών στο συναθροισμένο έγγραφο, συνοψίζεται (παραλείποντας τους σχετικούς ελέγχους) στα παρακάτω:

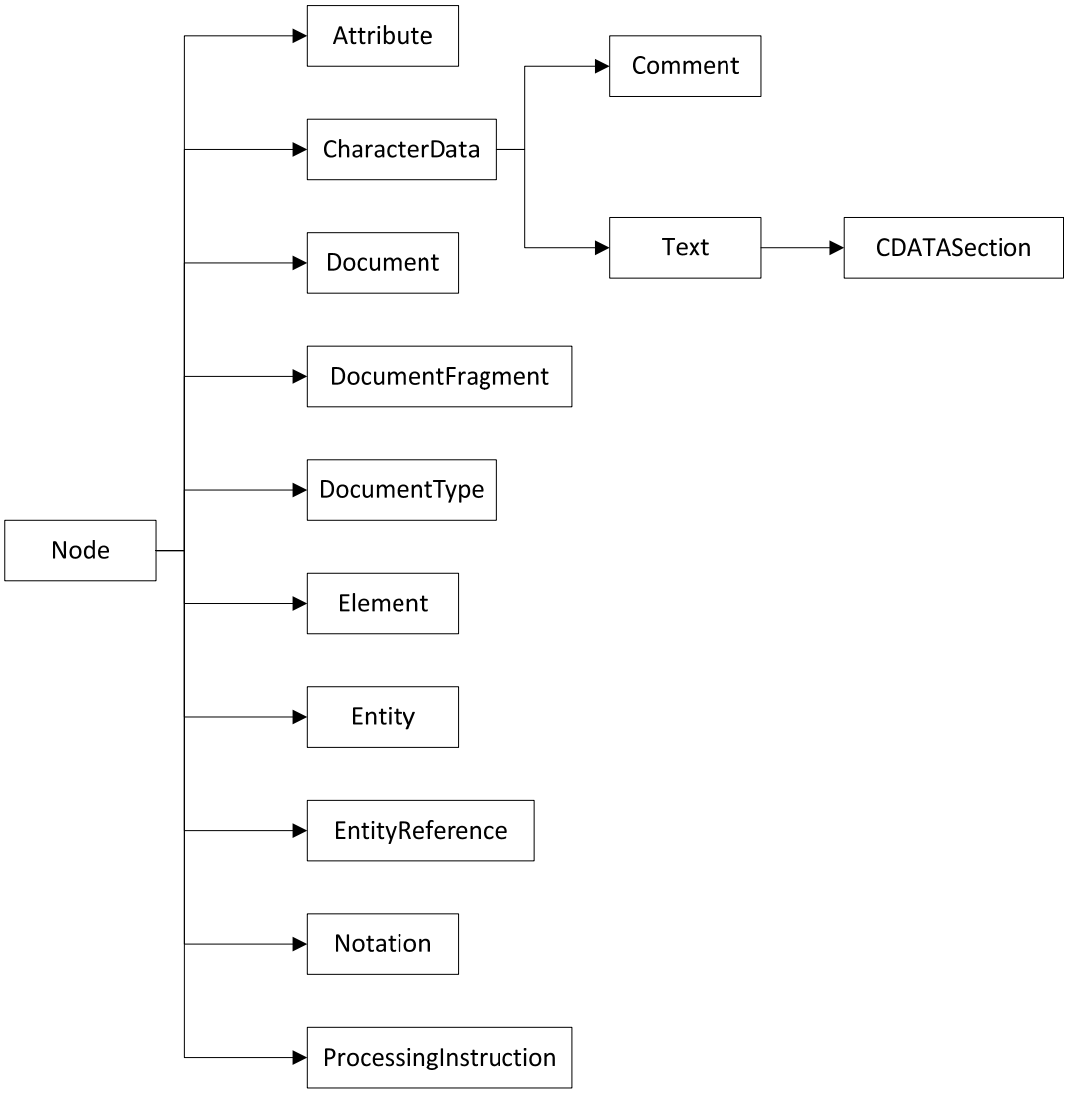
[13] Αμελείται επί του παρόντος την, ούτως ή άλλως αυτόνομη, διεργασία κωδικοποίησης, περιγραφή της οποίας ακολουθεί σε επόμενη παράγραφο.

```
element = ixmlDocument_createElement(doc, elementName);
if(elementValue != NULL) {
        text = ixmlDocument_createTextNode(doc, elementValue);
        ixmlNode_appendChild((IXML_Node*) element, text);
}
domNumber = (DOMString)itoa(docNumber,10);
int ret = ixmlElement_setAttribute ( element, "docNumber", domNumber );
IXML_NodeList *nList= ixmlDocument_getElementsByTagName(doc,"device");
IXML_Element *deviceElement = (IXML_Element *) ixmlNodeList_item ( nList, 0 );
ixmlNode_appendChild((IXML_Node *)deviceElement, element);
```

**Σχήμα 4.4: Ο κώδικας της updateElement**

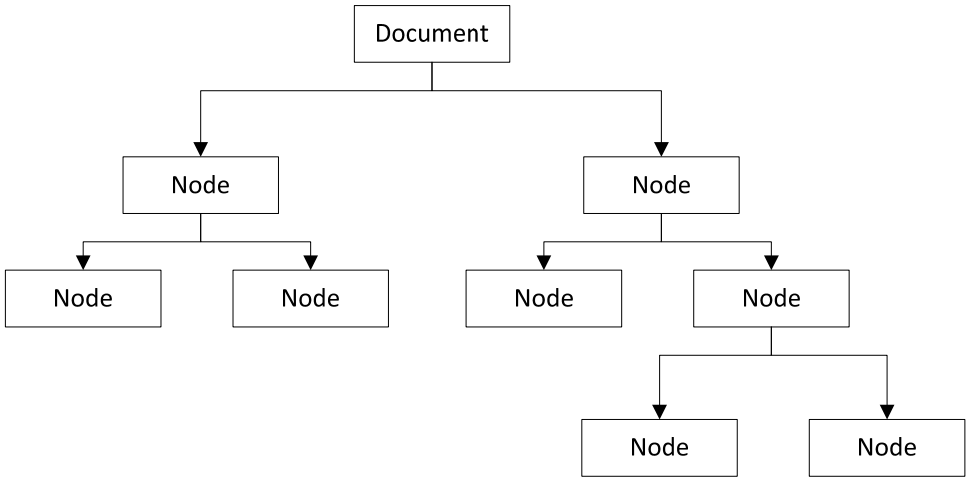
Προκειμένου να γίνει καλύτερα αντιληπτός ο τρόπος λειτουργίας αυτής της συνάρτησης, πρέπει να γίνει εν τάχει αναφορά στα χαρακτηριστικά του DOM interface, ως τρόπου αναπαράστασης XML αρχείων.

Το Document Object Model (DOM) (20) βοηθά στη θεώρηση της δενδρικής μορφής του XML κειμένου με αντικειμενοστραφή τρόπο και στην επέμβαση σε αυτό με συγκεκριμένα interfaces. Με το XML DOM μπορεί να δημιουργηθεί ένα XML κείμενο, να πραγματοποιηθούν διαδικασίες πλοήγησης μέσα σε αυτό και να προστεθούν, μεταβληθούν και να αφαιρεθούν στοιχεία του. Το XML κείμενο περνά από έναν parser, ο οποίος δημιουργεί και τα σχετικά αντικείμενα όπως προδιαγράφει το DOM. Με τα διατιθέμενα interfaces γίνονται οι επιθυμητές επεξεργασίες και κατόπιν, αν κάτι τέτοιο είναι επιθυμητό, δημιουργείται ένα νέο παραλλαγμένο κατά τις επιθυμίες του διαχειριστή του συστήματος XML κείμενο. Κεντρική ιδέα του DOM είναι το Node Object με το αντίστοιχό του Node Interface. Όμως εδώ σαν Node (κόμβος) νοείται όχι μόνον το κάθε στοιχείο (element) του XML, αλλά εκτός του Element Node, υπάρχει το Attribute Node, το Text Node, το CDATA Node και άλλα περιφερειακής σημασίας. Η όλη δενδρική δομή, στην οποία εντάσσεται κατά DOM κάθε κείμενο XML, δίδεται στο σχήμα που ακολουθεί.



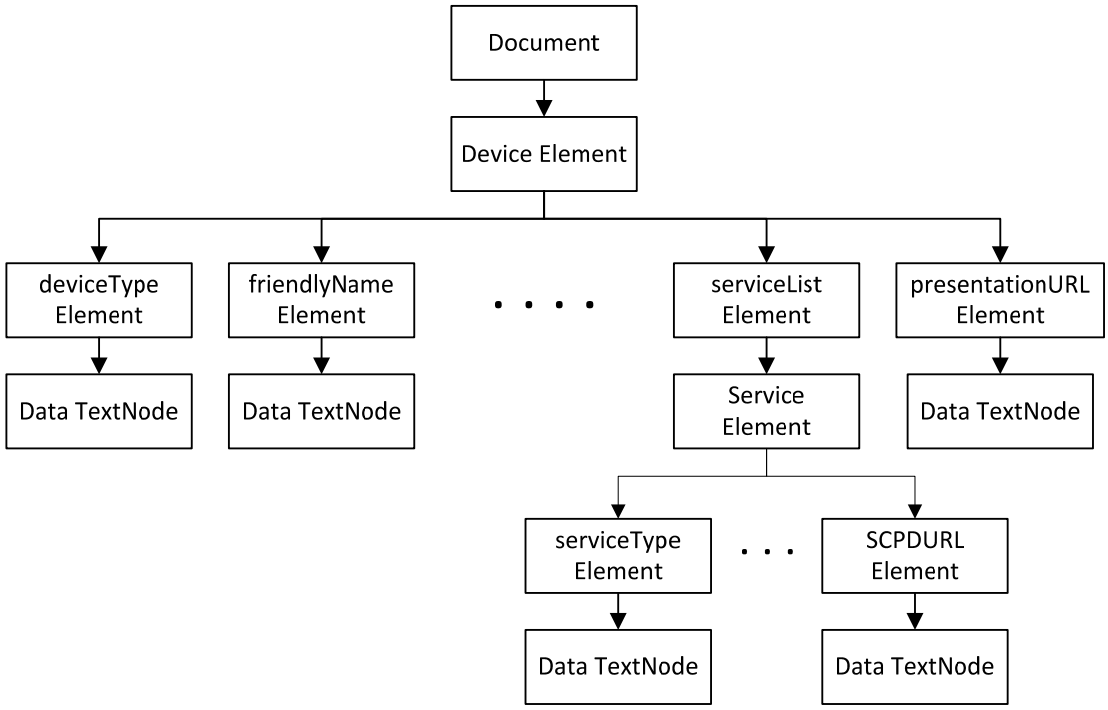

**Σχήμα 4.5: Εικονική αναπαράσταση της κατά DOM ιεραρχίας.**

Αξίζει να σημειωθούν κάποια πράγματα σχετικά με το παραπάνω σχήμα. Κατ' αρχήν παρατηρείται ότι τα πάντα σε μια κατά DOM αναπαράσταση ενός XML αρχείου είναι κόμβοι (Nodes) όπως εξ άλλου προαναφέρθηκε. Εκτός αυτού, παρατηρείται ότι υπάρχουν διάφοροι τύποι από Nodes, όπως για παράδειγμα Attribute, Document, Element κτλ. Φυσικά μια τέτοια αναπαράσταση δεν είναι ικανή να παρουσιάσει τη μορφή που έχει ένα ολοκληρωμένο έγγραφο XML. Στην πραγματικότητα, για την ολοκληρωμένη αναπαράσταση ενός XML αρχείου, πρέπει να παρατεθεί εκτός της προηγούμενης, και το επόμενο σχήμα:



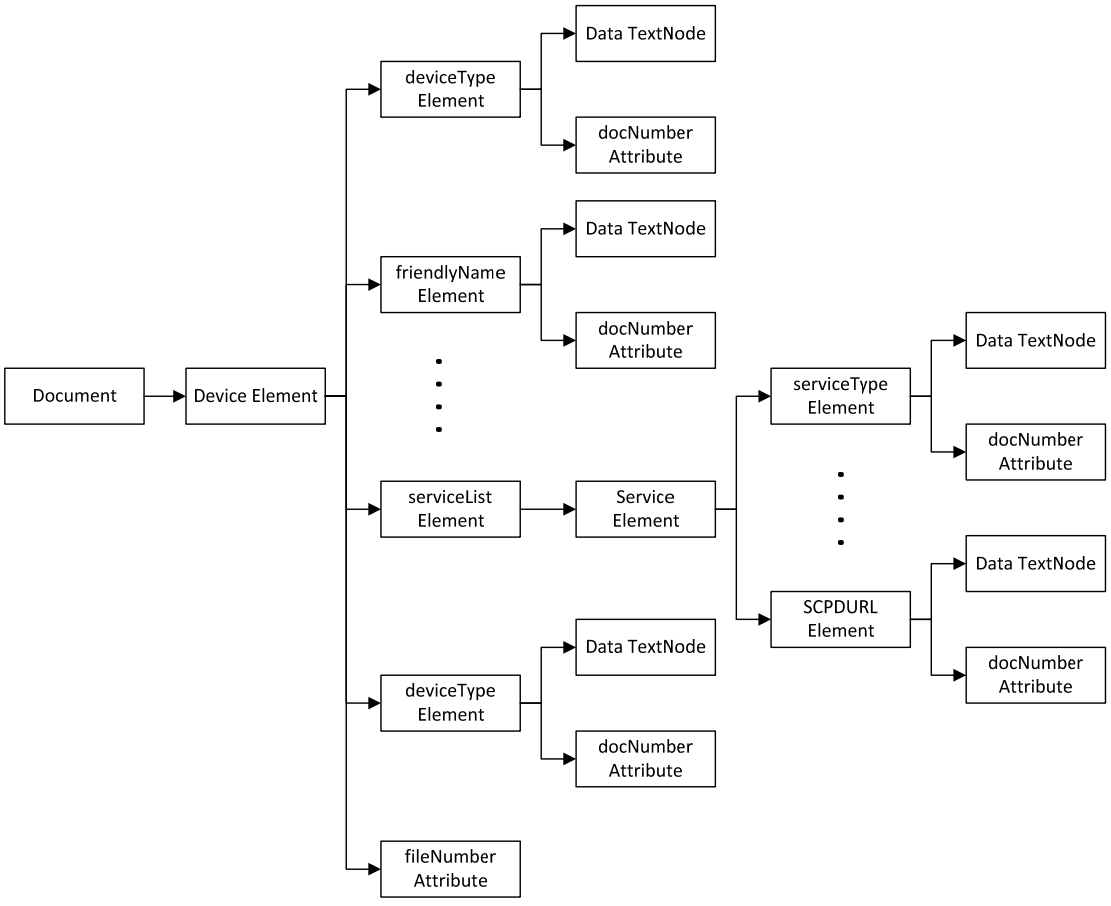

Σχήμα 4.6: Τυπική DOM δομή ενός τυχαίου XML εγγράφου.

Η παρουσίαση τώρα είναι σαφώς πιο ολοκληρωμένη. Συνδυάζοντας τα δύο προηγούμενα σχήματα, προκύπτει εύκολα το συμπέρασμα, ότι η ορθή κατά DOM μορφή ενός XML εγγράφου, αποτελείται από έναν κόμβο τύπου Document, ο οποίος στη συνέχεια αποτελείται από διαφορετικούς κόμβους, όπως Elements, Attributes, Comments κτλ. Υπάρχει δηλαδή μια δενδρική δομή, η οποία καθορίζει τον τρόπο με τον οποίο μπορούν να προσπελασθούν τα δεδομένα, να γίνουν αντικείμενα επεξεργασίας και στη συνέχεια να ενημερωθούν. Στην παρούσα εφαρμογή, η δομή του ορθού εγγράφου περιγραφής μια συσκευής έχει τη μορφή:




Σχήμα 4.7: Η ακριβής κατά DOM δομή του XML εγγράφου περιγραφής μιας συσκευής.

Με βάση τα όσα ανωτέρω αναλύθηκαν, καθίσταται πλέον ευκολότερη η ερμηνεία του κώδικα του Σχήματος 4.4 που παρουσιάζει το κυρίως κομμάτι κώδικα της updateElement. Έτσι, αρχικά δημιουργείται ένα νέο element Node, και προστίθεται σε αυτό (με τη μέθοδο ixmlNode_appendChild) ένα νέο Node (TextNode), που περιέχει την πληροφορία που πρέπει να προστεθεί. Στη συνέχεια, προστίθεται ένα νέο Attribute Node στο Element αυτό, το οποίο ονομάζεται docNumber και περιέχει τον αύξοντα αριθμό του αντικειμένου που το περιείχε πριν τη συνάθροιση. Τέλος, εισάγεται το νέο αυτό Element στο ήδη υπάρχον device Element, ανανεώνοντας με αυτόν τον τρόπο την υπάρχουσα πληροφορία του συναθροισμένου εγγράφου. Η τελική δομή κατά DOM ενός συναθροισμένου εγγράφου περιγραφής είναι:




**Σχήμα 4.8: Η κατά DOM αναπαράσταση του συναθροισμένου XML εγγράφου των συσκευών.**

Παραδειγματικά, και για περαιτέρω οπτικοποίηση όλων των ανωτέρω, έστω ότι υπάρχουν τέσσερα τροποποιημένα έγγραφα περιγραφής από τέσσερις υποτιθέμενες άλλες συσκευές που ανήκουν στην ίδια περιφέρεια ελέγχου, με μορφή που φαίνεται από το Σχήμα 4.3. Σε αυτήν την περίπτωση, το συναθροισμένο έγγραφο που προκύπτει, απεικονίζεται στην  που ακολουθεί.

```
<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
<specVersion>
<major>1</major>
<minor>0</minor>
</specVersion>
<device fileNumber="4">
<deviceType>urn:schemas-upnp-org:device:CURRENT_COUNTERdevice:1</deviceType>
<friendlyName>UPnP Current Counter Emulator</friendlyName>
<modelDescription>UPnP Current Counter Device Emulator 1.0</modelDescription>
<modelName>CurrentCounterEmulator</modelName>
<modelNumber>1.0</modelNumber>
<modelURL>http://users.ntua.gr/el02045/Current_Counter/</modelURL>
<serviceList>
<service>
<serviceType>urn:schemas-upnp-org:service:CURRENT_COUNTERcontrol:1</serviceType>
<serviceId>urn:upnp-org:serviceId:CURRENT_COUNTERcontrol:1</serviceId>
<controlURL>/upnp/control/CURRENT_COUNTERcontrol1</controlURL>
<eventSubURL>/upnp/event/CURRENT_COUNTERcontrol1</eventSubURL>
<SCPDURL>/CURRENT_COUNTERcontrolSCPD.xml</SCPDURL>
</service>
</serviceList>
<presentationURL>CURRENT_COUNTERdevicepres.html</presentationURL>
<serialNumber>123456789000 -- Update 1</serialNumber>
<UPC>123456780 -- Update 1</UPC>
<UDN>uuid:Upnp-Current_CounterEmulator-1_0-1234567890000 -- Update 1</UDN>
<manufacturer>Artemis Voulkidis by Intel Sample -- Update 1</manufacturer>
<manufacturerURL>http://users.ntua.gr/el02045/ -- Update 1</manufacturerURL>
<manufacturer docNumber="1">Artemis Voulkidis by Intel Sample -- Update 2</manufacturer>
<manufacturerURL docNumber="1">http://users.ntua.gr/el02045/ -- Update 2</manufacturerURL>
<serialNumber docNumber="1">123456789000 -- Update 2</serialNumber>
<UDN docNumber="1">uuid:Upnp-Current_CounterEmulator-1_0-1234567890000 -- Update 2</UDN>
<UPC docNumber="1">123456780 -- Update 2</UPC>
<manufacturer docNumber="2">Artemis Voulkidis by Intel Sample -- Update 3</manufacturer>
<manufacturerURL docNumber="2">http://users.ntua.gr/el02045/ -- Update 3</manufacturerURL>
<serialNumber docNumber="2">123456789000 -- Update 3</serialNumber>
<UDN docNumber="2">uuid:Upnp-Current_CounterEmulator-1_0-1234567890000 -- Update 3</UDN>
<UPC docNumber="2">123456780 -- Update 3</UPC>
<manufacturer docNumber="3">Artemis Voulkidis by Intel Sample -- Update 4</manufacturer>
<manufacturerURL docNumber="3">http://users.ntua.gr/el02045/ -- Update 4</manufacturerURL>
<serialNumber docNumber="3">123456789000 -- Update 4</serialNumber>
<UDN docNumber="3">uuid:Upnp-Current_CounterEmulator-1_0-1234567890000 -- Update 4</UDN>
<UPC docNumber="3">123456780 -- Update 4</UPC>
</device>
</root>
```

**Σχήμα 4.9: Συναθροισμένο έγγραφο τεσσάρων επιμέρους εγγράφων περιγραφής XML.**

Η συνάθροιση έχει ολοκληρωθεί σωστά, με τις επιμέρους πληροφορίες να εμφανίζονται ακέραιες στο νέο έγγραφο, δείγμα της ορθής διαχείρισης που υφίσταται η πληροφορία, ως προς την ορθότητα και ταυτοποίηση αυτής. Με αυτόν τον τρόπο λοιπόν διασφαλίζεται η εγκυρότητα της πληροφορίας που προωθείται στα σημεία ελέγχου προς περαιτέρω επεξεργασία. Μετά τη λήψη του ολικού συναθροισμένου εγγράφου περιγραφής συσκευών μιας περιφέρειας, τα σημεία ελέγχου πρέπει να έχουν τη δυνατότητα να εξάγουν τα

επιμέρους δομικά έγγραφα περιγραφής XML των συσκευών της περιφέρειας, για να μπορέσουν να λάβουν την πληροφορία που θέλουν. Έτσι τίθεται το θέμα της αποσυμπίεσης του ολικού εγγράφου, και η ανάκτηση της αρχικής πληροφορίας, στη μορφή που ήταν αρχικά και πριν τη συνάθροιση, προκειμένου να μην επηρεαστεί η συμβατότητα με το πρότυπο standard που ακολουθεί το πρωτόκολλο UPnP.

Η διαδικασία της από συμπίεσης και εξαγωγής της πληροφορίας που ενδιαφέρει το σημείο ελέγχου περιλαμβάνει τρία επιμέρους στάδια:

1. Αναγνώριση του αριθμού των συστατικών XML εγγράφων,
2. Εξαγωγή της πληροφορίας ξεχωριστά για κάθε συστατικό έγγραφο και μορφοποίηση αυτού στην προτυποποιημένη του μορφή, και τέλος
3. Παροχή των ανεξάρτητων πλέον συστατικών εγγράφων στο σημείο ελέγχου.

Στο πρώτο στάδιο (απαραίτητο για την ορθή εξαγωγή των επιμέρους πληροφοριών του συναθροισμένου XML εγγράφου) προσδιορίζεται ο συνολικός αριθμός των συσκευών που συνεισέφεραν στη δημιουργία του εγγράφου αυτού. Έχει ήδη αναφερθεί ότι κάθε φορά που ανανεώνεται το ολικό έγγραφο, ανανεώνεται και η τιμή που καταδεικνύει τον ολικό αριθμό των συστατικών εγγράφων. Η ύπαρξη αυτής της πληροφορίας στο τελικό έγγραφο είναι ζωτικής σημασίας καθώς καθορίζει σε απόλυτο βαθμό την ορθότητα και την ακεραιότητα της εξαγόμενης πληροφορίας. Αυτό ισχύει λόγω της επαναληπτικής φύσης της διαδικασίας της αποσυμπίεσης. Πιο συγκεκριμένα, μόλις το σημείο ελέγχου λάβει το συναθροισμένο έγγραφο που περιμένει, εκκινεί μια επαναληπτική διαδικασία για την εξαγωγή της πληροφορίας του εκάστοτε εγγράφου. Η διαδικασία αυτή επαναλαμβάνεται τόσες φορές όσα είναι τα συστατικά έγγραφα, αποφέροντας κάθε φορά ένα ανεξάρτητο, ορθά μορφοποιημένο κατά το πρότυπο του UPnP πρωτοκόλλου XML έγγραφο περιγραφής.

Σε κάθε επανάληψη, θεωρείται ένα νέο έγγραφο περιγραφής XML, το οποίο στη συνέχεια δομείται σταδιακά ανά Element Node, μέχρι και την τελική ολοκλήρωση του εγγράφου. Οι δύο βασικές συναρτήσεις που χρησιμοποιήθηκαν είναι οι getAggregatedElementValue και addDataToDocument, με αντίστοιχους ορισμούς:

```
char *getAggregatedElementValue ( IXML_Document *doc, char *elementName,
                                  int fileNumber,  int elementCount );

void addDataToDocument( IXML_Document *doc, char *elementName,
                        char *elementValue);
```

Η πρώτη από αυτές, δέχεται στην κλήση της ως ορίσματα το συναθροισμένο έγγραφο, το όνομα του Element που πρέπει να βρεθεί, τον αύξοντα αριθμό του εγγράφου το οποίο είναι το σημείο ενδιαφέροντος, και τον αριθμό των διαφοροποιημένων από το πρώτο επιμέρους έγγραφο περιγραφής XML που υπάρχει στο ολικό έγγραφο Element Nodes. Η τελευταία παράμετρος είναι σημαντική για θέματα επίδοσης, καθώς σε ένα έγγραφο για το οποίο εξ αρχής είναι γνωστός ο αριθμός των διαφοροποιημένων στοιχείων του, δεν πραγματοποιούνται άσκοπες επαναλήψεις ανεύρεσης νέων αλλαγών. Το γεγονός αυτό είναι ιδιαίτερα σημαντικό σε περιπτώσεις με μεγάλο αριθμό εγγράφων, όπου οι διαρκείς (άσκοπες) επαναλήψεις μπορούν να αποτελέσουν στενωπό επίδοσης του συστήματος, δεδομένου ότι οι υπολογιστικοί πόροι των διαθέσιμων υπολογιστικών μηχανών είναι περιορισμένοι, και ότι η ταχύτητα του συστήματος είναι σημαντική για την αξιοπιστία των αποτελεσμάτων που εξάγονται. Η μέθοδος getAggregatedElementValue λειτουργεί όπως καταδεικνύει και το όνομά της: λαμβάνει και δίνει ως έξοδο από το συναθροισμένο έγγραφο, την τιμή του Element Node το όνομα του οποίου διοχετεύεται στη συνάρτηση ως είσοδος.

Αναφέρθηκε νωρίτερα, πως για κάθε έγγραφο XML που πρέπει να «ληφθεί» από το ολικό έγγραφο, , θεωρείται ένα νέο έγγραφο, το οποίο στη συνέχεια δομείται σταδιακά ανά Element Node, μέχρι την τελική ολοκλήρωσή του. Σε αυτό το σημείο είναι ιδιαίτερα σημαντική η κλήση της συνάρτησης addDataToDocument, η οποία δεχόμενη ως εισόδους το νεοδημιουργηθέν έγγραφο, το όνομα ενός Element Node και την αντίστοιχη τιμή αυτού όπως λήφθηκε από την κλήση της getAggregatedElementValue, ανανεώνει το τρέχον έγγραφο με τις κατάλληλες τιμές, σε μορφή συμβατή με το πρότυπο που χρησιμοποιείται από την εφαρμογή (UPnP). Η δομή της είναι εξαιρετικά απλή, και μπορεί εύκολα να τροποποιηθεί σύμφωνα με τις ανάγκες της εκάστοτε εφαρμογής.

Μετά το πέρας της αποσυμπίεσης, το σημείο ελέγχου μπορεί πλέον να λάβει τα έγγραφα περιγραφής των συσκευών που ανήκουν στην περιφέρεια διαχείρισης του, και να προχωρήσει στις ενέργειες που καθορίζει ο διαχειριστής του συστήματος.

Στη συνέχεια, αναλύεται ένα άλλο κρίσιμο κομμάτι της εφαρμογής, η κρυπτογράφηση. Η τεχνική αυτή, που αφορά την προστασία του συστήματος σε περιπτώσεις επίθεσης, επιτρέπει στην εφαρμογή να μπορεί να ανανήψει μετά από κάποια κακόβουλη επίθεση, ή κάποια δυσλειτουργία του δικτύου που θα μπορούσε ενδεχομένως να αλλοιώσει τα δεδομένα που στέλνονται από τις συσκευές στα σημεία ελέγχου και το αντίστροφο, προσφέροντας με αυτόν τον τρόπο ένα είδος ασφάλειας στο σύστημα που εφαρμόζεται.

## 4.2 Κρυπτογράφηση

### 4.2.1 Γενικά για την Κρυπτογράφηση

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά "κρυπτός" και "γράφω", και είναι ο επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας, η οποία ασχολείται με την μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς ώστε 2 ή περισσότερες οντότητες να μπορούν να επικοινωνήσουν χωρίς κάποια άλλη οντότητα να είναι ικανή να αντιλαμβάνεται την πληροφορία. Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη "κρυπτός" και την λέξη "λόγος" και χωρίζεται σε δύο κλάδους: την Κρυπτογραφία και την Κρυπτανάλυση. Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή μετατροπή της πληροφορίας από μια κανονική κατανοητή μορφή σε έναν γρίφο, που χωρίς την γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στην γλωσσική δομή. Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση.

Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες, οι οποίες αποτελούν παράλληλα και τους αντικειμενικούς της στόχους (21). Οι λειτουργίες αυτές είναι οι:

- **Εμπιστευτικότητα:** Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στις εξουσιοδοτημένες οντότητες. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- **Ακεραιότητα:** Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- **Μη απάρνηση:** Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- **Πιστοποίηση**: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

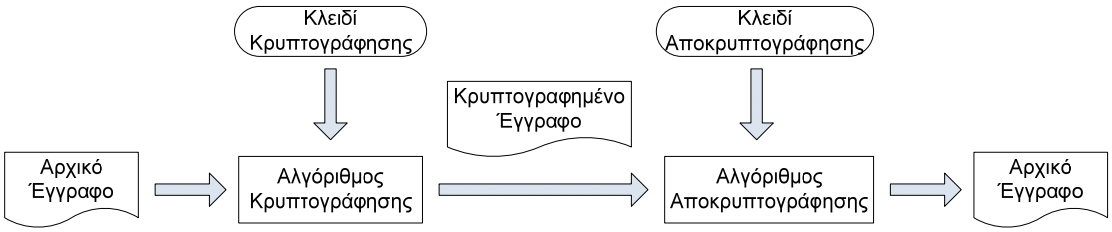
#### 4.2.1.1 Ορολογία – Βασικές έννοιες

Προτού γίνει αναφορά στο σχήμα κρυπτογράφησης που χρησιμοποιήθηκε στην εφαρμογή, κρίνεται σκόπιμο παρατεθούν εν συντομία κάποιοι βασικοί ορισμοί που θα διευκολύνουν την ανάγνωση του κειμένου του κεφαλαίου αυτού. Ορισμένοι από τους κρισιμότερους ορισμούς παρατίθενται κάτωθι:

- **Κρυπτογράφηση (encryption)**: Η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με την χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.
- **Αποκρυπτογράφηση (decryption)**: Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα.
- **Κρυπτογραφικός αλγόριθμος (cipher)**: Η μέθοδος μετασχηματισμού δεδομένων σε μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.
- **Αρχικό κείμενο (plaintext):** Το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης. Στην περίπτωση της παρούσας εφαρμογής τα πακέτα XML που ανταλλάσσονται μεταξύ των διαφόρων οντοτήτων του συστήματος.
- **Κλειδί (key):** Αριθμός (αρκετών bit) που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης.
- **Κρυπτογραφημένο κείμενο (ciphertext):** Το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.
- **Κρυπτανάλυση (cryptanalysis):** Η επιστήμη που ασχολείται με το «σπάσιμο» κάποιας κρυπτογραφικής τεχνικής, ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκρυπτογραφηθεί.

#### 4.2.1.2 Η διαδικασία της κρυπτογράφησης

Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα:




**Σχήμα 4.10: Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης.**

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης. Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στην μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bit. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

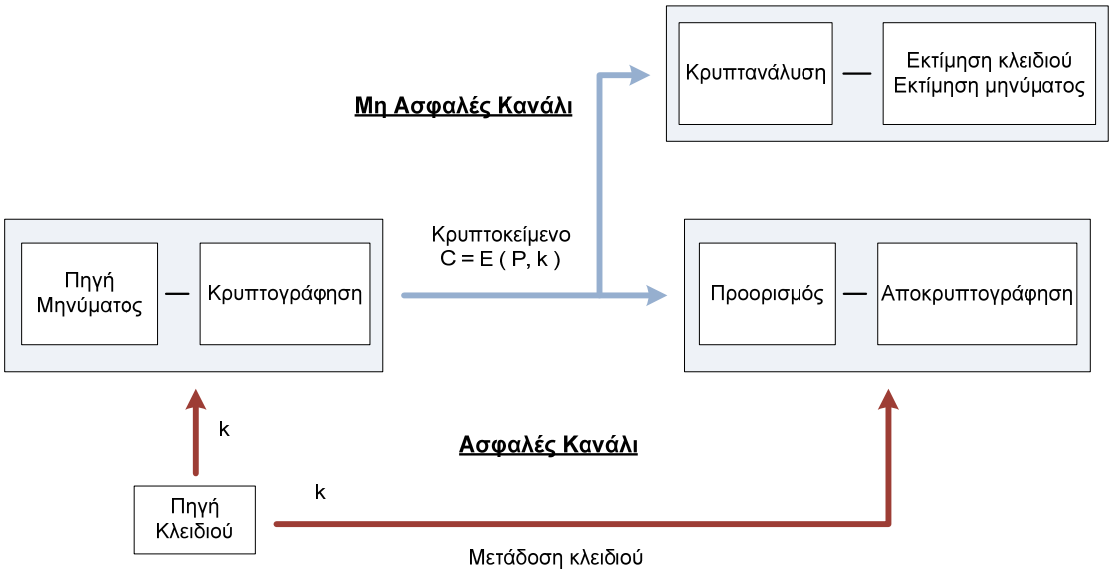
Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει την δυνατότητα σε 2 οντότητες, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε μια τρίτη, μη εξουσιοδοτημένη (ένας αντίπαλος – attacker), να μη μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P,C,k,E,D), όπου

- Ρ είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων,
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων,
- k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος,
- Ε είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση, και
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης.

Η συνάρτηση κρυπτογράφησης Ε δέχεται δύο παραμέτρους, μέσα από τον χώρο Ρ και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, τον χώρο C και τον χώρο k και παράγει

μια ακολουθία που ανήκει στον χώρο P. Για την καλύτερη κατανόηση των παραπάνω εννοιών, παρατίθεται το Σχήμα 4.11:




Σχήμα 4.11: Τυπικό Μοντέλο Συστήματος Κρυπτογραφίας (κρυπτοσυστήματος)

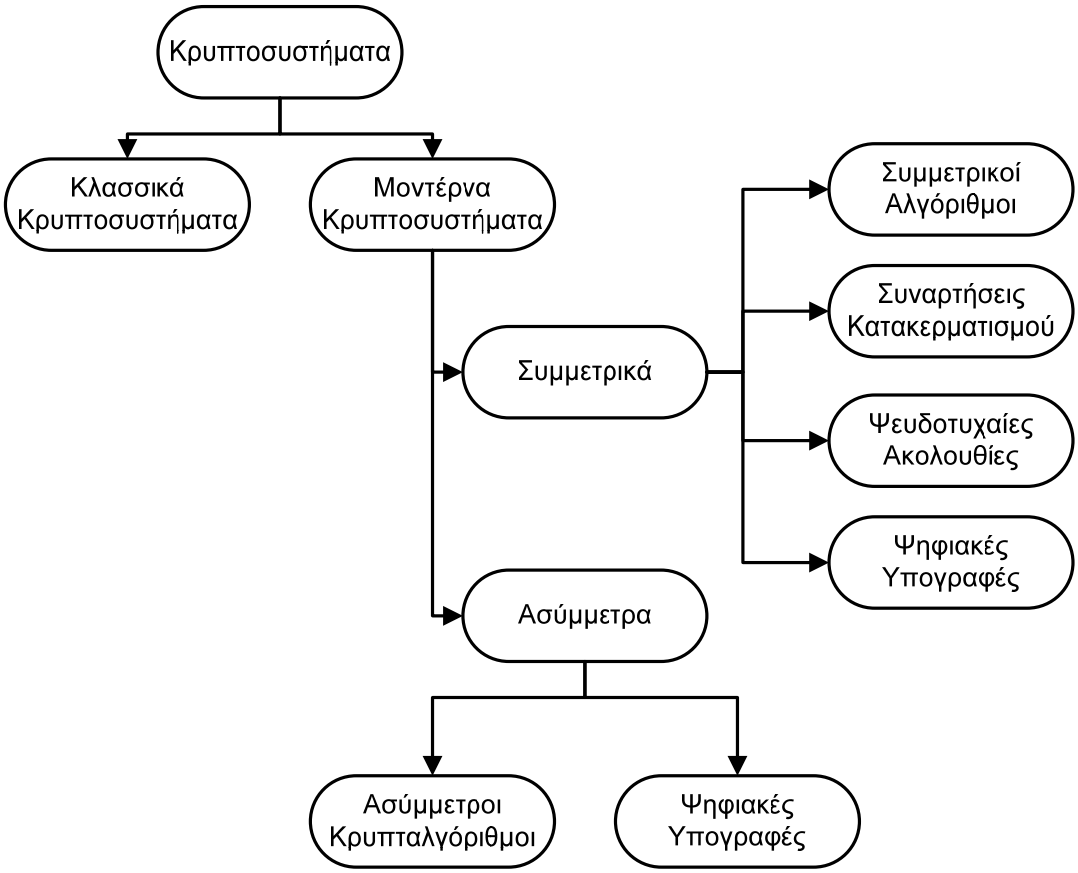
Το ανωτέρω κρυπτογραφικό σύστημα λειτουργεί με τον ακόλουθο τρόπο:

1. ο αποστολέας επιλέγει ένα κλειδί μήκους n από τον χώρο κλειδιών με τυχαίο τρόπο, όπου τα n στοιχεία του K είναι στοιχεία από ένα πεπερασμένο αλφάβητο.
2. Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.
3. Ο αποστολέας δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων.
4. Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (έναν γρίφο) και η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.
5. Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις 2 τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

Ο αντίπαλος που παρακολουθεί την επικοινωνία, ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση για την κλείδα που χρησιμοποιήθηκε και δεν μπορεί να αναδημιουργήσει το μήνυμα. Αν ο αντίπαλος επιλέξει να παρακολουθεί όλα τα μηνύματα θα προσανατολιστεί στην εξεύρεση του κλειδιού. Αν ο αντίπαλος ενδιαφέρεται μόνο για το υπάρχον μήνυμα θα παράγει μια εκτίμηση για την πληροφορία του μηνύματος.

### 4.2.2 Είδη κρυπτοσυστημάτων

Τα είδη κρυπτοσυστημάτων[14] χωρίζονται σε δύο μεγάλες κατηγορίες, τα Κλασσικά και τα μοντέρνα Κρυπτοσυστήματα. Όπως είναι φυσικά αναμενόμενο, οι δύο αυτές κατηγορίες χωρίζονται σε άλλες μικρότερες, σύμφωνα με το Σχήμα 4.12:




**Σχήμα 4.12: Είδη κρυπτοσυστημάτων**

Καθώς τα κλασσικά κρυπτοσυστήματα (με μερική γνώση του αρχικού κειμένου) είναι δυνατόν, σχετικά εύκολα με τα σημερινά υπολογιστικά δεδομένα, να «σπάσουν», η περαιτέρω ανάλυση θα περιοριστεί στα μοντέρνα συστήματα κρυπτογράφησης που θεωρούνται και τα πλέον ανεπτυγμένα και ασφαλή. Τα μοντέρνα κρυπτοσυστήματα χωρίζονται επίσης σε δύο μεγάλες κατηγορίες, τα συμμετρικά και τα ασύμμετρα υποσυστήματα, τα οποία και αναλύονται στη συνέχεια.

[14] Η έννοια του κρυπτοσυστήματος είναι διαφορετική από αυτή του συστήματος κρυπτογράφησης, καθώς ο όρος κρυπτοσύστημα αναφέρεται στο σύνολο των αλγορίθμων που είναι ικανοί να υλοποιήσουν μια δεδομένη μορφή (από)κρυπτογράφησης, ενώ δεύτερος όρος αναφέρεται στην υπολογιστική μηχανή που εμπεριέχει στοιχεία κρυπτογραφικής δραστηριότητας.

#### *4.2.2.1 Συμμετρική κρυπτογραφία*

Η συμμετρική κρυπτογραφία, γνωστή και ως κρυπτογραφία μυστικού κλειδιού, είναι σε χρήση εδώ και εκατοντάδες χρόνια, με διάφορες μορφές, που ποικίλουν από πολύ απλούς γρίφους αντικατάστασης μέχρι ιδιαίτερα πολύπλοκες δομές. Παρόλα αυτά, η ανάπτυξη τόσο των μαθηματικών όσο και της διαθέσιμης υπολογιστικής ισχύος έχουν καταστήσει δυνατή τη δημιουργία αλγορίθμων που είναι πρακτικά αδύνατο να σπάσουν. Τα συμμετρικά κρυπτοσυστήματα είναι γενικώς πολύ αποκρίσιμα αλλά και σχετικά ευπαθή, επειδή το κλειδί που χρησιμοποιείται για την κωδικοποίηση πρέπει να είναι γνωστό και κοινό μεταξύ των οντοτήτων που πρέπει να αποκρυπτογραφήσουν το μήνυμα. Ο αλγόριθμος DES της IBM έχει χρησιμοποιηθεί ευρέως στο παρελθόν, αλλά πλέον βρίσκεται σε στάδιο αχρηστίας και τείνει προς αντικατάσταση. Σε κάθε περίπτωση, είναι ιδιαίτερα σημαντικό στους εκάστοτε σχεδιαστές συστημάτων να μελετούν τον αλγόριθμο που κατασκευάζουν ή χρησιμοποιούν, λαμβάνοντας σοβαρά υπόψη τις ανταλλαγές χρόνου, υπολογιστικής ισχύος και ανθεκτικότητας του αλγορίθμου, για τη βελτιστοποίηση της απόδοσης του υπό σχεδίαση συστήματος.

Η συμμετρική κρυπτογράφηση, ή αλλιώς κρυπτογράφηση κρυφού κλειδιού, είναι σε χρήση εδώ και εκατοντάδες χρόνια, και περιλαμβάνει κάθε μορφή κωδικοποίησης όπου το ίδιο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση το εκάστοτε μήνυμα. Μια από τις απλούστερες μορφές είναι γνωστή και ως αλγόριθμος του Καίσαρα – τη χρησιμοποιούσε ο Ιούλιος Καίσαρας για να κρυπτογραφήσει τα μηνύματά του, σύμφωνα με την οποία το κάθε γράμμα του μηνύματος αντικαθίστατο με ένα άλλο, μετά από ολίσθηση *n* θέσεων. Μια παραλλαγή αυτού του απλού αλγόριθμου, θα μπορούσε να περιλαμβάνει τη χρήση ενός αυθαιρέτως ταξινομημένου αλφάβητου ίδιου μεγέθους με αυτό του αρχικού μηνύματος. Σε αυτήν την περίπτωση το κλειδί θα μπορούσε να είναι μια μακρά ακολουθία αριθμών όπως για παράδειγμα 5, 19, 1, 2, 11, … η οποία θα καταδείκνυε ότι το Α αντιστοιχεί στο Ε, το Β στο Σ, το Γ στο Α, το Δ στο Β, το Ε στο Κ κοκ. Τέτοια συστήματα είναι εξαιρετικά ευάλωτα, και αυτό είχε ως αποτέλεσμα τα μοντέρνα συστήματα να χρησιμοποιούν αλγορίθμους βασισμένους σε μαθηματικά προβλήματα που είναι δύσκολο να λυθούν, καθιστώντας τους αλγόριθμους πολύ στιβαρούς (22) και ανθεκτικούς σε επιθέσεις.

Η συμμετρική κρυπτογράφηση απαιτεί το κλειδί να είναι γνωστό αλλά ταυτόχρονα να παραμένει κρυφό στα πλαίσια μιας καθορισμένης ομάδας. Αυτό συμβαίνει καθώς θα ήταν αδύνατο σε μια οντότητα η οποία θεωρητικά θα όφειλε να έχει τη δυνατότητα να δει τα

δεδομένα, να κάνει κάτι τέτοιο χωρίς να έχει πρόσβαση στο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση των δεδομένων νωρίτερα. Φυσικά σε περίπτωση το κλειδί αυτό μαθευτεί από κάποια μη εξουσιοδοτημένη οντότητα, το αποτέλεσμα μπορεί να είναι καταστροφικό. Υπό αυτήν την έννοια, το κοινό πρόβλημα όλων των συστημάτων που διατηρούν τη μυστικότητα του κλειδιού, είναι το πρόβλημα της διαχείρισης των κλειδιών.

Συχνά γίνεται λόγος σχετικά με κλειδιά συγκεκριμένου μεγέθους, όπως 56-bit ή 128-bit. Αυτά τα μεγέθη είναι εκείνα που χρησιμοποιούνται από τους αλγορίθμους συμμετρικής κωδικοποίησης, ενώ τα μεγέθη των κλειδιών που χρησιμοποιείται στους ασύμμετρους αλγόριθμους - τουλάχιστον στο κρυφό τμήμα αυτών - είναι σαφώς μεγαλύτερα. Επιπλέον, δεν υπάρχει καμία σαφής συσχέτιση μεταξύ του μήκους των κλειδιών σε δύο ομάδες, και του επιπέδου ασφαλείας που μπορεί να επιτευχθεί σε κάθε περίπτωση σε δεδομένα συστήματα. Συν τοις άλλοις, ο Phil Zimmermann, δημιουργός του πολύ επιτυχημένου σχήματος κρυπτογράφησης PGP (Pretty Good Privacy), υποστηρίζει ότι ένα συμμετρικό κλειδί μεγέθους 80-bit, μπορεί να επιτύχει παρόμοια επίπεδα ασφάλειας με αυτά που θα ήταν εφικτά με χρήση ενός σχήματος ασύμμετρης κωδικοποίησης μεγέθους 1024-bit. Επίσης, για να μπορεί ουσιαστικά να ξεπεραστεί η ασφάλεια που μπορεί να παράσχει ένα κλειδί μεγέθους 128-bit, πρέπει να γίνει χρήση αντίστοιχου κλειδιού μεγέθους 3000-bit σε ασύμμετρη κωδικοποίηση! Παρόλα αυτά, σε κάθε ομάδα, το μέγεθος του κλειδιού μπορεί να καθορίσει σε μεγάλο βαθμό το βαθμό ασφάλειας ενός συστήματος κρυπτογράφησης, καθώς μεταβάλλεται η πιθανότητα να γίνει σπάσιμο του συστήματος από επιθέσεις τύπου brute force[15]. Φυσικά σε αυτό το σημείο δεν πρέπει να παραβλεφθεί το γεγονός ότι το μέγεθος του κλειδιού δεν είναι γραμμικό αλλά διπλασιάζεται με κάθε bit που προστίθεται. Έτσι για παράδειγμα, μια τιμή μεγέθους 128-bit, ισοδυναμεί με περίπου $340 \times 10^{34}$ πιθανά κλειδιά, νούμερο αρκετά μεγάλο για να θεωρείται ότι ο αλγόριθμος είναι πρακτικά προστατευμένος από κάθε πιθανή κακόβουλη επίθεση.

Ένα άλλο σημαντικό χαρακτηριστικό των συμμετρικών σχημάτων κρυπτογράφησης είναι το γεγονός ότι είναι σημαντικά ταχύτερα από τα αντίστοιχα ασύμμετρα, κι έτσι είναι προτιμητέα σε περιπτώσεις που πρέπει να εφαρμοστούν σε μηνύματα μεγάλου μήκους. Ένας αλγόριθμος όπως ο DES είναι τουλάχιστον 100 φορές ταχύτερος από τον ασύμμετρο RSA σε όρους λογισμικού, ενώ μπορεί να είναι και 10000 φορές ταχύτερος όταν υλοποιείται

[15] Για συμμετρικά κρυπτοσυστήματα, μια brute force attack σημαίνει τυπικά βίαιη αναζήτηση στο χώρο των πιθανών κλειδιών. Με άλλα λόγια, δοκιμάζεται κάθε πιθανό κλειδί στον κλειδοχώρο, με απώτερο στόχο την εύρεση του κλειδιού, και το σπάσιμο του αλγόριθμου που κωδικοποίησε το μήνυμα.

σε ειδικό hardware. Οι αλγόριθμοι κρυφού κλειδιού είναι καταλληλότεροι για την προστασία δεδομένων σε ένα περιβάλλον με μικρό αριθμό χρηστών, τυπικά μέσω της χρήσης passwords ή passphrases. Πρακτικά, σε μεγάλα, κατανεμημένα συστήματα διασποράς, είναι σαφώς προτιμητέα η ταυτόχρονη χρήση σχημάτων τόσο συμμετρικής όσο και ασύμμετρης κρυπτογράφησης.

Οι συμμετρικοί αλγόριθμοι υλοποιούνται πλέον συνήθως με τη μορφή block ή stream αλγορίθμων, που αναλύονται συνοπτικά παρακάτω. Θα αναλυθεί επίσης και η περίπτωση των Κωδικών Πιστοποίησης Μηνύματος (Message Authentication Codes - MACs), ενός μηχανισμού κάνει επιπλέον χρήση ενός κρυφού κλειδιού.

#### 4.2.2.1.1 Block αλγόριθμοι

Οι αλγόριθμοι block μετατρέπουν ένα απλό μήνυμα σε κρυπτογραφημένο κείμενο ιδίου μήκους, που είναι υπό τον έλεγχο ενός μυστικού κλειδιού. Η αποκωδικοποίηση είναι δυνατή μέσω της χρήσης του αντίστροφου μετασχηματισμού, και του ιδίου κλειδιού. Σε πολλούς block αλγορίθμους, το μέγεθος του block είναι 64 bits, αλλά αυτό είναι πιθανό να αυξηθεί στο μέλλον.

Τα απλά μηνύματα κειμένου είναι τυπικά πολύ μεγαλύτερα από το συγκεκριμένο μέγεθος του block που χρησιμοποιείται, ενώ χρησιμοποιούνται διαφορετικές τεχνικές, ή τρόποι εκτέλεσης, ανάλογα με την περίπτωση. Παραδείγματα τέτοιων τρόπων εκτέλεσης είναι τα ηλεκτρονικά βιβλία κωδικών (Electronic Codebooks – ECB), οι block αλγόριθμοι αλυσίδας (Cipher Block Chaining – CBC) ή οι αναδράσεις αλγορίθμων (Cipher Feedback – CFB). Σύμφωνα με τους ECB κάθε block απλού κειμένου κρυπτογραφείται, το ένα μετά το άλλο, χρησιμοποιώντας το ίδιο πάντα κλειδί. Κατά την εκτέλεση CBC, κάθε block απλού κειμένου υπόκειται σε μια πράξη τύπου XOR με το προηγούμενο block προτού κρυπτογραφηθεί, προσθέτοντας με αυτόν τον τρόπο επιπλέον πολυπλοκότητα στον αλγόριθμο, καθιστώντας τον έτσι πιο ανθεκτικό σε κάποιου είδους επιθέσεις. Η Output Feedback (OFB) εκτέλεση μοιάζει με την CBC, με μόνη διαφορά ότι η ποσότητα με την οποία το τρέχον block κειμένου γίνεται XOR, υπολογίζεται ανεξάρτητα. Η CBC εκτέλεση είναι αυτή που χρησιμοποιείται ευρύτερα, για παράδειγμα σε υλοποιήσεις αλγορίθμων DES (qv). Περαιτέρω πάντως ανάλυση σε αυτόν τον τομέα παρέχεται από επιλεγμένη βιβλιογραφία, και ξεφεύγει από τα πλαίσια του παρόντος κειμένου.

Οι επαναληπτικοί block αλγόριθμοι είναι εκείνοι όπου η διαδικασία της κρυπτογράφησης λαμβάνει χώρα σε πολλαπλά επίπεδα επανάληψης, βελτιώνοντας έτσι την ποιότητα και ασφάλεια των υπό προστασία συστημάτων επικοινωνίας. Σε κάθε επανάληψη, μπορεί να εφαρμοσθεί ένας κατάλληλος μετασχηματισμός χρησιμοποιώντας ένα κατάλληλο υποκλειδί που προέρχεται από μια ειδική συνάρτηση μετασχηματισμού, λαμβάνοντας υπόψη το αρχικό μυστικό κλειδί. Αναπόφευκτα, αυτή η επιπλέον υπολογιστική ανάγκη έχει ένα αντίχτυπο στην ολική ταχύτητα στην οποία μπορεί να ολοκληρωθεί ο αλγόριθμος. Έτσι είναι προφανές ότι υπάρχει μια ισορροπία μεταξύ των αναγκών ασφαλείας και της ταχύτητας εκτέλεσης.

Ορισμένοι χαρακτηριστικοί block αλγόριθμοι είναι οι DES, IDEA, SAFER, Blowfish και Skipjack, με τον τελευταίο να προτιμάται από την Εθνική Επιτροπή Ασφαλείας των ΗΠΑ (NSA) για πληθώρα εφαρμογών.

#### 4.2.2.1.2 Stream Αλγόριθμοι

Οι stream αλγόριθμοι μπορούν να γίνουν εξαιρετικά γρήγοροι σε σύγκριση με τους block, παρά το γεγονός ότι ορισμένοι block αλγόριθμοι όταν λειτουργούν με συγκεκριμένο τρόπο (όπως ο DES όταν εκτελείται κατά CFB ή OFB) τελικά λειτουργούν το ίδιο γρήγορα με τους πρώτους. Οι αλγόριθμοι stream λειτουργούν πάνω σε μικρές ομάδες από bit, τυπικά εφαρμόζοντας bit προς bit πράξεις XOR, χρησιμοποιώντας ως κλειδί μια ακολουθία από bits, γνωστή ως κλειδορεύμα (keystream). Ορισμένοι αλγόριθμοι stream βασίζονται σε αυτό που αποκαλείται Linear Feedback Shift Register (LFSR) , ένα μηχανισμό για την παραγωγή ακολουθιών από δυαδικά bits.

Οι αλγόριθμοι stream αναπτύσσονται μέσω ενός ειδικού αλγόριθμου, του Vernam. Παραδείγματα stream αλγορίθμων αποτελούν οι RC4, ο Αλγόριθμος Βέλτιστης Κωδικοποίησης Λογισμικού (SEAL), καθώς και ο αλγόριθμος Vernam που προαναφέρθηκε.

#### 4.2.2.1.3 Κωδικοί Πιστοποίησης Μηνύματος

Οι Κωδικοί Πιστοποίησης Μηνύματος δεν είναι ακριβώς αλγόριθμοι, αλλά περισσότερο ένα ειδικής μορφής άθροισμα (checksum) μήκους συνήθως 32 ψηφίων, το οποίο παράγεται με τη χρήση ενός κρυφού κλειδιού σε συνδυασμό με ένα ειδικό σχήμα πιστοποίησης και

προσαρτάται στο τέλος του μηνύματος. Προκειμένου φυσικά ο παραλήπτης να μπορέσει να επαληθεύσει τον κώδικα, πρέπει να έχει στη διάθεσή του το μυστικό κωδικό.

#### 4.2.2.1.4 Χαρακτηριστικά παραδείγματα συμμετρικών αλγορίθμων

##### *4.2.2.1.4.1 DES*

Ο Αλγόριθμος Κρυπτογράφησης Δεδομένων (Data Encryption Algorithm – DEA), του οποίο το επίσημο όνομα είναι Πρότυπο Κρυπτογράφησης Δεδομένων (Data Encryption Standard - DES) αποτελεί εργασία της IBM, η οποία στη συνέχεια, το 1977, υιοθετήθηκε από την κυβέρνηση των Ηνωμένων Πολιτειών Αμερικής. Είναι κατά πάσα πιθανότητα το πλέον διαδεδομένο σύστημα κρυφού κλειδιού, ιδιαίτερα στην προστασία τραπεζικών δεδομένων, και σχεδιάστηκε αρχικά για να τρέχει σε ειδικά σχεδιασμένο hardware. Οι Αυτόματες Μηχανές Ανάληψης (Automatic Teller Machines – ATM) λειτουργούν στη συντριπτική τους πλειοψηφία με τη βοήθεια του DES.

Ο DES χρησιμοποιεί ένα κλειδί μήκους 56-bit, με 8 επιπλέον bit ισοτιμίας ώστε το συνολικό μέγεθος του block να ανέλθει στα 64 bit. Πρόκειται για επαναληπτικό αλγόριθμο block, που κάνει χρήση των τεχνικών Feistel, όπου το block μηνύματος χωρίζεται σε δύο μέρη. Η συνάρτηση στρογγύλευσης εφαρμόζεται στο πρώτο μισό χρησιμοποιώντας ένα υποκλειδί και το αποτέλεσμα της πράξης αυτή υπόκειται σε μια διεργασία τύπου XOR με του υπόλοιπο μισό μήνυμα. Τα δύο μισά τότε εναλλάσσονται και η διαδικασία συνεχίζει ως έχει, χωρίς όμως να λαμβάνει η χώρα η εναλλαγή στην τελευταία από τις 16 επαναλήψεις κατά τις οποίες συντελείται η εκτέλεση του αλγορίθμου.

Η κύρια μορφή επίθεσης στο DES είναι αυτή που είναι η brute force attack που αναφέρθηκε νωρίτερα. Δεδομένου ότι ο DES χρησιμοποιεί κλειδιά μήκους 56-bit, εύκολα προκύπτει ότι υπάρχουν $2^{56}$ δυνατά κλειδιά προς ανακάλυψη. Με την αλματώδη αύξηση της υπολογιστικής ισχύος, κάτι τέτοιο καθιστά το DES πολύ λιγότερο ασφαλή από όταν είχε για πρώτη φορά υλοποιηθεί, παρά το γεγονός ότι για πρακτικούς λόγους θεωρείται ακόμη και σήμερα επαρκής. Παρόλα αυτά, ο DES πλέον ενδείκνυται κυρίως για παλαιότερα συστήματα και ένα νέο πρότυπο κρυπτογράφησης (AES) έχει εμφανισθεί.

Ένα κλασσικό παράγωγο του DES είναι ο τριπλός DES (Triple-DES), ένας μηχανισμός ο οποίος κρυπτογραφεί το μήνυμα 3 φορές, με χρήση ενός κλειδιού μεγέθους 168-bit. Αυτό συνήθως (αλλά όχι πάντα) προσδίδει σημαντικά μεγαλύτερη ασφάλεια στο σύστημα. Αν

μάλιστα τα τρία 56-bit τμήματα του κλειδιού είναι πανομοιότυπα μεταξύ τους, τότε ο τριπλός DES διατηρεί πλήρη προς τα πίσω συμβατότητα (backward compatibility) με τον απλό DES .

#### *4.2.2.1.4.2 AES*

Το Προχωρημένο Πρότυπο Κρυπτογράφησης (Advanced Encryption Starndard) έχει σκοπό να αντικαταστήσει το DES ως ένα νέο, ασφαλές πρότυπο, δεδομένου ότι ο αλγόριθμος DES που αναλύθηκε παραπάνω έχει φτάσει στο τέλος της χρήσιμης ζωής του. Το 1997, ανακηρύχθηκε ένας διαγωνισμός από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Intstitute of Standards and Technology) των Ηνωμένων Πολιτειών Αμερικής και οι 15 αρχικές συμμετοχές μειώθηκαν σταδιακά και μετά από επιλογή σε μόλις 5. Ο τελικός νικητής ήταν ένα προϊόν το οποίο υποβλήθηκε από τους Joan Daemen και Vincent Rijmen από το Βέλγιο, που ονομάστηκε Rijndael, και το οποίο έγινε αντικείμενο εκτενών δοκιμών και αξιολογήσεων με επιτυχία. Ο Rijndael είναι τεχνικά πολύπλοκος και κάπως διαφορετικός από ότι είχε παρουσιαστεί μέχρι την εμφάνισή του αλλά αποδείχθηκε ιδιαίτερα ασφαλής και πολύπλευρος υπό την έννοια ότι είναι ταχύς στην εκτέλεσή του, ταιριάζει στις αρχιτεκτονικές τάσεις του νεότερου hardware, ενώ παράλληλα έχει την ικανότητα να λειτουργεί το ίδιο καλά με διαφορετικού μεγέθους κλειδιά.

Τεχνικά, ο AES δεν είναι ακριβώς ο Rijndael (παρά το γεγονός ότι στην πράξη χρησιμοποιούνται οι δύο όροι χωρίς διαχωρισμό) καθώς ο Rijndael υποστηρίζει μεγαλύτερο αριθμό από μεγέθη block και κλειδιών (23). Ο AES έχει ένα καθορισμένο μέγεθος block 128-bits, ενώ το μέγεθος του κλειδιού ποικίλει μεταξύ των τιμών 128, 192 και 256 bits. Σε αντίθεση με αυτά, ο Rijndael μπορεί να λειτουργήσει με μεγέθη κλειδιού και block πολλαπλάσια των 32 bits, με ελάχιστο τα 128 και μέγιστο τα 256 bits έκαστο.

### 4.2.2.1.5 Σύνοψη

Το μέγεθος του κλειδιού είναι ένας από έναν αριθμό παραγόντων που επηρεάζουν το επίπεδο ασφαλείας που προσφέρει ένας αλγόριθμος. Όπως με όλα τα θέματα ασφαλείας, το σημαντικό θέμα είναι η ύπαρξη ισορροπίας μεταξύ ασφάλειας και κόστους, χρόνου, χρημάτων και άλλων παραγόντων. Κλειδιά μήκους για παράδειγμα 56-bit δεν είναι φυσικά πλέον ιδιαίτερα ασφαλή, αλλά οι περισσότεροι χρήστες δε χρειάζεται να επιστρατεύσουν υπερ-ασφαλείς αλγορίθμους προστασίας δεδομένων: κάτι τέτοιο θα μπορούσε να είναι ακόμα και ζημιογόνο σε κάποιες περιπτώσεις.

Οι μηχανικοί λογισμικού πρέπει να είναι σε θέση να αξιολογήσουν τι χρειάζεται να υλοποιηθεί σε κάθε περίπτωση, λαμβάνοντας υπόψη μια σειρά παραγόντων όπως είναι η ταχύτητα εκτέλεσης, το κόστος υλοποίησης ή το επίπεδο ασφαλείας. Προφανώς, πρέπει κάθε φορά να γίνεται χρήση του κατάλληλου αλγορίθμου που καταφέρνει να παρουσιάζει την πληρέστερη εικόνα σε σχέση με τους προαναφερθέντες παράγοντες, με γνώμονα πάντα την καλύτερη προστασία του υπό ενδεχόμενη επίθεση συστήματος.

#### *4.2.2.2 Ασύμμετρη Κρυπτογραφία*

Η ασφάλεια που παρέχεται από τα ασύμμετρα κρυπτοσυστήματα, εξαρτάται από μαθηματικά προβλήματα που είναι δύσκολο να λυθούν όπως είναι για παράδειγμα η παραγοντοποίηση μεγάλων ακεραίων σε πρώτους αριθμούς. Τα συστήματα δημοσίου κλειδιού χρησιμοποιούν δύο κλειδιά, με τρόπο ώστε ένα κλειδί, το δημόσιο, μπορεί να χρησιμοποιηθεί για να κρυπτογραφήσει ένα μήνυμα το οποίο τελικά μπορεί να αποκρυπτογραφηθεί μόνο με τη βοήθεια του καλά φυλαγμένου μυστικού κλειδιού.

Η ανάγκη για το διαμοιρασμό ενός κρυφού κλειδιού που απαιτείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση ενός μηνύματος, μπορεί να αποτελεί τεράστιο κενό ασφαλείας στις περιπτώσεις που χρησιμοποιείται συμμετρικός αλγόριθμος κρυπτογράφησης σε ένα σύστημα.

Στην ασύμμετρη, ή αλλιώς ιδιωτικού κλειδιού, κρυπτογραφία, κάτι τέτοιο δεν αποτελεί πρόβλημα καθ' αυτόν τον τρόπο. Δύο κλειδιά, μαθηματικά συνδεδεμένα, χρησιμοποιούνται και λειτουργούν μαζί με τέτοιο τρόπο ώστε το απλό μήνυμα που κρυπτογραφείται με το ένα κλειδί να μπορεί να αποκρυπτογραφηθεί μόνο με το άλλο. Ένα από αυτά τα κλειδιά πρέπει τυπικά να τηρηθεί κρυφό από μια οντότητα, έτσι πρακτικά δεν υπάρχει ανάγκη για διαμοιρασμό κλειδιών, αποφεύγοντας έτσι το πρόβλημα του διαμοιρασμού των κλειδιών ως κενό ασφαλείας. Το δεύτερο κλειδί, το αποκαλούμενο δημόσιο κλειδί, πρέπει να γίνει το γρηγορότερο δυνατό όσο διαδεδομένο όσο γίνεται.

Η διαδικασία (από)κωδικοποίησης μπορεί να λειτουργήσει και προς τις δύο κατευθύνσεις. Αυτό σημαίνει πως κάποιος μπορεί να κωδικοποιήσει ένα μήνυμα με χρήση του δικού του δημόσιου κλειδιού και να είναι σίγουρος ότι ο μόνος που μπορεί να διαβάσει το μήνυμα είναι αυτός που έχει το δικό του κρυφό κλειδί. Φυσικά μπορεί ο καθένας να κρυπτογραφήσει ένα μήνυμα με χρήση του ιδιωτικού κλειδιού μόνο που αυτό όπως είναι

λογικό δεν αποφέρει κάποιο κέρδος στην όλη διαδικασία, καθώς τότε μόνο ο ίδιος θα μπορεί να διαβάσει το μήνυμα αυτό.

Τα συμμετρικά και τα ασύμμετρα συστήματα έχουν τα δικά τους δυνατά και αδύνατα σημεία. Πιο συγκεκριμένα, τα ασύμμετρα συστήματα είναι ευάλωτα με πολλούς διαφορετικούς τρόπους, όπως για παράδειγμα η προσωποποίηση, και η ταχύτητα: οι ασύμμετροι αλγόριθμοι είναι κατά κανόνα αρκετά πιο βραδείς στην εκτέλεσή τους από ότι οι συμμετρικοί. Παρόλα αυτά, έχουν μερικά πολύ σημαντικά πλεονεκτήματα και, το σημαντικότερο, μπορούν να συνεργαστούν αποτελεσματικά με συμμετρικούς αλγόριθμους για να δημιουργήσουν αλγοριθμικούς μηχανισμούς που είναι πολύ αποτελεσματικοί και μπορούν να αποδώσουν υψηλού επιπέδου ασφάλεια (24).

Πριν αναλυθούν ορισμένα χαρακτηριστικά παραδείγματα ασύμμετρων αλγορίθμων κρυπτογράφησης, κρίνεται απαραίτητο να σχολιαστεί το γεγονός ότι παρά το ότι οι συναρτήσεις hash δεν είναι ίδιας φιλοσοφίας με τα ασύμμετρα συστήματα κρυπτογράφησης, εν τούτοις είναι βολικό να συμπεριλαμβάνονται σε αυτήν την κατηγορία, καθώς χρησιμοποιούνται συχνά για τη δημιουργία μηνυμάτων πιστοποίησης, όπως περίπου και οι MD5 που θα αναλυθούν παρακάτω.

#### 4.2.2.2.1 Χαρακτηριστικά παραδείγματα ασύμμετρων αλγορίθμων

##### *4.2.2.2.1.1 RSA*

Το 1997, οι Ron Rivest, Adi Shamir και Leonard Adelman, ανέπτυξαν ένα νέο αλγόριθμο κρυπτογράφησης, γνωστό ως RSA (ακρωνύμιο των αρχικών γραμμάτων των ονομάτων τους) ο οποίος αποτελεί τον πλέον διαδεδομένο αλγόριθμο κρυπτογράφησης δημοσίου κλειδιού σήμερα.

Όπως συμβαίνει και σε άλλα παρόμοια συστήματα, ο RSA κάνει χρήση μεγάλων πρώτων αριθμών για να δημιουργήσει το ζεύγος κλειδιών. Κάθε ζεύγος κλειδιών μοιράζεται το γινόμενο των δύο πρώτων αριθμών το υπόλοιπο, αλλά ο καθένα έχει επίσης και διαφορετικό εκθέτη. Σύμφωνα με τα εργαστήρια του RSA, ο αλγόριθμος λειτουργεί ως εξής: Δύο μεγάλοι πρώτοι αριθμοί, ο p και ο q, πολλαπλασιάζονται σύμφωνα με τη σχέση n=qp, όπου n είναι το γινόμενό τους. Έστω τώρα αριθμός e ο οποίος είναι πρώτος ως προς το γινόμενο (q-1)(p-1), δηλαδή ο (q-1)(p-1) και ο e δεν έχουν κοινό πολλαπλάσιο εκτός του 1. Στη συνέχεια, έστω αριθμός d τέτοιος ώστε ο (ed-1) να είναι ακέραιο πολλαπλάσιο του (q-1)(p-1). Οι τιμές e και d καλούνται δημόσιος και κρυφός εκθέτης αντίστοιχα. Το δημόσιο κλειδί είναι το ζεύγος (n, e), και το ιδιωτικό, κρυφό κλειδί είναι το (n,d).

Όπως γίνεται εύκολα κατανοητό, η γνώση του δημόσιου κλειδιού μπορεί να προσφέρει ένα δρόμο προς την ανάκτηση του ιδιωτικού κλειδιού, αλλά κάτι τέτοιο τελικά εξαρτάται από την παραγοντοποίηση του γινομένου στους συστατικούς του πρώτους αριθμούς. Αυτό είναι ιδιαίτερα δύσκολο και μπορεί να γίνει πρακτικά αδύνατο αν επιλεχθούν σχετικά μεγάλα μήκη κλειδιών. Τα εργαστήρια του RSA επί του παρόντος προτείνουν μήκη κλειδιών μεγαλύτερα από 1024 bits για γενική χρήση, και διπλάσια, δηλαδή 2048 bits, για εξαιρετικά σημαντικά δεδομένα (25). Για συνηθισμένη χρήση, κλειδιά μήκους 768 bits είναι επαρκή καθώς δε μπορούν να σπάσουν εύκολα με τα σύγχρονα τεχνικά μέσα. Όπως πάντα, το κόστος της κωδικοποίησης πρέπει να συνυπολογιστεί ταυτόχρονα με την αξία του υλικού, ενώ πρέπει να δοθεί ιδιαίτερη βάση στο ενδεχόμενο να είναι υπερβολικού μεγέθους το κόστος μέχρι την τελική αποκρυπτογράφηση του μηνύματος. Σχετικές έρευνες εξάλλου των εργαστηρίων RSA έχουν καταδείξει ότι αυτός ο κίνδυνος είναι υπαρκτός, και καθόλου απίθανος στο να συμβεί.

Είναι φυσικά σημαντικό να τονιστεί ότι οι σχέσεις μεταξύ ταχύτητας και κόστους εύρεσης του κατάλληλου κλειδιού που αναφέρονται ανωτέρω αφορούν τη μέση περίπτωση και σε καμία περίπτωση δε σημαίνουν ότι ένα κλειδί ή ένα ζεύγος κλειδιών δε μπορούν να βρεθούν σε χρόνους πολύ ταχύτερους του αναμενόμενου. Επίσης η δυσκολία του αλγόριθμου βασίζεται στο γεγονός ότι η παραγοντοποίηση σε πρώτους αριθμούς είναι ένα δύσκολο μαθηματικά πρόβλημα. Αν κάποια στιγμή ανακαλυφθούν νέες μαθηματικές τεχνικές οι οποίες καθιστούν το πρόβλημα αυτό πλέον λιγότερο πολύπλοκο σε λύση, τότε όπως είναι προφανές η δυναμική του αλγόριθμου θα μειωθεί σημαντικά, και θα γίνει πρακτικά άχρηστος.

Αξίζει επίσης να σημειωθεί ότι υπάρχει όπως πάντα σχέση ανταλλαγής μεταξύ ταχύτητας εκτέλεσης των διαδικασιών (από)κρυπτογράφησης όταν τα ζεύγη κλειδιών μεταβάλλουν το μέγεθός τους. Ενδεχόμενος διπλασιασμός του γινομένου θα έχει ως αποτέλεσμα περίπου τον τετραπλασιασμό του απαιτούμενου, για την ολοκλήρωση των απαραίτητων διαδικασιών που σχετίζονται με το δημόσιο κλειδί, χρόνου, ενώ θα οκταπλασίαζε τον αντίστοιχο χρόνο εκτέλεσης των σχετιζόμενων με το ιδιωτικό κλειδί διαδικασιών. Επιπλέον,, η δημιουργία των κλειδιών θα αυξανόταν κατά ένα παράγοντα 16. Παρόλα αυτά, δεδομένης της διαρκούς και αυξανόμενης αύξησης της υπολογιστικής ισχύος και του ότι η ασύμμετρη κρυπτογράφηση λαμβάνει συνήθως χώρα σε μικρά μηνύματα, ο προαναφερθείς χρονικός περιορισμός δεν αναμένεται να είναι πρόβλημα στα μελλοντικά χρόνια.

#### *4.2.2.2.1.2 MD4 και MD5*

Οι MD2, MD4 και MD5 αποτελούν αλγορίθμους συνόψισης μηνύματος (message digest) που δημιουργήθηκαν από το Ron Rivest για χρήση σε εφαρμογές ψηφιακής υπογραφής όπου ένα μήνυμα συμπιέζεται σε μια σύνοψη (digest) και εν συνεχεία κρυπτογραφείται μέσω ενός ιδιωτικού κλειδιού. Ο MD2 σχεδιάστηκε για 8-bit υπολογιστικά συστήματα, ενώ οι MD4 και MD5 αναπτύχθηκαν για 32-bit υπολογιστικά συστήματα. Ο MD4 κατασκευάστηκε το 1990, και πλέον θεωρείται ξεπερασμένος και μη ασφαλής.

Ο αλγόριθμος MD5 περιγράφεται από τα εργαστήρια του RSA ως «Ένας βελτιωμένος MD4», και παρά το ότι είναι βραδύτερος από τον MD4, είναι αρκετά ασφαλής. Όπως συμβαίνει και με τον MD4, ένα απλό μήνυμα ένα απλό μήνυμα κειμένου (plain text) δημιουργείται, προκειμένου να εξασφαλίσει ότι το μέγεθός του σε bits αν προστεθούν 448 είναι πολλαπλάσιο του 512. Μια δυαδική 64-bit αναπαράσταση του μήκους του αρχικού μηνύματος προστίθεται στη συνέχεια και το μήνυμα υπόκειται επεξεργασία σε blocks των 512 bits με χρήση μιας επαναληπτικής συνάρτησης συμπίεσης, με κάθε block να γίνεται αντικείμενο επεξεργασίας για 4 διακριτούς γύρους.

### 4.2.2.2.2 Σύνοψη

Η κρυπτογραφία δημοσίου κλειδιού αποτελεί σημαντικό μέρος των τεχνικών που χρησιμοποιούνται κυρίως για την πιστοποίηση αντικειμένων. Παρά το γεγονός ότι ένα σύστημα δημοσίου κλειδιού θα μπορούσε να χρησιμοποιηθεί απλά για την κρυπτογράφηση απλών μηνυμάτων κειμένου, η πρακτική του αξία μάλλον βρίσκεται πιο κοντά σε άλλες διαδικασίες, όπως είναι η σύνοψη μηνυμάτων. Αντίστοιχα, τα συμμετρικά συστήματα τείνουν να χρησιμοποιούνται κυρίως για να υποστηρίξουν την ασφαλή πιστοποίηση και μεταφορά πακέτων πληροφορίας.

Κρυπτοσυστήματα δημοσίου κλειδιού όπως ο RSA χρησιμοποιούν μεγάλο μέγεθος κλειδιού – πλέον συνίσταται η χρήση κλειδιών μεγαλύτερων των 768 ψηφίων. Η παραγοντοποίηση σε πρώτους αριθμούς αποτελεί βασικότατη μέθοδο αντιμετώπισης επιθέσεων, καθώς η λύση των αντίστοιχων μαθηματικών προβλημάτων αποτελεί διαδικασία αυξημένης πολυπλοκότητας. Όσο η επεξεργαστική ισχύς αυξάνεται, κλειδιά που παλαιότερα θεωρούνταν ασφαλή, μπορεί να θεωρούνται ξεπερασμένα ειδικά αναφορικά με τις

επιθέσεις brute force, έτσι είναι σημαντικό να διασφαλιστεί το ότι τα κλειδιά είναι ικανοποιητικού μεγέθους για να προσφέρουν αντίστοιχα ικανοποιητική ασφάλεια.

### 4.2.3 Εισαγωγή κρυπτογράφησης στην εφαρμογή ελέγχου

Όπως αναφέρεται αναλυτικά στο δεύτερο κεφάλαιο του παρόντος κειμένου, ένα σύστημα προκειμένου να θεωρείται αυτόνομο, πρέπει να διαθέτει κάποια ειδικά χαρακτηριστικά που θα της επιτρέψουν να λάβει το χαρακτηρισμό «αυτόνομο» (βλ. παράγραφο 2.1.2). Δύο από αυτές είναι η αυτο–ίαση και η αυτο–προστασία, δύο έννοιες που απασχολούν, όπως έχει ήδη φανεί στην πορεία του παρόντος κεφαλαίου, ιδιαίτερα τα σημερινά συστήματα, κυρίως όταν αυτά είναι αυξημένης μάλιστα ειδικής βαρύτητας όπως είναι το σύστημα διαχείρισης ενός διεθνικού ηλεκτρικού δικτύου. Η ανάγκη εύρεσης του καταλληλότερου σχήματος προστασίας του συστήματος φαντάζει ιδιαίτερα σημαντική, καθώς τα δεδομένα που θα μεταφέρονται από συσκευή σε συσκευή κατά μήκος του δικτύου μέχρι και τα διάφορα σημεία ελέγχου αποτελούν στη γενική περίπτωση ευαίσθητα δεδομένα, που χρίζουν προστασίας και διαφύλαξης.

Η επιλογή του κατάλληλου κρυπτοσυστήματος εξαρτάται από πολλούς παράγοντες, καθώς εγγενώς, το υπάρχον υπό προστασία σύστημα επιβάλει διάφορους περιορισμούς, οι οποίοι πρέπει να τηρηθούν, προκειμένου αυτό να είναι λειτουργικό.

#### *4.2.3.1 Η επιλογή του κατάλληλου κρυπτοσυστήματος*

Οι διάφοροι περιορισμοί που η ίδια η φύση του προβλήματος θέτει συνοψίζονται στην παρακάτω λίστα.

- **Αυξημένη προστασία**: Ο αλγόριθμος που θα επιλεγεί, απαιτείται να προσφέρει υψηλού επιπέδου ασφάλεια και προστασία από ένα μεγάλο εύρος απειλών, καθώς τα δεδομένα διαχείρισης ενός τόσο μεγάλου δικτύου, πρέπει να είναι όσο το δυνατόν καλύτερα προστατευμένα. Επίσης, στην περίπτωση που τίθεται θέμα εμπορικής διάθεσης του συστήματος στο ευρύ κοινό, με παράλληλη ύπαρξη υπηρεσιών internet, voice over IP, IPTV κτλ, η ύπαρξη ισχυρής κρυπτογράφησης των δεδομένων τόσο πάνω στο δίκτυο, όσο και στους εκάστοτε κόμβους κρίνεται επιβεβλημένη.

- **Αυξημένη ταχύτητα**: Η περιορισμένων υπολογιστικών δυνατοτήτων φύση τόσο των σημείων ελέγχου όσο των ενδιάμεσων σημείων συνάθροισης, υποβάλει έναν έμμεσο περιορισμό σε ό,τι έχει να κάνει με την ταχύτητα εκτέλεσης των αλγορίθμων (από)κρυπτογράφησης. Ειδικά τα ενδιάμεσα σημεία συνάθροισης καταδεικνύουν σε εντονότερο βαθμό την ανάγκη αυτή, καθώς σε περίπτωση αναζήτησης από τα σημεία ελέγχου κάποιου δεδομένου, θα έχουν να εκτελέσουν όσο το δυνατό γρηγορότερα (για να διατηρηθεί ο απαιτούμενος πραγματικού χρόνου χαρακτήρας της εφαρμογής). Τα σημεία ελέγχου πρέπει επίσης να είναι σε θέση να μπορούν ταχύτατα να επεξεργαστούν τα δοθέντα αποτελέσματα, γεγονός ιδιαίτερα δύσκολο αν αναλογισθεί κανείς τον αριθμό των κειμένων που πρέπει διαδοχικά να επεξεργαστούν.
- **Υπολογιστικοί πόροι**: Για λόγους ευελιξίας και οικονομίας, οι μικροϋπολογιστές που θα υπάρχουν σε κάθε συσκευή ελέγχου θα αποτελείται από hardware χαμηλού κόστους και δυνατοτήτων. Το γεγονός αυτό, περιορίζει την ικανότητα των συσκευών για γρήγορη επεξεργασία των δεδομένων που αποκομίζουν από το δίκτυο. Ενδεχόμενη ανάγκη για μεγάλη ποσότητα υπολογιστικών πόρων θα μπορούσε να οδηγήσει το σύστημα σε δυσλειτουργία. Έτσι, θα ήταν καλό, οι υπολογιστικοί πόροι που απαιτούνται για την εκτέλεση του αλγορίθμου κρυπτογράφησης να ήταν περιορισμένοι.
- **Δυνατότητα ανάκτησης αλλοιωμένων δεδομένων**: Λάθη κατά τη διάρκεια της μετάδοσης δεδομένων συμβαίνουν σε όλα τα τηλεπικοινωνιακά συστήματα. Στο παρόν όμως υπό μελέτη σύστημα, θα ήταν εξαιρετικά θετικό αν ο αλγόριθμος κρυπτογράφησης εκτός από δυνατότητα ανίχνευσης ενδεχομένων λαθών, είχε και δυνατότητα διόρθωσης αυτών.

Η προσπάθεια ικανοποίησης όλων αυτών των κριτηρίων που προαναφέρθηκαν, περιόρισε την επιλογή στους συμμετρικούς αλγόριθμους, καθώς αυτοί παρουσιάζουν αυξημένες απαιτήσεις χρόνου και υπολογιστικών πόρων.

Από την ανάλυση που έγινε νωρίτερα, είναι φανερό ότι ο πλέον υποσχόμενος αλγόριθμος συμμετρικής κρυπτογράφησης είναι ο AES, ή αλλιώς Rijndael[16]. Μια πολλά υποσχόμενη εφαρμογή κρυπτογράφησης βασισμένη στον αλγόριθμο αυτό, είναι η ccrypt. Η εφαρμογή αυτή βασίζεται στον Rijndael και σχεδιάστηκε αρχικά με απώτερο στόχο να αντικαταστήσει τη γερασμένη πλέον σχετική εφαρμογή του Unix, crypt. Η ccrypt πληροί όλα τα κριτήρια

[16] Αν και όπως έχει ήδη αναφερθεί, οι δύο αυτοί δεν είναι ταυτόσημοι αλγόριθμοι.

που τέθηκαν προηγουμένως, πετυχαίνοντας να κρυπτογραφήσει δεδομένα σε υψηλές ταχύτητες, χωρίς να χρησιμοποιεί εξοντωτικούς υπολογιστικούς πόρους, ενώ διαθέτει και δυνατότητες επαναφοράς αλλοιωμένων αρχείων.

Εκτός των προαναφερθέντων χαρακτηριστικών (που ήδη την καθιστούν πολύ ελκυστική λύση), η ccrypt μπορεί να λειτουργεί πάνω στα δεδομένα χωρίς να τα αντιγράφει κάπου, αλλά απ ευθείας σε αυτά, χωρίς να υπάρχει δυνατότητα διακοπής του αλγορίθμου κατά τη διάρκεια εκτέλεσης. Εκτός αυτού, αν για κάποιο λόγο η εκτέλεση διακοπεί, για παράδειγμα λόγω πτώσης ηλεκτρικής τάσης ή αστοχίας υλικού, τότε η ccrypt, μπορεί δεδομένου του κλειδιού, να ανακτήσει πλήρως τα αρχικά δεδομένα, επιτρέποντας έτσι τη μη απώλεια κρίσιμων δεδομένων (26). Η εγγραφή των νέων κρυπτογραφημένων δεδομένων πάνω στα παλιά, εξασφαλίζει την ελάχιστη κατανάλωση σε φυσική μνήμη του αλγορίθμου, καθώς λόγω του χαρακτήρα του block αλγορίθμου, κρυπτογραφούνται κάθε φορά μόνο μερικά bytes πληροφορίας.

Σχετικά με την ασφάλεια που μπορεί να παράσχει η ccrypt, είναι καλό να ειπωθεί ξανά ότι βασίζεται στον Rijndael, ο οποίος βασίζεται στον AES που αποτελεί το πρότυπο κρυπτογράφησης των Ηνωμένων Πολιτειών Αμερικής, αλλά είναι κάπως βελτιωμένος. Συγκεκριμένα, η ccrypt ζητά από το χρήστη να εισάγει ένα κλειδί οποιουδήποτε μεγέθους, το οποίο στη συνέχεια, μέσω κατάλληλων hash συναρτήσεων, αντιστοιχεί σε ένα άλλο κλειδί μήκους 256-bit. Έτσι, συνολικά, η ccrypt επιτυγχάνει κρυπτογράφηση με μέγεθος κλειδιού ίσο με 256-bit, μέγεθος που οι επιστήμονες θεωρούν ότι καθιστά τον αλγόριθμο *απόλυτα ασφαλή* τουλάχιστον για τις επόμενες δεκαετίες. Έχουν μέχρι σήμερα γίνει πολλές προσπάθειες, από διάφορα ερευνητικά κέντρα, για να σπάσει ο αλγόριθμος, όμως σε αντίθεση με τον παραδοσιακό crypt, κάτι τέτοιο δεν έχει ακόμα γίνει.

Σε σχέση με τα όσα αναφέρονται στις παραγράφους 4.2.2.1.1 και 4.2.2.1.2, αξίζει να τονιστεί ότι η ccrypt είναι πρακτικά μια stream υλοποίηση του αλγόριθμου Rijndael, λειτουργώντας τον Rijndael block αλγόριθμο κατά CFB τρόπο, με μέγεθος block επίσης στα 256 bits (26).

Τελικά, με βάση όλα τα χαρακτηριστικά που συνδυάζει, η υλοποίηση αυτή του Rijndael αλγορίθμου, είναι αυτή που επιλέχθηκε ως εφαρμογή κρυπτογράφησης του υπό μελέτη συστήματος.

# 5 Πραγματοποίηση μετρήσεων – Αξιολόγηση

Οι μετρήσεις που έγιναν για την αξιολόγηση του συστήματος, αφορούν τοπολογίες όπου υπάρχουν διάφορες συσκευές ελέγχου, διάφορα ενδιάμεσα σημεία, και ένα μόνο σημείο ελέγχου. Κάτι τέτοιο είναι ρεαλιστικό, καθώς οι διάφορες γεωγραφικές περιοχές της επικρατείας θα χωριστούν σε διάφορες περιφέρειες, σύμφωνα με το Σχήμα 4.2, όπου τελικά το σημείο ελέγχου θα είναι μόλις ένα. Απλοποιώντας ακόμη περισσότερο το σενάριο, αυτό που παρουσιάζει ενδιαφέρον είναι όχι τόσο αυτή καθ' εαυτή η ακριβής διάταξη των διαφόρων υπολογιστικών συστημάτων στο χώρο (είτε πρόκειται για συσκευές ελέγχου, είτε ενδιάμεσες συσκευές, είτε τερματικά σημεία ελέγχου), αλλά η απόδοση του συστήματος επιλεκτικά σε κάθε σταθμό που εκτελεί τις διαδικασίες που απαιτούν υπολογιστική ισχύ, και μετρήσιμο χρόνο εκτέλεσης. Έτσι, οι συσκευές ελέγχου, για την κατασκευή και ενημέρωση των κατάλληλων εγγράφων XML, δεν παρουσιάζουν κάποιο ειδικό ενδιαφέρον, δεδομένου ότι η απλή καταγραφή μερικών byte δεδομένων σε αρχεία και η ταυτόχρονη εκτέλεση ενός πολύ απλού δαίμονα που θα «ακούει» για αιτήσεις από το σημείο ελέγχου, δεν αποτελούν αξιόλογη καθυστέρηση ή υπολογιστική επιβάρυνση, ακόμη και για τις αναμενόμενα περιορισμένων δυνατοτήτων συσκευές ελέγχου.

Για την υλοποίηση των πειραματικών μετρήσεων έγινε χρήση δύο διαφορετικών υπολογιστικών συστημάτων, προκειμένου να καταδειχθούν οι όποιες διαφορές στην απόδοση των αλγορίθμων, να καθοριστούν τα σημεία που αποτελούν στενωπούς στην επίδοση του συστήματος, και τέλος, μετά την αξιολόγηση των αποτελεσμάτων, να προταθούν τρόποι βελτιστοποίησης του συστήματος. Τα χαρακτηριστικά των δύο αυτών συστημάτων συνοψίζονται ως εξής:

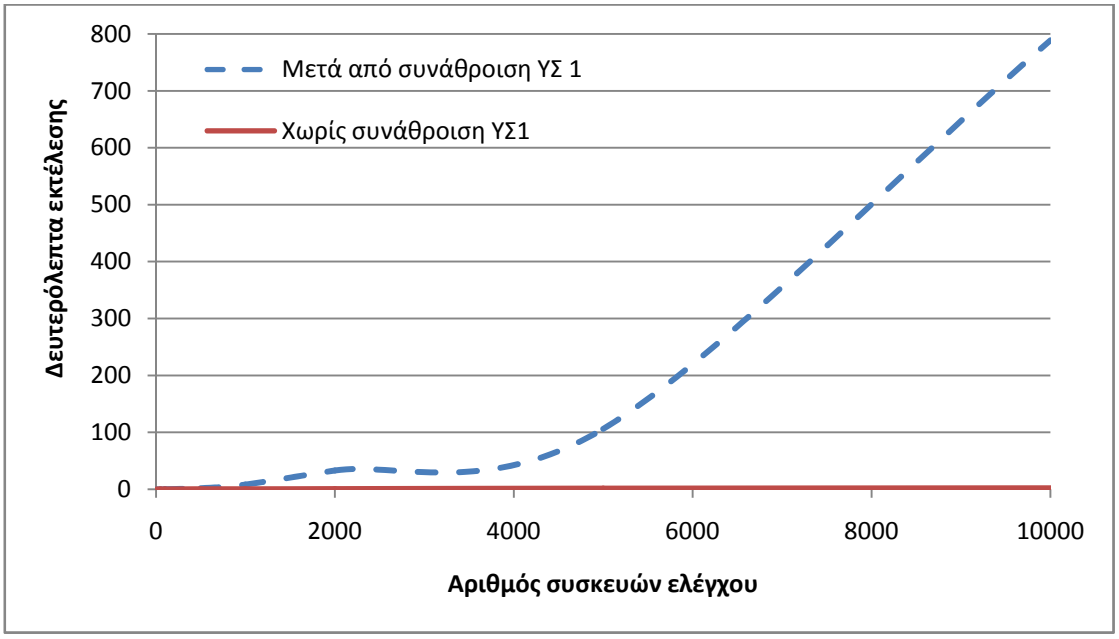
- **Υπολογιστικό Σύστημα 1 (ΥΣ 1)**:
  - → Επεξεργαστής: Μονού πυρήνα, Intel® Pentium® 4, Συχνότητας 2.4GHz
  - → Φυσική μνήμη 512MB, Συχνότητας 333MHz
- **Υπολογιστικό Σύστημα 2 (ΥΣ 2)**:
  - → Επεξεργαστής: Διπλού πυρήνα, Intel® Core™ Duo T2300, Συχνότητας 1.66GHz ο κάθε πυρήνας
  - → Φυσική Μνήμη 1024MB, Συχνότητας 667MHz

Τα λοιπά τεχνικά χαρακτηριστικά δεν αναφέρονται καθώς δε θεωρήθηκε ότι επηρεάζουν την αξιοπιστία των αποτελεσμάτων των μετρήσεων, καθώς στη διάρκεια των τελευταίων οι

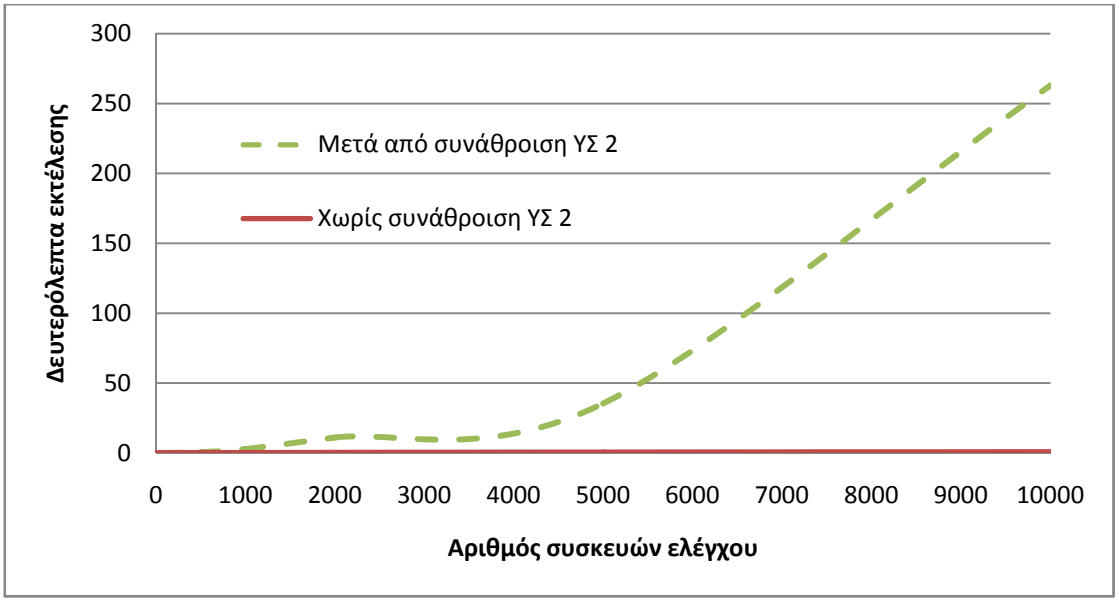
επεξεργαστές δούλευαν κοντά στο 100% των δυνατοτήτων τους, οπότε περιορισμοί από άλλους, εξώτερους παράγοντες (όπως για παράδειγμα διεπαφή σκληρών δίσκων κτλ) δεν υπήρχαν.

## 5.1 Κρυπτογράφηση

Αρχικά θεωρήθηκε σύστημα μεταβλητού πλήθους συσκευών ελέγχου, κάθε μία από τις οποίες χαρακτηριζόταν από ένα έγγραφο περιγραφής XML μεγέθους περίπου 1.3kB (τυπικό μέγεθος). Στη συνέχεια, με αυξανόμενο αριθμό συσκευών από 10 έως και 10.000, έγιναν μετρήσεις σχετικές με την ταχύτητα απόδοσης του συστήματος σε ότι αφορά τη συνολικό χρόνο που απαιτήθηκε για την κρυπτογράφηση των δεδομένων, παρουσία και μη του σχήματος συνάθροισης. Τα αποτελέσματα απεικονίζονται στα σχήματα 5.1 και 5.2:

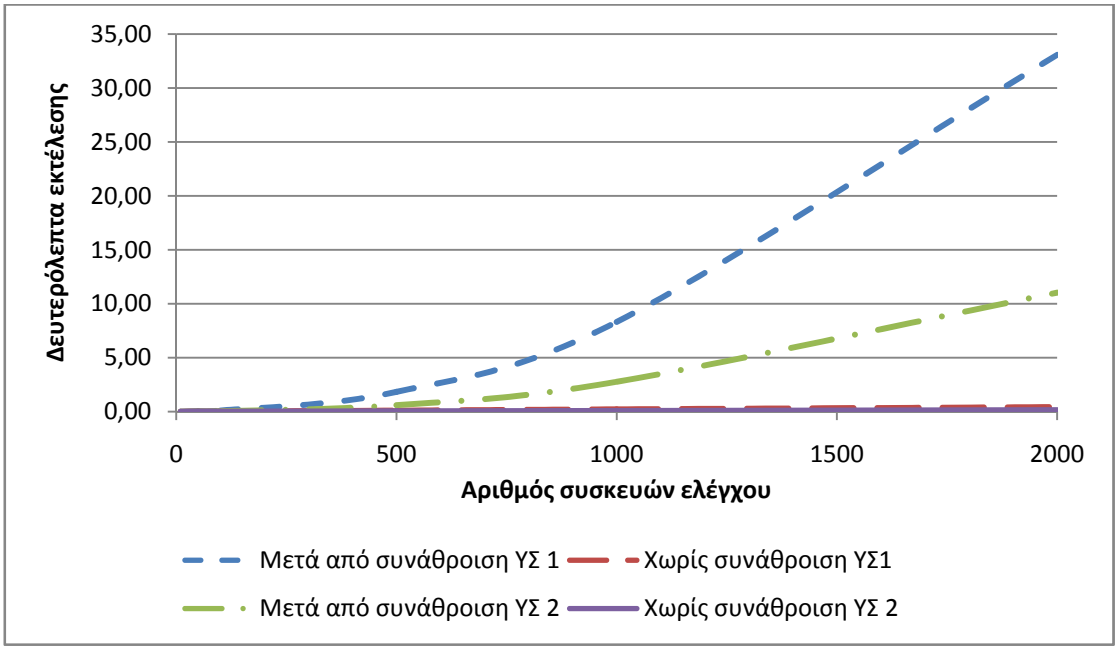



**Σχήμα 5.1: Διάγραμμα περιγραφής της σχέσης συνολικού χρόνου εκτέλεσης – αριθμού συσκευών στο υπολογιστικό σύστημα 1.**




**Σχήμα 5.2: Διάγραμμα περιγραφής της σχέσης συνολικού χρόνου εκτέλεσης – αριθμού συσκευών στο υπολογιστικό σύστημα 2.**

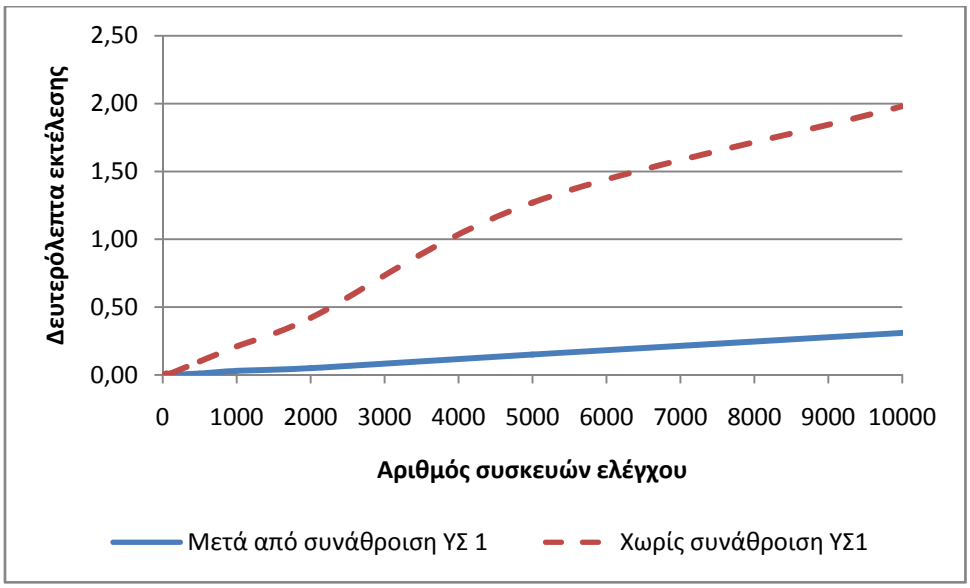
Τα παραπάνω διαγράμματα καταδεικνύουν ότι υπάρχει σχεδόν εκθετική αύξηση του χρόνου εκτέλεσης σε γραμμική αύξηση του αριθμού των συσκευών. Κάτι τέτοιο, φαίνεται ακόμη καλύτερα στο συγκεντρωτικό διάγραμμα του Σχήματος 5.3, όπου καταγράφεται συγκριτικά και για τα δύο υπολογιστικά συστήματα ο χρόνος εκτέλεσης της διαδικασίας από την αρχή της μέχρι το τέλος της κρυπτογράφησης.




**Σχήμα 5.3: Συγκεντρωτικό διάγραμμα απόδοσης για περιορισμένο αριθμό συσκευών.**

Αξίζει να παρατηρηθεί το γεγονός ότι για συνολικό αριθμό συσκευών μικρότερο από περίπου 500 ανά περιφέρεια, η διαφορά επεξεργαστικής ισχύος είναι αδιόρατη, καθώς ο χρόνος εκτέλεσης είναι σε κάθε περίπτωση μικρότερος του 1 δευτερολέπτου! Αυτή η παρατήρηση είναι εξαιρετικά κρίσιμη, καθώς στη συνέχεια, θα μπορούσε να θέσει ένα κατώφλι (ανάλογο φυσικά και με την υπολογιστική ισχύ των ενδιάμεσων μονάδων συνάθροισης, θεωρώντας ότι η ισχύς των σημείων ελέγχου είναι επαρκώς μεγάλη ώστε να μην επηρεάζει τη σχεδίαση του συστήματος) για τον καθορισμό του μεγέθους των περιφερειών ελέγχου που καθορίζεται από την παρουσία του σημείου συνάθροισης.

Ενδιαφέρον παρουσιάζει και ο χρόνος στον οποίο γίνεται η κρυπτογράφηση ως διαδικασία, πάνω από απλά XML έγγραφα, αλλά και από συναθροισμένα XML έγγραφα. Το παρακάτω διάγραμμα καταδεικνύει τη σχέση που υπάρχει μεταξύ αριθμού XML εγγράφων και χρόνου, σε περίπτωση που υπάρχει και που δεν υπάρχει σχήμα συνάθροισης:



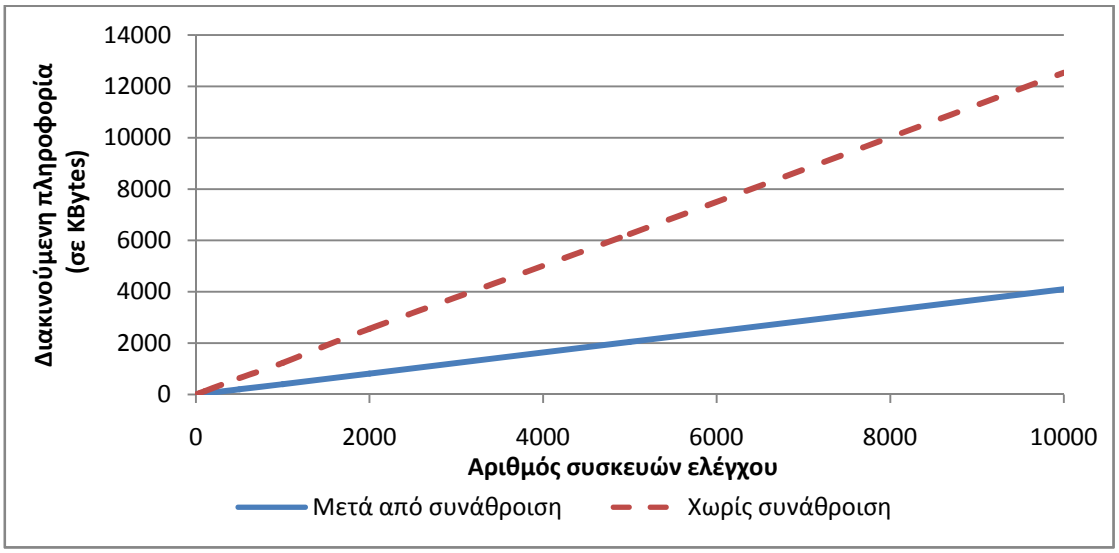

**Σχήμα 5.4: Χρόνος εκτέλεσης αλγορίθμου κρυπτογράφησης μετά από και χωρίς συνάθροιση.**

Αίσθηση προκαλεί φυσικά το γεγονός ότι για μικρό αριθμό συσκευών ο χρόνος εκτέλεσης ακόμα και για το λιγότερο ισχυρό υπολογιστικό σύστημα είναι εξαιρετικά μικρός, γεγονός που καταδεικνύει ότι η ccrypt εκτελείται ταχύτατα, ακόμα και σε συστήματα μικρότερης ισχύος.

Το παραπάνω διάγραμμα ενισχύει ακόμα περισσότερο την άποψη ότι ο διαμελισμός της επικράτειας σε περιφέρειες αναμένεται να επηρεάσει σε τεράστιο βαθμό την απόδοση του συστήματος. Το Σχήμα 5.4, συγκρινόμενο με τα σχήματα 5.1, 5.2 και 5.3, υποδεικνύει ότι ο περισσότερος χρόνος εκτέλεσης της εφαρμογής στα ενδιάμεσα σημεία συνάθροισης και

στα σημεία ελέγχου αφορά στη διαδικασία της συνάθροισης, και όχι στην κρυπτογράφηση των εκάστοτε δεδομένων. Έτσι, η εξάρτηση του συστήματος από την κατάτμηση των περιφερειών γίνεται ακόμη ισχυρότερη. Περαιτέρω ανάλυση των ανωτέρω θα ακολουθήσει σε επόμενη παράγραφο.

Τα προηγούμενα διαγράμματα αφορούσαν την απόδοση της εκτέλεσης της εφαρμογής στα υπολογιστικά συστήματα, και συνέβαλαν στην κατανόηση ορισμένων περιορισμών που τίθενται εμμέσως στην υλοποίηση και το σχεδιασμό του συστήματος διαχείρισης. Τα αποτελέσματα που εξήχθησαν αποδεικνύουν ότι το μεγαλύτερο ποσοστό του χρόνου εκτέλεσης δαπανάται στην επεξεργασία των XML εγγράφων στη διαδικασία της συνάθροισης. Θα μπορούσε κάποιος να υποθέσει ότι η διαδικασία αυτή είναι παρασιτική ως προς τη λειτουργία του γενικότερου συστήματος, και χωρίς κανένα λόγο ύπαρξης. Κάτι τέτοιο δεν είναι παρόλα αυτά αληθές. Οι ευεργετικές επιδράσεις της συνάθροισης φαίνονται στο Σχήμα 5.5, όπου παρουσιάζεται η σχέση μεταξύ του όγκου πληροφορίας που κινείται στο δίκτυο, και του αριθμού συσκευών ελέγχου του δικτύου.




**Σχήμα 5.5: Σχέση του όγκου διακινούμενης πληροφορίας και του αριθμού συσκευών ελέγχου.**

Στο διάγραμμα αυτό φαίνεται καθαρά η επίδραση που έχει η συνάθροιση στον όγκο της διακινούμενης πληροφορίας στο δίκτυο. Παρατηρείται σαφής μείωση του όγκου της διακινούμενης πληροφορίας, αν και το μέγεθος της μείωσης αυτής εξαρτάται σε άμεσο βαθμό από τη σχετική διαφοροποίηση στο περιεχόμενο των XML εγγράφων που συναθροίζονται. Φυσικά, αν τα XML έγγραφα όλων των συσκευών ήταν ίδια μεταξύ τους, τότε η μείωση αυτή θα ήταν πρακτικά άπειρη, αν και κάτι τέτοιο σε καμία περίπτωση δε μπορεί να ισχύει, καθώς τουλάχιστον 3 πεδία θα είναι διαφορετικά (αυτά του UDN, UPC και

Serial Number) στα έγγραφα περιγραφής συσκευών. Στις μετρήσεις που ελήφθησαν, θεωρήθηκε ότι τα διάφορα XML αρχεία περιγραφής είχαν κατά μέσο όρο 5 διαφορετικά πεδία μεταξύ τους. Στη γενική περίπτωση πάντως, και σε ένα πραγματικό σύστημα, όπου οι διάφοροι υποσταθμοί μέτρησης θα ήταν εγκατεστημένοι από μεγάλη εταιρία μετά από αντίστοιχη οικονομική συμφωνία, αναμένεται σαφώς ο αριθμός των κοινών στοιχείων να είναι κατά μέσο όρο παρόμοιος με αυτόν που θεωρήθηκε για τη διεξαγωγή των πειραμάτων. Αυτό συμβαίνει γιατί πεδία όπως είναι τα manufacturer, manufacturerURL κτλ, θα είναι παρόμοια, ενώ τα διαφορετικά (εκτός των τριών δεδομένων διαφοροποιήσεων) από τα υπόλοιπα πεδία δεδομένων περιέχουν πληροφορία μικρή σε μέγεθος, οπότε δεν επηρεάζουν σε μεγάλο βαθμό τις μετρήσεις. Μια άλλη παρατήρηση που θα μπορούσε να γίνει, σχετίζεται και πάλι με τη διαμέλιση της επικρατείας σε περιφέρειες: όσο πιο κατανεμημένο και διαιρεμένο είναι το σύστημα διαχείρισης κι ελέγχου, τόσο μικρότερο θα είναι το κέρδος σε διακινούμενη πληροφορία, καθώς το τελευταίο είναι περίπου αύξουσα γραμμική συνάρτηση του αριθμού των συσκευών.

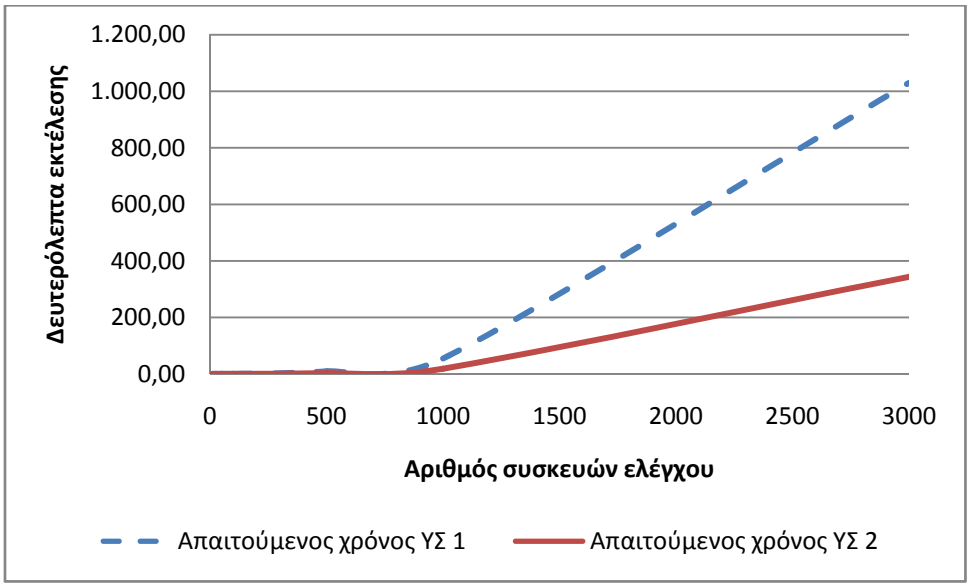
Ένα ακόμη ενδιαφέρον σημείο που προέκυψε από τις πειραματικές μετρήσεις είναι το γεγονός ότι το διαφορετικό μέγεθος κλειδιού στην κρυπτογράφηση δεν επηρεάζει σημαντικά την ταχύτητα της κωδικοποίησης, καθώς το πραγματικό μέγεθος του κλειδιού παραμένει 256-bits: ο κωδικός που εισάγεται από την οντότητα που εκτελεί τον αλγόριθμο επηρεάζει μόνο την τελική μορφή του κλειδιού και όχι το μέγεθός του.

## 5.2 Αποκρυπτογράφηση

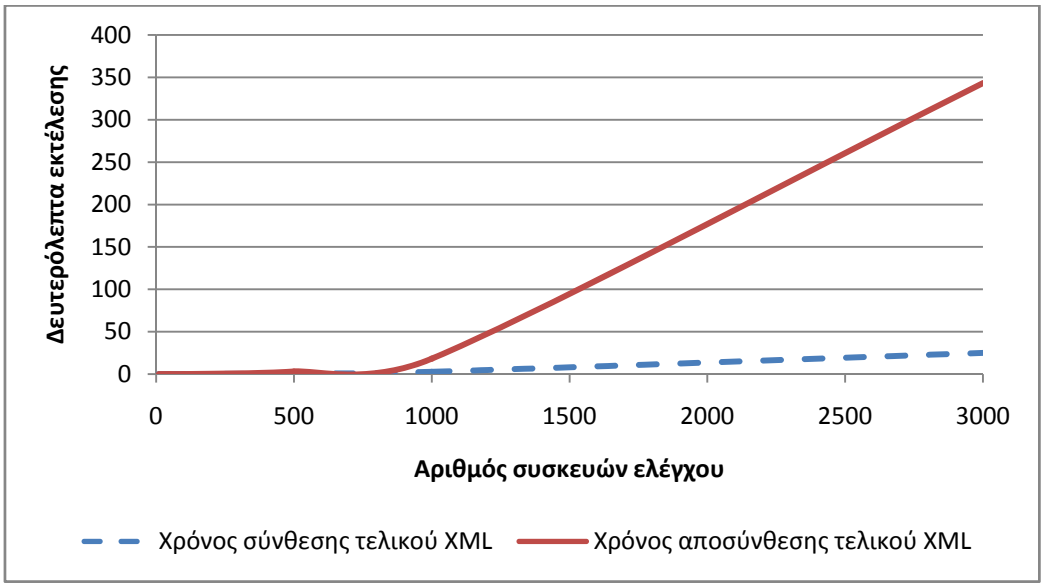
Οι πειραματικές μετρήσεις που πραγματοποιήθηκαν για την αξιολόγηση της εφαρμογής αναφορικά με τη διαδικασία αποσύνθεσης και αποκρυπτογράφησης του τελικού συναθροισμένου εγγράφου, έγιναν κάτω από παρόμοιες συνθήκες με αυτές της σύνθεσης αυτού. Το έγγραφο που είχε δημιουργηθεί μέσω της συνάθροισης και κρυπτογράφησης που περιγράφθηκε ανωτέρω, υπόκειτο σε μια διαδικασία αποκρυπτογράφησης κατόπιν αποσύνθεσης, προκειμένου η εφαρμογή ελέγχου να μπορέσει να εκμεταλλευτεί τα παρεχόμενα αποτελέσματα της εκάστοτε αναζήτησης.

Οι μετρήσεις που πραγματοποιήθηκαν στη συνέχεια, παρουσιάζονται στα σχήματα 5-6 και 5-7. Τα δύο αυτά σχήματα, καταγράφουν με έντονο τρόπο ότι υπάρχει μεγάλη διαφορά στην απόδοση των δύο αντίστροφων διαδικασιών σύνθεσης και αποσύνθεσης. Η εκθετική

συμπεριφορά του αλγορίθμου σύνθεσης του συναθροιστικού XML εγγράφου κάνει ακόμη πιο έντονη την παρουσία της στην αποσύνθεση αυτού.




**Σχήμα 5.6: Σχέση χρόνου – αριθμού συσκευών ελέγχου για την αντίστροφη διαδικασία της συνάθροισης.**




**Σχήμα 5.7: Διάγραμμα σύγκρισης χρόνου σύνθεσης και αποσύνθεσης του τελικού συναθροισμένου XML εγγράφου.**

Αυτό που είναι επίσης ορατό είναι η ανάγκη για επιπλέον υπολογιστική ισχύ και ιδιαίτερα φυσική μνήμη στα σημεία όπου μεγάλος αριθμός εγγράφων χρίζει επεξεργασίας. Τα σημεία αυτά δεν είναι άλλα από κάποια κομβικά σημεία συνάθροισης καθώς και τα κεντρικά

σημεία ελέγχου, όπου ούτως ή άλλως όπως έχει ήδη καταδειχθεί, η ανάγκη για υπολογιστική ισχύ είναι σαφώς αυξημένη.

Το γεγονός ότι ο απαιτούμενος για την αποσύνθεση του εγγράφου χρόνος είναι μεγαλύτερος από τον αντίστοιχο που απαιτείται για τη σύνθεση είναι κάτι αναμενόμενο, και αυτό διότι κατά τη διάρκεια της αποσύνθεσης, το υπολογιστικό σύστημα πρέπει επαναληπτικά να ελέγχει ολόκληρο το συναθροισμένο έγγραφο XML, προκειμένου να διαπιστώσει τις οντότητες που αντιστοιχούν σε κάθε ένα XML έγγραφο περιγραφής. Κάτι τέτοιο φυσικά δεν ίσχυε γενικά στην περίπτωση της σύνθεσης του συναθροισμένου εγγράφου, καθώς μόνο στο τελευταίο, πριν το σημείο ελέγχου, σημείο συνάθροισης ο αριθμός των XML αρχείων είναι αρκετά μεγάλος ώστε να μπορεί να δημιουργήσει πρόβλημα. Τίθεται δηλαδή και πάλι θέμα βελτιστοποίησης της κατανομής των συσκευών ελέγχου και συναθροίσεως, όπως ακριβώς έγινε και νωρίτερα.

Τέλος, ένα άλλο γεγονός που χρίζει σχολιασμού είναι το ότι σε κάθε περίπτωση, φαίνεται να υπάρχει ένα κατώφλι απόδοσης του συστήματος, στην περίπτωση που πραγματοποιείται επεξεργασία περίπου 1000 αρχείων (άρα και συσκευών ανά περιφέρεια) ταυτόχρονα. Η παρατήρηση αυτή μπορεί να αποδειχθεί ιδιαίτερα κρίσιμη στο σχεδιασμό του συστήματος, καθώς μπορεί να καθορίσει σε μεγάλο βαθμό την αποκρισιμότητα αυτού.

## 5.3 Αξιολόγηση μετρήσεων

Μετά το πέρας των μετρήσεων, τα συμπεράσματα που εξάγονται είναι αρκετά και σημαντικά. Όπως σε κάθε μεγάλο και πολύπλοκο σύστημα, παρατηρείται το γεγονός ότι οι στόχοι που τίθενται δεν πραγματοποιούνται πάντα με τον ιδανικότερο τρόπο. Έτσι, όπως εξάλλου ήταν αναμενόμενο, υπάρχει τεράστια ανταλλαγή απόδοσης του συστήματος σε χρόνο, υπολογιστικό κόστος και κερδισμένο εύρος ζώνης. Κατάλληλη κατάτμηση του συστήματος σε περιφέρειες θα οδηγούσε σε καλύτερη αξιοποίηση των πόρων του συστήματος, χωρίς να το φθείρει, ενώ μακροσκοπικά, το κέρδος σε εύρος ζώνης θα ήταν πολύ μεγάλο.

Το πρόβλημα της διαμέλισης του συστήματος εισάγει ένα νέο πρόβλημα, το οποίο έχει να κάνει με τον αναγκαίο εξοπλισμό που πρέπει να αποκτηθεί για την υλοποίηση του συστήματος. Οι συσκευές μέτρησης, οι οποίες ως χρέος έχουν την περισυλλογή δεδομένων, δεν έχουν να επιτελέσουν κάποιο ιδιαίτερα πολύπλοκο έργο, κι έτσι θα μπορούσαν χωρίς κάποιο κόστος στην απόδοση του συστήματος να αποτελούνται από πραγματικά χαμηλού

κόστους και ισχύος μικροσυστήματα. Αντίθετα με αυτό, οι συναθροιστικές συσκευές πρέπει να είναι σχετικά ισχυρές, αν οι περιφέρειες είναι σχετικά αυξημένου μεγέθους, ή και λιγότερο ισχυρές, αν οι περιφέρειες είναι περιορισμένες σε μερικές εκατοντάδες μονάδες ελέγχου η κάθε μία. Τα σημεία ελέγχου, τα οποία ούτως ή άλλως αναμένεται να είναι λίγα σε αριθμό, πρέπει να είναι πολύ ισχυρά, αν ο συνολικός αριθμός των συσκευών ελέγχου είναι μεγάλος, καθώς πρέπει κατά τακτά χρονικά διαστήματα να επιδεικνύουν μεγάλη υπολογιστική δύναμη για την όσο το δυνατόν εγκυρότερη απεικόνιση της κατάστασης του δικτύου.

Σε κάθε περίπτωση, χρέος του μηχανικού που θα σχεδιάσει το τελικό σύστημα αποτελεί η αξιολόγηση των διάφορων μεταβλητών που εισάγονται άμεσα και έμμεσα στο σχεδιασμό. Για κάθε σύστημα, οι μεταβλητές αυτές θα δημιουργούν ένα κατώφλι επίδοσης, το οποίο καλείται να αναγνωρίσει και να αξιοποιήσει καλύτερα, προς όφελος τόσο της απόδοσης του συστήματος όσο και της οικονομίας της υλοποίησης αυτού.

# 6 Συμπεράσματα – Προτάσεις για μελλοντική έρευνα

Η απελευθερωμένη αγορά των τηλεπικοινωνιών έχει ωθήσει πολλούς εναλλακτικούς παρόχους τηλεπικοινωνιακών υπηρεσιών να αναζητήσουν λύση για τη δυναμική εισαγωγή τους στην αγορά των επικοινωνιών, προσπαθώντας να πετύχουν φυσικά μεγιστοποίηση του κέρδους τους, με ταυτόχρονη ελαχιστοποίηση των εξόδων τους και του κινδύνου επένδυσης. Τα συστήματα PLC, και ιδιαίτερα το ευρυζωνικό κομμάτι αυτών το λεγόμενο BPL, παρουσιάζονται ως μια πολλά υποσχόμενη νέα τεχνολογία, η οποία φαίνεται να έχει βιώσιμο και επικερδή χαρακτήρα. Τα συστήματα BPL δομούνται με τρόπο κυψελωτό πάνω από τα υπάρχοντα δίκτυα μεταφοράς ηλεκτρικής ενέργειας, προσφέροντας ένα στιβαρό και σύγχρονο τηλεπικοινωνιακό περιβάλλον, πλήρως προσαρμοσμένο στις σημερινές ανάγκες του τηλεπικοινωνιακού κόσμου.

Τα συστήματα BPL εκτός από τα πολλαπλά πλεονεκτήματα στην αγορά των επικοινωνιών, παρουσιάζει χαρακτηριστικά που το καθιστούν εξαίρετο μέσο διαχείρισης του ηλεκτρικού δικτύου μιας εταιρίας παροχής ηλεκτρικής ισχύος. Το γεγονός ότι τα BPL συστήματα βασίζονται στα υπάρχοντα ηλεκτρικά δίκτυα, μπορεί να επιτρέψει την καλύτερη διαχείριση και τον αποτελεσματικότερο έλεγχο των δικτύων αυτών.

Τα έξυπνα δίκτυα ηλεκτρικής ενέργειας (Smart Grids) αποτελούν τη μετεξέλιξη των κλασσικών σχημάτων μεταφοράς ενέργειας, τα οποία πλέον δείχνουν την ηλικία τους, όντας δυσκίνητα, τεχνολογικά ξεπερασμένα, δύσκολα στη διαχείριση ενώ ταυτόχρονα παρουσιάζουν αδυναμία αποτελεσματικής ενσωμάτωσης των ταχέως αναπτυσσόμενων εναλλακτικών πηγών ενέργειας. Τα έξυπνα δίκτυα ηλεκτρικής ενέργειας έχουν όχι μόνο τη δυνατότητα να υπερκαλύψουν όλα αυτά τα μειονεκτήματα, αλλά μπορούν επίσης να προσθέσουν και νέα πλεονεκτήματα, όπως είναι οι νέες θέσεις εργασίας, η καλύτερη διακρατική συνεργασία για την καλύτερη εκμετάλλευση της παραγόμενης ενέργειας και η βελτίωση της ποιότητας της παρεχόμενης ενέργειας. Όλα αυτά, φαίνεται να εκφράζονται και με άλλους τρόπους, όπως είναι για παράδειγμα η εμφάνιση του όρου της ενέργειας negawatt. Ο όρος αυτός εκφράζει την ενέργεια που προκύπτει από εξοικονόμηση, και όχι από αντίστοιχη αύξηση της παραγωγής. Με την εισαγωγή του negawatt ως εμπορεύσιμης μονάδας εξοικονομημένης ΗΕ, ένας ιδιώτης ή φορέας μπορεί να «παράγει» negawatt αυξάνοντας την ενεργειακή απόδοση μιας συγκεκριμένης εφαρμογής ή περιοχής και να πωλήσει φθηνότερα την ΗΕ που εξοικονομείται σε ένα μεγάλο βιομηχανικό καταναλωτή.

Όπως γίνεται εύκολα αντιληπτό, κάτι τέτοιο μπορεί να έχει ευεργετικά αποτελέσματα σε σχέση με το υπάρχον κατεστημένο παραγωγής και κατανάλωσης ενέργειας. Με δεδομένη τη σταδιακή εξάντληση των πρώτων υλών παραγωγής ενέργειας και τις επιπτώσεις της παραγωγής αυτής με τις ύλες αυτές, η εξοικονόμηση ενέργειας προσφέρει εκτός από τεράστια οικονομικά, πολλαπλά περιβαλλοντικά οφέλη. Φυσικά, προκειμένου να καταστεί δυνατή η ορθή εκμετάλλευση της εξοικονομούμενης ενέργειας , πρέπει να ληφθούν κάποια μέτρα και να ευρεθούν νέοι τρόποι από τις εκάστοτε ρυθμιστικές αρχές παραγωγής ενέργειας (27). Πιο συγκεκριμένα, πρέπει να γίνει επαναπροσδιορισμός του ενεργειακού προβλήματος ώστε να βρεθούν οι καλύτεροι τρόποι εξοικονόμησης ενέργειας και οι καλύτεροι εναλλακτικοί τρόποι παραγωγής αυτής, ενώ ταυτόχρονα να δοθούν τα εχέγγυα για τη διαμόρφωση και σταθεροποίηση του νέου ενεργειακού περιβάλλοντος που θα δημιουργηθεί. Φυσικά, πρέπει τα εταιρικά βιομηχανικά συμφέροντα βρουν νέους τρόπους έκφρασης, χωρίς φυσικά κάτι τέτοιο να έχει επιπτώσεις στον ανταγωνισμό που επικρατεί στα πλαίσια μιας απελευθερωμένης αγοράς ενέργειας. Τα συστήματα BPL φαίνονται λόγω των μοναδικών ιδιοτήτων τους να μπορούν να κάνουν πραγματικότητα τα έξυπνα δίκτυα, και να καταστήσουν τον όρο negawatt μέρος της καθημερινής μας ζωής.

Φυσικά όλα αυτά, πρέπει να μπορούν να λειτουργούν σε ένα αυτοματοποιημένο, πλήρως προστατευμένο περιβάλλον, που θα μπορεί να λειτουργεί με διαφανή τρόπο, έχοντας παράλληλα τη δυνατότητα αυτόματου ελέγχου του συστήματος, και αυτόματης παραμετροποίησης αυτού. Η πιθανή δυνατότητα ανάνηψης σε περίπτωση επίθεσης θα ήταν φυσικά ευπρόσδεκτη. Τα παραπάνω χαρακτηριστικά αποτελούν τις ιδιότητες των αποκαλούμενων αυτόνομων συστημάτων, τα οποία έχει δειχθεί ότι μπορούν να αυξήσουν την παραγωγικότητα και την ποιότητα λειτουργίας των συστημάτων στα οποία ενσωματώνονται. Δεδομένης λοιπόν της σημασίας των αρχών των αυτόνομων συστημάτων, έγινε προσπάθεια ανεύρεσης ενός πρωτοκόλλου το οποίο θα μπορούσε να βοηθήσει στον έλεγχο του έξυπνου δικτύου ενέργειας. Ένα πρωτόκολλο το οποίο παρουσιάζει όλα τα χαρακτηριστικά των αυτόνομων συστημάτων, χωρίς όμως να θέτει περιορισμούς στον καθορισμό των απαραίτητων κάθε φορά παραμέτρων λειτουργίας του, είναι το Universal Plug and Play (UPnP).

Η εφαρμογή που δημιουργήθηκε στα πλαίσια αυτής της διπλωματικής εργασίας, βασίστηκε στο UPnP, όντας πλήρως προσαρμοσμένη στις ανάγκες ελέγχου ενός έξυπνου δικτύου. Μέσω αυτής μπορεί να καταστεί δυνατή η απομακρυσμένη διαχείριση ολόκληρου του δικτύου διανομής ενέργειας, με τρόπο διαφανή και αυτό – προσαρμοζόμενο, χωρίς

ανθρώπινη παρέμβαση. Ένα σημαντικό χαρακτηριστικό του πρωτοκόλλου UPnP είναι η αυτόματη αναγνώριση των πρωτοεμφανιζόμενων συσκευών ελέγχου στο δίκτυο, χαρακτηριστικό ιδιαίτερα σημαντικό όπως εύκολα γίνεται αντιληπτό. Στη συνέχεια, και μετά τη δημιουργία του πρωτοκόλλου, δημιουργήθηκε στα πρότυπα των Ασύρματων Δικτύων Αισθητήρων ένα σχήμα συνάθροισης της πληροφορίας ελέγχου που ρέει μέσω XML πακέτων (όπως ορίζει το UPnP) με απώτερο στόχο την ελαχιστοποίηση της ροής της πληροφορίας στο δίκτυο. Κατόπιν, μελετήθηκαν διάφορα σχήματα κρυπτογράφησης της πληροφορίας αυτής, με απώτερο στόχο τη θωράκιση του συστήματος απέναντι σε πιθανές επιθέσεις εναντίον του. Τελικά, επιλέχθηκε ένα σχήμα το οποίο συνδυάζει πολύ καλές επιδόσεις σε θέματα ασφαλείας, και ταυτόχρονα εκτελείται γρήγορα, χωρίς ανάγκη αυξημένων υπολογιστικών πόρων.

Οι πειραματικές μετρήσεις οι οποίες έγιναν, επιβεβαίωσαν τις προσδοκίες μείωσης της μεταφερόμενης κίνησης, όμως κατέδειξαν ότι υπάρχει τεράστια συσχέτιση της απόδοσης του συστήματος με την αρχιτεκτονική του δικτύου ελέγχου. Το μέγεθος των περιφερειών ελέγχου που θα δημιουργηθούν με βάση τα ενδιάμεσα κομβικά σημεία συνάθροισης καθορίζει τόσο το μέγεθος της μεταφερόμενης κίνησης της πληροφορίας, όσο και την υπολογιστική ισχύ που απαιτείται για τη διεκπεραίωση των απαιτούμενων εργασιών.

Με βάση τα παραπάνω, απομένει να μελετηθεί και να μοντελοποιηθεί αρχικά σε θεωρητική και κατόπιν σε πρακτική βάση, ένα σχήμα απόφασης που θα αποφασίζει πότε και πού ένας κόμβος συνάθροισης πρέπει να εισαχθεί στο σύστημα, και τι επίπτωση θα έχει κάτι τέτοιο στην ολική απόδοση του συστήματος. Η θεωρία παιγνίων αναμένεται να διαδραματίσει σημαντικό ρόλο στην εύρεση του σχήματος αυτού. Η ολοκλήρωση της εφαρμογής ελέγχου με όλα τα χαρακτηριστικά που μπορεί να επιθυμεί ένας πάροχος ηλεκτρικής ενέργειας είναι κάτι επίσης πολύ σημαντικό. Τέλος, ένα άλλο τελείως διαφορετικό αλλά κρίσιμο σημείο μελέτης, είναι η εύρεση κατάλληλων τρόπων αυτόματης ένταξης στο δίκτυο εναλλακτικών και κατανεμημένων πηγών ενέργειας, καθώς και της έννοιας των negawatt ισχύος που αναμένεται να βρεθεί στο προσκήνιο ήδη μέσα στα επόμενα χρόνια.

# 7 Βιβλιογραφία


1. **Halid Hrasnica, Abdelfatteh Haidine, Ralf Lehnert.** *Broadband PowerLine Communications - Network Design.* s.l. : John Wiley & Sons, Ltd, 2004.

2. **National Telecommunications and Information Administration.** *Potential Interference From Broadband Over Power Line (BPL) Systems To Federal Goverment Radiocommunications at 1.7-80 MHz Vol. 1.* s.l. : NTIA, Απρίλιος 2004.

3. **Federal Communication Commission.** *Part 15 - Radio Frequency Devices.* 2006.

4. **Bart Jacob, Richard Lanyon-Hogg, Devaprasad K Nadgir, Amr F Yassin.** *A Practical Guide to the IBM Autonomic Toolkit.* s.l. : IBM, 2004.

5. **IBM Corporation.** *Autonomic computing:strengthening manageability for SOA implementations.* New York : IBM, 2006.

6. **European Commission.** Green Paper: A European strategy for sustainable, competitive and secure energy. *European Commission - Energy - The Green Paper Energy.* [Ηλεκτρονικό] 8 Μαρτίου 2006. http://ec.europa.eu/energy/green-paper-energy/index_en.htm.

7. **European Comission.** Towards Smart Power Networks. s.l. : European Comission, 2005.

8. **European Commission.** European Smartgrids Technology Platform. s.l. : European Commission, 2006.

9. **Mazza, Patrick.** *Powering up the Smart Grid.* s.l. : Climate Solutions, 2005.

10. **Kannberg, LD et al.** The benefits of a Transformed Energy System. s.l. : Pacific Northwest National Laboratory, 2003.

11. **Harbor Research.** Smart Power: Pervasive Internet Technology in a Changing Energy Market. 2005.

12. **Baer , Walter S et al.** *Estimating the Benefits of the Gridwise Initiative.* s.l. : RAND Science and Technology, 2004.

13. *Squeezing more out of renewable energy.* **Storck, Pascal.** Seattle : s.n., 2003.

14. *Critical Thinking about Energy: The case for Decentralized Generation of Electricity.* **Casten, Thomas R, Brennan Downes.** s.l. : Skeptical Inquirer, 2005, Τόμ. January/February.

15. **Νικολαΐδης, Απόστολος.** *Απομακρυσμένη διαχείριση του IP συνδρομητικού εξοπλισμού με χρήση XML τεχνολογιών.* Αθήνα : Εθνικό Μετσόβιο Πολυτεχνείο, 2006.

16. **UPnP Forum.** *UPnP Device Architecture 1.0.* s.l. : UPnP Forum, 2006.

17. **Brent Miller, Toby Nixon, Charlie Tai, Mark Wood.** Home Networking with Universal Plug and Play. *IEEE Communications Magazine.* December, 2001.

18. **Intel Corporation.** *Linux SDK for UPnP Devices Version 1.4.* s.l. : Intel Corporation, 2003.

19. **UPnP Forum.** Internet Gateway Device (IGD) V 1.0. *UPnP Forum.* [Ηλεκτρονικό] 19 Νοέμβριος 2001. http://www.upnp.org/standardizeddcps/igd.asp.

20. **Rajgopal Kannan, S. Sitharama Iyengar.** Game-Theoretic Models for Reliable Path-Length and Energy-Constrained Routing With Data Aggregation in Wireless Sensor Networks. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.* 6 AUGUST , 2004, Τόμ. 22, 2004.

21. **Apostolos Nikolaidis, et al.** Management Traffic in Emerging Remote Configuration Mechanisms for Residential Gateways and Home Devices. *IEEE Communications Magazine.* May, 2005.

22. **W3C.** Document Object Model (DOM). *W3C - World Wide Web Consortium.* [Ηλεκτρονικό] http://www.w3.org/DOM/.

23. **Βικιπαίδεια.** Κρυπτογραφία. *Βικιπαίδεια.* [Ηλεκτρονικό] 2007. http://el.wikipedia.org/wiki/Κρυπτογραφία.

24. **Mactaggart, Murdoch.** Introduction to cryptography, Part 2: Symmetric cryptography. [Ηλεκτρονικό] http://www.ibm.com/developerworks/library/s-crypt02.html.

25. **Menezes et.al.** *Handbook of Applied Cryptography.* s.l. : CRC Press, 2001.

26. **Mactaggart, Murdoch.** Introduction to cryptography, Part 3: Asymmetric cryptography. [Ηλεκτρονικό] http://www.ibm.com/developerworks/library/s-crypt03.html.

27. **Laboratories, RSA.** RSA FAQ. *RSA Laboratories.* [Ηλεκτρονικό] http://www.rsa.com/rsalabs/node.asp?id=2152.

28. **Selinger, Peter.** ccrypt - FAQ. *ccrypt.* [Ηλεκτρονικό] 2007. http://ccrypt.sourceforge.net/faq.html.

29. **Κωττής, Παναγιώτης.** Το negawatt & το έξυπνο δίκτυο. *EvThesis.* [Ηλεκτρονικό] 20 Ιούνιος 2007. http://www.enthesis.net/index.php?news=469.