ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μελέτη των Ευφυών Δικτύων Ενέργειας (Smart Grid) από την σκοπιά των τεχνολογιών Δικτύων και Ασφάλειας

Του φοιτητή

Λιάππη Γεωργίου

Αρ. Μητρώου: 07/3242

Επιβλέπων καθηγητής

Δρ. Περικλής Χατζημίσιος

Αναπληρωτής Καθηγητής ΑΤΕΙΘ

Θεσσαλονίκη 2014

ΠΡΟΛΟΓΟΣ

Τα ευφυή δίκτυα ενέργειας αποτελούν μια από τις πιο καινοτόμες ιδέες των τελευταίων ετών. Η ανάγκη για καλύτερη διαχείριση της παραγόμενης ενέργειας, το κόστος αυτής, αλλά και η ανάγκη παραγωγής ενέργειας από ανανεώσιμες πηγές οδηγούν στην εξέλιξη του κλασικού ηλεκτρικού δικτύου. Επίσης, η ανάγκη δημιουργίας ενός κατανεμημένου δικτύου, όπου παρέχει υψηλή αξιοπιστία και διαθεσιμότητα έχουν οδηγήσει στην εξέλιξη αυτή. Ένα ευφυές δίκτυο ενέργειας, δεν είναι τίποτα άλλο, από ένα μοντέρνο δίκτυο ηλεκτρικής ενέργειας, όπου οι καταναλωτές, σαν οντότητες συμμετέχουν ενεργά στην διαχείριση της ενέργειας, αλλά και στην παραγωγή αυτής. Ο όρος ευφυές πηγάζει ακριβώς από αυτή την λεπτομέρεια, ότι στο δίκτυο αυτό, η διαχείριση της ενέργειας γίνεται δυναμικά και ζωντανά. Ωστόσο, αυτό απαιτεί την χρήση τεχνολογιών επικοινωνίας ανάμεσα στα τμήματα που απαρτίζουν ένα ευφυές δίκτυο ενέργειας με σκοπό η επικοινωνία να είναι αμφίδρομη.

Με την εισαγωγή των τεχνολογιών επικοινωνίας τα ευφυή δίκτυα ενέργειας αποκτούν μια άλλη διάσταση, συγκρινόμενα με υποδομές όπως είναι το διαδίκτυο, λόγω ότι κάθε οικία συνδέεται στο ευφυές δίκτυο ενέργειας, ενώ η γεωγραφική κάλυψη είναι πολύ μεγάλη. Η χρήση των ήδη υπαρχόντων τεχνολογιών όμως δεν είναι εύκολη υπόθεση, γιατί τα ευφυή δίκτυα ενέργειας, έχουν ιδιαίτερες απαιτήσεις, συνεπώς απαιτείται ακόμα χρόνος για την κατάλληλη σχεδίαση τεχνολογιών, προτύπων και πρωτοκόλλων για την χρήση τους στα ευφυή δίκτυα ενέργειας. Σε ένα δίκτυο επικοινωνιών τέτοιας ευρείας κλίμακας, σημαντικό παράγοντας είναι η διαθεσιμότητα του δικτύου όπου πρέπει να εξασφαλίζεται με τα κατάλληλα μέτρα προστασίας. Λόγω της σημαντικότητας των ευφυών δικτύων ενέργειας, μιας και σχετίζονται με την παροχή ενέργειας, όπως είναι λογικό συγκεντρώνουν το ενδιαφέρον για επιθέσεις κακόβουλων χρηστών. Έτσι κάθε ευφυές δίκτυο ενέργειας, είναι απαραίτητο να σχεδιάζεται εξ αρχής με γνώμονα την λήψη όλων των μέτρων προστασίας. Συνεπώς, η επικοινωνία και η ασφάλεια είναι καθοριστικοί παράγοντες για την λειτουργία των ευφυών δικτύων ενέργειας.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία έχει ως αντικείμενο την μελέτη των ευφυών δικτύων ενέργειας από την σκοπιά των τεχνολογιών επικοινωνίας και ασφάλειας. Αρχικά πραγματοποιείται μελέτη των τεχνολογιών επικοινωνίας που είναι κατάλληλες για εφαρμογή στα ευφυή δίκτυα ενέργειας, για την κάλυψη των απαιτήσεων και όλων των ιδιαιτεροτήτων που παρουσιάζουν τα ευφυή δίκτυα ενέργειας. Οι απαιτήσεις εστιάζονται στην καθυστέρηση του δικτύου, στο ρυθμό μετάδοσης δεδομένων, στην αξιοπιστία, στην ασφάλεια και στην διαθεσιμότητα. Έκτος όμως από τις απαιτήσεις αυτές, άλλοι σημαντικοί παράγοντες είναι η αρχιτεκτονική του δικτύου επικοινωνιών, η γεωγραφική κάλυψη αλλά και το κόστος υλοποίησης του δικτύου επικοινωνιών. Για την κάλυψη των αναγκών αυτών, οι τεχνολογίες ταξινομούνται σε ασύρματες και ενσύρματες, μελετιούνται οι καθεμία ξεχωριστά για τον τρόπο που μπορούν να έχουν εφαρμογή στα ευφυή δίκτυα ενέργειας και σε ποιες περιοχές τους. Σε δεύτερη φάση, σε αυτή την πτυχιακή εργασία ασχολούμαστε με την μελέτη της ασφάλειας για την προστασία του δικτύου και των δεδομένων που διακινούνται σε αυτό. Γίνεται ανάλυση των ευπαθειών και των απειλών που παρουσιάζονται στα ευφυή δίκτυα ενέργειας, με κύριο στόχους να αποτελούν η διαθεσιμότητα του δικτύου, η ακεραιότητα και η ιδιωτικότητα των δεδομένων, ενώ παρουσιάζονται καινούριες επιθέσεις που εμφανίζονται για πρώτη φορά στα ευφυή δίκτυα ενέργειας. Για την κάλυψη αυτών των βασικών στόχων απαιτούνται να ληφθούν μέτρα ασφαλείας για όλο το εύρος ενός ευφυούς δικτύου ενέργειας. Ενώ, οι στόχοι είναι κοινοί παντού για κάθε περιοχή μπορούν να διαφέρουν σε βαρύτητα. Χαρακτηριστικά η διαθεσιμότητα στο WAN έχει τον πρώτο λόγο σε σχέση με τους άλλους δυο στόχους. Τα μέτρα ασφαλείας, εστιάζουν στην έγκαιρη ανίχνευση των επιθέσεων και στην αντιμετώπιση τους, στη χρήση τεχνικών αυθεντικοποίησης που έχουν σχεδιασθεί αποκλειστικά για τα ευφυή δίκτυα ενέργειας, στην εξασφάλιση της ακεραιότητας αλλά και την προστασία της ιδιωτικότητας των δεδομένων. Η ιδιωτικότητα αποτελεί μεγάλο πεδίο έρευνας ενώ ο στόχος είναι η σχεδίαση σχημάτων που προσθέτουν μικρό φόρτο στην επικοινωνία. Τέλος, πραγματοποιείται αναλυτική μελέτη όλων των προτύπων και πρωτοκόλλων που σχετίζονται με τις επικοινωνίες και την ασφάλεια και ειδικότερα αυτών που έχουν σχεδιασθεί αποκλειστικά για χρήση στα ευφυή δίκτυα ενέργειας.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω όλους όσους με στήριξαν κατά την διάρκεια των σπουδών μου και στην συγγραφή αυτής της πτυχιακής εργασίας για την απόκτηση του πτυχίου μου από το τμήμα Μηχανικών Πληροφορικής του Α.Τ.Ε.Ι.Θ.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ

Η παρούσα πτυχιακή εργασία εστιάζει στην μελέτη των ευφυών δικτύων ενέργειας από την σκοπιά των τεχνολογιών επικοινωνίας και ασφάλειας. Στόχος είναι η μελέτη των τεχνολογιών επικοινωνίας που βρίσκουν εφαρμογή στα ευφυή δίκτυα ενέργειας και όλων των μέτρων προστασίας που πρέπει να ληφθούν για την προστασία των ευφυών δικτύων ενέργειας. Η πτυχιακή αυτή εργασία, χωρίζεται σε επτά κεφάλαια. Το πρώτο κεφάλαιο πραγματοποιεί μια εισαγωγή στα ευφυή δίκτυα ενέργειας που είναι απαραίτητη για την καλύτερη κατανόηση του αντικειμένου. Στο δεύτερο κεφάλαιο παρουσιάζεται η αρχιτεκτονική των ευφυών δικτύων ενέργειας, από την πλευρά των δικτύων ενώ καθορίζονται οι βασικές απαιτήσεις επικοινωνίας. Στο τρίτο κεφάλαιο, γίνεται διεξοδική μελέτη των ασύρματων τεχνολογιών που έχουν εφαρμογή στα ευφυή δίκτυα ενέργειας, και ειδικότερα με πιο τρόπο γίνεται η εφαρμογή αυτή αλλά και οι ιδιαιτερότητες που παρουσιάζουν. Αντίστοιχα, στο τέταρτο κεφάλαιο γίνεται μελέτη των ενσύρματων τεχνολογιών. Στο σημείο αυτό, έχει ολοκληρωθεί η μελέτη του πρώτου μέρους που σχετίζεται με τις επικοινωνίες. Στο δεύτερο μέρος που ξεκινάει από το πέμπτο κεφάλαιο, πραγματοποιείται μελέτη της ασφάλειας των ευφυών δικτύων ενέργειας, και ειδικότερα της ασφάλειας των επικοινωνιών και των δεδομένων που διακινούνται στο δίκτυο. Έτσι λοιπόν, στο πέμπτο κεφάλαιο καθορίζονται οι βασικές αρχές που πάνω σε αυτές στηρίζεται η μελέτη, ενώ αναλύονται οι ευπάθειες και οι απειλές που εμφανίζονται στα ευφυή δίκτυα ενέργειας. Κάποιες από τις απειλές αυτές είναι ήδη γνωστές, ενώ μερικές από αυτές είναι νέες και εμφανίζονται αποκλειστικά στα ευφυή δίκτυα ενέργειας, εκμεταλλευόμενες το δίκτυο και τις αδυναμίες προτύπων και πρωτοκόλλων. Στο έκτο κεφάλαιο, αφού έχουν καθοριστεί οι βασικοί στόχοι και απειλές, γίνεται μελέτη των μέτρων προστασίας που πρέπει να ληφθούν στα ευφυή δίκτυα ενέργειας και η ταξινόμηση αυτών με βάση τις τρεις περιοχές που χωρίζεται το δίκτυο επικοινωνιών. Τα μέτρα προστασίας εστιάζουν στην ανίχνευση και αντιμετώπιση επιθέσεων, στην διαθεσιμότητα του δικτύου επικοινωνιών, στην ακεραιότητα και την εμπιστευτικότητα των δεδομένων, αλλά και στην αυθεντικοποίηση χρηστών και συσκευών. Τέλος, στο έβδομο και τελευταίο κεφάλαιο γίνεται αναφορά και παρουσίαση όλων των προτύπων και πρωτοκόλλων που σχετίζονται με τις τεχνολογίες επικοινωνιών και ασφάλειας. Στο τέλος του κεφαλαίου υπάρχει συγκεντρωτικός πίνακας για την συνοπτική παρουσίαση τους.

ΚΕΦΑΛΑΙΟ 1

SMART GRID - ΕΝΑ ΕΞΥΠΝΟ ΗΛΕΚΤΡΙΚΟ ΔΙΚΤΥΟ

ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό, πραγματοποιείται μια εισαγωγή στα ευφυή δίκτυα ενέργειας, ώστε ο αναγνώστης να μπορεί να κατανοήσει το σκοπό λειτουργίας τους και τα βασικά συστατικά μέρη που αποτελείται ένα ευφυές δίκτυο ενέργειας. Όπως θα δούμε, υπάρχουν πολλοί διαφορετικοί ορισμοί για ένα ευφυές δίκτυο ενέργειας, ο καθένας από διαφορετική σκοπιά περιγράφοντας όμως την ίδια ιδέα. Επίσης, παρουσιάζεται ένα αφαιρετικό μοντέλο που θεωρείται η βάση για την σχεδίαση ευφυών δικτύων ενέργειας.

1.1 ΟΡΙΖΟΝΤΑΣ ΤΟ SMART GRID

Σύμφωνα με την Institute of Electrical and Electronics Engineers (IEEE) το Smart Grid, ορίζεται ως «η επόμενη γενιά δικτύου ηλεκτρικής ενέργειας, όπου χαρακτηρίζεται από αυξημένη χρήση τεχνολογιών επικοινωνιών και πληροφορικής, στην παραγωγή, διανομή και κατανάλωση της ηλεκτρικής ενέργειας» (IEEE, IEEE Smart Grid). Σε μια άλλη εκδοχή, η Ευρωπαϊκή Ένωση ορίζει το Smart Grid ως (Grids, 2010) «ένα ηλεκτρικό δίκτυο, όπου μπορεί να ενσωματώσει τους χρήστες και την συμπεριφορά τους που είναι συνδεδεμένοι σε αυτό. Παραγωγούς ενέργειας, καταναλωτές ή και τα δύο, με σκοπό την καλύτερη διαχείριση της παραγόμενης ενέργειας με μικρές απώλειες και υψηλή ποιότητα». Μια άλλη προσέγγιση από τον οργανισμό International Electrotechnical Commission(IEC) (Commission) αναφέρει ότι ο όρος Smart Grid, είναι ένα όρος του μάρκετινγκ, και όχι ένας τεχνικός όρος. Για αυτό και σήμερα υπάρχουν διαφορετικοί ορισμοί για το Smart Grid, με την δυσκολία καθορισμού τι είναι ευφυές και τι όχι. Η γενική παραδοχή, αναφέρει ότι ένα Smart Grid, είναι ο εκμοντερνισμός του κλασσικού δικτύου ηλεκτρικής ενέργειας και περιλαμβάνει κάθε σημείο που παράγει ενέργεια και κάθε σημείο που καταναλώνει ενέργεια. Είναι ένα ηλεκτρικό δίκτυο, που ενσωματώνει καταναλωτές που είναι συνδεδεμένοι με αυτό, παράγοντας ενέργεια, καταναλώνοντας ενέργεια ή και τα δύο με σκοπό την παραγωγή, διανομή και καλή διαχείριση της ηλεκτρικής ενέργειας.

Από τους παραπάνω ορισμούς είναι κατανοητό, πως ένα Smart Grid, δηλαδή ένα ευφυές δίκτυο ενέργειας, δεν είναι τίποτα άλλο παρά η εξέλιξη των παραδοσιακών δικτύων ηλεκτρικής ενέργειας. Η κύρια διαφορά είναι ότι πλέον η παραγωγή ενέργειας, δεν γίνεται μόνο από κεντρικές υποδομές αλλά είναι κατανεμημένη, με την συμμετοχή των καταναλωτών. Αυτό γεννά, την ανάγκη της αμφίδρομης επικοινωνίας μεταξύ των τμημάτων που αποτελείται ένα ευφυές δίκτυο ενέργειας. Εκτός όμως από την παραγωγή ενέργειας εισάγονται και νέες καινοτόμες ιδέες όπως είναι η χρήση ηλεκτρικών οχημάτων αλλά και η παραγωγή ενέργειας από ανανεώσιμες πηγές.

1.2 ΠΛΕΟΝΕΚΤΗΜΑΤΑ SMART GRID

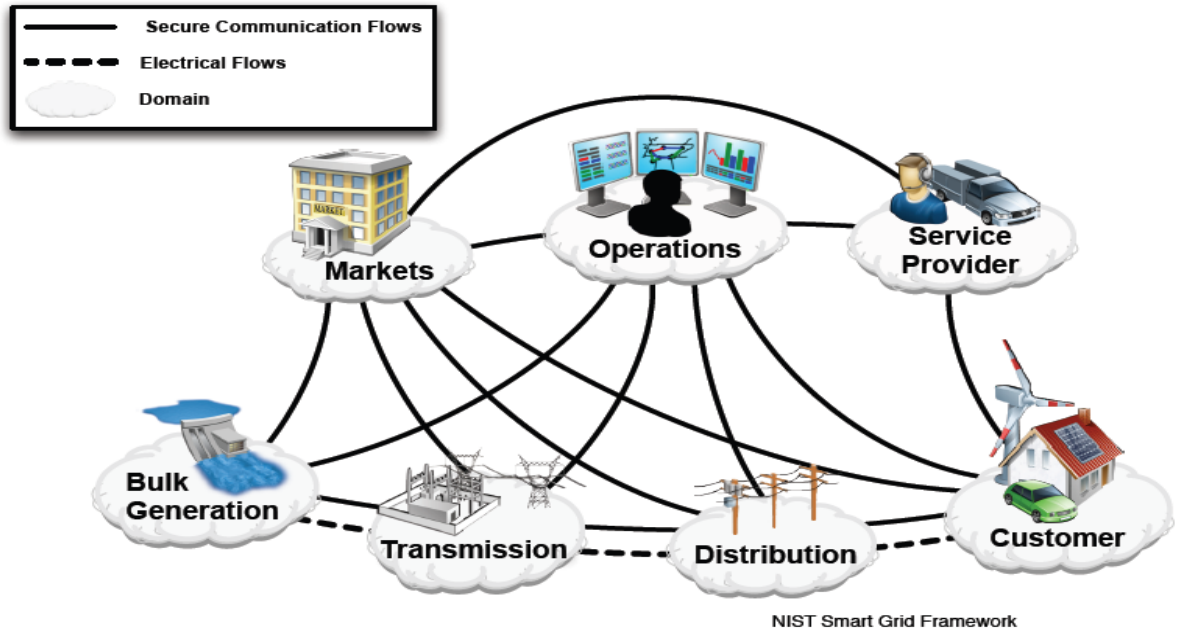
Ένα κύριο ερώτημα που δημιουργείται είναι, ότι πια είναι τα πλεονεκτήματα που παρέχουν τα ευφυή δίκτυα ενέργειας. Στο (Zahedi, 2011) παρουσιάζονται τα πλεονεκτήματα που προσφέρουν τα ευφυή δίκτυα ενέργειας:

1. Τα ευφυή δίκτυα μπορούν να βελτιώσουν την ενεργειακή απόδοση στο δίκτυο ηλεκτρικής ενέργειας καθώς σε αυτά ενσωματώνονται προηγμένες τεχνολογίες πληροφοριών (IT) και πλήθος έξυπνων συσκευών.
2. Τα ευφυή δίκτυα είναι σε θέση να αυτοματοποιήσουν, να παρακολουθούν και να ελέγχουν την αμφίδρομη ροή ηλεκτρικής ενέργειας χρησιμοποιώντας προηγμένους μετρητές, αισθητήρες και ψηφιακούς ελεγκτές.
3. Χρησιμοποιώντας το έξυπνο δίκτυο, οι εταιρίες παροχής ηλεκτρισμού θα είναι σε θέση να βελτιώσουν τον έλεγχο που διεξάγουν πάνω στο δίκτυο και θα μπορούν να συλλέγουν σύνθετες πληροφορίες πραγματικού χρόνου σχετικά με την απόδοση του δικτύου.
4. Το ευφυές δίκτυο εμποδίζει αυτόματα διακοπές και βελτιώνει την ανίχνευση υπερφορτίσεων στις γραμμές μεταφοράς.
5. Οι έξυπνοι μετρητές (βασικό συστατικό στοιχείο του έξυπνου δικτύου) δίνουν την δυνατότητα στους καταναλωτές να γνωρίζουν πόση ηλεκτρική ενέργεια καταναλώνουν στα σπίτια και στα γραφεία τους. Έξυπνες εφαρμογές μπορούν επίσης να ενημερώνουν τους καταναλωτές για το πως αυτοί μπορούν να αλλάξουν την ενεργειακή τους κατανάλωση κατά τις περιόδους αιχμής προκειμένου να εξοικονομήσουν χρήματα στους λογαριασμούς ηλεκτρικού ρεύματος.
6. Επιπλέον στο ευφυές δίκτυο μπορούν να χρησιμοποιηθούν έξυπνες εφαρμογές που να είναι έτσι προγραμματισμένες ώστε να λειτουργούν σε ώρες εκτός αιχμής. Αυτές μπορούν επίσης να θέτουν σε λειτουργία κλιματιστικά ώστε αυτά να ελέγχονται εξ αποστάσεως. Με αυτόν τον τρόπο δίνεται η δυνατότητα στους πελάτες να διαχειρίζονται καλύτερα την κατανάλωσή τους, με σκοπό να μειωθεί η ζήτηση ενέργειας σε περιόδους αιχμής
7. Το ευφυές δίκτυο καθιστά επίσης ευκολότερη την ενσωμάτωση ανανεώσιμών πηγών ενέργειας στο δίκτυο ενέργειας. Επομένως τα σπίτια και οι επιχειρήσεις που παράγουν ενέργεια μέσω τέτοιων πηγών θα μπορούν πιο εύκολα να την μοιράζονται με άλλους καταναλωτές μέσω του ευφυούς δικτύου.
8. Μέσω του ευφυούς δικτύου, ηλεκτρικά αυτοκίνητα μπορούν να φορτίζονται σε κατάλληλες χρονικές περιόδους ώστε να λειτουργούν σαν μέσα αποθήκευσης.

1.3 ΜΟΝΤΕΛΟ ΑΝΑΦΟΡΑΣ NIST

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογιών (National Institute of Standards and Technology) των Η.Π.Α, ορίζει ένα εννοιολογικό μοντέλο για τα ευφυή δίκτυα, που διαιρείται σε επτά τμήματα. Τα τμήματα αυτά περιγράφουν όχι μόνο τεχνικές λειτουργίες του δικτύου ενέργειας, αλλά και τα μέρη εκείνα που εμπλέκονται άμεσα στην παροχή ηλεκτρικής ενέργειας. Τα τμήματα αυτά είναι η, παραγωγή, μεταφορά, διανομή, πελάτες, αγορές, λειτουργίες και πάροχοι.

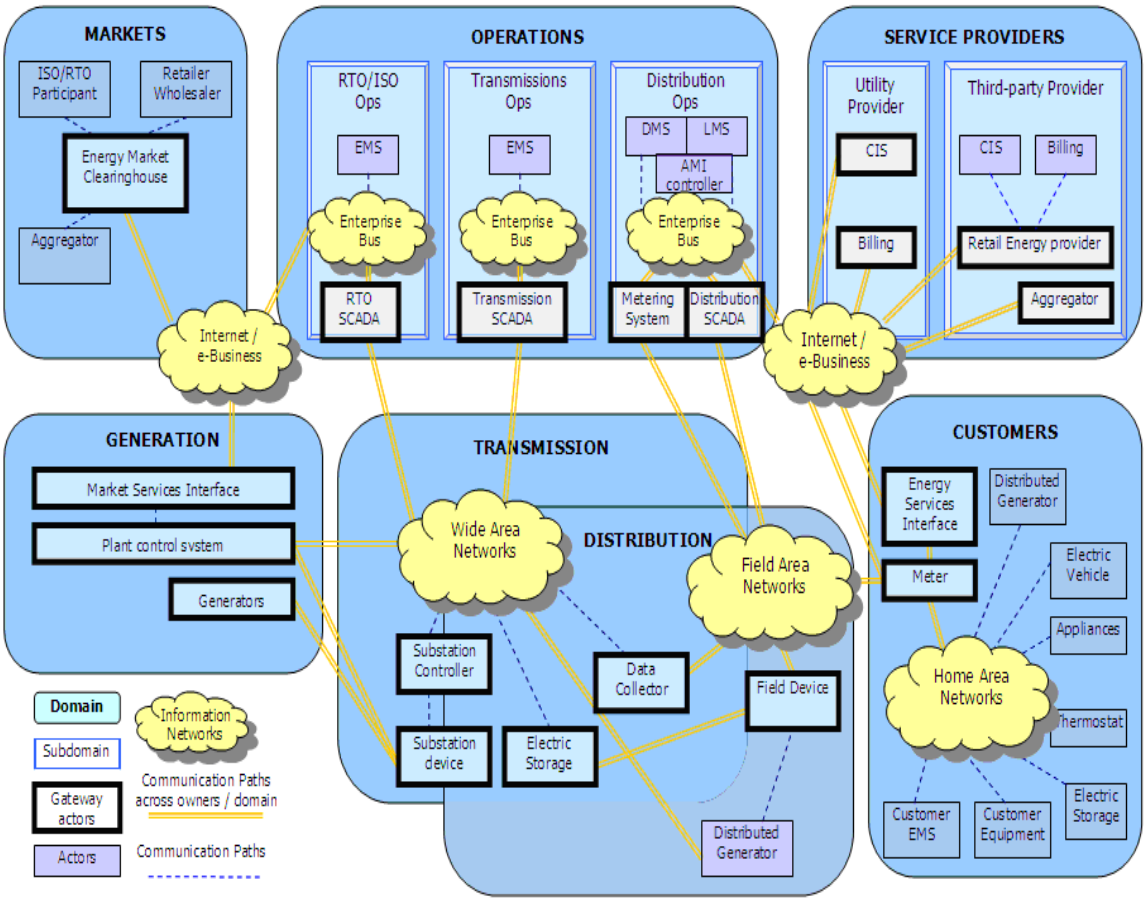
Η εικόνα 1 παρουσιάζει το πλαίσιο που προτείνεται από το NIST, για τα μονοπάτια επικοινωνίας που πρέπει να έχουν αναπτυχθεί για την ιδανική επικοινωνία. Οι τέσσερεις χαμηλότερες περιοχές είναι η, παραγωγή, μεταφορά, διανομή και οι πελάτες. Οι περιοχές αυτές περιγράφουν την παροχή και την ροή της ενέργειας. Η περιοχή της αγοράς, σχετίζεται με αγορά της ενέργειας, την συνεργασία με άλλους παρόχους ενέργειας, αλλά και την τιμή αναλόγως προσφοράς και ζήτησης. Το τμήμα τον λειτουργιών είναι υπεύθυνο για την χρέωση των πελατών, την κατανάλωση ενέργειας και την διαχείριση των λογαριασμών των πελατών γενικότερα. Τέλος, το τμήμα του παρόχου έχει ως ευθύνη την ανάπτυξη, υπηρεσιών και εφαρμογών, για τις εταιρίες ενέργειας αλλά και για τους πελάτες για την σωστή διαχείριση της ενέργειας. Τα επτά αυτά επιμέρους τμήματα είναι απαραίτητο να είναι διασυνδεμένα με συγκεκριμένα μονοπάτια επικοινωνίας αλλά και συγκεκριμένες απαιτήσεις για το καθένα ώστε να ικανοποιούν απαιτήσεις όπως real-time επικοινωνίας, ποιότητας των υπηρεσιών, και ασφάλειας συστημάτων.



Εικόνα 1 "Αφαιρετικό μοντέλο του NIST και η αλληλεπίδραση μεταξύ των μερών του" (NIST, 2012)

Στο παραπάνω μοντέλο επίσης, προτείνετε η υλοποίηση δικτύων επικοινωνίας για την υποστήριξη, συσκευών, βάσεων δεδομένων, και άλλων επιμέρους υπηρεσιών του ευφυούς δικτύου. Επειδή, όμως κάθε περιοχή έχει διαφορετικές απαιτήσεις, έτσι εφαρμόζονται διαφορετικού είδους αρχιτεκτονικές δικτύων, όπως για παράδειγμα, τοπικά δίκτυα και ευρείας περιοχής. Για το τμήμα παραγωγής ενέργειας, προτείνονται ένα σύνολο βιομηχανικών πρωτοκόλλων και τεχνολογιών σε συνδυασμό με την χρήση τοπικού δικτύου για την επικοινωνία των σταθμών παραγωγής ενέργειας. Για τα τμήματα μεταφοράς και διανομής ενέργειας, που συνδέουν υποσταθμούς και υποδομές παραγωγής ενέργειας(ανανεώσιμες πηγές, κοινές πηγές κτλ) προτείνετε η χρήση δικτύων ευρείας ζώνης(Wide Area Networks) και δικτύων περιορισμένης ζώνης(Field Area Network). Για το τμήμα πελατών, προτείνετε υλοποίηση τοπικού δικτύου με την χρήση τεχνολογιών περιορισμένης σχετικά εμβέλειας(ZigBee, Wi-Fi, Bluetooth).

Στην εικόνα παρακάτω παρουσιάζεται ένα μοντέλο αναφοράς που και αυτό έχει αναπτυχθεί από το NIST, όπου περιλαμβάνει τα επί μέρους τμήματα(domains), της πύλες δικτύου(gateways), τα μονοπάτια επικοινωνίας(communication paths), και οι οντότητες(actors).



Εικόνα 2 "Μοντέλο του NIST και τα επιμέρους τμήματα" (Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0, 2009)

Τα δίκτυα πληροφοριών(Information networks) παρουσιάζουν ένα αφαιρετικό σύνολο όπου το σύνολο της πληροφορίας μεταδίδεται για να εξυπηρετήσει την διανομή της ηλεκτρικής ενέργειας. Για παράδειγμα, το δίκτυο πληροφοριών που περιγράφεται ως Internet/e-Business, είναι κατανοητό ότι γίνεται χρήση του διαδικτύου για την επικοινωνία μεταξύ των τμημάτων, και περιλαμβάνουν χρήση τοπικών δικτύων, εξυπηρετητές, vpn, τοίχων προστασίας(firewall), πρωτοκόλλων ασφαλείας κτλ. Το δίκτυο πληροφοριών που αναφέρεται ως Enterprise, περιγράφει το εσωτερικό δίκτυο επικοινωνίας της εταιρίας παραγωγής ενέργειας ή των εταιριών αν είναι περισσότερες, που σχετίζεται με την επικοινωνία μεταξύ των διαφόρων τμημάτων, υποσταθμών κτλ. Τα δίκτυα αυτά από πλευράς αρχιτεκτονικής είναι τύπου τοπικού δικτύου(LAN) ή ασύρματων τοπικού δικτύου(WLAN) και σε συνδυασμό με πρωτόκολλα και τεχνολογίες αυτοματισμών εξυπηρετούν την επικοινωνία ανάμεσα σε υποδομές του ευφυούς δικτύου. Τα δίκτυα, Wide Area Networks και Field Area Networks, υλοποιούν τις απαιτήσεις επικοινωνίας ανάμεσα στα τμήματα μεταφοράς και διανομής της ηλεκτρικής ενέργειας. Ένα χαρακτηριστικό των δικτύων αυτών είναι θα πρέπει να υποστηρίζουν επικοινωνίας μακρινής εμβέλειας σε απόσταση που ορίζεται έως και 10 χιλιόμετρα. Τέλος το δίκτυο Home Area Network, αναφέρεται όπως είναι κατανοητό στο δίκτυο, στην μικρή εμβέλεια ενός σπιτιού ώστε να υποστηρίζονται όλοι οι αυτοματισμοί και εφαρμογές που σχετίζονται με την κατανάλωση ηλεκτρικής ενέργειας αλλά και παρακολούθησης αυτής με την χρήση των έξυπνων μετρητών.

Οι πύλες δικτύου(gateways) των τμημάτων(domain), βοηθούν στην επικοινωνίας μεταξύ των τμημάτων, χρησιμοποιώντας τεχνολογίες αναλόγως των τμημάτων που συνδέουν. Παράδειγμα, για το τμήμα του παρόχου, δύο σημαντικές πύλες είναι οι Billing, που περιγράφει την επικοινωνία που απαιτείται να υπάρχει για την καταγραφή των χρεώσεων της ηλεκτρικής ενέργειας, αλλά και το Customer Information System(CIS), που περιγράφει την επικοινωνία που απαιτείται να υπάρχει για την εξυπηρέτηση των πελατών του δικτύου από τον πάροχο. Επίσης, στο τμήμα των πελατών οι δύο πύλες που υπάρχουν είναι οι Meter, που περιγράφει την επικοινωνία των έξυπνων μετρητών που υπάρχουν σε κάθε κατοικία, για την καταγραφή της κατανάλωσης και Energy Services Interface, που σχετίζεται με την συλλογή δεδομένων από το τοπικό δίκτυο της κατοικίας που αναφερόμαστε σε αυτό ως Home Area Network, ως προς την χρήση αλλά και παραγωγή εάν υφίσταται ηλεκτρικού ρεύματος.

ΕΠΙΛΟΓΟΣ

Μέχρι στιγμής έχουμε αναφέρει βασικές πληροφορίες σχετικά με τα ευφυή δίκτυα ενέργειας, τον ορισμό τους, τα πλεονεκτήματα, και το μοντέλο αναφοράς του NIST. Η αναφορά των βασικών συστατικών και τμημάτων που αποτελείται ένα ευφυές δίκτυο ενέργειας, είναι απαραίτητο για την κατανόηση της γενικής ιδέας και το σκοπό δημιουργία των ευφυών δικτύων ενέργειας. Στο επόμενο κεφάλαιο

εστιάζουμε στο κομμάτι των επικοινωνιών και ειδικά στα συστατικά μέρη που αποτελείται το δίκτυο επικοινωνιών, στην αρχιτεκτονική όλου του δικτύου, αλλά και στις απαιτήσεις της επικοινωνίας. Ο καθορισμός των απαιτήσεων επικοινωνίας είναι πολύ σημαντικός για την επιλογή της κατάλληλης τεχνολογίας επικοινωνίας, ενσύρματης ή ασύρματης. Θα δούμε ότι για κάθε περιοχή του δικτύου ενός ευφυούς δικτύου ενέργειας οι απαιτήσεις διαφέρουν.

ΚΕΦΑΛΑΙΟ 2

ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΚΤΥΟΥ ΚΑΙ ΑΠΑΙΤΗΣΕΙΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

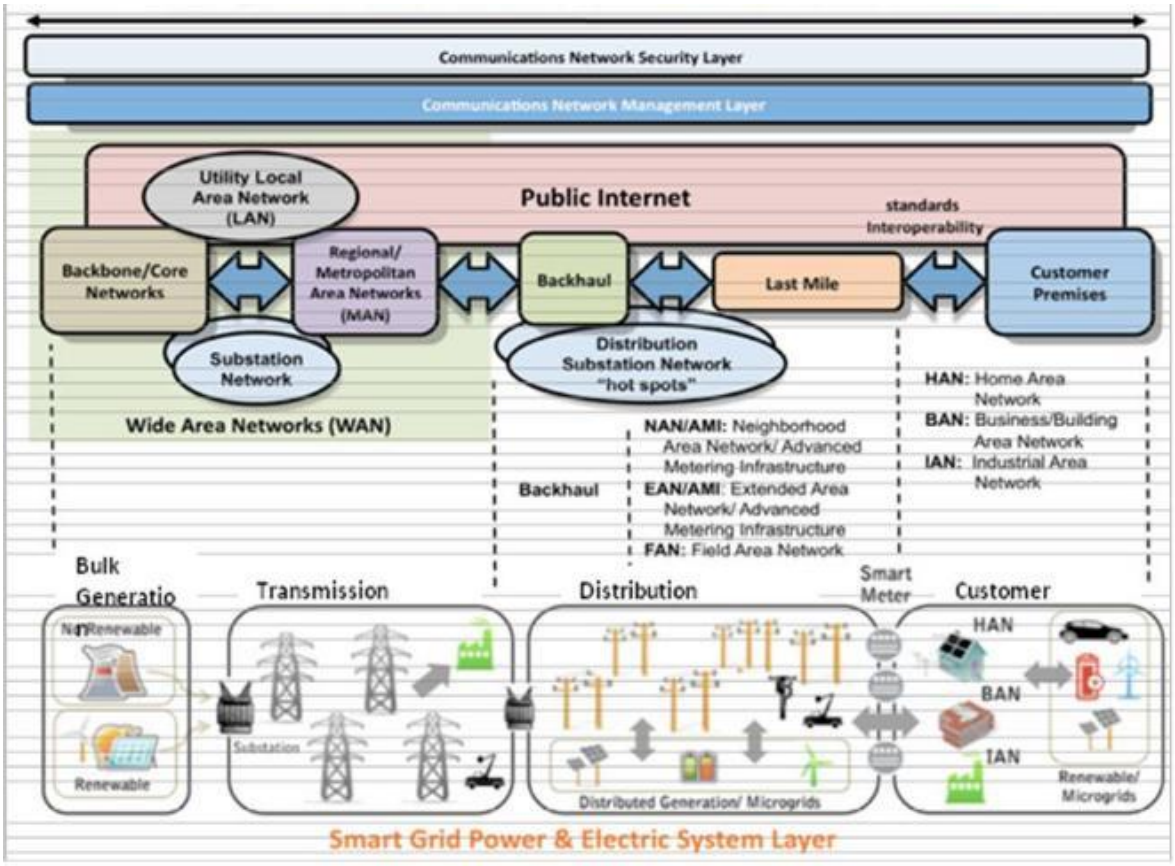
ΕΙΣΑΓΩΓΗ

Για την σχεδίαση του δικτύου επικοινωνίας ενός ευφυούς δικτύου ενέργειας, αρχικά προκύπτει το πρόβλημα που καθορισμού των οντοτήτων από τις οποίες αποτελείται. Στο κεφάλαιο αυτό, αρχικά παρουσιάζεται το πρότυπο IEEE 2030, το οποίο σχετίζεται με την διαλειτουργικότητα στα ευφυή δίκτυα ενέργειας, ώστε μέσα από οδηγίες που παρέχονται να μπορούν να καθοριστούν τα βασικά συστατικά μέρη, η ονομασία με την οποία θα χαρακτηρίζεται το καθένα και πως θα επικοινωνούν μεταξύ τους. Στην συνέχεια, αναλύονται τα τρία βασικά υπό-δίκτυα που αποτελείται ένα ευφυές δίκτυο ενέργειας, το WAN, NAN και το HAN, και πως αυτά δομούνται, ενώ αναλύονται και βασικές απαιτήσεις της επικοινωνίας για όλο το εύρος των ευφυών δικτύων ενέργειας. Κρίσιμης σημασίας για τα ευφυή δίκτυα ενέργειας είναι και η καθυστέρηση στην επικοινωνία, ενώ θα μπορούσαμε να την χαρακτηρίσουμε την σημαντικότερη παράμετρο, μιας και υπάρχουν δίκτυα όπως το WAN, όπου είναι απαιτήσεις είναι μεγάλες οποιαδήποτε παραβίαση θα δημιουργήσει προβλήματα στην λειτουργία του ευφυούς δικτύου ενέργειας.

2.1 ΜΟΝΤΕΛΟ ΕΠΙΚΟΙΝΩΝΙΑΣ IEEE P2030

Το πρότυπο του Institute of Electrical and Electronics Engineers P2030, παρέχει οδηγίες σχετικά με την κατανόηση την διαλειτουργικότητας (interoperability) στα ευφυή δίκτυα. Παρουσιάζει ένα μοντέλο αναφοράς και παρέχει, μια γνωστική βάση με ορολογία, χαρακτηριστικά, λειτουργίες, αρχές για την ανάπτυξη υποδομών, εφαρμογών και λύσεων για ένα εξελιγμένο δίκτυο μεταφοράς ενέργειας. Τα ευφυή δίκτυα, αναφέρονται σαν “System of the Systems” και οι στόχοι επικεντρώνονται στην διαλειτουργικότητα των επικοινωνιών, της παραγωγής ενέργειας και της τεχνολογίας της πληροφορίας. Επίσης, πρέπει να αναφερθεί ότι σχετίζεται άμεσα με της οδηγίες προτυποποίησης που δημοσιεύουν ο NIST και ο IEC.

Η End-to-end επικοινωνία, που χαρακτηρίζεται στον χώρο τον τηλεπικοινωνιών ως παροχή ολοκληρωμένης επικοινωνίας, είναι καθοριστικός παράγοντας στην σχεδίαση μιας αρχιτεκτονικής επικοινωνιών στα ευφυή δίκτυα. Το πρότυπο αυτό, προτείνει μια δομή που αποτελείται επί μέρους επίπεδα με διαφορετικούς στόχους το καθένα. (IEEE, IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads, 2011)



Εικόνα 3 "End-to-end μοντέλο επικοινωνίας βασισμένο στο πρότυπο IEEE P2030" (Leccese, 2012)

Στο πρώτο επίπεδο, ξεκινώντας από την κορυφή είναι το επίπεδο που σχετίζεται με την παροχή ασφάλειας στα δεδομένα που μεταδίδονται στο δίκτυο. Το δεύτερο επίπεδο, σχετίζεται με την παροχή ελέγχου στις επικοινωνίες που υπάρχουν στο ευφυές δίκτυο και ειδικότερα, στις απαιτήσεις στην ποιότητα των υπηρεσιών(Qos). Ενώ, στο τρίτο επίπεδο γίνεται χρήση του διαδικτύου ως διεπαφή για τα δίκτυα επικοινωνιών που λειτουργούν στην υποδομή του ευφυές δικτύου .

Στο κλασικό ηλεκτρικό δίκτυο που γνωρίζουμε η ηλεκτρική ενέργεια αλλά και η ροή πληροφοριών, όπως είναι η κατανάλωση, γίνεται από τα κεντρικές υποδομές ή υποσταθμούς του δικτύου προς τον τελικό καταναλωτή. Σε ένα εξελιγμένο δίκτυο, όπως είναι το ευφυές δίκτυο, η ροή της ενέργειας αλλά και των πληροφοριών είναι δύο κατευθύνσεων γιατί οι τελικοί καταναλωτές συμμετέχουν ενεργά στην διαχείριση και παραγωγή της ενέργειας κάθε χρονική στιγμή.

2.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΚΤΥΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ

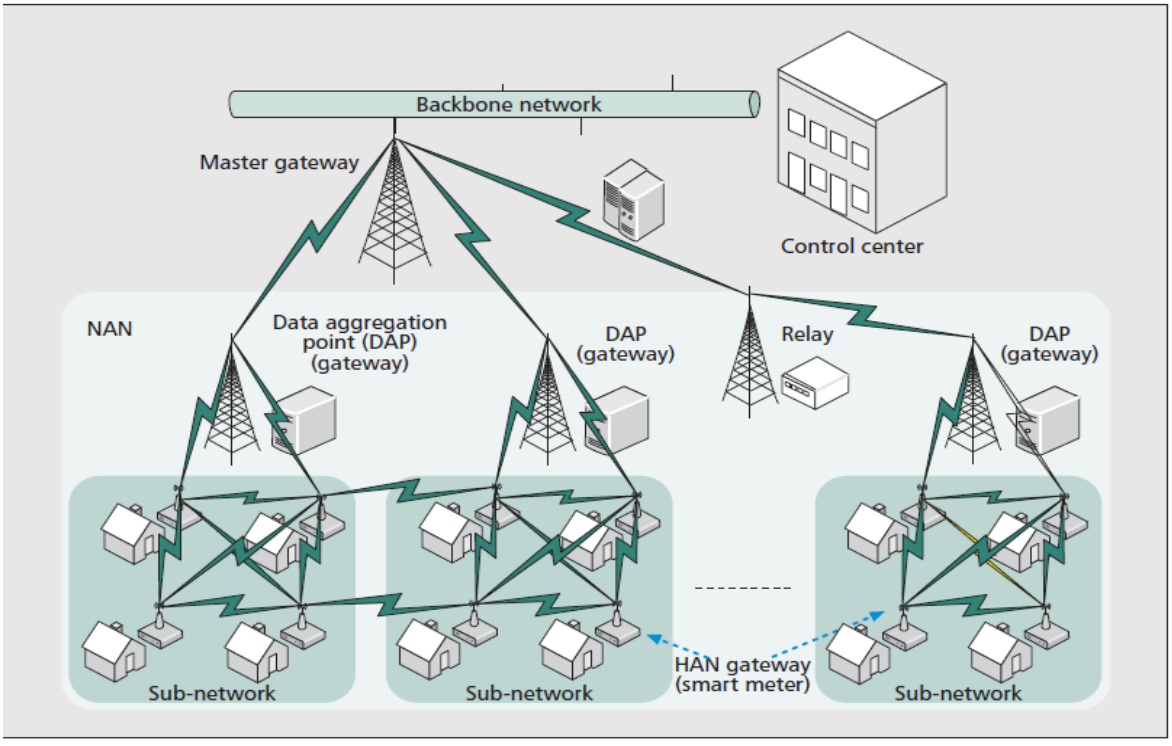
Για να περιγράψουμε τις επικοινωνίες στα ευφυή δίκτυα είναι απαραίτητο να ορίσουμε ένα πλαίσιο με την αρχιτεκτονική του δικτύου και με τις ξεχωριστές απαιτήσεις που έχει κάθε περιοχή για την επικοινωνία. Στην βιβλιογραφία η αρχιτεκτονική δικτύου σύμφωνα με τα μοντέλα που προτείνουν οι διεθνείς οργανισμοί περιγράφεται από τρείς περιοχές/δίκτυα, τα Wide Area Network, Neighborhood Area Network και Home Area Network. Παρακάτω, γίνεται μια περιγραφή της κάθε περιοχής.

1. Wide Area Network

Το WAN δίκτυο παρέχει επικοινωνία ανάμεσα στα κεντρικές υποδομές της εταιρίας παροχής ηλεκτρικής ενέργειας, τους υποσταθμούς, τις μονάδες παραγωγής ηλεκτρικής ενέργειας, τις μονάδες αποθήκευσης ηλεκτρικής και γενικά όλα τα μέρη εκείνα που παίρνουν μέρος στην παραγωγή, μεταφορά και διαχείριση της ηλεκτρικής ενέργειας. Χρησιμοποιείται για την παρακολούθηση του δικτύου ενέργειας για την κατάσταση του μέσω αισθητήρων που υπάρχουν στους υποσταθμούς ακόμη, συντελούν στην επικοινωνία μεταξύ των Intelligent Electronic Device(IED) και των κέντρων ελέγχων του παρόχου ηλεκτρικής ενέργειας. Οι συσκευές αυτές εγκαθίστανται κατά μήκος των γραμμών μεταφοράς και στους υποσταθμούς για να καταγράφουν πληροφορίες, και να ενεργούν βάση των εντολών ελέγχου που στέλνουν τα κέντρα ελέγχου. Στην πραγματικότητα είναι μικρές υπολογιστικές μονάδες, όπου επεξεργάζονται τα δεδομένα που λαμβάνουν από τους αισθητήρες που βρίσκονται στο δίκτυο ενέργειας. Τα δεδομένα σχετίζονται με την κατάσταση του δικτύου ενέργειας, όπως είναι η τάση, συχνότητα και η φάση του ηλεκτρικού ρεύματος. Έχουν την δυνατότητα να δέχονται και να εκτελούν εντολές, σύμφωνα με τα δεδομένα που λαμβάνουν. Γνωστό πρότυπο που σχετίζεται με την επικοινωνία ανάμεσα σε IED και με έμφαση στην διαλειτουργικότητα είναι το IEC 61850. Για να μπορούν να επιτευχθούν τα παραπάνω, απαιτείται ένα δίκτυο υψηλού εύρους ζώνης, για μετάδοση σε μακρινές αποστάσεις. Σε επίπεδο εφαρμογών, κάθε εφαρμογή έχει διαφορετικές απαιτήσεις επικοινωνίας και ποιότητας των υπηρεσιών, όπως η επικοινωνία των υποσταθμών απαιτεί υψηλό εύρος και μικρή χρονική καθυστέρηση, ενώ οι εφαρμογές που λειτουργούν σε συσκευές AMI, απαιτούν ευζωνικούς ρυθμούς μετάδοσης. Επίσης, μέσω των δικτύων αυτών μεταφέρονται μετρήσεις πραγματικού χρόνου, σχετικές με την κατανάλωση ενέργειας που λαμβάνονται από τους καταναλωτές μέσω των AMI και αντίστροφα πληροφορίες και το κόστος της ενέργειας ανά μονάδα προς τις συσκευές που υπάρχουν στους καταναλωτές. Οι καταλληλότερες τεχνολογίες που ταιριάζουν σε αυτά τα δίκτυα, είναι το WiMAX και κυψελοειδής τεχνολογίες, αλλά και ενσύρματες όπως οι οπτικές ίνες γιατί προσφέρουν υψηλές ταχύτητες σε μακρινές αποστάσεις και αξιόπιστες συνδέσεις. Ακόμη, οι υποσταθμοί, λειτουργούν και ως back-haul δίκτυο επικοινωνιών και ως aggregation point ανάμεσα στο WAN και FAN δίκτυο για την συγκέντρωση των μετρικών δεδομένων των καταναλωτών και προώθηση τους προς το δίκτυο του WAN. (Nico Saputro, 2012) (V. Cagri Gungor, 2012)

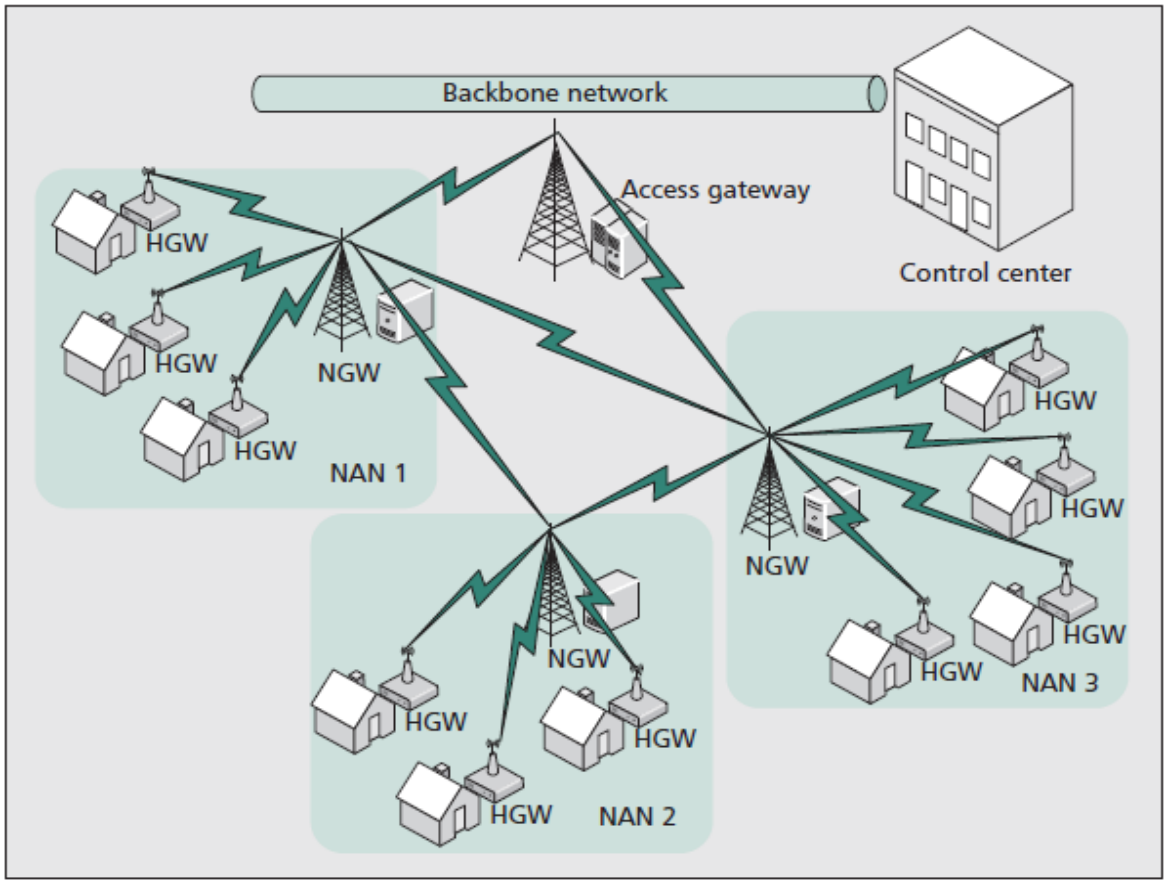
2. Neighborhood Area Network/Field Area Network

Το NAN/FAN δίκτυο καλύπτει την περιοχή ανάμεσα στο WAN και στο HAN δίκτυο ενώ, λειτουργεί σαν γέφυρα ανάμεσα σε αυτά τα δύο δίκτυα, για την ανταλλαγή δεδομένων ανάμεσα στο κέντρο ελέγχου και στους τελικούς καταναλωτές. Το NAN είναι αυτό που στην πραγματικότητα συλλέγει τα δεδομένα των μετρήσεων των καταναλωτών από του έξυπνους μετρητές. Η καταλληλότερη αρχιτεκτονική θεωρείται η αρχιτεκτονική τύπου mesh, που περιλαμβάνει έξυπνους μετρητές και συσκευές συγκέντρωσης των δεδομένων των μετρήσεων. Με την χρήση τοπολογίας mesh, τα πλεονεκτήματα είναι, επεκτασιμότητα, μικρό κόστος λειτουργίας και υποδομών. Στην βιβλιογραφία, οι όροι FAN και NAN, εκφράζουν το ίδιο δίκτυο, αλλά ένας διαχωρισμός τους είναι ότι το FAN, είναι αυτό που συγκεντρώνει τα δεδομένα από γραμμές μεταφοράς ηλεκτρικού ρεύματος, από συσκευές συγκέντρωσης δεδομένων. Οι έξυπνοι μετρητές στέλνουν τα δεδομένα που συλλέγουν από το HAN του καταναλωτή και λειτουργούν και ως πύλη ανάμεσα στα δύο αυτά δίκτυα. Επίσης, οι μετρητές αυτοί έχουν την δυνατότητα με την χρήση πρωτοκόλλων δρομολόγησης να πραγματοποιούν δρομολόγηση για να βρίσκουν την ιδανική διαδρομή για μεταφορά των δεδομένων αλλά και για την λήψη πληροφοριών όπως είναι το κόστος της ενέργειας μια δεδομένη χρονική στιγμή. Αυτό γίνεται γιατί κάθε μετρητής έχει την δυνατότητα να διατηρεί, μια λίστα με γειτονικούς, ώστε σε περίπτωση προβλήματος επικοινωνίας να υπάρχει μια επιπλέον επιλογή για δρομολόγηση των δεδομένων που ανταλλάσσονται. Με αυτό τον τρόπο το mesh δίκτυο προσφέρει αξιοπιστία και επεκτασιμότητα επειδή υπάρχουν πολλαπλά μονοπάτια επικοινωνίας. (Nico Saputro, 2012)



Εικόνα 4 NAN σε αρχιτεκτονική mesh για last-mile επικοινωνία (multi-hop)" (Weixiao Meng, 2014)

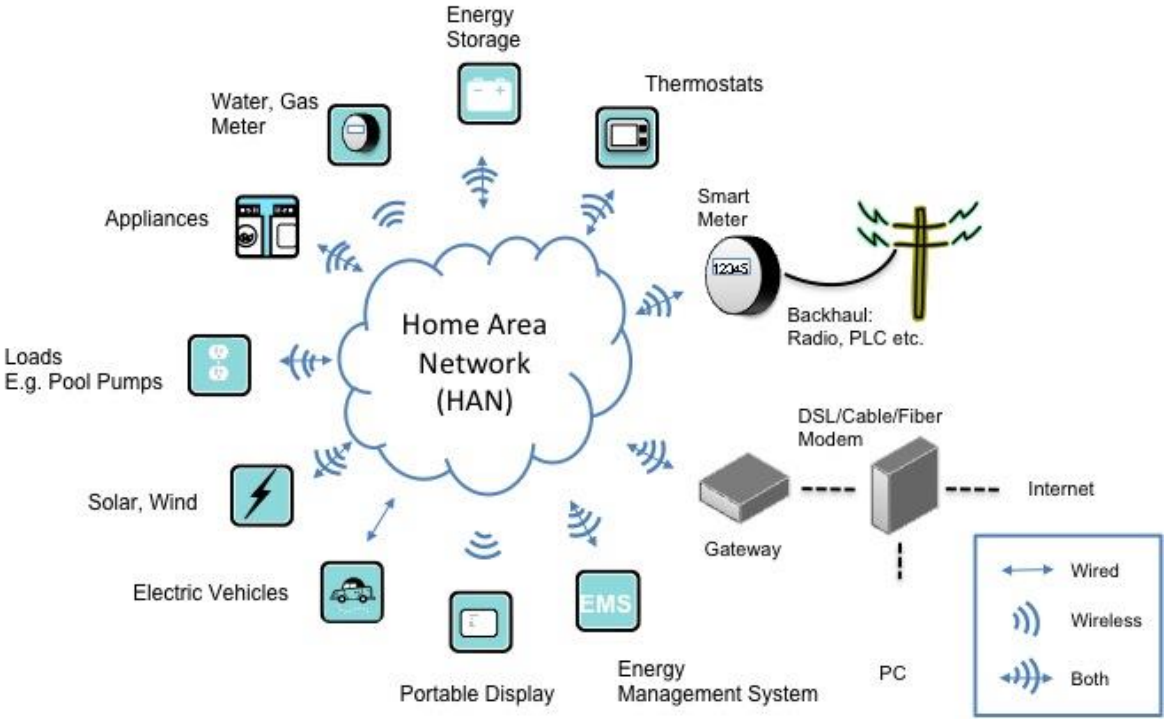
Εκτός από ασύρματες mesh τεχνολογίες, μπορούν να χρησιμοποιηθούν και άλλες ασύρματες τεχνολογίες όπως είναι το WiMAX, κυψελοειδής 3G, 4G αλλά και σε κάποιες περιπτώσεις και ενσύρματες όπως είναι η τεχνολογία PLC, οπτικών ινών ανάμεσα στους υποσταθμούς και τους συλλέκτες δεδομένων. Εάν, θέλουμε να κάνουμε μια ταξινόμηση των αρχιτεκτονικών που μπορούν να υλοποιηθούν σε ένα δίκτυο NAN, οι δύο κατηγορίες είναι, η multi-hop και η single approach. Στην multi-hop κατηγορία ανήκουν οι αρχιτεκτονικές τύπου mesh, όπου η σύνδεση του HAN δικτύου με το WAN δεν είναι άμεση αλλά τα δεδομένα που ανταλλάσσονται μεταφέρονται μέσω και άλλων συσκευών, όπως συλλέκτες κτλ. Ενώ, στην κατηγορία single approach ανήκουν αρχιτεκτονικές όπου τα δεδομένα που ανταλλάζονται μεταφέρονται άμεσα στο WAN δίκτυο, χωρίς να παρεμβάλλονται άλλες συσκευές ή να διέρχονται από άλλα δίκτυα. Ένα τέτοιο παράδειγμα εφαρμογής είναι η χρήση της τεχνολογίας WiMAX, για σύνδεση των έξυπνων μετρητών κατευθείαν στους υποσταθμούς του WAN δικτύου. Το παραπάνω προϋποθέτει ότι οι έξυπνοι μετρητές που λειτουργούν ως πύλη για το HAN να υποστηρίζουν από πλευράς υλικού και από πλευράς λογισμικού την τεχνολογία WiMAX ή να συνδέονται (παράδειγμα με το 802.11 ή με το 802.15.4) με άλλη συσκευή που υποστηρίζει το WiMAX.



Εικόνα 5 "NAN σε αρχιτεκτονική point to point (single approach)" (Weixiao Meng, 2014)

3. Home Area Network

Το δίκτυο HAN καλύπτει την περιοχή της οικίας ενός πελάτη και παρέχει επικοινωνία ανάμεσα στην εταιρία ηλεκτρικής ενέργειας και το δίκτυο του πελάτη με πύλη τον έξυπνο μετρητή που υπάρχει εγκατεστημένος σε κάθε οικία. Κάθε συσκευή που λειτουργεί στην οικία στα πλαίσια του ευφυούς δικτύου, στέλνει δεδομένα μετρήσεων κατανάλωσης ηλεκτρικής ενέργειας μέσω του HAN στον έξυπνο μετρητή και επιπλέον κάθε συσκευή θεωρείται έξυπνη, γιατί μπορεί να δέχεται εντολές ελέγχου από τον έξυπνο μετρητή. Για παράδειγμα, να τεθεί μια συσκευή οικιακής χρήση σε λειτουργία, όταν το κόστος της ηλεκτρικής ενέργειας είναι φθηνότερο. Ο έξυπνος μετρητής λειτουργεί ως η συσκευή που πραγματοποιεί την διασύνδεση ανάμεσα στα δίκτυα HAN και NAN, και στην ουσία συμμετέχει στην δρομολόγηση των δεδομένων που ανταλλάζονται. Στο HAN, επίσης, εφαρμόζονται τεχνικές αυτοματισμού για τις συσκευές που λειτουργούν σε μια οικία αλλά και παρακολούθησης και διαχείρισης της κατανάλωσης κάθε συσκευής που λειτουργεί. Ακόμη, περιλαμβάνει, διαφόρου τύπου αισθητήρες, για την εκτέλεση λειτουργιών όπως είναι έλεγχος φωτισμού, απομακρυσμένο έλεγχο συσκευών, ασφάλεια, απομακρυσμένη υποστήριξη κτλ. Από πλευράς της εταιρίας ηλεκτρικής ενέργειας, ανά μικρά χρονικά διαστήματα, στέλνονται δεδομένα σχετικά με το κόστος της ηλεκτρικής ενέργειας ανά μονάδα (Kwh) στον έξυπνο μετρητή, ώστε ο καταναλωτής να μπορεί να ρυθμίσει την χρήση των συσκευών του, έτσι ώστε να εξοικονομεί ηλεκτρική ενέργεια. Όπως είναι κατανοητό, στο οικιακό αυτό δίκτυο απαιτείται να υπάρχει αξιοπιστία αλλά και ασφάλεια στην επικοινωνία ανάμεσα στις συσκευές και στο έξυπνο μετρητή. Τα ασύρματες επικοινωνίες είναι προτιμότερες από τις ενσύρματες, γιατί παρέχουν ευελιξία και μικρότερο κόστος, ως προς την υποδομή(καλωδίωση κτλ) για την επικοινωνία με το έξυπνο μετρητή. Από πλευράς απαιτήσεων, και συγκεκριμένα ρυθμού μετάδοσης, ένα εύρος της τάξης από 1 έως 100 kbps επαρκεί για την ανταλλαγή δεδομένων γιατί ο κύριος όγκος δεδομένων αφορά λειτουργίας παρακολούθησης και διαχείρισης των συσκευών. Μία ακόμη σημαντική παράμετρος είναι, το κόστος υλοποίησης του HAN, αλλά και τις κατανάλωσης ενέργειας να διατηρούνται σε όσο χαμηλότερα επίπεδα γίνεται. Τεχνολογίες ασύρματης δικτύωσης που προτιμούνται είναι το ZigBee, όπου υποστηρίζει mesh αρχιτεκτονική και sleep-mode δηλαδή κατάσταση αναμονής εξοικονομώντας ενέργεια, επίσης εύκολα υλοποιείται και το Wi-Fi, ενώ από πλευράς ενσύρματης δικτύωσης τεχνολογίες PLC. (V. Cagri Gungor, 2012) (Nico Saputro, 2012)



Εικόνα 6 "Επικοινωνία συσκευών στο HAN" (Home)

2.3 ΑΠΑΙΤΗΣΕΙΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

Σε ένα ευφυές δίκτυο, η αξιοπιστία, η απόδοση αλλά και η ποιότητα στην επικοινωνία είναι βασικό κομμάτι, για την σωστή λειτουργία στο πλαίσιο του ευφυούς δικτύου. Προβλήματα στην υποδομή των επικοινωνιών, μπορούν να οδηγήσουν μέχρι και σε υπολειτουργία μέρους ή ολόκληρου του ευφυούς δικτύου, από την παραγωγή μέχρι και την διανομή την ηλεκτρικής ενέργειας. Για την προστασία και την διασφάλιση της επικοινωνίας είναι απαραίτητο να πληρούνται οι παρακάτω απαιτήσεις. (Wenye Wang Y. X., 2011)

1. Καθυστέρηση δικτύου

Η καθυστέρηση δικτύου ορίζεται ως τον μέγιστο χρόνο που χρειάζεται μια συγκεκριμένη πληροφορία να φτάσει στον παραλήπτη της μέσα από ένα δίκτυο επικοινωνιών. Στο πλαίσιο των επικοινωνιών των ευφυών δικτύων, οι απαιτήσεις ως προς την καθυστέρηση του δικτύου διαφέρουν ανά περιοχή(HAN, NAN,WAN). Η χρονική καθυστέρηση είναι πολύ σημαντική γιατί η αλληλεπίδραση ανάμεσα στις κεντρικές υποδομές και τους πελάτες θεωρείται real-time και όπως είναι κατανοητό τα χρονικά όρια περιορίζουν την εφαρμογή τεχνολογιών και την χρήση μέσων επικοινωνίας αναλόγως τις απαιτήσεις που ορίζονται στο κάθε σημείο του δικτύου. Ακόμη, οι ρυθμοί μετάδοσης των τεχνολογιών που χρησιμοποιούνται φυσικό είναι να επηρεάζουν την καθυστέρηση, σχετικά με το πόσο γρήγορα θα φτάσει η πληροφορία στον παραλήπτη, διερχόμενη μέσα από διαφορετικές συσκευές δικτύου, τεχνολογιών, μέσων αυξάνοντας ή μειώνοντας την συνολική καθυστέρηση. Για παράδειγμα, με χρήση οπτικών ινών, η καθυστέρηση υπολογίζεται σε 5μs ανά χιλιόμετρο μήκους. Ενώ, με χρήση τεχνολογίας WiMAX

μεταξύ υποσταθμού και τελικού καταναλωτή(σημείο CPE), υπολογίζεται σε μικρότερη ή ίση με 10ms. (V.K. Sood, 2009) Σημαντικό είναι να αναφερθούμε ότι η καθυστέρηση δικτύου που εξετάζουμε αφορά την συνολική καθυστέρηση (καθυστέρηση διάδοσης, μετάδοσης, ουράς κτλ)

2. Κρισιμότητα παράδοσης δεδομένων

Οι σουίτες πρωτοκόλλων που χρησιμοποιούνται για την υλοποίηση εφαρμογών στα πλαίσια του ευφυούς δικτύου ενέργειας, είναι απαραίτητο να παρέχουν, διαφορετικά επίπεδα ελέγχου παράδοσης δεδομένων με βάση της απαιτήσεις των εφαρμογών. Αυτό όμως μπορεί να επιτυγχάνεται την στιγμή που πραγματοποιείται η σύνδεση ανάμεσα σε δύο εφαρμογές. Τα επίπεδα που κατηγοριοποιούνται είναι τρία. (Wenye Wang Y. X., 2011)

- Υψηλό επίπεδο

  Χρησιμοποιείται εκεί όπου η επιβεβαίωση παράδοσης δεδομένων είναι απαραίτητη. Σε περίπτωση αποτυχίας παράδοσης, πραγματοποιείται επανάληψη της αποστολής.

- Μεσαίο επίπεδο

  Χρησιμοποιείται εκεί όπου η επιβεβαίωση παράδοσης δεδομένων είναι δεν απαραίτητη από τον παραλήπτη, αλλά είναι ικανός να ανιχνεύσει την απώλεια δεδομένων.

- Μη κρίσιμο επίπεδο

  Χρησιμοποιείται εκεί όπου η απώλεια δεδομένων δεν είναι καθοριστική για τον παραλήπτη. Σε αυτή την περίπτωση, η αξιοπιστία μπορεί να βελτιωθεί με επαναλαμβανόμενα μηνύματα. Για παράδειγμα, μπορεί να χρησιμοποιηθεί σε δεδομένα που στέλνονται περιοδικά με στόχο την παρακολούθηση του δικτύου.

3. Αξιοπιστία

Όλες οι συσκευές επικοινωνιών που λειτουργούν στα πλαίσια ενός ευφυούς δικτύου ενέργειας βασίζονται στο δίκτυο κορμού του τμήματος που ανήκουν για την αποστολή και λήψη κρίσιμων μηνυμάτων για την διατήρηση της σταθερότητας. Είναι κατανοητό ότι είναι πολύ σημαντικό το δίκτυο κορμού να είναι αξιόπιστο, για την επιτυχή και χρονικά σωστή παράδοση(εντός χρονικών ορίων) των πληροφοριών. Η αξιοπιστία του δικτύου κορμού, επηρεάζεται από έναν αριθμό πιθανών προβλημάτων-αποτυχιών. Συγκεκριμένα, περιλαμβάνονται, αποτυχίες δικτύου, χρονικές αποτυχίες(time-out) και αποτυχίες πόρων. Ειδικότερα, χρονικές αποτυχίες συμβαίνουν όταν ο χρόνος απάντησης σε μηνύματα ελέγχου ξεπεράσει το χρονικό όριο που θέτουν οι εκάστοτε απαιτήσεις. Μια αποτυχία δικτύου, μπορεί να πραγματοποιηθεί, όταν, υπάρχει αποτυχία σε ένα επίπεδο μιας σουίτας πρωτοκόλλου που χρησιμοποιείται. Για παράδειγμα, ένα πρωτόκολλο δρομολόγησης, μπορεί να εμποδίσει μια μήνυμα-πακέτο από το να φτάσει στον προορισμό του, παρά την ύπαρξη μιας σύνδεσης. Επίσης, θόρυβος και παραφωνίας στο φυσικό μέσο, μπορούν να δημιουργήσουν προβλήματα σε

επικοινωνίες. Τέλος, μια αποτυχία πόρου, αναφέρεται στην αποτυχία λήψης ενός μηνύματος από τον παραλήπτη, ενώ η πληροφορία έχει φτάσει μέσα από ένα δίκτυο επικοινωνιών σε αυτόν, αλλά δεν την έχει λάβει. Συμπερασματικά, η αξιοπιστία είναι απαραίτητο να λαμβάνεται υπόψη, κατά την σχεδίαση ενός δικτύου επικοινωνιών και στην πορεία να γίνονται βελτίωσης.

4. Ασφάλεια

Η ασφάλεια επικοινωνιών θεωρείται ως ένα από τα κρισιμότερα χαρακτηριστικά σε ένα ευφυές δίκτυο ενέργειας, και ειδικότερα η κυβερνό-ασφάλεια λόγω των αυξανόμενων περιστατικών επιθέσεων και παραβιάσεων. Έτσι, η κυβερνό-ασφάλεια καλείται να παρέχει μεθόδους για την προστασία, έναντι κακόβουλων (πελατών, υπαλλήλων, βιομηχανικής κατασκοπείας κτλ) αλλά και έναντι σφαλμάτων χρηστών του δικτύου, προβλημάτων συσκευών και φυσικών καταστροφών. Οι αδυναμίες που ενδέχεται να υπάρξουν σε ένα δίκτυο επικοινωνιών ευφυούς δικτύου, υπάρχει η πιθανότητα να επιτρέψουν την πρόσβαση σε έναν επιτιθέμενο, να διεισδύσει σε ένα δίκτυο, να αποκτήσει πρόσβαση σε λογισμικό ελέγχου με αποτέλεσμα να προκαλέσει προβλήματα σε σημεία του δικτύου με απρόβλεπτες συνέπειες. Υπάρχουν πολλοί οργανισμοί που καθορίζουν ποιες πρέπει να είναι οι προδιαγραφές και οι απαιτήσεις για την ασφάλεια σε ένα ευφυές δίκτυο ενέργειας. Παράδειγμα ο NIST, μέσω του Cyber Security Working Group καθορίζει τις απαιτήσεις ασφαλείας για τα διάφορα τμήματα ενός ευφυούς δικτύου. Το σχέδιο που καθορίζει της απαιτήσεις αυτές είναι το NIST 768 και είναι κατανοητό ότι η σχεδίαση και η υλοποίηση ενός ευφυούς δικτύου ενέργειας πρέπει οπωσδήποτε να βασίζεται σε τέτοιες οδηγίες, για να διασφαλίζεται σε όσο μεγαλύτερο βαθμό η ασφάλεια, επεκτασιμότητα για να μπορεί να υπάρξει ανάπτυξη του δικτύου. Ειδικότερα, η ασφάλεια επικοινωνιών ενός ευφυούς δικτύου βασίζεται σε τεχνικές αυθεντικοποίησης, εξουσιοδότησης, και ιδιωτικότητας. Τεχνικές που μπορούν να χρησιμοποιηθούν για κρυπτογράφηση είναι με χρήση αλγορίθμου Advanced Encryption Standard (AES), Triple Data Encryption Algorithm (3DES), που προσφέρουν, ασφάλεια, υψηλή απόδοση, και διαθεσιμότητα. Οι επιλογή της τεχνικής βασίζεται κυρίως στα δεδομένα ή στον τύπο των επικοινωνιών που προτίθετο να προστατέψει. Ακόμη, η ασύρματες επικοινωνίες είναι ασφαλείς με τεχνολογίες όπως το 802.11i (WPA2) και το 802.16e ενώ οι ενσύρματες προστατεύονται με τείχη προστασίας, Vpn, IPSec κτλ. Σε υψηλότερο επίπεδο, μηχανισμοί ασφαλείας όπως είναι το Secure Shell Protocol (SSH), και το Secure Socket Layer (SSL) / Transport Layer Security (TLS) μπορούν να προσφέρουν προστασία στην επικοινωνία. Πολλές φορές οι σχεδιαστές αρχιτεκτονικών και συστημάτων, αναγνωρίζουν τις απαιτήσεις, και προτείνουν την χρήση πρωτοκόλλων ασφαλείας, όπως είναι το SSH, και το IPSec αλλά δεν δίνουν βαρύτητα στις λεπτομέρειες της χρήσης των τεχνικών αυτών. Μια τέτοια προσέγγιση, έχει ως αποτέλεσμα για παράδειγμα η διαχείριση των κλειδιών να γίνεται δύσκολη ως λειτουργική διαδικασία. Δηλαδή, όταν ένα σχεδιαστής ενός συστήματος, δεν συμπεριλάβει στην σχεδίαση και την διαδικασία διαχείρισης των κλειδιών και οι χρήστες έχουν περιορισμένες μεθόδους διαχείρισης των κλειδιών,

ακόμη και μέσω μη-αυτοματοποιημένων διαδικασιών, είναι απλό στην σχεδίαση, αλλά με μεγάλο κόστος για των διαχειριστή του συστήματος. Τα συστήματα διαχείρισης εμπιστευτικότητας κλειδιών βασίζονται σε υποδομές δημοσίων κλειδιών(Public Key Infrastructure) και έχουν την δυνατότητα παραμετροποίησης ώστε να χρησιμοποιηθούν σε ένα ευφυές δίκτυο ενέργειας. Τέλος, όλες οι παραπάνω τεχνικές βασίζονται στον τρόπο που γίνεται οι διαχείριση των κλειδιών που χρησιμοποιούνται, σε συνδυασμό με ότι ένα ευφυές δίκτυο, περιλαμβάνει ακόμη και εκατομμύρια συσκευές όπου πρέπει να πιστοποιούνται, η διαχείριση των κλειδιών είναι απαραίτητο να είναι επεκτάσιμη σε όλα τα επίπεδα. Δηλαδή, πρέπει να παρέχεται, υψηλή ασφάλεια(πιστοποίηση και εξουσιοδότηση), διαλειτουργικότητα, και υψηλά επίπεδα απόδοσης, για μείωση του επιπλέον κόστους, διαχείρισης των κλειδιών. Είναι κατανοητό, ότι πιθανόν να χρειαστούν να σχεδιαστούν στο μέλλον καινούριες τεχνικές διαχείριση κλειδιών ώστε να καλύπτονται οι απαιτήσεις ασφάλειας των επικοινωνιών ενός ευφυούς δικτύου. (Ye Yan, A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges, FIRST QUARTER 2013)

5. Συγχρονισμός

Πολλές συσκευές που λειτουργούν μέσα σε ένα ευφυές δίκτυο ενέργειας είναι απαραίτητο να είναι συγχρονισμένες. Οι απαίτηση για συγχρονισμό μιας συσκευής σχετίζεται με την κρισιμότητα λειτουργίας της συσκευής αυτής. Η ανοχή των χρονικών απαιτήσεων του συγχρονισμού είναι αυστηρές για συσκευές τύπου Intelligent Electronic Device (IED) που επεξεργάζονται δεδομένα ευαίσθητα ως προς τον χρόνο. Για παράδειγμα, συσκευές τύπου phasor measurement units(PMU) έχουν τις αυστηρότερες απαιτήσεις συγχρονισμού λόγω ότι παρέχουν ζωντανά μετρήσεις ηλεκτρικής ενέργειας (τάση και ένταση ρεύματος) από διάφορα σημεία του δίκτυο παραγωγής και μεταφοράς ενέργειας για ανάλυση και διαχείριση. Ένα πρωτόκολλο που χρησιμοποιείται στα πλαίσια λειτουργίας των έφυαν δικτύων είναι το Precision Time Protocol (PTP) που ορίζεται από το πρότυπο της IEEE,1588 παρέχοντας χρονικό συγχρονισμό μέχρι και ακρίβειας nanosecond σε δίκτυ Ethernet. Άλλες μέθοδοι χρονικού συγχρονισμού είναι με χρήση του γνωστού Global Positioning System (GPS) ή μέσω του Simple Time Network Protocol (STNP). (Wenye Wang Y. X., 2011)

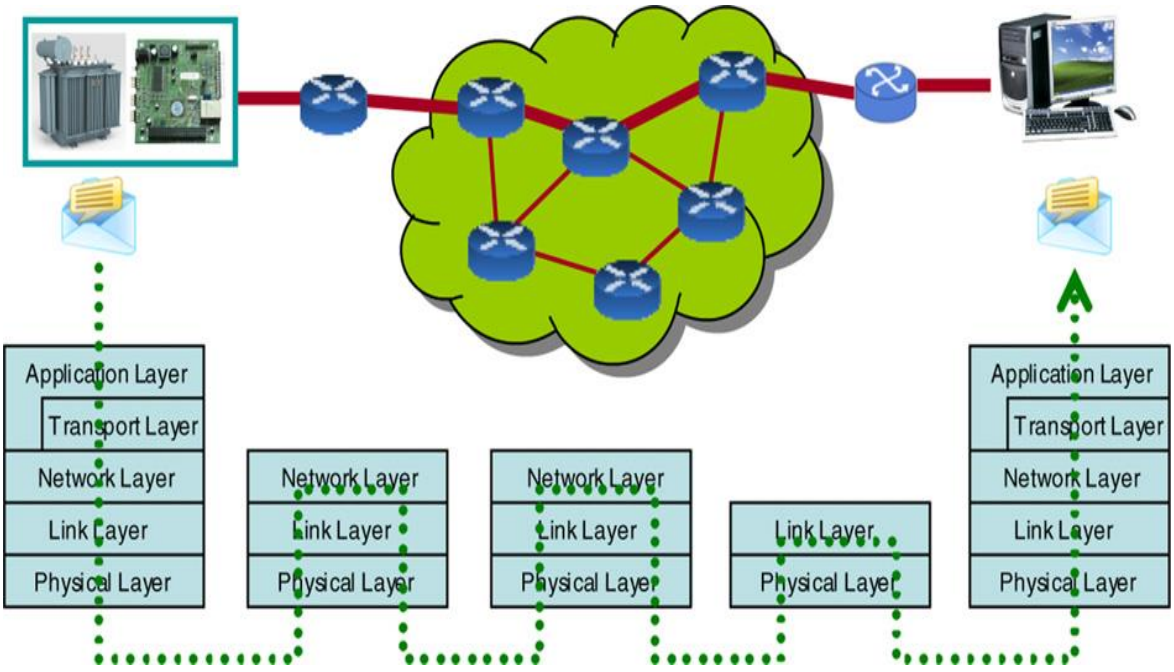
6. Υποστήριξη Multicast

Στα δίκτυα υπολογιστών, η τεχνική παράδοσης πληροφοριών multicast θεωρείται μία από τις σημαντικότερες, έτσι, και για τα ευφυή δίκτυα ενέργειας παίζει σημαντικό ρόλο στις επικοινωνίες όπου θέλουμε να γίνεται παράδοση πληροφοριών σε συγκεκριμένους παραλήπτες, από έναν και μόνο αποστολέα την ίδια χρονική στιγμή. Αντί να γίνεται αποστολή σε κάθε μοναδική διεύθυνση που απαιτείται για τον κάθε παραλήπτη, η πληροφορία στέλνεται σε μία multicast διεύθυνση όπου προωθείται στους παραλήπτες που ανήκουν σε αυτό το multicast group. Με αυτόν τον τρόπο, οι παραλήπτες απορρίπτουν την ανεπιθύμητη πληροφορία, όπου αυτό είναι χρήσιμο για συσκευές τύπου IED, όπου

ανταλλάσουν ευαίσθητες πληροφορίες μεταξύ τους, σχετικά με την κατάσταση του δικτύου παραγωγής και μεταφοράς της ηλεκτρικής ενέργειας. (Wenye Wang Y. X., 2011)

2.4 ΑΠΑΙΤΗΣΕΙΣ ΚΑΘΥΣΤΕΡΗΣΗΣ ΚΑΙ ΡΥΘΜΟΥ ΜΕΤΑΔΟΣΗΣ

Όπως έχει αναφερθεί και στο προηγούμενο κεφάλαιο, ο χρόνος είναι κρίσιμο σημείο στο δίκτυο επικοινωνιών ενός ευφυούς δικτύου ενέργειας και επίσης είναι και η κύρια διαφορά από άλλα δίκτυα επικοινωνιών. Υπάρχουν τύποι πληροφοριών που ανταλλάσσονται ανάμεσα σε ηλεκτρικές συσκευές του δικτύου που είναι χρήσιμες μόνο μέσα σε ένα προκαθορισμένο χρονικά εύρος. Έτσι, ένα η καθυστέρηση ξεπεράσει αυτό το προκαθορισμένο όριο, η πληροφορία αυτή πλέον δεν εξυπηρετεί τον σκοπό της, αλλά μπορεί να προκαλέσει και προβλήματα στην κίνηση του δικτύου. Για παράδειγμα, για τα συστήματα προστασίας των ηλεκτρικών συσκευών, το ρελέ ασφαλείας πρέπει να ανοίξει αμέσως αν η τάση ή η ένταση σε μία συσκευή ξεπεράσει τα όρια που ορίζει ο κατασκευαστής. Τα όρια που ορίζονται για την χρονική καθυστέρηση είναι κατανοητό πως είναι πολύ μικρά και είναι έως 3ms για να είναι αποτελεσματικά. Η IEEE και η IEC έχουν ορίσει μέσω προτύπων της απαιτήσεις καθυστέρησης για της πληροφορίες που διακινούνται σε ένα ευφυές δίκτυο ενέργειας. Τέλος, όταν σχεδιάζεται η υποδομή επικοινωνιών είναι απαραίτητο να λαμβάνονται υπόψη και να ικανοποιούνται οι απαιτήσεις καθυστέρησης. (Wenye Wang Y. X., 2011)

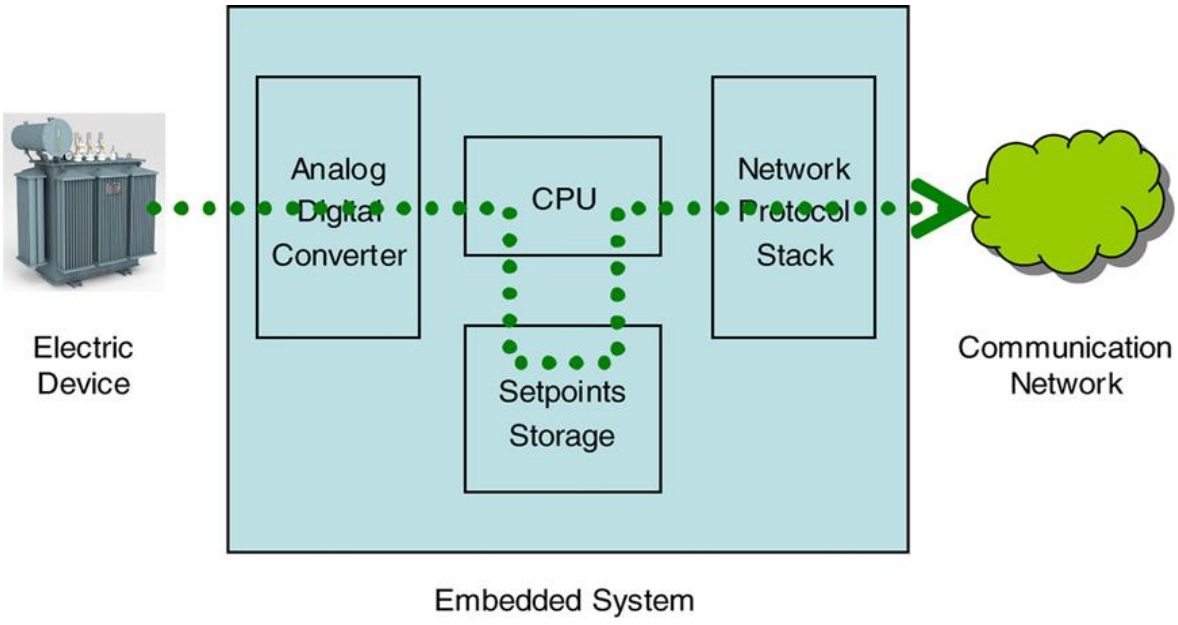


Εικόνα 7 "Η καθυστέρηση σε ένα δίκτυο επικοινωνιών ορίζεται από άκρο σε άκρο και περιλαμβάνει, την επεξεργασία και μετάδοση από τον αποστολέα μέχρι τον παραλήπτη και κάθε ενδιάμεσο κόμβο όπου διέρχεται" (Wenye Wang Y. X., 2011)

1. Ορισμός καθυστέρησης

Η καθυστέρηση επικοινωνίας στα ευφυή δίκτυα ενέργειας, ορίζεται ως ο συνολικός χρόνος ανάμεσα στην αποστολή και την λήψη και υπολογίζεται όταν δύο ίδιες εφαρμογές τρέχουν στον αποστολέα και στον παραλήπτη. Ειδικότερα, στην εικόνα η καθυστέρηση υπολογίζεται ως το άθροισμα του χρόνου που απαιτείται για να επεξεργασία (κωδικοποίηση) και την προώθηση από τον αποστολέα, τον χρόνο για την επεξεργασία και την προώθηση από κάθε κόμβο όπου διέρχεται η πληροφορία, και τον χρόνο για την επεξεργασία (αποκωδικοποίηση) και λήψη από τον παραλήπτη.

Επειδή οι IED συσκευές δεν έχουν δυνατότητες επικοινωνίας, σε κάθε τέτοια συσκευή, προσαρμόζεται ένα μικρό υπολογιστικό σύστημα για να υπάρχει δυνατότητα επικοινωνίας και να λειτουργεί ως διεπαφή με το δίκτυο επικοινωνίας. Μια ηλεκτρική συσκευή μαζί με ένα μικρό υπολογιστικό σύστημα, αποτελούν μια συσκευή τύπου IED. Η επεξεργασία της πληροφορίας από το υπολογιστικό σύστημα, και τα τμήματα από όπου διέρχεται παρουσιάζονται στην παραπάνω εικόνα. Συγκεκριμένα, ο μετατροπέας από αναλογικό σε ψηφιακό σήμα, πραγματοποιεί την μετατροπή σε ψηφιακό σήμα της μετρήσεις που λαμβάνονται από την ηλεκτρική συσκευή, ο επεξεργαστής, επεξεργάζεται τα ψηφιακά πλέον δεδομένα μετρήσεων, όπου αποθηκεύονται σε μία μικρή μονάδα αποθήκευσης (buffer), και η στοίβα πρωτοκόλλων επικοινωνίας αναλαμβάνουν την επεξεργασία, την μορφοποίηση και προώθηση της πληροφορίας στο δίκτυο επικοινωνία.



Εικόνα 8 "Τμήματα ενός προσαρμοσμένου υπολογιστικού συστήματος, που αποτελείται μια συσκευή τύπου IED" (Wenye Wang Y. X., 2011)

2. Ταξινόμηση χρονικών ορίων

Ένα πρότυπο που καθορίζει την επικοινωνία ανάμεσα στους υποσταθμούς είναι το IEC 61850, το ίδιο καθορίζει τύπους μηνυμάτων θέτοντας όρια στην καθυστέρηση. Στην εικόνα 9 παρουσιάζονται συνοπτικά.

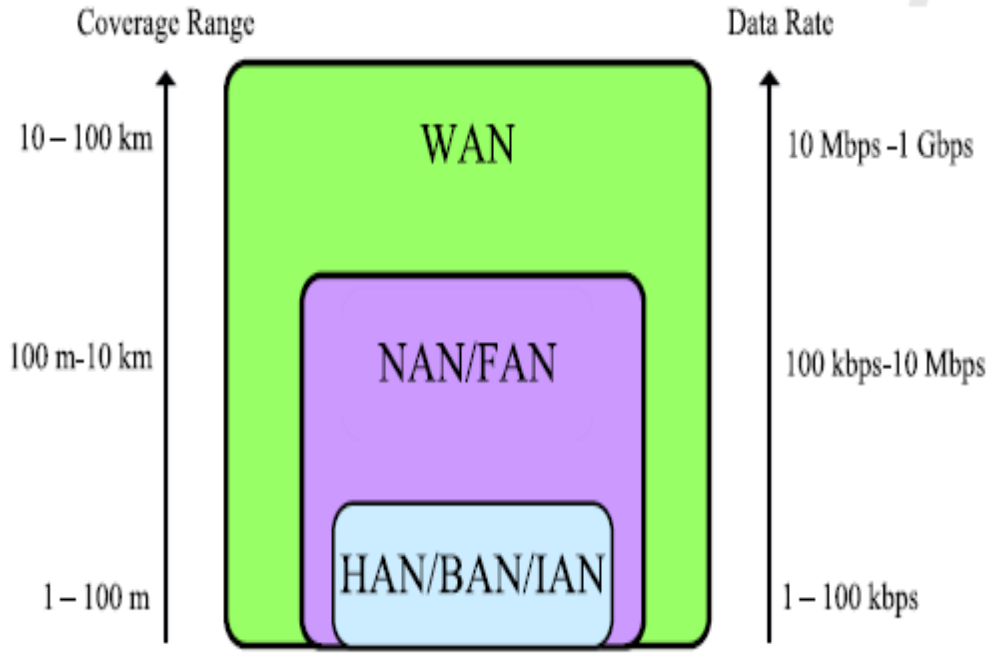
IEC 61850 communication networks and systems in substations: communication requirements for functions and device models.

Message Types	Definitions	Delay requirements
Type 1	Messages requiring immediate actions at receiving IEDs.	1A: 3 ms or 10 ms; 1B: 20 ms or 100 ms
Type 2	Messages requiring medium transmission speed	100 ms
Type 3	Messages for slow speed auto-control functions	500 ms
Type 4	Continuous data streams from IEDs	3 ms or 10 ms
Type 5	Large file transfers	1000 ms (not strict)
Type 6	Time synchronization messages	No requirement.
Type 7	Command messages with access control	Equivalent to Type 1 or Type 3.

Εικόνα 9 "Απαιτήσεις καθυστέρησης ανά τύπο επικοινωνίας όπως ορίζεται από το IEC 61850" (Wenye Wang Y. X., 2011)

Διαπιστώνουμε ότι τα δεδομένα που είναι κρίσιμα για την λειτουργία του δικτύου και την προστασία απαιτούν το μικρότερο χρονικό όριο των 10ms. Παράδειγμα, το χρονικό όριο αυτό ορίζεται για την επικοινωνία ανάμεσα σε συσκευές IED και του κέντρου ελέγχου για κατάσταση συναγερμού όταν δημιουργηθεί πρόβλημα στο δίκτυο ενέργειας, και την απόκριση του κέντρου ελέγχου προς τις IED συσκευές. Ακόμη, να αναφερθεί ότι αυτές οι κρίσιμες πληροφορίες μεταδίδονται στο δίκτυο επικοινωνίας του ευφυές δικτύου ενέργειας μαζί με άλλες πληροφορίες, που πιθανόν να είναι λιγότερο σημαντικές για την λειτουργία του δικτύου, όποτε παραμένει ένα ερευνητικό πρόβλημα προς επίλυση η ικανοποίηση των χρονικών ορίων των κρίσιμων πληροφοριών. (Wenye Wang Y. X., 2011)

Μέχρι στιγμής, έχουμε παρουσιάσει τις απαιτήσεις καθυστέρησης για το WAN, και τα τμήματα που αποτελείται όπως είναι οι υποσταθμοί. Το WAN έχει τις μεγαλύτερες απαιτήσεις όχι μόνο καθυστέρησης, αλλά και αξιοπιστίας και διαθεσιμότητας του δικτύου. Στην βιβλιογραφία γενικότερα υπάρχει έλλειψη καθορισμού των απαιτήσεων, ενώ όσες προσπάθειες γίνονται είναι διαφορετικές μεταξύ τους ως προς τα αποτελέσματα. Πρόσφατα, έχει αρχίσει να γίνεται μια προσπάθεια καθορισμού των απαιτήσεων του WAN, NAN και HAN, γενικότερα και όχι σύμφωνα με την χρήση κάποιου προτύπου, με βάση το μέγεθος των δεδομένων που διακινούνται και την συχνότητα. Στο (Manisa Pipattanasomporn, 2014) μπορούμε να βρούμε την μελέτη αυτή. Επισημαίνεται ότι στο HAN, οι απαιτήσεις είναι μικρότερες, από πλευράς καθυστέρησης και ρυθμού μετάδοσης, ειδικότερα σε μέγεθος είναι περίπου 100Kbps. Αντίστοιχα στο NAN, οι απαιτήσεις αυξάνονται μιας και το NAN είναι το δίκτυο που συγκεντρώνει τα δεδομένα από τους έξυπνους μετρητές.



Εικόνα 10 "Ρυθμοί μετάδοσης που απαιτούνται στο WAN, NAN, HAN" (Manisa Pipattanasomporn, 2014)

Οι απαιτήσεις από πλευράς καθυστέρησης στο NAN, είναι της τάξης των μερικών δευτερολέπτων, θα μπορούσαμε να πούμε ότι δεν είναι “time-critical” όπως το WAN, και ο μόνος σκοπός είναι να υπάρχει κατάλληλος συγχρονισμός για την καταγραφή της καταναλωμένης ενέργειας, είτε αυτή ζητείται μια συγκεκριμένη χρονική στιγμή από το κέντρο διαχείρισης του ευφυούς δικτύου ενέργειας, είτε είναι προγραμματιζόμενη για αποστολή από τον έξυπνο μετρητή. Άλλες λειτουργίες, όπως είναι η αλλαγή χρέωσης και αυτές έχουν καθυστέρηση της τάξης των μερικών δευτερολέπτων, ενώ κρισιμότερες θα μπορούσαμε να αναφέρουμε ότι θεωρούνται καταστάσεις όπως είναι η ανίχνευση βλάβης στο δίκτυο ηλεκτρισμού ή επικοινωνιών που σχετίζεται άμεσα με τους καταναλωτές και απαιτείται ενημέρωση μέσω του δικτύου. Με βάση τα παραπάνω, για WAN και το NAN, απαιτείται προσεκτική σχεδίαση του δικτύου, όπως και της αρχιτεκτονικής που θα επιλεγεί να υλοποιηθεί, ενώ αντίστοιχα προσοχή θέλει στην επιλογή της τεχνολογίας ή των τεχνολογιών που θα υλοποιηθούν στα δύο αυτά δίκτυα. (Manisa Pipattanasomporn, 2014)

ΕΠΙΛΟΓΟΣ

Στο δεύτερο κεφάλαιο έγινε ανάλυση του προτύπου IEEE P2030, που παρουσιάζει ένα έφυες δίκτυο ενέργειας ως ένα υπερσύστημα που αποτελείται από μικρότερα τμήματα και δίνει έμφαση στην διαλειτουργικότητα και στην από άκρη σε άκρη επικοινωνία. Ακόμη, σε συνεργασία με τον NIST και χρησιμοποιώντας τα τμήματα και της οντότητες που χρησιμοποιούνται από τον NIST, παρουσιάζεται ένα μοντέλο αναφοράς για την υλοποίηση των βασικών

σημείων για την σωστή λειτουργία ενός ευφυές δικτύου. Προτείνονται επίσης, ενσύρματες αλλά και ασύρματες τεχνολογίες για την υλοποίηση του δικτύου επικοινωνιών. Στο τρίτο υποκεφάλαιο, γίνεται μια αναλυτική μελέτη της αρχιτεκτονικής δικτύου που συνίσταται για την υλοποίηση του δικτύου επικοινωνιών, παρουσιάζοντας τρείς περιοχές (HAN, NAN, WAN) και τις τεχνολογίες δικτύου που μπορούν να εφαρμοσθούν σε κάθε περιοχή. Στο τέταρτο υποκεφάλαιο μελετούνται οι απαιτήσεις επικοινωνίας που είναι απαραίτητο να εφαρμόζονται για την σωστή, αξιόπιστη και ασφαλή ανταλλαγή δεδομένων, δίνοντας έμφαση στην καθυστέρηση, στην κρισιμότητα των δεδομένων, στον ασφάλεια αλλά και στον συγχρονισμό που είναι απαραίτητος για την λειτουργία πολλών συσκευών στα πλαίσια λειτουργία ενός ευφυούς δικτύου ενέργειας. Τέλος στο πέμπτο υποκεφάλαιο, ορίζεται η καθυστέρηση επικοινωνίας και παρουσιάζονται οι χρονικές απαιτήσεις που πρέπει να τηρούνται αυστηρά ανάλογα τον τύπο των δεδομένων που ανταλλάσσονται για την λειτουργία του δικτύου.

ΚΕΦΑΛΑΙΟ 3

ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΥΡΜΑΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΕΙΣΑΓΩΓΗ

Η χρήση ασύρματων τεχνολογιών στα ευφυή δίκτυα ενέργειας, έρχεται να καλύψει τις ανάγκες επικοινωνίας στα WAN, NAN και HAN. Μέσα από μια πληθώρα ασύρματων τεχνολογιών που έχουν σχεδιασθεί τα τελευταία χρόνια, έχουμε την δυνατότητα να υλοποιήσουμε ασύρματα δίκτυα που καλύπτουν εξ ολοκλήρου όλο το εύρος λειτουργίας ενός ευφυούς δικτύου ενέργειας. Κάθε περιοχή σε ένα ευφυές δίκτυο ενέργειας έχει διαφορετικές απαιτήσεις και σε συνδυασμό με τα χαρακτηριστικά που διαθέτει η κάθε τεχνολογία, προσπαθούμε να βρούμε πια είναι η κατάλληλη για κάθε περιοχή. Μερικές φορές, μπορεί δύο ή και περισσότερες τεχνολογίες να καλύπτουν τις ανάγκες μια περιοχής, για την υλοποίηση όμως εξαρτάται η αρχιτεκτονική η οποία ακολουθείται και υποστηρίζεται από μια τεχνολογία ασύρματης δικτύωσης. Στο κεφάλαιο αυτό, μελετούνται όλες οι ασύρματες τεχνολογίες που έχουν εφαρμογή στα ευφυή δίκτυα ενέργειας, καθώς και τα πρότυπα και πρωτόκολλα που συνδέονται με αυτές και έχουν σχεδιασθεί με γνώμονα την χρήση τους στα ευφυή δίκτυα ενέργειας. Τέλος, η επιλογή μιας ασύρματης τεχνολογίας επηρεάζεται από πολλούς παράγοντες, όπως είναι το οικονομικό κόστος της υλοποίησης, η κάλυψη ενδεχόμενων αναγκών στο μέλλον και η ασφάλεια που απαιτείται σε συνδυασμό με την εκάστοτε τεχνολογία.

3.1 ZIGBEE

Το πρότυπο IEEE 802.15.4 είναι ένα πρότυπο ασύρματης επικοινωνίας για χαμηλού ρυθμού ασύρματα προσωπικά δίκτυα (LR-WPAN) και συγκεκριμένα ορίζει το φυσικό επίπεδο (PHY) και το επίπεδο MAC. Σε γενικές γραμμές το επίπεδο MAC παρέχει δύο λειτουργίες, την beacon-enabled και την non beacon-enabled. Στην beacon-enabled λειτουργία, σε κάθε Beacon Interval (BI), ένα beacon μεταδίδεται από τον συντονιστή του Personal Area Network (ως συντονιστής λειτουργεί η συσκευή εκείνη που πραγματοποιεί την διαμόρφωση στο δίκτυο και επιλέγει το PAN ID) για τον συγχρονισμό των συσκευών. Στην non-beacon λειτουργία, χρησιμοποιείται η τεχνική CSMA/CA για πρόσβαση στο μέσο, για βελτίωση της ρυθμό-απόδοσης και μείωση της καθυστέρησης. Το τρέχον πρότυπο ορίζεται ως το 802.15.4-2011, ενώ το προηγούμενα είναι τα 802.15.4-2006 και 802.15.4-2003. Ο κύριος στόχος είναι να παρέχει ασύρματη επικοινωνία με χαμηλή κατανάλωση ενέργειας, χαμηλό κόστος και μικρό ρυθμό μετάδοσης δεδομένων. (Ahmad Usman, 2013)

Το ZigBee βασίζεται στο 802.15.4 και έχει αναπτυχθεί από τον οργανισμό ZigBee Alliance, έναν μη κερδοσκοπικό οργανισμό, και λειτουργεί στην συχνότητα των 868 MHz με ρυθμό μετάδοσης τα 20kbps για την Ευρώπη, στα 915 MHz με

ρυθμό μετάδοσης τα 40kbps για την Αμερική και στα 2.4 GHz με ρυθμό μετάδοσης 250kbps με παγκόσμια εμβέλεια.

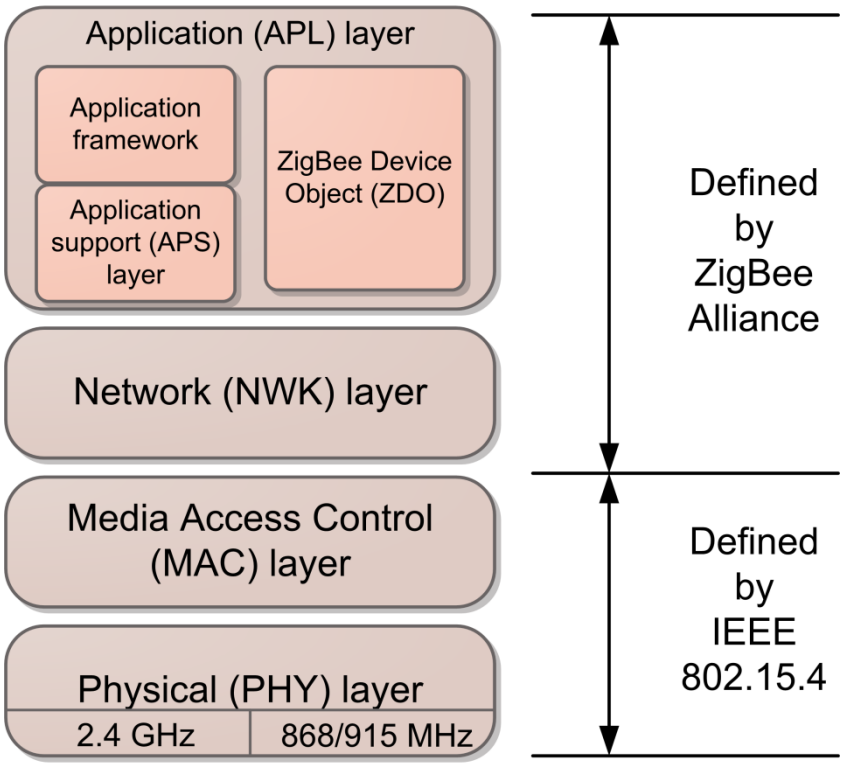
Η στοίβα του πρωτοκόλλου ZigBee αποτελείται από 4 κύρια επίπεδα.

1. Επίπεδο εφαρμογών
2. Επίπεδο δικτύου
3. Επίπεδο MAC
4. Φυσικό επίπεδο

Τα δύο πρώτα επίπεδα ορίζονται από το ZigBee Alliance και τα υπόλοιπα δύο από το πρότυπο 802.15.4. Στο επίπεδο εφαρμογών ανήκει το ZigBee Device Object (ZDO), όπου είναι διαθέσιμο για παραμετροποίηση. Στο επίπεδο δικτύου ανήκει η δρομολόγηση και διαχείριση του δικτύου, ενώ στο επίπεδο MAC, ανήκει η τεχνική CSMA-CA. (Alliance Z. , 2010)

ZigBee network standards on top of IEEE 802.15.4								
Freq.	Local	Data rate per channel (kbits/s)	Number of channels	Modulation	Approximate indoor range		Approximate outdoor range	
					(m)	(ft)	(m)	(ft)
2.4 GHz	Worldwide	250	16	DSSS w OQPSK	10	33	75	250
915 MHz	Americas	40	16	DSSS w/ BPSK	10	33	75	250
868 MHz	Europe	20	16	DSSS w/BPSK	10	33	75	250

Εικόνα 11 "Συχνότητες λειτουργίας ZigBee , ρυθμοί μετάδοσης, και εύρος λειτουργίας"



Εικόνα 12 "Στοίβα ZigBee με τα επίπεδα που αποτελείται" (Alliance Z. , 2010)

Στα πλαίσια λειτουργία του ZigBee υπάρχουν δύο τύποι συσκευών:

1. Full Function Device (FFD)
2. Reduced Function Device (RFD)

Ένα δίκτυο αποτελείται από τουλάχιστον ένα FFD που λειτουργεί ως συντονιστής. Μια συσκευή τύπου RFD χρειάζεται ελάχιστους πόρους ενέργειας ενώ με χρήση μπαταρίας πετυχαίνει μεγάλη αυτονομία για να δέχεται και να στέλνει δεδομένα. Επίσης μπορεί να επικοινωνήσει μόνο με άλλες συσκευές FFD, όπου αυτές διαθέτουν ικανούς πόρους για να πραγματοποιούν την δρομολόγηση του δικτύου. Επιπλέον οι συσκευές FFD μπορούν να ανιχνεύσουν και να επικοινωνήσουν και με τους δύο τύπους συσκευών.

Επίσης στο δίκτυο καθορίζονται τρεις τύποι κόμβων:

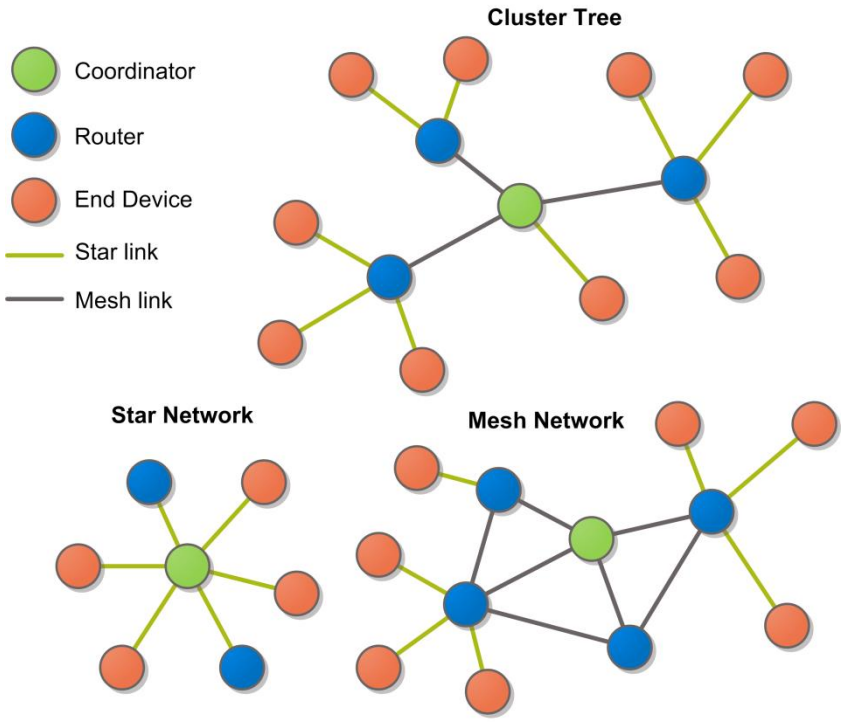
1. ZigBee Coordinator
2. ZigBee Router
3. ZigBee End Device

Οι συσκευές FFD μπορούν να είναι οποιουδήποτε τύπου κόμβου από τα παραπάνω, ενώ οι συσκευές RFD μπορούν να είναι μονό End Devices. Η ευθύνη της λειτουργίας και διαχείρισης του δικτύου ανήκει στον ZigBee Coordinator, ενώ ο ZigBee Router είναι υπεύθυνος για την δρομολόγηση των δεδομένων ανάμεσα στον Coordinator και στις End Devices. Οι κόμβοι όπου είναι Coordinator και

Router είναι ικανοί να επικοινωνούν με όλες τις συσκευές και λειτουργούν με μπαταρίες, και επιπλέον απαγορεύεται να μπαίνουν σε κατάσταση αναμονής (sleep-mode) στις περισσότερες περιπτώσεις εφαρμογών. Οι End Devices, μπορούν να επικοινωνούν μόνο με τους Coordinator και Router. Συνήθως είναι σε κατάσταση αναμονής(sleep-mode), και βρίσκονται σε κατάσταση λειτουργίας (wake-up) ανά τακτά χρονικά διαστήματα ώστε να στέλνουν δεδομένα, και επανέρχονται σε κατάσταση αναμονής. Με αυτόν τον τρόπο λειτουργίας είναι κατανοητό ότι διαθέτουν την ικανότητα να έχουν χαμηλή κατανάλωση ενέργειας με αξιόπιστη λειτουργία σε σχέση με την χρήση άλλων ασύρματων τεχνολογιών. (B.E. Bilgin, 2012)

Πίνακας 1 "Συσχέτιση τύπου συσκευής με κόμβους"

	Coordinator Καθιέρωση συνδέσεων και διαχείριση δικτύου	**Router** Υποστήριξη δρομολόγησης δεδομένων, επικοινωνία με Coordinator και End Devices	**End Device** Μπορεί να επικοινωνεί μόνο με Coordinator και Router
Full Function Device (FFD)	NAI	NAI	NAI
Reduced Function Device (RFD)	OXI	OXI	NAI



Εικόνα 13 "Τοπολογίες δικτύου ZigBee"

Η ZigBee Alliance έχει καθορίσει στα πλαίσια λειτουργία του ZigBee σε HAN δίκτυα, ένα πρότυπο, το ZigBee Smart Energy(SEP) για την υποστήριξη των επικοινωνιών ανάμεσα σε έξυπνους μετρητές και συσκευές που χρησιμοποιούνται για την παρακολούθηση, την καταγραφή και την διαχείριση της ηλεκτρικής ενέργειας που καταναλώνεται από τις οικιακές συσκευές σε ένα δίκτυο HAN. Με το πρότυπο αυτό για να επιτυγχάνονται οι στόχοι της εξοικονόμησης ενέργειας και κόστους είναι απαραίτητο να υποστηρίζονται οι παρακάτω λειτουργίες: (Laboratories, 2013)

1. Ζωντανή παρουσίαση κατανάλωσης ενέργειας

   Ο πελάτης πρέπει να έχει να δυνατότητα να ενημερώνεται για την ενέργεια που καταναλώνεται από τις οικιακές συσκευές και το κόστος της kWh. Επίσης να υπάρχει η δυνατότητα καταγραφής της ενέργειας που καταναλώνεται ανά συσκευή, ώστε να ενθαρρύνεται ο πελάτης να πραγματοποιεί καλύτερη διαχείριση της ηλεκτρικής ενέργειας παίρνοντας αποφάσεις σχετικές με την χρήση η όχι μιας οικιακής συσκευής την δεδομένη χρονική στιγμή. Για παράδειγμα, βλέποντας ότι μια συσκευή καταναλώνει μεγάλα ποσά ενέργεια μια ώρα αιχμής, μπορεί να πάρει την απόφαση, να κάνει χρήση της συσκευής αυτής τις ώρες όπου το κόστος της KWh είναι χαμηλό.

2. Διαχείριση από το κέντρο ελέγχου του παρόχου ηλεκτρικής ενέργειας(demand response)

Στο δίκτυο HAN, είναι φυσικό να υπάρχουν συσκευές που είναι ιδιαίτερα ενεργότερες, με την δυνατότατα διαχείρισης από το κέντρο διαχείρισης της ηλεκτρικής ενέργειας, σε περιπτώσεις όπου η παραγωγή ενέργειας δεν επαρκεί για την κάλυψη της ζήτησης των καταναλωτών, μπορεί το κέντρο διαχείρισης να δώσει εντολή απομακρυσμένα για την μείωση της κατανάλωση του πελάτη την δεδομένη χρονική στιγμή. Για παράδειγμα, εάν η ζήτηση ενέργειας είναι υψηλή μια δεδομένη χρονική στιγμή, το κέντρο ελέγχου μπορεί να ζητήσει την μείωση της κατανάλωσης μιας συσκευής ή την διακοπή της λειτουργίας της. Αυτό προσθέτει ένα πλεονέκτημα στην διαχείριση της ηλεκτρικής ενέργειας ώστε να αποφεύγονται καταστάσεις διακοπών παροχής ενέργειας και πρόληψη ζημιών στην υποδομή του δικτύου μεταφοράς.

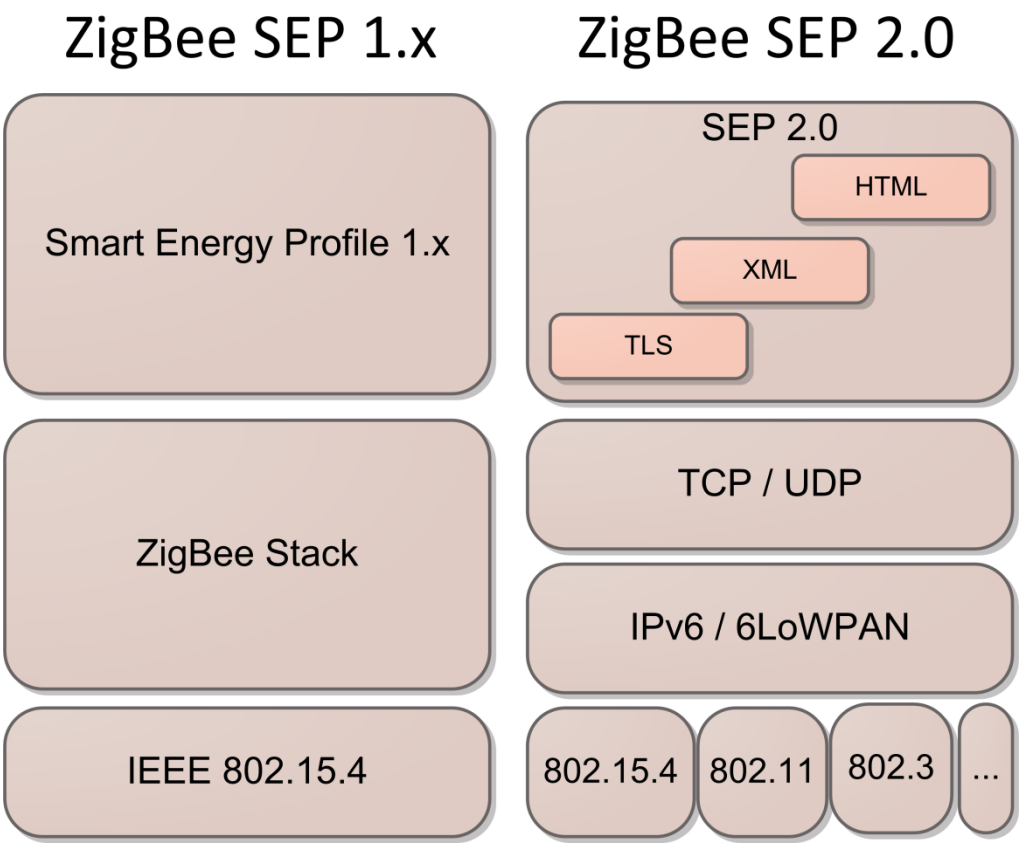
3. Έξυπνες συσκευές

Με την εφαρμογή του προτύπου σε οικιακές συσκευές όπου είναι πιστοποιημένες από την ZigBee Alliance, υπάρχει η δυνατότητα να δέχονται εντολές ελέγχου από το κέντρο διαχείρισης αναλόγως την χρήση μια δεδομένη χρονική στιγμή.

4. Παραγωγή ενέργειας από οικιακούς πελάτες

Οι οικιακοί πελάτες, εκτός από καταναλωτές ηλεκτρικής ενέργειας στο πλαίσιο λειτουργίας ενός ευφυούς δικτύου ενέργειας, λαμβάνουν ενεργό μέρος στην παραγωγή ενέργειας. Αυτό, επιτυγχάνεται με την χρήση φωτοβολταικών συστημάτων παραγωγής ηλεκτρικής ενέργειας κυρίως αλλά και με άλλους τρόπους. Με την χρήση του προτύπου, επιτυγχάνεται η μέτρηση της ενέργειας που παράγεται, και επιστρέφεται στο ευφυές δίκτυο, το χρηματικό όφελος που έχει ο καταναλωτής, και ενημέρωση του κέντρου διαχείρισης για τα δεδομένα αυτά μέσω των έξυπνων μετρητών που είναι εφαρμοσμένοι σε κάθε οικία.

Κατά την εξέλιξη του προτύπου έχουν δημιουργηθεί τρείς εκδόσεις, η 1, 1.1, και η 2.0 η οποία οριστικοποιήθηκε μέσα στο 2013. Η κύριες διαφορές ανάμεσα στις εκδόσεις είναι ότι η έκδοση 2 έχει σχεδιαστεί ώστε να λειτουργεί σε διαφορετικά φυσικά επίπεδα, όπως παράδειγμα, να μπορεί να λειτουργήσει πάνω σε ένα δίκτυο power line, ή σε ένα Wi-Fi πέραν του 802.15.4. Επίσης, έχει σχεδιαστεί να λειτουργεί πάνω σε ένα δίκτυο που χρησιμοποιεί το Internet Protocol (IP) και αυτό του δίνει ένα μεγάλο πλεονέκτημα σε σχέση με την έκδοση 1. Να αναφερθεί ότι ενώ το πρότυπο είναι διαθέσιμο προς υλοποίηση, ακόμη από τους κατασκευαστές έξυπνων μετρητών αλλά και έξυπνων συσκευών δεν έχει υλοποιηθεί στις συσκευές τους. Αυτό αναμένεται να γίνει στα επόμενα χρόνια.



Εικόνα 14 "Διαφορές στην στοίβα των δύο εκδόσεων" (Laboratories, 2013)

Οι τύποι των συσκευών που καθορίζονται από το πρότυπο ZigBee SEP 2.0 είναι οι παρακάτω:

1. In-Premises Displays

Οι συσκευές αυτές παρέχουν πληροφορίες στους καταναλωτές σχετικά με την κατανάλωση ενέργειας, το κόστος της KWh, τάση, ιστορικό, πληροφορίες που αποστέλλει η εταιρία παροχής ενέργειας κτλ. Πολλές φορές οι συσκευές αυτές επιτρέπουν την αλληλεπίδραση με τον χρήστη, μέσω οθόνης αφής, ή πληκτρολογίου.

2. Smart Thermostats

Είναι θερμοστάτες για τον έλεγχο της θερμοκρασίας μιας οικίας, αλλά παρέχουν και πληροφορίες σχετικά με το κόστος λειτουργίας ώστε να επιτυγχάνονται χαμηλές καταναλώσεις. Σε κρίσιμες καταστάσεις, μπορούν να δεχθούν εντολές ελέγχου από το ευφυές δίκτυο, για περιορισμό λειτουργίας ή για παύση. Από την άλλη μεριά θα πρέπει να διαθέτουν και σύστημα παράκαμψης για τον έλεγχο από τους καταναλωτές. Συνήθως οι πληροφορίες εμφανίζονται σε οθόνη, και μπορεί μαζί με ενσωματώνονται σε μια συσκευή μαζί με τις In-Premises Displays.

3. Load Controllers

Είναι συστήματα, τα οποία δέχονται εντολές τύπου demand response, για τον περιορισμό ή την παύση της λειτουργίας μια συσκευής. Συνήθως είναι ενσωματωμένα μέσα σε συσκευές υψηλής κατανάλωσης ενέργειας. Θα πρέπει όμως να υπάρχει επιλογή παράκαμψής από τον καταναλωτή.

4. Metering

Ανήκουν οι συσκευές, όπου καταγράφουν την κατανάλωση ενέργειας, έχουν προσαρμοσμένη πάνω τους συσκευή δικτύωσης ZigBee για να επικοινωνούν με τις οικιακές συσκευές ή με κάποιον άλλον δρομολογητή που υποστηρίζει το ZigBee. Επίσης η συσκευή αυτή μπορεί να βρίσκεται προσαρμοσμένη πάνω στο ESI.

5. Smart Appliances

Στην κατηγορία αυτήν ανήκουν οι συσκευές που συνδέονται στο HAN δίκτυο μέσω του ZigBee, και επικοινωνούν μέσω του ESI, με ευφυές δίκτυο ενέργειας. Συνήθως διαθέτουν οθόνη, όπου εμφανίζονται πληροφορίες σχετικά με την κατανάλωση ενέργειας και το κόστος αυτής. Μπορούν όμως να δεχθούν και εντολές ελέγχου από το ευφυές δίκτυο, σε κρίσιμες περιπτώσεις(υπερφόρτωση, υψηλή ζήτηση) που αντιμετωπίζει το δίκτυο για την προστασία του.

6. Range Extenders

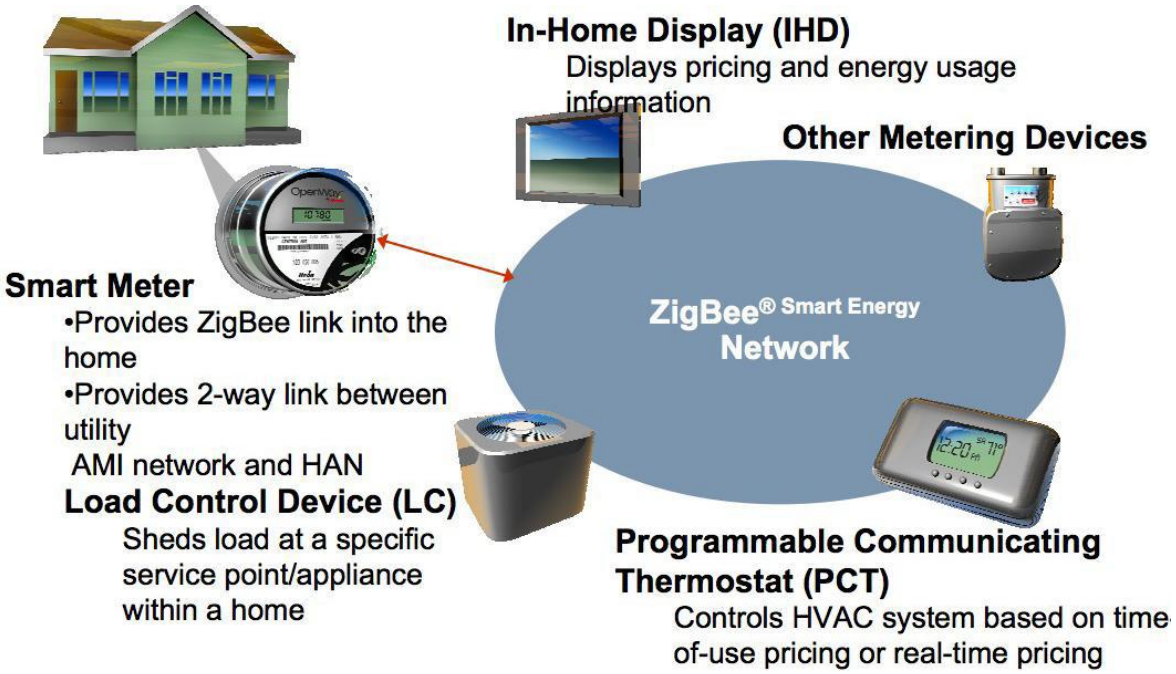
Ανήκουν οι συσκευές που εκτελούν χρέη δρομολογητή ZigBee, και χρησιμοποιούνται για την επέκταση του δικτύου σε μεγαλύτερη απόσταση.

7. Energy Services Interfaces (ESI)

Χαρακτηρίζεται η συσκευή, που συνδέει το HAN με το υπόλοιπο δίκτυο επικοινωνιών του ευφυούς δικτύου ενέργειας. Μια τέτοια συσκευή, μπορεί παρέχει λειτουργίες όπως ένας έξυπνος μετρητής ή μια οθόνη πληροφοριών. Δέχεται και λαμβάνει μυνήματα από το δίκτυο.

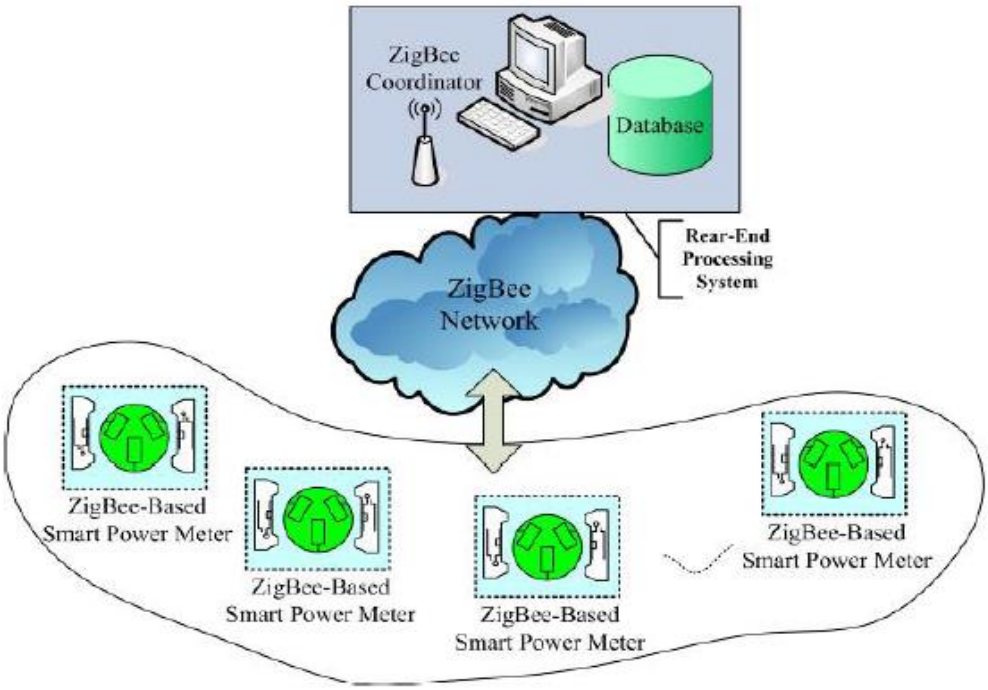
8. Pre-Payment Terminals

Είναι συσκευές που επιτρέπουν, την πληρωμή μέσω πιστωτικών καρτών ή κωδικών πληρωμής, για την ενέργειας που καταναλώθηκε, ή για να χρεωθεί το πόσο στον λογαριασμό του πελάτη για μελλοντική χρήση. Συνήθως προσφέρουν εκπτώσεις στην αξία της ηλεκτρικής ενέργειας. (Jennic, 2009)



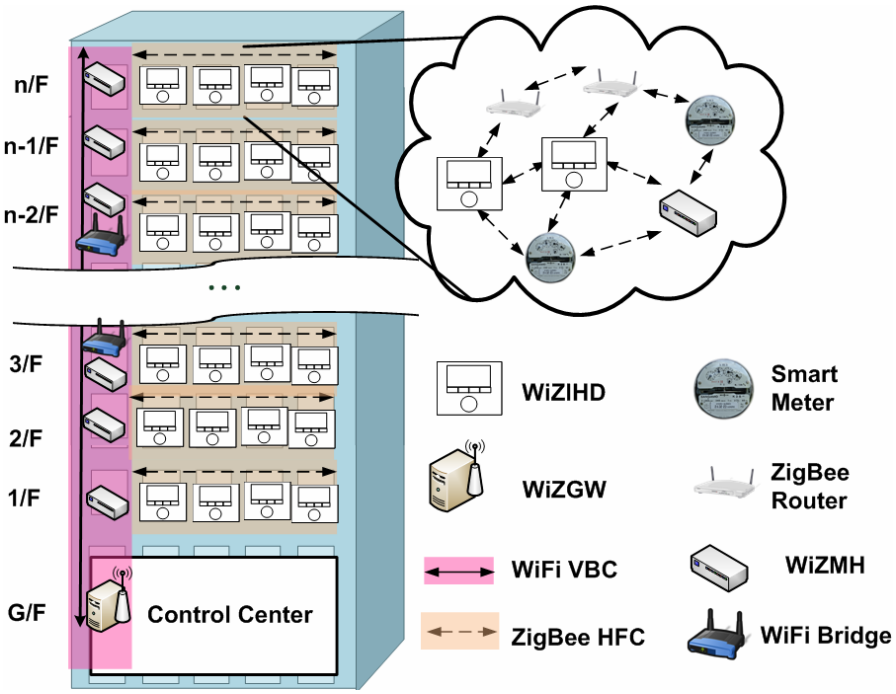
Εικόνα 14 "Έξυπνες συσκευές σε ένα HAN" (McCain)

Η χρήση του ZigBee θεωρείται ως η καταλληλότερη για το δίκτυο HAN και την επικοινωνία ανάμεσα στις οικιακές συσκευές και τον έξυπνο μετρητή που είναι προσαρμοσμένος σε κάθε οικία. Αυτό βασίζεται στο ότι τα πλεονεκτήματα που προσφέρει όπως είναι το χαμηλό-κόστος και χαμηλή κατανάλωση ενέργειας, είναι δύο από τα βασικά στοιχεία επιλογής της τεχνολογίας αυτής για ένα HAN. Ακόμη, έχουν αναπτυχθεί πολλά συστήματα έξυπνων μετρητών σε συνδυασμό με το ZigBee. Ένα τα τέτοιο σύστημα παρουσιάζεται από τους (Luan S, 2010) και αποτελείται από δύο τμήματα, το πρώτο είναι ο έξυπνος μετρητής ενέργειας, και το δεύτερο το σύστημα που καταγράφει τα δεδομένα που δέχεται από τον μετρητή σχετικά με την κατανάλωση ηλεκτρικής ενέργειας, την τάση της παροχής κτλ. Το παραπάνω επιτυγχάνεται με τον συνδυασμό λογισμικού υλικού.



Εικόνα 15 "Αρχιτεκτονική δικτύου βασισμένη στο ZigBee " (Luan S, 2010)

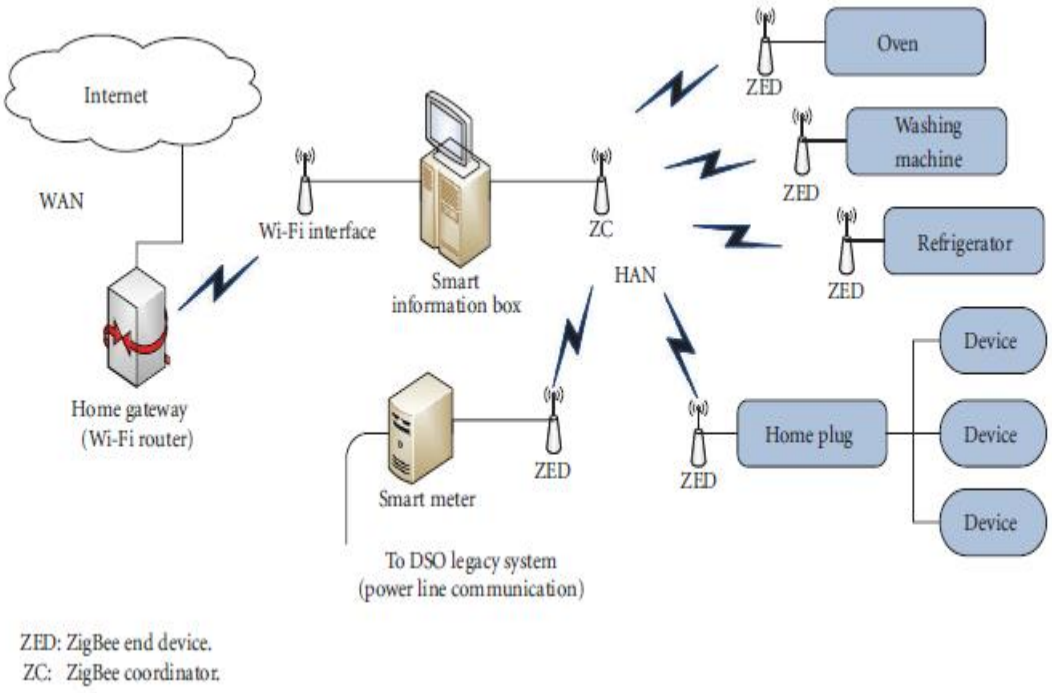
Η προτεινόμενη αρχιτεκτονική αποτελείται από συσκευές ZigBee, Coordinator και End Devices, και με τα χαρακτηριστικά λειτουργίας του ZigBee δικτύου δημιουργείται ένα αξιόπιστο δίκτυο. Αφού οι συσκευές βρεθούν στο ίδιο δίκτυο, ανά τακτά χρονικά διαστήματα στέλνονται από τον coordinator, εντολές ζήτησης των δεδομένων που έχουν συλλέξει οι έξυπνοι μετρητές και αυτοί απαντούν αποστέλλοντας τα δεδομένα, και μπαίνοντας σε κατάσταση sleep-mode. Τα δεδομένα αυτά εφόσον ληφθούν από τον ZigBee Coordinator, όπου και αποθηκεύονται, μπορούν να προβληθούν στην οθόνη που μπορεί να διαθέτει το σύστημα αυτό, ώστε ο καταναλωτής να ενημερώνεται άμεσα για το κόστος της ενέργειας όπου καταναλώνει. Υπάρχουν περιπτώσεις όπου το ZigBee μπορεί να συνδυαστεί και με άλλες ασύρματες τεχνολογίες υποστηρίζοντας την επικοινωνία που απαιτείται μεταξύ HAN και του δικτύου NAN και WAN ενός ευφυούς δικτύου. Στην βιβλιογραφία πολλές φορές αναφέρεται μια δομή δικτύου ως Building Area Network(BAN), θεωρώντας πολλές οικίες μαζί στο ίδιο κτήριο με πολλά διαφορετικά HAN. Όπως είναι κατανοητό, η κίνηση του δικτύου και το μεγάλο εύρος ανταλλαγής δεδομένων, απαιτούν ένα υβριδικό σύστημα, με συνδυασμό διαφορετικών τεχνολογιών δικτύωσης. Ένα τέτοιου είδους σύστημα παρουσιάζεται από τους (Hoi Yan Tung, 2012), με την ονομασία WiZBAN και ως στόχο έχει την σωστή απόδοση κάτω από συνθήκες όπου το δίκτυο έχει υψηλή κίνηση.



Εικόνα 16 "WiZBAN αρχιτεκτονική" (Hoi Yan Tung, 2012)

Το WiZBAN αποτελείται από δύο επίπεδα. Το πρώτο είναι το VBC και το δεύτερο είναι το HFC. Σε κάθε όροφο υπάρχουν διαφορετικά HAN, και το καθένα διαθέτει έναν έξυπνο μετρητή και μια οθόνη ενημέρωσης(In Home Display) για την κατανάλωσης ηλεκτρικής ενέργειας. Η επικοινωνία ανάμεσα στον έξυπνο μετρητή και στην συσκευή όπου λειτουργεί ως συγκεντρωτής δεδομένων (WiZMH) γίνεται με το ZigBee. Η συσκευή WiZMH εκτός από το ZigBee υποστηρίζει και το Wi-Fi, και επικοινωνεί με μια άλλη συσκευή, την WiZGW, όπου λειτουργεί ως πύλη για όλο το δίκτυο BAN. Η επιλογή της χρήσης του Wi-Fi, για την επικοινωνία ανάμεσα στις δύο αυτές συσκευές γίνεται με γνώμονα το εύρος της απόστασης όπου υποστηρίζει το Wi-Fi και του μεγαλύτερου εύρους ζώνης. Στο μοντέλο αυτό η συσκευή WiZGW, έχει την δυνατότητα να υποστηρίξει επικοινωνία με το υπόλοιπο δικτύου τους ευφυούς δικτύου ενέργειας, με κυψελοειδής τεχνολογίες, ή ενσύρματές τύπου Ethernet.

Στο (Bacchillone, 2012), επίσης γίνεται παρουσίαση ενός μοντέλου δικτύου του HAN, με την χρήση του ZigBee, ενώ η επικοινωνία προς το κέντρο ελέγχου γίνεται μέσω διαδικτύου. Στο δίκτυο υπάρχει μια συσκευή με την ονομασία Home Energy Angel box, και οι λειτουργίες που εκτελεί είναι να συλλέγει τα δεδομένα από τις οικιακές συσκευές, να καταγράφει την συνολική κατανάλωση, αλλά και την παραγόμενη ενέργεια σε περίπτωση χρήσης συστημάτων παραγωγής ανανεώσιμων μορφών ενέργειας. Επίσης έχει την δυνατότητα, να στέλνει εντολές στις συσκευές που είναι συνδεμένες στο δίκτυο και να παρέχει πληροφορίες στους καταναλωτές παρουσιάζονται τα δεδομένα σε ηλεκτρονικό υπολογιστή ή σε φορητή συσκευή.



Εικόνα 17 "Υλοποίηση HAN με τεχνολογία ZigBee" (Bacchillone, 2012)

Οι έξυπνες συσκευές στο δίκτυο διαθέτουν ενσωματωμένο ελεγκτή δικτύου τεχνολογίας ZigBee, ενώ για παλιότερες συσκευές μπορεί να προσαρμοστεί στο καλώδιο τροφοδοσία ρεύματος μια εξωτερική συσκευή με ενσωματωμένο ελεγκτή ZigBee, για να μπορούν να συνδεθούν στο δίκτυο. Το Home Energy Angel box, διαθέτει ελεγκτή ZigBee και εκτελεί χρέη ZigBee Coordinator ως συσκευή για την συλλογή δεδομένων. Διαθέτει επιπλέον και ελεγκτή Wi-Fi για την σύνδεση με τον δρομολογητή για την απομακρυσμένη σύνδεση μέσω διαδικτύου. Τα δεδομένα αφού συλλέγονται από το Home Energy Angel box, μπορούν να σταλούν στον έξυπνο μετρητή που είναι εγκατεστημένος σε κάθε οικία καταναλωτή με την χρήση του ZigBee, και από εκεί μέσο του NAN όπου είναι συνδεμένο μετρητής να μεταφέρονται τα δεδομένα των μετρήσεων προς το κέντρο ελέγχου του ευφυές δικτύου ενέργειας. Με την τοποθέτηση, του Home Energy Angel box, πρακτικά η οικία αποκτά δύο πύλες για την μεταφορά δεδομένων σχετικά με την ενεργειακή κατάσταση της.

Συμπερασματικά, το ZigBee είναι κατάλληλο για δίκτυα, που απαιτούν χαμηλό ρυθμό μεταφοράς δεδομένων και χαμηλή κατανάλωση ενέργειας. Τα ευφυή δίκτυα ενέργειας εκτός από την σωστή διαχείριση της ενέργειας έχουν ως στόχο την χρήση συσκευών που έχουν χαμηλή κατανάλωση, την αξιοπιστία και κάλυψη των αναγκών επικοινωνίας. Το HAN είναι ένα δίκτυο όπου υπερκαλύπτεται από τα χαρακτηριστικά που έχει το ZigBee, έτσι με αυτόν τον τρόπο από πολλούς σχεδιαστές αρχιτεκτονικών και υποδομών θεωρείται ως η πρώτη επιλογή για την δικτύωση στο HAN. Να αναφερθεί επίσης ότι το ZigBee σε σχέση με το Wi-Fi που είναι μια ανταγωνιστική τεχνολογία για το HAN, καταναλώνει 2.2 φορές λιγότερη

ενέργεια. Το παραπάνω έχει προκύψει από προσομοιώσεις στο (Jeff Drake, 2010) που έχουν πραγματοποιηθεί και με τις δύο τεχνολογίες για το ίδιο HAN. Το συνολικό κόστος ενέργειας από την επιλογή του ZigBee είναι 370 Megawatt ενέργειας και με εξοικονομημένο κόστος 315 εκατομμυρίων δολαρίων. Η διαφορά αυτή έχει προκύψει από την κατανάλωση του hardware, αλλά και του τρόπου λειτουργίας. Χαρακτηριστικά, λόγω υψηλότερου ρυθμού μετάδοσης δεδομένων του Wi-Fi, ο χρόνος μετάδοσης είναι μικρότερο σε σχέση με το ZigBee αλλά σε περιόδους που δεν γίνεται μετάδοση η κατανάλωση ενέργειας είναι μεγαλύτερη και τελικώς η συνολική μέση κατανάλωση ενέργειας είναι μεγαλύτερη. Στην αντίθετη περίπτωση που ο όγκος των δεδομένων είναι μεγάλος σε ένα δίκτυο HAN που χρησιμοποιείται και για άλλες χρήσεις(streaming video, παρακολούθηση μέσω καμερών) η χρήση του ZigBee θα έχει αυξημένη κατανάλωση ενέργειας λόγω ότι υποστηρίζει μικρό ρυθμό μετάδοσης δεδομένων και ο χρόνος μετάδοσης θα είναι αυξημένος. Σε αυτήν την περίπτωση το Wi-Fi θα ήταν καλύτερη επιλογή μιας και έχει σχεδιαστεί για να επιτυγχάνει μεγάλους ρυθμούς μετάδοσης δεδομένων με μεγαλύτερή απόσταση λειτουργίας. Για αποκλειστική χρήση όμως για ένα ευφυές δίκτυο ενέργεια η χρήση του ZigBee φαίνεται να είναι μονόδρομος. Πέραν από την κατανάλωση και το κόστος κατασκευής των τσιπ που χρησιμοποιούνται στους ελεγκτές δικτύου στο ZigBee είναι φθηνότερα. Άρα μειώνεται και το κόστος υλοποίησης του δικτύου εκτός και από το όφελος της μειωμένης κατανάλωσης ενέργειας.

Πίνακας 2 "Σύγκριση κατανάλωσης ενέργειας ανάμεσα στο ZigBee και στο Wi-Fi για HAN" (Jeff Drake, 2010)

Τεχνολογία	Average Watts(W)	Average Current(mA)
ZigBee	.39	32.64
Wi-Fi	.87	73.57

3.2 WI-FI

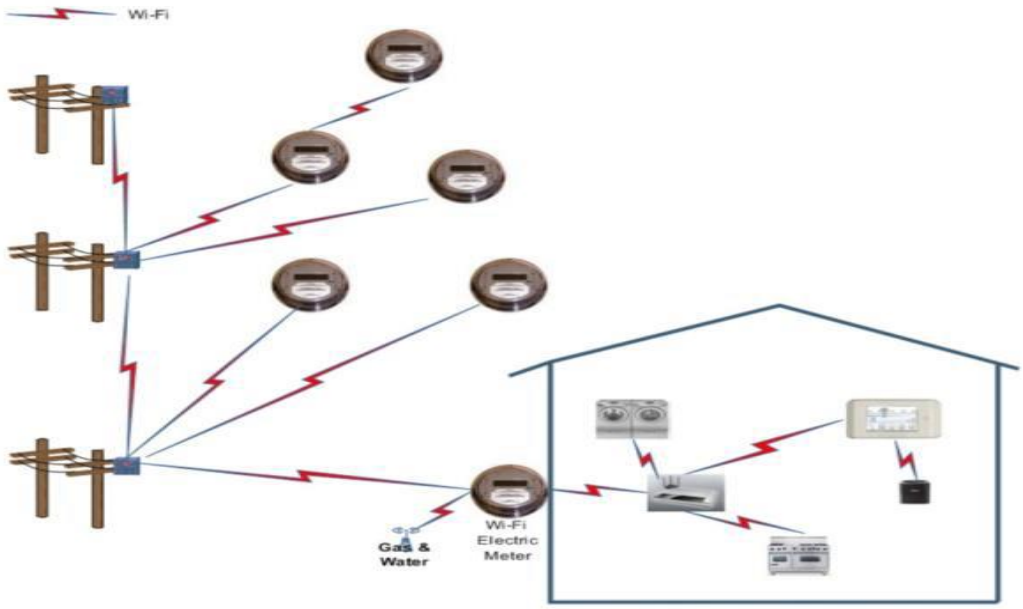
Το IEEE 802.11, είναι σύνολο προτύπων που καθορίζει το φυσικό(PHY) και το επίπεδο MAC των ασύρματων τοπικών δικτύων. Οι συχνότητες λειτουργίας καθορίζονται στα 2.4, 3,6 και 5 GHz. Τα πρότυπα είναι ευρύτερα γνωστά ως Wi-Fi, επειδή η Wi-Fi Alliance, ένας οργανισμός ανεξάρτητος της IEEE, παρέχει πιστοποίηση για τα προϊόντα που ακολουθούν της προδιαγραφές του 802.11. Ο όρος Wi-Fi χρησιμοποιείται για να προσδιορίσει τις συσκευές εκείνες που βασίζονται στις προδιαγραφές των 802.11 b/g/n και λειτουργούν στην ελεύθερη συχνότητα των 2.4GHz. Το IEEE 802.11b χρησιμοποιεί την τεχνική Direct Sequence Spread spectrum(DSSS) και ο ρυθμός μετάδοσης είναι έως 11Mbps για εσωτερικούς χώρους και 1Mbps για εξωτερικούς χώρους. Το εύρος του φτάνει τα 30-40 μέτρα για εσωτερικούς χώρους ενώ για εξωτερικούς τα 90-100 μέτρα. Το νεότερο IEEE 802.11g χρησιμοποιεί την τεχνική πολυπλεξίας Orthogonal

Frequency Division Multiplexing technique (OFDM) με ρυθμό μετάδοσης μέχρι και 54Mbps και είναι πλήρως συμβατό με το 802.11b. Η τελευταία έκδοση είναι η 802.11n, η οποία παρέχει υψηλότερους ρυθμούς μετάδοσης δεδομένων έως 150Mbps βασιζόμενη στην τεχνική Multiple-Input Multiple-Output (MIMO) με την χρήση πολλαπλών κεραιών. Ακόμη, χρησιμοποιεί την τεχνική OFDM που χρησιμοποιούν και οι προηγούμενες γενιές και λειτουργεί σε δύο συχνότητες, στην 2.4GHz που είναι η πιο συνηθισμένη αλλά υποστηρίζει και την συχνότητα των 5GHz. Η απόσταση εξαρτάται από παράγοντες, όπως είναι ο τύπος των κεραιών αλλά και αν είναι σε εξωτερικό ή εσωτερικό χώρο. (Emilio Ancillotti, 2013) (Ahmad Usman, 2013). Εκτός από τα παραπάνω υπάρχουν και άλλα πρότυπα που υπάρχει η δυνατότητα να υλοποιηθούν στα ευφυή δίκτυα ενέργειας. Χαρακτηριστικό παράδειγμα είναι το 802.11s, το οποίο υλοποιεί mesh δίκτυα. Το 802.11s μελετάτε ως προς την εφαρμογή του στα ευφυή δίκτυα ενέργειας στο υποκεφάλαιο τον mesh δικτύων.

Η χρήση του Wi-Fi στα ευφυή δίκτυα ενέργειας, καλύπτει περιοχές όπως είναι το HAN, αλλά και το NAN. Ακόμη, υπάρχουν περιπτώσεις όπου μπορεί να χρησιμοποιηθεί σε τμήματα του WAN καλύπτοντας βέβαια τις απαιτήσεις. Όπως έχει αναφερθεί προηγούμενος το HAN είναι το δίκτυο με το οποίο υλοποιείται η επικοινωνία ανάμεσα στις οικιακές συσκευές και στον έξυπνο μετρητή που είναι εγκατεστημένος σε κάθε οικία. Με τα χαρακτηριστικά που προσφέρει το Wi-Fi, όπως είναι η απόσταση λειτουργίας, αλλά και ο σχετικά κάλος ρυθμός μετάδοσης δεδομένων που επιτυγχάνει επαρκεί για την κάλυψη των αναγκών σε ένα HAN. Με την ευρεία διάδοση του τα τελευταία χρόνια η Wi-Fi Alliance θέτει στις συσκευές που καλύπτουν τις προδιαγραφές της με την πιστοποίηση Wi-Fi Certified. Με αυτόν τον τρόπο εξασφαλίζεται η διαλειτουργικότητα ανάμεσα στις διαφορετικές εκδόσεις Wi-Fi (IEEE 802.11 a/b/g/n) αλλά η εφαρμογή τεχνικών εξοικονόμησης ενέργειας για την ασύρματη δικτύωση. Στο (Alliance W.-F. , 2010) παρουσιάζονται οι εφαρμογές του Wi-Fi στα ευφυή δίκτυα ενέργειας και ειδικότερα για το HAN, περιγράφεται ότι προσφέρει διπλή επικοινωνία με την χρήση δρομολογητών Wi-Fi, μία προς το δίκτυο NAN και μία προς το διαδίκτυο μέσω του οποίου έχει πρόσβαση ο πελάτης ώστε να διαχειρίζεται και να παρακολουθεί την κατάσταση του δικτύου και των συσκευών του. Στο (Serbulent Tozlu, 2012) μελετάται η χρήση του Wi-Fi στους αυτοματισμούς ενός έξυπνου σπιτιού για την επικοινωνία ανάμεσα στους διάφορους αισθητήρες που είναι προσαρμοσμένοι στις οικιακές συσκευές. Επιπλέον, δίνεται έμφαση στην εξοικονόμηση ενέργειας χρησιμοποιώντας την τεχνική που διαθέτει το Wi-Fi, Power Saving Mode(PS). Η τεχνική αυτή είναι σημαντική προσθήκη μιας στα πλαίσια των ευφυών δικτύων ενέργειας, μελετάται και η κατανάλωση των συσκευών δικτύωσης. Χαρακτηριστικά αναφέρεται ότι η κατανάλωση περιορίζεται με παραμετροποίηση του ρυθμού μετάδοσης αλλά και το μέγεθος των πακέτων επιτυγχάνοντας καλύτερες καταναλώσεις ενέργειας. Συμπερασματικά, σε χαμηλούς ρυθμούς μετάδοσης και με μικρό μέγεθος πακέτου παρατείνεται αύξηση της κατανάλωσης ενέργειας. Το ίδιο συμβαίνει σε περίπτωση πολλών αναμεταδόσεων πακέτων λόγω

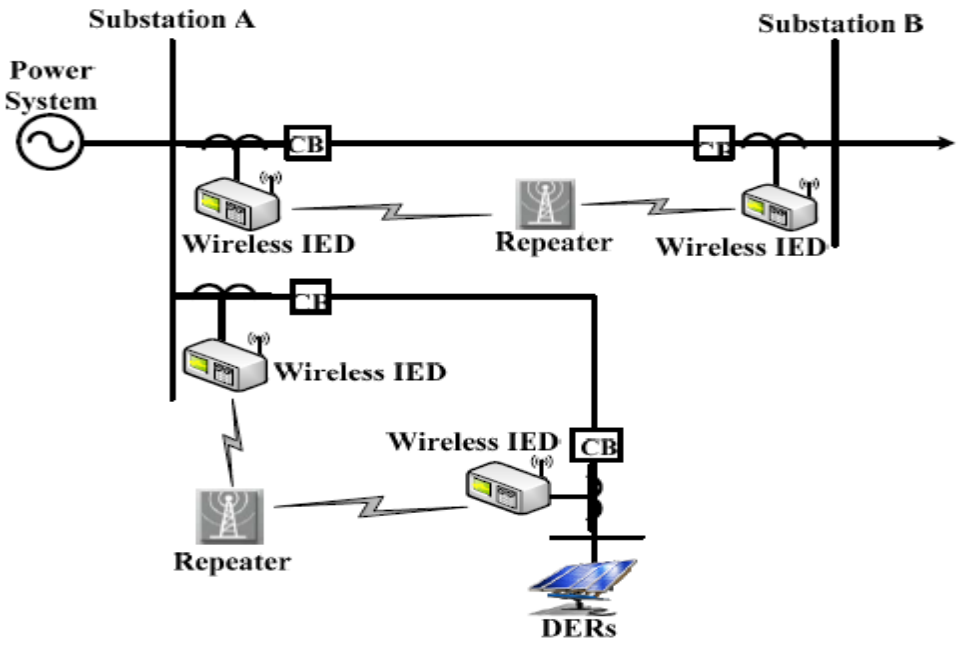
παρεμβολών. Ένα δίκτυο βασισμένο στο Wi-Fi και με την χρήση δρομολογητή με διαθέσιμη πρόσβαση στον διαδίκτυο αποτελεί ιδανική λύση για απομακρυσμένο έλεγχο συσκευών όπως είναι ένας θερμοστάτης. Επίσης, η απόσταση λειτουργίας ενός δικτύου Wi-Fi επιτρέπει τον έλεγχο συσκευών από κινητές συσκευές όπως είναι tablets, smart phones, με το κατάλληλο λογισμικό το οποίο πολλές φορές διατίθεται δωρεάν από τους κατασκευαστές των συσκευών. Αυτό είναι ακόμα ευκολότερο με το Wi-Fi Direct(Wi-Fi P2P) που επιτρέπει την σύνδεση δύο συσκευών που διαθέτουν Wi-Fi χωρίς την χρήση κάποιου σημείου πρόσβασης, όπως είναι ένας δρομολογητής Wi-Fi. Σαν αποτέλεσμα, ο έλεγχος μιας συσκευής γίνεται ευκολότερος και χωρίς να περιπλέκεται το δίκτυο επικοινωνιών. Για παράδειγμα, μια οικιακή συσκευή μπορεί να απενεργοποιηθεί ή να αλλαχθεί η ώρα λειτουργίας της όταν η αξία της ενέργειας είναι μεγάλη μια δεδομένη χρονική στιγμή.

Εκτός από το HAN η Wi-Fi τεχνολογία έχει τις δυνατότητες να χρησιμοποιηθεί και στο NAN για συλλογή δεδομένων από τους έξυπνους μετρητές, παρέχοντας επικοινωνία δύο κατευθύνσεων. Ειδικότερα, μπορεί να καλύψει το κομμάτι του “last-mile” ανάμεσα σε έναν έξυπνο μετρητή και ένα συλλέκτη δεδομένων, ο οποίος συγκεντρώνει δεδομένα από τα HAN. Οι συλλέκτες βρίσκονται συνήθως σε σημεία όπου ανήκουν στο δίκτυο ηλεκτρικής ενέργειας για καλύτερη διαχείριση και προστασία του εξοπλισμού. Στην παρακάτω εικόνα παρουσιάζεται μια τέτοια υλοποίηση.

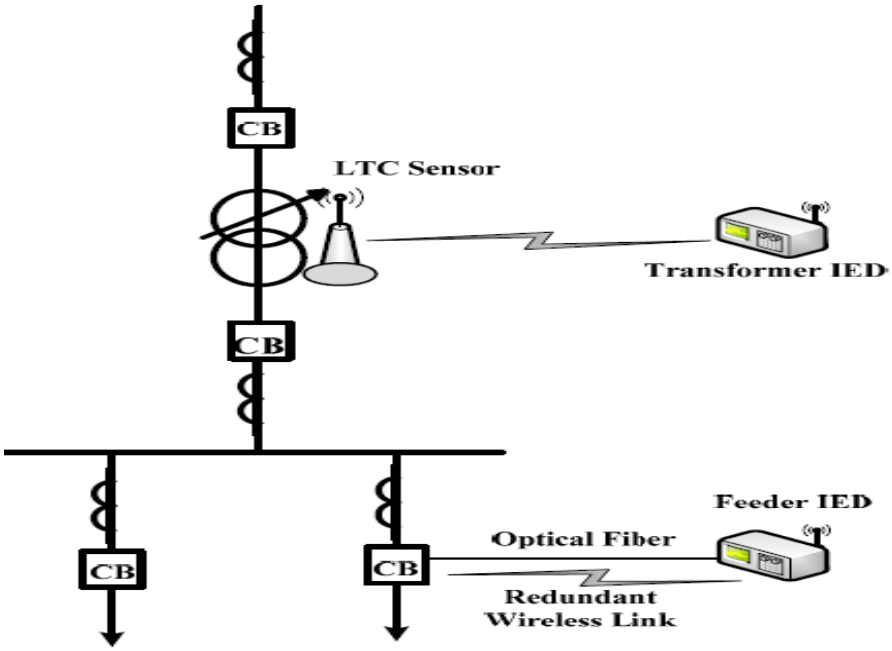


Εικόνα 18 "Επικοινωνία “last-mile” με χρήση Wi-Fi" (Alliance W.-F. , 2010)

Υπάρχουν δύο επιλογές για την υλοποίηση βασισμένη στο Wi-Fi, μία point to point και μία mesh ανάμεσα σε έναν έξυπνο μετρητή και έναν συλλέκτη δεδομένων. Η δεύτερη μελετάται σε παρακάτω υποκεφάλαιο στο οποίο παρουσιάζονται όλες οι τεχνολογίες που υλοποιούν δίκτυα mesh. Για μια point to point σύνδεση η τελευταία και βελτιωμένη έκδοση του Wi-Fi, 802.11n, φαίνεται να είναι μια πολύ καλή επιλογή ανάμεσα στις έκδοσης της ίδιας τεχνολογίας με βάση τα χαρακτηριστικά που έχουν αναφερθεί. (Emilio Ancillotti, 2013) (Kalkunte, 2010). Από την άλλη μεριά η point to point συνδέσεις μειονεκτούν σε σχέση με τις mesh στην αξιοπιστία λόγω αρχιτεκτονικής. Σε περίπτωση που παρουσιαστεί πρόβλημα επικοινωνίας σε έναν συλλέκτη ή σε έναν έξυπνο μετρητή το αποτέλεσμα είναι να χαθούν δεδομένα των μετρήσεων, φυσικά εάν το πρόβλημα είναι στο συλλέκτη, που στην προκειμένη περίπτωση είναι ένα σημείο πρόσβασης (Access Point) Wi-Fi, θα χαθεί η επικοινωνία με όλους τους έξυπνους μετρητές που συνδέονται σε αυτόν. Ένα mesh δίκτυο υλοποιημένο με το 802.11s όμως παρέχει μεγαλύτερη αξιοπιστία και μεγαλύτερη γεωγραφική κάλυψη με μικρότερο κόστος, μιας και δεν απαιτούνται τόσα πολλά σημεία πρόσβασης όσο σε μια point to point αρχιτεκτονική. Η υλοποίηση όμως ενός mesh δικτύων για το κομμάτι του “last-mile” θέτει σοβαρά θέματα ασφάλειας των δεδομένων που ανταλλάσσονται μιας και τα δεδομένα από τους μετρητές διασχίζουν όλο το mesh δίκτυο. Σαν αποτέλεσμα οποιαδήποτε αλλοίωση δεδομένων, ενδέχεται να δημιουργήσει σοβαρά προβλήματα για την λειτουργία του δικτύου. Εκτός από τις παραπάνω περιπτώσεις έχει την δυνατότητα να υλοποιηθεί και σε υποσταθμούς του δικτύου ενέργειας για την κάλυψη των αναγκών σε επικοινωνία ανάμεσα σε IED για την παρακολούθηση της κατάστασης του δικτύου.



Εικόνα 19 "Χρήση Wi-Fi για την επικοινωνία ανάμεσα σε υποσταθμούς ηλεκτρικής ενέργειας" (Palak P. Parikh, 2010)



Εικόνα 20 "Χρήση Wi-Fi για αναπληρωματική σύνδεση ανάμεσα σε συσκευές παρακολούθησης του δικτύου ενέργειας" (Palak P. Parikh, 2010)

Στο άρθρο (Palak P. Parikh, 2010) αναφέρονται περιπτώσεις χρήσης όπως οι παραπάνω. Η σύνδεση γίνεται point to point ανάμεσα στις συσκευές IED που χρησιμοποιούνται για την παρακολούθηση της κατάστασης του δικτύου ενέργειας. Ακόμη, σε περί-αστικές περιοχές που υπάρχουν εγκαταστάσεις ανανεώσιμων πηγών ενέργειας απαιτείται επικοινωνία των υποδομών αυτών με το ευφυές δίκτυο ενέργειας, για την παρακολούθηση της λειτουργίας, για την φυσική ασφάλειας της υποδομής κτλ. Με την χρήση αναμεταδοτών υπάρχει η δυνατότητα να υπάρξει επικοινωνία ανάμεσα στις υπόλοιπες υποδομές του δικτύου ενέργειας και το υποδομών αυτών. Το Wi-Fi μπορεί να υλοποιηθεί με μικρό κόστος σε σχέση με άλλες τεχνολογίες δικτύωσης λόγω της ευρείας αποδοχής του. Υπάρχουν περιπτώσεις που η υλοποίηση μιας σύνδεσης Wi-Fi ανάμεσα σε δύο συσκευές IED λειτουργεί ως δευτερεύον σε περίπτωση που παρουσιαστεί πρόβλημα στην κύρια σύνδεση. Η κύρια σύνδεση σε περιπτώσεις που είναι κοντινή η απόσταση μπορεί να είναι με χρήση οπτικής ίνας.

Η υλοποίηση ενός δικτύου κορμού βασισμένο στο Wi-Fi για την κάλυψη των αναγκών ενός ευφυούς δικτύου ενέργειας, λόγω των χαρακτηριστικών του 802.11, που παρέχει μικρό σχετικά εύρος για τις ανάγκες ενός WAN, δεν μπορεί να υποστηρίξει αποκλειστικά μόνο του την επικοινωνία. Ενώ το κόστος που εξοπλισμού είναι χαμηλό μιας και είναι από η πιο γνωστή ασύρματη τεχνολογία, ο αριθμός των σημείων πρόσβασης που απαιτείται είναι μεγάλος. Επιπλέον, η συχνότητα λειτουργίας των 2.4 GHz σε πολλές περιοχές παρουσιάζει παρεμβολές λόγω ότι η συχνότητα αυτή είναι ελεύθερη στο κοινό προς χρήση. Για την εφαρμογή είναι απαραίτητο να ληφθούν τα στοιχεία αυτά υπόψη κατά την σχεδίαση του δικτύου.

3.3 WiMAX

Η τεχνολογία δικτύωσης World Interoperability for Microwave Access(WiMAX), έχει οριστεί από το πρότυπο της IEEE 802.16, ενώ η ονομασία έχει προκύψει από τον οργανισμό WiMAX Forum. Το WiMAX σχεδιάστηκε τον 2001 για να καλύψει την ανάγκη της επικοινωνίας σε διάφορες υποδομές, στο κομμάτι που ορίζεται ως “last mile” και αφορά το κομμάτι εκείνο ενός δικτύου επικοινωνιών που είναι υπεύθυνο για την τελική σύνδεση και παράδοση των δεδομένων στον παραλήπτη. Η πιο διαδεδομένη έκδοση του προτύπου είναι η 802.16e 2005, όπου η IEEE ορίζει το φυσικό επίπεδο(PHY) και το επίπεδο MAC. Στο φυσικό επίπεδο εφαρμόζεται η τεχνική Orthogonal Frequency Division Multiple Access(OFDMA) μαζί με άλλες δυνατότητες, όπως είναι το Multiple In Multiple Out(MIMO) για Non-Line of Sight δυνατότητα. Το WiMAX χρησιμοποιεί δύο εύρη συχνοτήτων, μία για Line of sight , με εύρος 11-66GHz και μία Non-Line of Sight με εύρος 2-11GHz, ενώ η απόσταση που μπορεί να μεταδώσει δεδομένα είναι μέχρι και 30 μίλια (50 χιλιόμετρα) και με ταχύτητα μέχρι 70Mbps. Μία από τις κοινές παρανοήσεις που πιθανώς συμβαίνουν στο WiMAX είναι το ότι πρόκειται να αποδίδει ταχύτητα της τάξεως των 70 Mbps σε απόσταση 48 χιλιομέτρων. Το παραπάνω είναι αληθές αλλά σε ιδανικές συνθήκες, συνεπώς στις περισσότερες περιπτώσεις δεν θα υφίστανται τέτοιου μεγέθους ταχύτητες σε τέτοιες αποστάσεις. Πρακτικά, σε περιβάλλοντα όπως είναι οι επαρχιακές περιοχές όπου οι κεραίες μετάδοσης θα έχουν οπτική επαφή και θα απέχουν μεταξύ τους 10 χιλιόμετρα θα αγγίζουν ταχύτητες της τάξης των 10 Mbps. Σε αστικά όμως περιβάλλοντα πιθανώς το 30% των κεραιών μετάδοσης να μην έχουν οπτική επαφή και συνεπώς οι χρήστες θα αγγίζουν ταχύτητες της τάξεως των 10 Mbps σε απόσταση 2 χιλιομέτρων. Τα κύρια χαρακτηριστικά του WiMAX μπορούν να οριστούν ως εξής: (Forum W. , 2006) (tutorialspoint.com) (Ahmad Usman, 2013) (Paolin, 2010)

1. Χρησιμοποιεί την τεχνική OFDMA για Non-Line of Sight επικοινωνία
2. Υποστήριξη Quality Of Service(QoS)
3. Υψηλό ρυθμό μεταφοράς δεδομένων, με την χρήση της τεχνικής MIMO
4. Υποστήριξη internet protocol(IP)
5. Υποστήριξη χρήσης πολλαπλών κεραιών
6. Ασφάλεια, με χρήση Extensible Authentication Protocol(EAP), advance encryption standard(AES), Cipher based Message Authentication Code(CMAC), και Hashed Message Authentication Code(HMAC).

Ένα σύστημα επικοινωνίας WiMAX αποτελείται από δύο κύρια μέρη:

1. Σταθμός Βάσης(Base Station)

Λειτουργεί ως κεραία εκπομπής και αποτελείται από ηλεκτρονικές συσκευές για αυτόν τον σκοπό. Μοιάζει σαν τις κεραίες που χρησιμοποιούν τα κυψελοειδή δίκτυα κινητής τηλεφωνίας. Το εύρος που καλύπτουν θεωρητικά είναι μέχρι 30 μίλια(περίπου 50 χιλιόμετρα), ενώ σε πραγματικές εφαρμοσμένες συνθήκες η απόσταση αυτή είναι αρκετά μικρότερη λόγω γεωγραφιών περιορισμών,

εμποδίων, καιρικών συνθηκών κτλ. Μία φυσιολογική απόσταση είναι περίπου τα 10 χιλιόμετρα.

2. Δέκτης(Receiver)

Είναι η συσκευή εκείνη που λαμβάνει τα δεδομένα που στέλνονται από τον σταθμό βάσης και συνδέεται στον δίκτυο WiMAX μέσω του ίδιου σταθμού. Μπορούν να είναι εγκατεστημένες μέσα σε μία συσκευή, ή να συνδέονται ως εξωτερική συσκευή. Συνήθως, επειδή είναι εγκατεστημένες σε ένα χρήστη/καταναλωτή, αναφερόμαστε σε αυτές με τον όρο Customer Premise Equipment(CPE), λόγω ότι οριοθετούν το κοινό δίκτυο, από το δίκτυο του χρήστη.

Από πλευράς μετάδοσης σήματος μπορούμε να διακρίνουμε δυο περιπτώσεις που αναφέρθηκαν παραπάνω:

1. Light of Sight(LOS)

Στην LOS σύνδεση, το σήμα ταξιδεύει στο μέσο, που στην προκειμένη περίπτωση είναι ο ατμοσφαιρικός αέρας, και έχει άμεση οπτική επαφή ο σταθμός βάσης με τον δέκτη. Σε περίπτωση που υπάρχουν εμπόδια και το σήμα μπλοκάρετε τότε η ένταση του σήματος πέφτει δραματικά με αποτέλεσμα την δυσκολία της συνδεσιμότητας. Τα κύρια χαρακτηριστικά είναι:

- Χρησιμοποιούνται οι υψηλότερες συχνότητες(10GHz μέχρι 66GHz)
- Μεγαλύτερη γεωγραφική κάλυψη
- Μικρές παρεμβολές
- Ανάγκη μη ύπαρξης εμποδίων

2. Non-Line of Sight(NLOS)

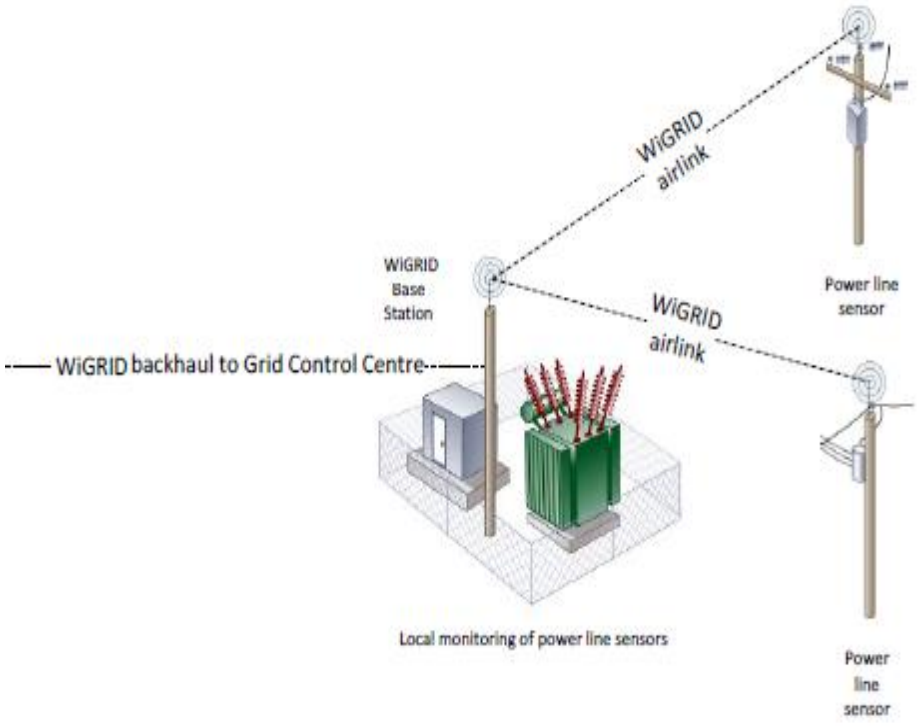
Στην NLOS σύνδεση, το σήμα ταξιδεύει στο μέσο μέσα από ανακλάσεις, διαθλάσεις, απορρόφηση γιατί δεν έχει άμεση επαφή με τον δέκτη, λόγω ότι υπάρχει εμπόδια. Το αποτέλεσμα, είναι το σήμα να φτάνει σε διαφορετικές χρονικές στιγμές με εξασθένιση. Το WiMAX έχει καλή απόδοση σε συνδέσεις NLOS γιατί βασίζεται στην τεχνική OFDM, που μπορεί να διαχειριστεί την καθυστέρηση που προκύπτει από το NLOS. Τα κύρια χαρακτηριστικά είναι:

- Χρησιμοποιεί την τεχνική AMC και MIMO
- Η τεχνική MIMO βοηθάει στην βελτίωση του έντασης του σήματος και της ρυθμό-απόδοσης.
- Στην NLOS σύνδεση, η ταχύτητα είναι μεγαλύτερη αλλά η γεωγραφική κάλυψη είναι μικρότερη. (Eugene Crozier)

Η χρήση της τεχνολογίας WiMAX έχει προταθεί και έχει εφαρμοσθεί σε πολλές περιπτώσεις υλοποιημένων ευφυών δικτύων ενέργειας. Αν και πολλοί ερευνητές θεωρούν ότι από τις τεχνολογίες τέταρτης γενιάς θα υπάρξει προτίμηση προς το LTE και όχι τόσο προς το WiMAX τα επόμενα χρόνια η IEEE και το WiMAX Forum συνεχίζουν την εξέλιξη του WiMAX στα πλαίσια εφαρμογής του στα ευφυή δίκτυα ενέργειας. Το WiMAX Forum δημιούργησε το “Smart Grid Working Group” τον

Μάρτιο του 2011 με σκοπό να καθοριστούν οι απαιτήσεις της υποδομής ενός ευφυούς δικτύου ενέργειας, την αξιολόγηση της καταλληλότητας του 802.16e για τα ευφυή δίκτυα, αλλά και την βελτιστοποίηση του 802.16e για την εφαρμογή του σε υποδομές. Ο κύριος στόχος ήταν η ανάπτυξη μια νέας εφαρμογής του WiMAX στα πλαίσια των ευφυών δικτύων ενέργειας με την ονομασία WiGRID. Οι απαιτήσεις και οι εφαρμογές στο δίκτυο επικοινωνιών ενός ευφυούς δικτύου ενέργειας καθορίζονται από το: WiMAX Forum System Profile Requirements for Smart Grid Applications Requirements for WiMAX, T31-001-RXXXv01 (Byrne, 2013) . Επίσης μετά από έρευνα μεγάλου χρονικού διαστήματος και με την συμμετοχή εταιριών παροχής ηλεκτρικής ενέργειας που δραστηριοποιούνται στην εξέλιξη και εφαρμογή των ευφυών δικτύων ενέργειας, παρουσιάζονται επτά σενάρια εφαρμογής της τεχνολογίας WiMAX σε όλο το εύρος που δικτύου επικοινωνιών, από το WAN που περιλαμβάνει το δίκτυο κορμού, μέχρι το NAN και μεταφοράς ηλεκτρικής ενέργειας, αλλά και μέχρι την άμεση επικοινωνίας με τους έξυπνους μετρητές όπου λειτουργούν ως η πύλη του HAN. (Forum W. , 2013)

1. Χρήση WiMAX για την επικοινωνία υποσταθμών με δίκτυο διανομής(τηλεμετρία)



Εικόνα 21 "Επικοινωνία υποσταθμών με δίκτυο διανομής με WiMAX" (Forum W. , 2013)

Το δίκτυο μεταφοράς και διανομής ηλεκτρικής ενέργειας περιλαμβάνει στοιχεία όπως είναι γραμμές μεταφοράς, μετασχηματιστές, αισθητήρες παρακολούθησης της τάσης, θερμοκρασιών, σφαλμάτων κτλ που σχετίζονται γενικά με την κατάσταση του δικτύου, και συλλέγουν δεδομένα που είναι απαραίτητα για την αξιόπιστη λειτουργία του δικτύου. Τα δεδομένα αυτά, είναι απαραίτητο να συγκεντρώνονται και να καταγράφονται στο κέντρο διαχείρισης του δικτύου ενέργειας, αυτό σαν αποτέλεσμα έχει την ανάγκη της επικοινωνίας, ανάμεσα στους υποσταθμούς και στο δίκτυο διανομής. Ακόμη, οι αισθητήρες που συλλέγουν τις πληροφορίες σχετικά με την κατάσταση του δικτύου, για την καλύτερη αξιοπιστία και εξοικονόμηση ενέργειας, μπορούν να λειτουργούν σε κατάσταση αναμονής(sleep mode) και ανά τακτά χρονικά διαστήματα να συλλέγουν τα δεδομένα και να ξαναμπαίνουν σε κατάσταση αναμονής. Η επικοινωνία των υποσταθμών με το κέντρο διαχείρισης του δικτύου ηλεκτρικής ενέργειας, μπορεί να πραγματοποιηθεί και με άλλες τεχνολογίες εκτός από το WiMAX, όπως είναι με χρήση οπτικών ινών. Τα χαρακτηριστικά που WiMAX, με το δυνατότητα υψηλού ρυθμού απόδοσης, ποιότητα των υπηρεσιών, μικρή καθυστέρηση και μεγάλο εύρος γεωγραφικής κάλυψης το καθιστούν ιδανικό για την συλλογή των δεδομένων αυτών από το δίκτυο διανομής. (Forum W. , 2013)

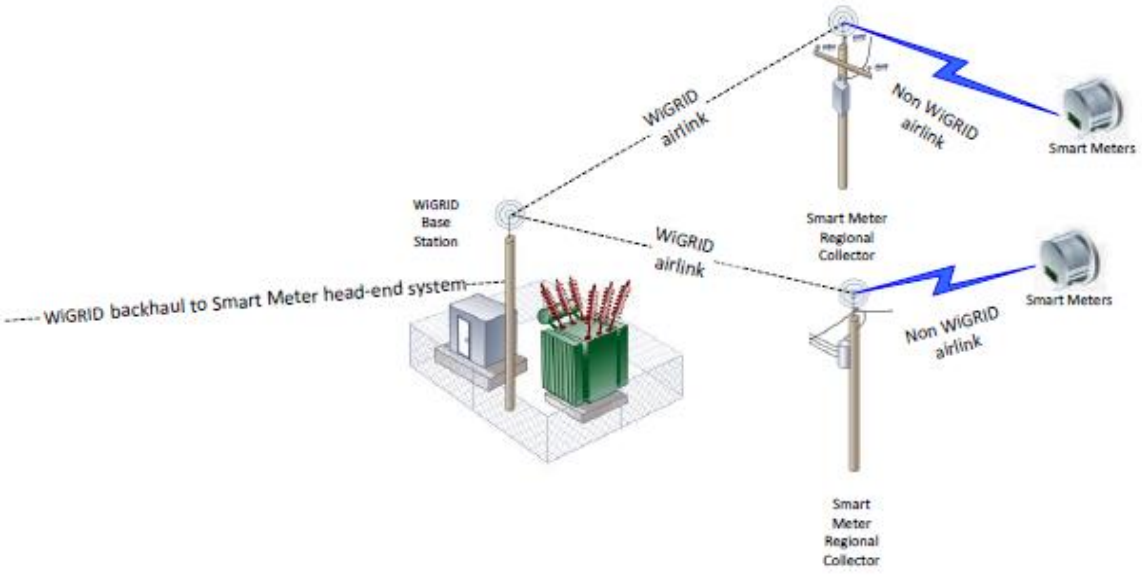
1. Παρακολούθηση δικτύου διανομής ενέργειας με την τεχνολογία WiMAX

Το δίκτυο διανομής ηλεκτρικής ενέργειας περιλαμβάνει συσκευές IED, όπου συλλέγουν δεδομένα από αισθητήρες σχετικά με το δίκτυο, όπως είναι η τάση, αστάθεια φάσης κτλ. Οι συσκευές IED έχουν την δυνατότητα με την χρήση μικροεπεξεργαστών να δίνουν εντολές σύμφωνα με τα δεδομένα που δέχονται ώστε να επιτυγχάνεται η σωστή λειτουργία του δικτύου. Επίσης, είναι απαραίτητο να επικοινωνούν με το κέντρο διαχείρισης και αυτό γίνεται προσαρμόζοντας εξοπλισμό που υποστηρίζει την τεχνολογία WiMAX, για αποστολή και λήψη δεδομένων. Από πλευράς καθυστέρησης, εξαρτάται το είδος των δεδομένων, για να πραγματοποιείται το QoS. Ειδικότερα, για δεδομένα, όπως είναι η μεταβίβαση εντολών από το κέντρο διαχείρισης προς μια συσκευή IED, οι απαιτήσεις, είναι να υπάρχει η μικρότερη δυνατή καθυστέρηση, μια και ο παράγοντας χρόνος είναι σημαντικός. Ενώ, δεδομένα που συλλέγονται μία φορά την ημέρα και αφορούν για παράδειγμα στατιστικά στοιχεία για την κατάσταση του δικτύου μια συγκεκριμένη ημέρα δεν έχουν περιορισμούς στην καθυστέρηση. Ακόμη, οι απαιτήσεις στην ρυθμό-απόδοση σχετίζονται με την λειτουργία που προορίζονται. Δεδομένα που όπως αναφέραμε, σχετικά με την κατάσταση του δικτύου, δεν απαιτούν υψηλή ρυθμό-απόδοση, μιας ο όγκος των δεδομένων είναι σχετικά μικρός(μικρότερο από 100kbits). Ενώ, από την άλλη πλευρά, η χρήση κλειστού κυκλώματος καμερών ασφαλείας για λογούς προστασίας των υποδομών του ευφυούς δικτύου ενέργειας, απαιτούν μεγάλη ρυθμό-απόδοση(τουλάχιστον 700 με 1000kbps).

2. Έλεγχος και διαχείριση του δικτύου διανομής ηλεκτρικής ενέργειας με την τεχνολογία WiMAX

Το δίκτυο διανομής ηλεκτρικής ενέργειας, περιλαμβάνει κρίσιμες στοιχεία, όπως είναι μετασχηματιστές, υποσταθμούς χαμηλής και υψηλής τάσης κτλ. Το κέντρο διαχείρισης συλλέγοντας τα δεδομένα από το δίκτυο διανομής, λαμβάνει αποφάσεις που σχετίζονται με τον φόρτο του δικτύου, την ζήτησης της ενέργειας και την κατάσταση του δικτύου. Με την χρήση του WiMAX, πάνω σε συσκευές που υπάρχουν στο δίκτυο διανομής, όπως είναι τα switch ηλεκτρικής ενέργειας, μεταβιβάζονται εντολές ώστε να εκτελέσουν συγκεκριμένες λειτουργίες, όπως είναι απομόνωση γραμμής μεταφοράς ηλεκτρισμού. Το πρότυπο IEC 61850, σχετίζεται με την προτυποποίηση της επικοινωνίας ανάμεσα σε ένα κέντρο διαχείρισης και έναν υποσταθμό. Σχετίζεται και με άλλα πρότυπά όπως είναι το Generic Object Oriented Substation Events (GOOSE) που καθορίζει τη μορφή των μνημάτων που μεταβιβάζονται προς εκτέλεση σε έναν υποσταθμό. Επίσης υποστηρίζει και την εφαρμογή του πάνω σε άλλα γνωστά πρωτοκολλά ανταλλαγής δεδομένων όπως είναι το TCP/IP. Οι απαιτήσεις στην καθυστέρηση, είναι αυστηρές διότι και εδώ απαιτείται η μικρότερη δυνατή καθυστέρηση, ωστόσο με την χρήση του WiMAX αυτό είναι εφικτό. Το αντίθετο ισχύει για την ρυθμό-απόδοση που οι απαιτήσεις δεν είναι τόσο αυστηρές, μιας και ο όγκος των δεδομένων είναι μικρός. Ωστόσο, πρέπει να αναφερθεί ότι σημαντικό ρόλο παίζει η αξιοπιστία και η διαθεσιμότητα του δικτύου, μιας και αν δεν εφαρμοσθούν κρίσιμες εντολές την κατάλληλη χρονική στιγμή, μπορεί να οδηγηθεί το δίκτυο διανομής σε προβληματική λειτουργία, ακόμη και καταστροφή του εξοπλισμού. (Forum W. , 2013)

3. Συλλογή δεδομένων των έξυπνων μετρητών από τους συλλέκτες με την τεχνολογία WiMAX



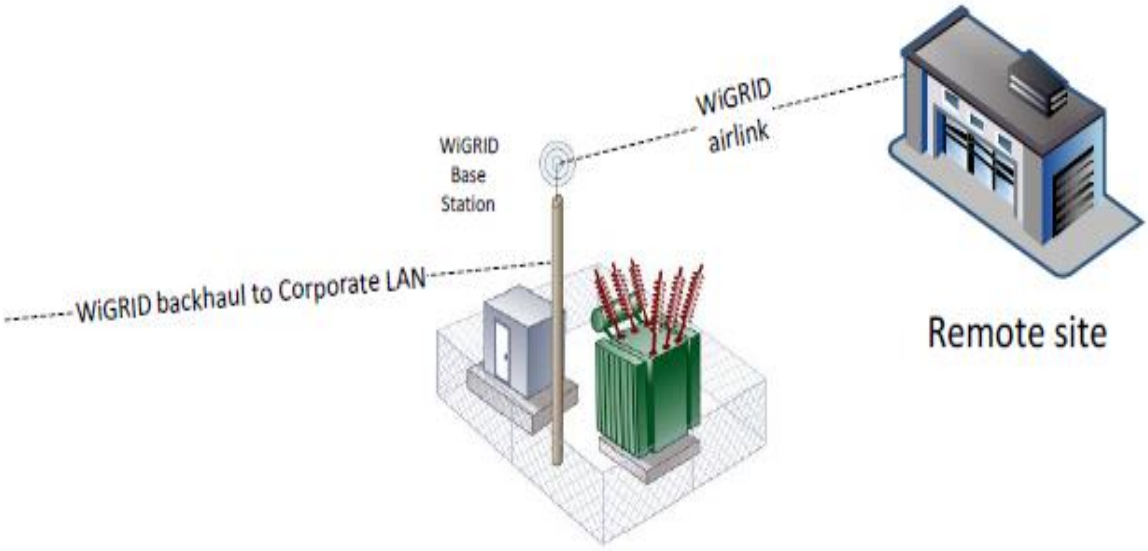
Εικόνα 22 "Επικοινωνία ανάμεσα σε υποσταθμό και συλλέκτες δεδομένων με χρήση WiMAX" (Forum W. , 2013)

Οι συλλέκτες δεδομένων (Regional collectors ή Data Aggregation Points) είναι συσκευές που σκοπό έχουν την συλλογή των δεδομένων από τους έξυπνους μετρητές και την προώθηση τους προς το NAN. Κάθε συλλέκτης έχει την δυνατότητα να επικοινωνεί με πολλούς έξυπνους μετρητές. Στο μοντέλο που παρουσιάζεται, χρησιμοποιείται το WiMAX, για την προώθηση των δεδομένων από τους έξυπνους μετρητές προς το εσωτερικό δίκτυο NAN, και κατ'επέκταση από εκεί για το WAN, και το κέντρο διαχείρισης.

Οι υποσταθμοί συνδέονται με το κέντρο διαχείρισης όπου καταλήγουν τα δεδομένα, με WiMAX. Ενώ, οι έξυπνοι μετρητές για να προωθήσουν τα δεδομένα στους συλλέκτες θα μπορούσε να γίνει με Wi-Fi με την προϋπόθεση ότι οι συλλέκτες βρίσκονται μέσα στο εύρος κάλυψης του Wi-Fi δικτύου (100 μέτρα περίπου για το 802.11b/g και 200 περίπου για το 802.11n). Τα δεδομένα συλλέγονται ανά προκαθορισμένα χρονικά διαστήματα (ανά ώρα) από τους συλλέκτες και ο μέσος ρυθμός ανά συλλογή από μετρητή είναι συνήθως 20kb/sec και σε στιγμές φόρτου 64kb/sec. Φυσικά, η συλλογή δεδομένων δεν γίνεται μόνο σε προκαθορισμένα διαστήματα, αλλά και κατάσταση ζήτησης(on demand), προς έναν συγκεκριμένο έξυπνο μετρητή, μέσω του συλλέκτη, ο όγκος των δεδομένων είναι μικρότερος από 50kb. Δεδομένο θεωρείται, ότι ο όγκος αυτός αυξάνεται όσο αυξάνεται η συλλογή από περισσότερους έξυπνους μετρητές. Οι έξυπνοι μετρητές εκτός από δεδομένα των μετρήσεων, ανταλλάσουν πληροφορίες σχετικές με την κατάσταση του δικτύου ενέργειας (διακοπές, υπερφορτώσεις) σε μια οικία, τα δεδομένα αυτά είναι πολύ μικρού μεγέθους (μικρότερα από 10kb ανά αποστολή), αλλά σε μια γενικευμένη διακοπή ηλεκτρικού ο φόρτος από τους έξυπνους μετρητές πολλαπλασιάζεται. Με την συγκέντρωση των δεδομένων αυτών στα κέντρα διαχείρισης, γίνεται αξιολόγηση της κατάστασης του δικτύου διανομής και εξετάζονται οι τρόποι με τους οποίους μπορεί να βελτιωθεί το δίκτυο διανομής ηλεκτρικής ενέργειας.

4. Επικοινωνία WAN με χρήση WiMAX

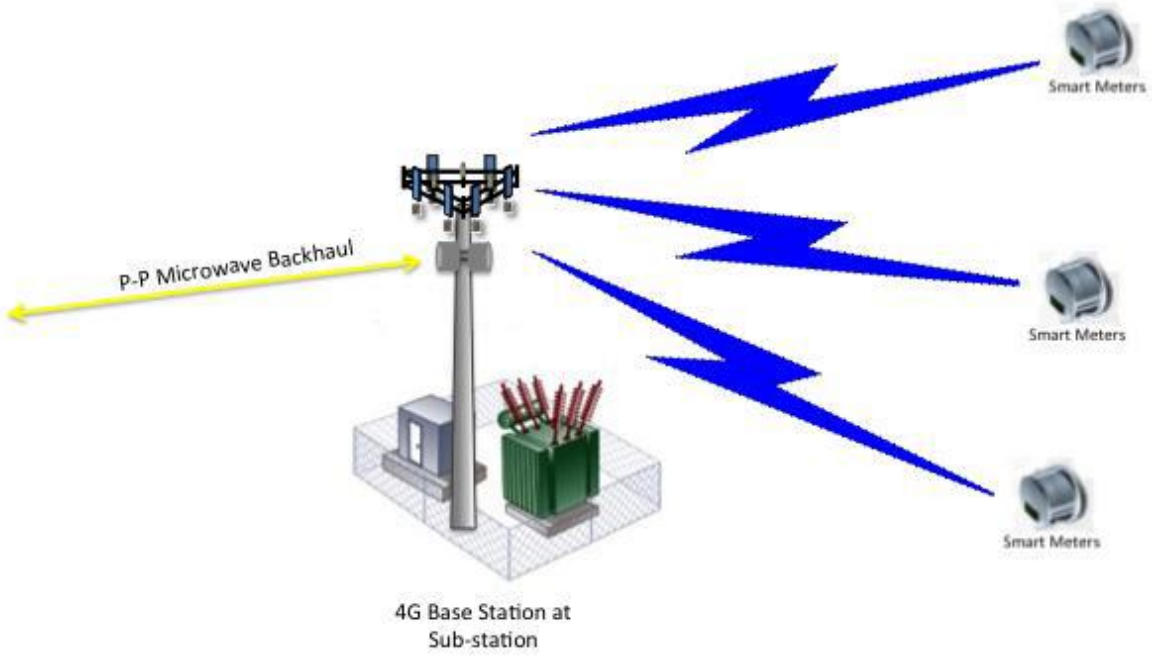
Οι υποδομές ενός ευφυούς δικτύου ενέργειας, λόγω ότι τα δίκτυα ενέργειας καλύπτουν μεγάλες γεωγραφικές περιοχές δεν μπορούν να είναι συγκεντρωμένα σε μια περιοχή. Η επικοινωνία ανάμεσα στις υποδομές που αποτελούν το WAN ενός ευφυούς δικτύου ενέργειας είναι καθοριστική για την αξιοπιστία και την λειτουργικότητα. Η υποδομή πέραν από τα κέντα διαχείρισης, αποτελείται από υποσταθμούς, γραφεία εξυπηρετήσεων, τεχνικές εγκαταστάσεις, που για την επικοινωνία μεταξύ τους η τεχνολογία WiMAX με το εύρος γεωγραφικής απόστασης που υποστηρίζει, τις μεγάλες ταχύτητες και το QoS καθίσταται ιδανική για αυτήν την περίπτωση. Σε κάθε κτηριακή υποδομή με την τοποθέτηση ενός δέκτη WiMAX, και τη εγκατάσταση στο άλλο άκρο ενός σταθμού βάσης που βρίσκεται σε περιοχή που ανήκει WAN δίκτυο, δίνεται η δυνατότητα επικοινωνίας. Ο σκοπός που εξυπηρετεί η επικοινωνία αυτή, είναι οι εσωτερικές λειτουργίες που απαιτούνται για το ευφυές δίκτυο, όπως είναι τηλεφωνία με την χρήση VoIP, email, εσωτερικό δίκτυο κτλ. (Forum W. , 2013)



Εικόνα 23 "Επικοινωνία ανάμεσα σε απομακρυσμένες υποδομές WAN" (Forum W. , 2013)

5. Άμεση επικοινωνία με έξυπνους μετρητές με χρήση WiMAX

Μία από τις κύριες απαιτήσεις για την λειτουργία ενός ευφυούς δικτύου ενέργειας είναι η σύνδεση των έξυπνων μετρητών με το κέντρο διαχείρισης. Πέρα, από τα παραπάνω σενάρια επικοινωνίας, όπου η επικοινωνία ανάμεσα σε συλλέκτες δεδομένων και έξυπνους μετρητές μπορεί να πραγματοποιηθεί και με άλλες τεχνολογίες δικτύωσης όπως είναι το 802.11, το εύρος που καλύπτει γεωγραφικά η WiMAX τεχνολογία υπερτερεί σε σχέση με το 802.11, άρα υπάρχει η δυνατότητα να δημιουργηθεί σύζευξη για ακόμα και απομακρυσμένα HAN, με την απαίτηση να υπάρχουν λιγότεροι σταθμοί βάσης για τη συγκέντρωση των δεδομένων. Τα δεδομένα που ανταλλάσσονται σχετικά με τις μετρήσεις καταναλώσεις είναι δύο ειδών, αυτά που είναι λαμβάνονται ανά προκαθορισμένα χρονικά διαστήματα και αυτά που λαμβάνονται ζωντανά(real-time) από κάθε έξυπνο μετρητή ανεξάρτητα. Τα πρώτα λαμβάνονται ανά λεπτό ή ανά ώρα από τους συλλέκτες δεδομένων που στην προκειμένη περίπτωση είναι ο σταθμός βάσης που είναι εγκατεστημένος σε υποσταθμό του ευφυούς δικτύου ενέργειας. Στο δεύτερο είδος, τα δεδομένα ζητούνται από το κέντρο διαχείρισης προς έναν συγκεκριμένο μετρητή, και αυτός απαντάει με τα δεδομένα που έχει συγκεντρώσει από το HAN. Ο όγκος των δεδομένων και στις δύο περιπτώσεις είναι μικρός, με την λεπτομέρεια ότι προφανώς στην πρώτη περίπτωση ο όγκος είναι μεγαλύτερος λόγω ότι τα δεδομένα των μετρήσεων προέρχονται από πολλούς έξυπνους μετρητές που συνδέονται στον ίδιο σταθμό βάσης.



Εικόνα 24 "Άμεση επικοινωνία έξυπνων μετρητών με σταθμό βάσης WiMAX" (Forum W. , 2013)

Εκτός από τα παραπάνω, οι έξυπνοι μετρητές έχουν την δυνατότητα να προβάλλουν μέσω οθόνης που είναι ενσωματωμένη, μηνύματα προς τους καταναλωτές για ενημέρωση τους σχετικά με το κόστος της ηλεκτρικής ενέργειας αλλά και την κατάσταση του δικτύου. Επίσης, δίνεται η δυνατότητα να αναβαθμίζεται το λογισμικό των έξυπνων μετρητών απομακρυσμένα, για την βελτίωση της υποδομής του ευφυούς δικτύου ενέργειας, με ελάχιστο κόστος. (Forum W. , 2013) (Palak P. Parikh, 2010)

Η χρήση του WiMAX στο δίκτυο επικοινωνιών ενός ευφυούς δικτύου ενέργειας, απαιτεί να ληφθεί υπόψη κατά την σχεδίαση του δικτύου επικοινωνιών. Αυτό συμβαίνει λόγω τις απαραίτητης υποδομής(σταθμοί βάσης) που πρέπει να εγκατασταθούν στο δίκτυο επικοινωνιών για να υπάρχει η δυνατότητα να λειτουργήσει ένα δίκτυο βασιζόμενο στο WiMAX. Η χρήση του όπως παρουσιάστηκε στα παραπάνω μοντέλα, καλύπτει ολόκληρο το δίκτυο επικοινωνιών ενός ευφυούς δικτύου ενέργειας, με κύριο χαρακτηριστικό το μεγάλο εύρος γεωγραφικής κάλυψης που παρέχει, τη χαμηλή καθυστέρηση και την υψηλή ταχύτητα. Συνοπτικά τα πλεονεκτήματα που παρέχει είναι: (Rossi)

1. Παρέχει επικοινωνία σε μεγάλη απόσταση από τον σταθμό βάσης
2. Ιδανικό για απομακρυσμένες περιοχές ή γεωγραφικά δύσβατες
3. Υψηλοί ρυθμοί ταχύτητας

Ενώ, τα αρνητικά είναι:

1. Όσοι περισσότεροι χρήστες συνδέονται με τον ίδιο σταθμό βάσης τόσο μειώνεται το διαθέσιμο bandwidth
2. Ανάγκη για σχεδίαση της εγκατάστασης των σταθμών βάσης για να καλύπτουν την εκάστοτε γεωγραφική περιοχή

3. Υψηλό κόστος εγκατάστασης

Εκτός από τις προτάσεις του WiMAX Forum, για την χρήση του WiMAX στα ευφυή δίκτυα ενέργειας, υπάρχουν και μελέτες ανεξάρτητων ερευνητών για την χρήση του WiMAX και την απόδοση του. Επιπλέον, το WiMAX, μπορεί να συνδυαστεί και με κάποια άλλη τεχνολογία δικτύωσης, δημιουργώντας ένα υβριδικό σύστημα. Μια πρόταση χρήσης του WiMAX μελετάται στο (Qing Wang, 2012) για την παρακολούθηση του δικτύου μεταφοράς και διανομής ενέργειας. Η μελέτη γίνεται πάνω σε πραγματικά στοιχεία με αποστάσεις που φτάνουν τα 200 χιλιόμετρα μεταξύ υποσταθμών του δικτύου ενέργειας. Η συλλογή δεδομένων από το δίκτυο μεταφοράς γίνεται με αισθητήρες που αποστέλλουν τα δεδομένα με Wi-Fi, σε μια συσκευή που λειτουργεί ως γέφυρα ανάμεσα στο Wi-Fi και το WiMAX και αναλαμβάνει την προώθηση των δεδομένων που συλλέγονται στο σταθμό βάσης WiMAX, όπου βρίσκεται στους υποσταθμούς του δικτύου. Σε περιπτώσεις, οπού οι αποστάσεις είναι πολύ μεγάλες, και απαιτείται ενίσχυση του σήματος, χρησιμοποιείται ένα σταθμός, Relay Station, ως ενδιάμεσος. Με την αρχιτεκτονική αυτή, καλύπτονται μεγάλες αποστάσεις του δικτύου μεταφοράς ηλεκτρικής ενέργειας.

Ένα άλλο υβριδικό σχήμα, παρουσιάζεται στο (Ronald Mao, 2012), για end-to end επικοινωνία στο AMI. Οι έξυπνοι μετρητές επικοινωνούν με τους συλλέκτες δεδομένων ή άμεσα με το κόμβο που επικοινωνεί με το Base Station του WiMAX δικτύου με Wi-Fi. Το ιδιαίτερο στην μελέτη αυτή, είναι ότι εστιάζει στην ανταλλαγή δεδομένων πάνω στο σχήμα αυτό και ειδικότερα σε σενάρια όπου εμφανίζεται στο δίκτυο traffic burst. Δηλαδή μια κατάσταση, όπου ταυτόχρονα πολλοί έξυπνοι μετρητές ξαφνικά αποστέλλουν δεδομένα δημιουργώντας συνθήκες μεγάλου φόρτου διακίνησης δεδομένων. Η κατάσταση αυτή περιγράφεται ως αναμενόμενη στο AMI, λόγω ότι έξυπνοι μετρητές, αποστέλλουν δεδομένα ανά συγκεκριμένα χρονικά διαστήματα, εξαιτούνται βέβαια περιπτώσεις όπου πληροφορίες έκτακτα αποστέλλονται από το κέντρο διαχείρισης με προορισμό τους έξυπνους μετρητές. Για την λύση του προβλήματος αυτού προτείνεται η εφαρμογή ενός πρωτοκόλλου με την ονομασία Time Controlled Scheduling, όπου η τεχνική του βασίζεται στο ότι οι έξυπνοι μετρητές, συνδέονται σε προκαθορισμένα διαστήματα και για συγκεκριμένο χρονικό διάστημα για την αποστολή δεδομένων. Όμως, με την τεχνική αυτή προκύπτουν δύο προβλήματα, ένα είναι ότι ο έξυπνος μετρητής πως θα έχει την δυνατότητα να επικοινωνήσει έκτακτα εκτός που προκαθορισμένου διαστήματος και δεύτερον σε περίπτωση όπου το ευφυές δίκτυο ενέργειας, θέλει να επικοινωνήσει με έναν συγκεκριμένο έξυπνο μετρητή. Για την επίλυση του δεύτερης περίπτωσης μια λύση που προτείνεται είναι το ευφυές δίκτυο ενέργειας, να αποστείλει ένα αίτημα σε έναν γειτονικό έξυπνο μετρητή που βρίσκεται συνδεμένος στο χρονικό διάστημα που έχει διαθέσιμο ώστε να το προωθήσει στον έξυπνο μετρητή, ο οποίος με την σειρά του μπορεί να στείλει ένα μήνυμα αιτώντας να λάβει τις πληροφορίες που εκκρεμούν. Για να γίνει αυτό, όμως απαιτείται οι έξυπνοι μετρητές να επικοινωνούν με τους γειτονικούς τους δημιουργώντας ένα δίκτυο αρχιτεκτονικής mesh. Εκτός από αυτή την λύση προτείνεται η δημιουργία

multicast group, όπου τα αιτήματα θα στέλνονται σε ένα σύνολο μετρητών, και μέσω των μεταξύ τους συνδέσεων οι έξυπνοι μετρητές θα προωθούν τα αιτήματα προς τον τελικό παραλήπτη. Ένας καθοριστικός παράγοντας για την χρήση του WiMAX στα ευφυή δίκτυα ενέργειας είναι η χρήση των QoS τύπων. Το WiMAX παρέχει πέντε τύπους υπηρεσιών για διαφορετικές απαιτήσεις QoS. Αυτοί είναι: (Felipe Gómez-Cuba, 2012)

1. Unsolicited Grant Service(UGS)

Έχει σχεδιασθεί για read-time επικοινωνία, το μέγεθος των πακέτων είναι σταθερό με μικρό overhead, ενώ είναι κατάλληλο για Voice over IP(VoIP).

2. Real Time Polling Service(rtPS)

Έχει σχεδιασθεί για real-time επικοινωνία, ενώ το μέγεθος των πακέτων μπορεί να είναι μεταβλητό. Όταν ο σταθμός βάσης ανιχνεύει ότι έναν σταθμός θέλει να αποστείλει δεδομένα, δεσμεύει πόρους, και επιτρέπει να αποστείλει ο σταθμός αίτημα Bandwidth Request(BR).

3. Extended Real Time Polling Service(ertPS)

Έχει σχεδιασθεί για read-time επικοινωνία με μεταβλητό ρυθμό μετάδοσης δεδομένων.

4. Non-Real Time Polling Service(nrtPS)

Έχει σχεδιασθεί για μη ζωντανή επικοινωνία, με μεταβλητό μέγεθος. Πχ για χρήση File Transfer Protocol(FTP).

5. Best Effort Service(BE)

Έχει σχεδιασθεί για επικοινωνία best effort, δηλαδή ο ρυθμός μετάδοσης δεν είναι σταθερός, ενώ δεν παρέχεται αναφορά παράδοσης των δεδομένων στο παραλήπτη.

Στο (Felipe Gómez-Cuba, 2012), μελετάται η χρήση του WiMAX στο last-mile, ενώ γίνεται μια ταξινόμηση των δεδομένων που ανταλλάσσονται ανάμεσα στο σταθμό βάσης και τους έξυπνους μετρητές. Ειδικότερα, διακρίνονται τρεις κατηγορίες με βάση τις απαιτήσεις καθυστέρησης, για αυτήν με την απαίτηση να υπάρχει η μικρότερη καθυστέρηση όπως είναι η ανταλλαγή κρίσιμων μηνυμάτων για την κατάσταση του δικτύου, επιλέγεται η υπηρεσία ertPS, ενώ για συλλογή δεδομένων όπως και για την ανταλλαγή μηνυμάτων για ενημέρωση του κόστους ενέργειας στους έξυπνους μετρητές, επιλέγεται η UGS. Επίσης, για δεδομένα που δεν απαιτείται ζωντανή επικοινωνία, όπως είναι η αποστολή ενημερώσεων λογισμικού στους έξυπνους μετρητές αλλά υπάρχει μεγάλος όγκος δεδομένων σε σχέση με τις προηγούμενες περιπτώσεις επιλέγεται η υπηρεσία BE. Αυτό συμβαίνει, γιατί με αυτό τον τρόπο υπάρχει δυνατότητα να επιτευχθεί μεγαλύτερος ρυθμός μετάδοσης δεδομένων, χωρίς να είναι κρίσιμη η αποστολή από πλευράς καθυστέρησης(delay-tolerant). Όπως έχουμε αναφέρει με βάση τα σενάρια που παρουσιάσθηκαν το WiMAX, έχει την δυνατότητα να χρησιμοποιηθεί για παρακολούθηση του δικτύου ενέργειας σχετικά με την κατάσταση του. Στην

συγκεκριμένη περίπτωση η καθυστέρηση είναι κρίσιμη, στο (Reduan H. Khan, Wide area PMU communication over a WiMAX network in the smart grid, 2012) δοκιμάζεται η χρήση του IEEE C37.118 σε συνδυασμό με το WiMAX και τις υπηρεσίες QoS που είναι οι καταλληλότερες. Πραγματοποιείται προσομοίωση όπου επιλέγεται η TDD διπλεξία, μιας και ο όγκος των δεδομένων είναι στο uplink. Οι τύποι των υπηρεσιών QoS που εξετάζονται είναι οι BE, UGS και rtPS, ενώ προκύπτει ότι οι UGS και rtPS καλύπτουν τις απαιτήσεις καθυστέρησης. Να σημειωθεί ότι όσο αυξάνονται οι συσκευές που διασυνδέονται και συλλέγουν δεδομένα αυξάνεται και οι καθυστέρηση, γιατί οι σταθμοί χρειάζονται περισσότερο χρόνο για να αποκτήσουν δικαίωμα πρόσβασης για χρήση. Συνολικά το UGS, παρουσιάζει μικρότερη καθυστέρηση σε σχέση με το rtPS ενώ το BE παρουσιάζει την χειρότερη απόδοση και δεν καλύπτει τις απαιτήσεις. Μέχρι στιγμής, στο αντικείμενο του QoS παρατηρούμε ότι η ερευνητική μελέτη είναι περιορισμένη σε προσομοιώσεις με διαφορετικές παραμέτρους και περιοχή υλοποίησης. Είναι απαραίτητο να γίνει περισσότερη διερεύνηση του QoS και των ήδη υπαρχόντων υπηρεσιών ώστε αν δεν καλύπτονται οι απαιτήσεις να γίνει σχεδίαση νέων υπηρεσιών κατάλληλων για την εφαρμογή στα ευφυή δίκτυα ενέργειας.

3.4 LONG TERM EVOLUTION

Η τεχνολογία Long Term Evolution (LTE), είναι μια κυψελοειδής τεχνολογία δικτύου και είναι διάδοχος του Universal Mobile Communication System (UMTS),και παρέχει ασύρματη δικτύωση με υψηλούς ρυθμούς μετάδοσης δεδομένων. Το πρότυπο αναπτύχθηκε από το 3rd Generation Partnership Project (3GPP) και η πρώτη του έκδοση παρουσιάστηκε το 2008 με την ονομασία “Release 8”. Τα κύρια χαρακτηριστικά αφορούν βελτιώσεις σε σχέση με τις προηγούμενες κυψελοειδής τεχνολογίες και υποστήριξη, υψηλών ρυθμών μετάδοσης δεδομένων, μέχρι 100Mbps για κατέβασμα δεδομένων από το δίκτυο σε μια συσκευή(downlink) και 50Mbps για ανέβασμα δεδομένων(uplink), από μια συσκευή προς το δίκτυο. Επίσης, παρέχει μικρή καθυστέρηση, και συγκεκριμένα μικρότερη από 100ms, ευελιξία στο εύρος ζώνης μέχρι 20MHz και συμβατότητα με παλιότερες τεχνολογίες όπως είναι το UMTS και HSPA+. Χρησιμοποιεί δυο τεχνικές διπλεξίας, την Frequency Division Duplexing (FDD) και την Time Division Duplexing (TDD). (Jason Brown, Key performance aspects of an LTE FDD based Smart Grid communications network, 2012) (3gpp)

Αναλυτικότερα τα χαρακτηριστικά της Long Term Evolution τεχνολογίας είναι:

1. Μέγιστος ρυθμός δεδομένων 100Mbps downlink
2. Μέγιστος ρυθμός δεδομένων 50Mbps uplink
3. Υποστήριξη τεχνικών FDD και TDD
4. Υποστήριξη IP
5. Υποστήριξη μεταβλητού bandwidth, 1.4, 3, 5, 10, 15, 20 MHz
6. Στο φυσικό επίπεδο υποστηρίζει την τεχνική OFDMA για downlink και SC-FDMA για uplink

7. Υποστήριξη multicast και broadcast
8. Υποστήριξη QoS

Τα παραπάνω είναι κάποια από τα κυριότερα χαρακτηριστικά της τεχνολογίας αυτής. Παρόλα αυτά, το LTE δεν σχεδιάστηκε για να καλύψει τις απαιτήσεις επικοινωνίας στα ευφυή δίκτυα ενέργειας, αλλά μέσω των χαρακτηριστικών του, όπως είναι η μικρή καθυστέρηση, η μεγάλη γεωγραφική κάλυψη με την χρήση των σταθμών βάσης, αλλά και ο υψηλός ρυθμός μετάδοσης δεδομένων το καθιστά μία από τις ανερχόμενες τεχνολογίες τέταρτης γενιάς για την κάλυψη των επικοινωνιακών αναγκών ενός ευφυούς δικτύου ενέργειας. Η εφαρμογή της τεχνολογίας LTE σε ένα ευφυές δίκτυο ενέργειας, απαιτεί σωστή σχεδίαση και μελέτη των απαιτήσεων για την κάλυψη των απαιτούμενων αναγκών. Όπως έχει αναφερθεί στο κεφάλαιο 2 σχετικά με τις απαιτήσεις του δικτύου επικοινωνιών, η καθυστέρηση παίζει σημαντικό ρόλο στον κομμάτι αυτό. Το πρότυπο το οποίο ασχολείται με το καθορισμό των απαιτήσεων της επικοινωνίας στο τμήμα των υποσταθμών, των αυτοματισμών και γενικώς του δικτύου μεταφοράς ενέργειας είναι το IEC 61850. Είναι απαραίτητο να καλυφθούν οι απαιτήσεις που ορίζονται από το πρότυπο για την σωστή λειτουργία του δικτύου επικοινωνιών.

Στο (paper, September 2013) υπολογίζεται ότι η καθυστέρηση είναι μεταξύ 30 με 40ms, για ένα δίκτυο που καλύπτει το FAN με χρήση ενός αποκλειστικού δικτύου LTE, δηλαδή ενός δικτύου αφιερωμένο στο ευφυές δίκτυο ενέργειας και όχι κοινό δίκτυο μισθωμένο από κάποιον τηλεπικοινωνιακό πάροχο. Ακολουθώντας το πρότυπο IEC 61850, η τεχνολογία LTE, καλύπτει τις απαιτήσεις των περισσότερων αυτοματισμών του δικτύου ενέργειας. Με σωστή σχεδίαση και παραμετροποίηση του δικτύου LTE μέσω τεχνικών όπως είναι το scheduling, υπάρχει η πρόβλεψη ότι στον μέλλον θα καλυφθούν οι ανάγκες και των πιο απαιτητικών ορίων των μικρότερων από 10ms που σχετίζονται με την μηνύματα που ανταλλάσσονται σχετικά με την ασφάλεια του δικτύου(P1, P2 τύποι του IEC61850). (paper, September 2013) Στο (James Weimer, 2012) παρουσιάζεται ένα μοντέλο που βασίζεται στο LTE και πραγματοποιούνται πειραματικές δοκιμές για την πρόβλεψη της καθυστέρησης που υπολογίζεται σε 15ms και 25ms για δύο σενάρια και σαν συμπέρασμα προκύπτει ότι για καθυστέρηση μικρότερη από 15ms, πρέπει να αναπτυχθούν νέοι αλγόριθμοί scheduling για τους σταθμούς βάσης ώστε να μειωθεί η καθυστέρηση. Για την εφαρμογή της τεχνολογίας LTE στους έξυπνους μετρητές, από πλευράς απαιτήσεων καλύπτονται οι απαιτήσεις τις καθυστέρησης και του ρυθμού δεδομένων, μιας και τα όρια της καθυστέρησης είναι υψηλότερα από τα όρια που απαιτούνται στους υποσταθμούς και γενικά στους αυτοματισμούς που δικτύου ενέργειας, ενώ ο όγκος των δεδομένων που ανταλλάσσονται και αφορά κυρίως τις μετρήσεις καταναλώσεις των HAN είναι μικρός. Το LTE όπως αναφέρθηκε παραπάνω, είναι κυψελοειδής τεχνολογία, έτσι, υποστηρίζει τους τρείς τύπους κυψελών(femtocells, picoshells, macrocell) για απόσταση μερικών μέτρων μέχρι αρκετών χιλιομέτρων(100χλμ). Στις χαμηλότερες συχνότητες λειτουργίας, που χρησιμοποιούνται για επαρχιακές, εκτός πόλεων περιοχές η απόσταση είναι περίπου 5 χιλιόμετρα, ενώ μέχρι τα 30 χιλιόμετρα η

απόδοση του δικτύου είναι ικανοποιητική. Στις πόλεις και στις περιαστικές περιοχές, που χρησιμοποιούνται οι υψηλότερες συχνότητες λειτουργίας(2.6 GHz για την Ευρώπη) για υψηλότερους ρυθμούς μετάδοσης δεδομένων το εύρος είναι περίπου 1 χιλιόμετρο.

Όπως αναφέραμε το LTE υποστηρίζει δύο τεχνικές διπλεξίας, την FDD και την TDD, θεωρώντας ότι η κίνηση στο δίκτυο θα είναι μεγαλύτερη από τους έξυπνους μετρητές από το ευφυές δίκτυο ενέργειας, σε ένα δίκτυο που χρησιμοποιείται η τεχνολογία LTE, ένα θέμα που προκύπτει είναι πια τεχνική είναι η καταλληλότερη. Η τεχνική FDD, ο χωρισμός του uplink και του downlink γίνεται με βάση την συχνότητα, δηλαδή απαιτούνται δύο διαφορετικά κανάλια επικοινωνίας ενώ η μετάδοση μπορεί να γίνεται ταυτόχρονα και προς τις δύο κατευθύνσεις. Στην τεχνική TDD, το uplink και το downlink μοιράζονται την ίδια συχνότητα και γίνεται διαχωρισμός σε χρόνο, δηλαδή σε time slots για την εκπομπή, οπότε δεν είναι ταυτόχρονη η αποστολή και η λήψη στις δύο κατευθύνσεις. Από την άλλη μεριά, η τεχνική TDD, έχει πλεονεκτήματα όπως είναι το φθηνότερο κόστος του υλικού εξοπλισμού και φθηνότερο κόστος χρήσης των συχνοτήτων από παρόχους, μιας δεν μένουν αδιάθετες συχνότητες, και γίνεται καλύτερη διαχείριση των διαθέσιμων συχνοτήτων.

Στο (Jason Brown, Performance analysis of an LTE TDD based smart grid communications network for uplink biased traffic, 2012) γίνεται μελέτη χρήση της τεχνολογίας LTE βασισμένη στην τεχνική TDD σύμφωνα με τις απαιτήσεις των ευφυών δικτύων ενέργειας, έμφαση δίνεται στην εφαρμογή στους έξυπνους μετρητές για συλλογή δεδομένων. Αρχικά, επισημαίνεται ότι οι απαιτήσεις των ευφυών δικτύων ενέργειας, είναι διαφορετικές από την χρήση των δικτύων LTE, μιας και η όγκος των δεδομένων αφορά την συλλογή δεδομένων από έξυπνους μετρητές δηλαδή στο uplink, και όχι στο downlink, όπως ένα κοινό δίκτυο LTE για ανάγκες κινητής τηλεπικοινωνίας. Συνεπώς, το πλεονέκτημα χρήσης της τεχνικής TDD, είναι η διανομή των πόρων του uplink και του downlink γίνεται σύμφωνα με τον όγκο των δεδομένων. Να σημειωθεί, ότι το LTE TDD, υποστηρίζει επτά διαφορετικές κατανομές για το uplink/downlink. Με βάση ότι ο κύριος όγκος των δεδομένων είναι στο uplink, προτείνεται η χρήση των κατανομών 0, 1 και 6 μιας και αυτές είναι που έχουν το μεγαλύτερο uplink. Από την άλλη μεριά, η χρήση των πιο ασύμμετρων κατανομών, μπορεί να οδηγήσει σε προβλήματα απόδοσης, γιατί σε μια σύνδεση η ανταλλαγή δεδομένων πότε δεν είναι μια κατεύθυνσης. Χαρακτηριστικό παράδειγμα, στην κατεύθυνση που έχει την μικρότερη κατανομή, δημιουργείται καθυστέρηση, μιας και εκεί μπορούν να αποστέλλονται μηνύματα επιβεβαίωσης και μέχρι να ληφθούν δημιουργείται η καθυστέρηση. Το πρόβλημα αυτό είναι αρκετά σοβαρό για την λειτουργία ενός δικτύου βασισμένο στην τεχνολογία LTE σε συνδυασμό με την τεχνική TDD, και ιδιαίτερα στα ευφυή δίκτυα ενέργειας, που όπως αναφέραμε ο φόρτος είναι το uplink. Στην ίδια μελέτη επισημαίνεται, ότι η καθυστέρηση στο uplink, εξαρτάται από το χρόνο που χρειάζεται ένα πακέτο να φτάσει στο παραλήπτη του, το οποίο εξαρτάται από χρονισμό των frame. Δηλαδή εάν ένα πακέτο έχει μπει σε buffer του uplink για

αποστολή και εκείνη την δεδομένη στιγμή, το sub-frame χρησιμοποιείται για downlink, τότε θα περιμένει μέχρι να έρθει ο κατάλληλος χρονισμός για ένα sub-frame που προορίζεται για uplink. Είναι κατανοητό, πως ο παραπάνω τρόπος λειτουργίας δημιουργεί σημαντική καθυστέρηση σε μεγάλο όγκος δεδομένων. Η λύση έρχεται να δοθεί με την ανάπτυξη μεθόδων για την υπολογισμό της καθυστέρησης που εμφανίζεται στις κατανομές 0,1, και 6. Συμπερασματικά, σύμφωνα με την προσομοίωση που πραγματοποιείται με βάση τα παραπάνω δεδομένα, προκύπτει ότι οι τρεις αυτές κατανομές είναι οι καταλληλότερες, ενώ, η κατανομή 1, έχει την μικρότερη καθυστέρηση και η 6 έχει την μεγαλύτερη. Όμως όσο αυξάνεται ο όγκος των δεδομένων, η κατανομή 1 εμφανίζει χειρότερη απόδοση από την κατανομή 0, λόγω του χρόνου που απαιτείται για την επεξεργασία των uplink sub-frames. Η ιδανική κατάσταση είναι, η αλλαγή κατανομής από την 1 στην 0, όταν αυξάνεται κατά πολύ ο όγκος των δεδομένων και ξεπεραστούν όρια τα οποία πρέπει να έχουν προκαθοριστεί. Μέχρι στιγμής η τεχνολογία LTE με την τεχνική TDD, δεν υποστηρίζει αλλαγή κατανομής δυναμικά και χρειάζεται περισσότερη ανάπτυξη στο κομμάτι αυτό. Οι ίδιοι συγγραφείς στο (Jason Brown, Performance comparison of LTE FDD and TDD based Smart Grid communications networks for uplink biased traffic, 2012) πραγματοποιούν μια σύγκριση ανάμεσα στις δύο τεχνικές, TDD και FDD, και όπως αναφέραμε η τεχνική FDD, χρησιμοποιεί δύο διαφορετικές συχνότητες, μία για το uplink και μια για το downlink. Η χαμηλότερη συχνότητα χρησιμοποιείται για το uplink, ενώ η υψηλότερη για το downlink. Οι συσκευές διαθέτουν φίλτρα για τον διαχωρισμό των μεταδόσεων uplink και downlink. Το αποτέλεσμα που προκύπτει από την σύγκριση στο συγκεκριμένο σενάριο είναι ότι η τεχνική FDD υπερτερεί, δηλαδή παρουσιάζει μικρότερη καθυστέρηση σε σχέση με την τεχνική TDD, για το συγκεκριμένο bandwidth, συχνότητες λειτουργίας και όγκο δεδομένων του σεναρίου. Αυτό προκύπτει επειδή η τεχνική TDD, από την απαίτηση να χρειάζεται να αναμένει ένα πακέτο για αποστολή στο buffer, μέχρι να έρθει το κατάλληλο sub-frame του uplink. Η τεχνική TDD όμως, δίνει μεγαλύτερη ευελιξία, ως προς τον όγκο δεδομένων κάθε χρονική στιγμή. Τέλος, το πια τεχνική υπερτερεί εξαρτάται και από παράγοντες όπως το μέγεθος των πακέτων, ως ένα σημείο για το πια θα εμφανίσει καλύτερη απόδοση σε ένα συγκεκριμένο σενάριο.

Ένα άλλο θέμα που προκύπτει από την χρήση του LTE στα ευφυή δίκτυα ενέργειας, είναι η χρήση ενός αποκλειστικού δικτύου(private LTE network) ή η χρήση ενός δικτύου με μίσθωση από κάποιον πάροχο δικτύου LTE(public LTE network). Η επιλογή του τύπου επηρεάζεται από πολλές παραμέτρους που αφορούν την χρήση του LTE. Ενδεικτικά, κάποια από τα ερωτήματα που προκύπτουν είναι, μπορεί το ευφυές δίκτυο ενέργειας, να χρησιμοποιήσει συγκεκριμένη συχνότητα λειτουργίας; Είναι αυτή διαθέσιμη; Μπορεί να λειτουργήσει κάτω από τους κανονισμούς που ισχύουν σε κάθε γεωγραφική περιοχή; Θα χρησιμοποιηθεί η τεχνολογία LTE μόνο στους έξυπνους μετρητές ή και σε μεγαλύτερο εύρος(επικοινωνία WAN, σύνδεση της υποδομής του δικτύου ενέργειας, υποσταθμοί, μονάδες παραγωγής ενέργειας); Εν συντομία, δεν

υπάρχει πάντα η δυνατότητα επιλογής, μιας και περιορισμοί για την χρήση συχνοτήτων σχετίζονται με την περιοχή που προτίθεται να χρησιμοποιηθεί η τεχνολογία LTE. Από την άλλη, υπάρχει η δυνατότητα χρήσης, ενός private virtual network σε ένα κοινό δίκτυο LTE(public network), ξεχωρίζοντας τα δεδομένα που ανταλλάσσονται στο δίκτυο, αυτά που αφορούν το ευφυές δίκτυο ενέργειας, από υπόλοιπα δεδομένα του δικτύου LTE. Ένα private LTE δίκτυο που λειτουργεί και βρίσκεται σε δοκιμαστικό στάδιο είναι της Αυστραλέζικης εταιρίας παροχής ηλεκτρικής ενέργειας AusGrid. Αρχικά το 2009, η AusGrid επένδυσε στην δημιουργία ενός δικτύου βασιζόμενου στην τεχνολογία WiMAX, για την κάλυψη των WAN και NAN του δικτύου της και το 2011 έκανε στροφή και σε συνεργασία με την Ericsson υλοποιήθηκε ένα δίκτυο τεχνολογίας LTE που συλλέγει δεδομένα από 12000 έξυπνους μετρητές. (Ericsson). Στην περίπτωση χρήσης ενός κοινού δικτύου(public network) ενός τηλεπικοινωνιακού παρόχου για το δίκτυο επικοινωνιών ενός ευφυούς δικτύου ενέργειας, υπάρχουν διαφορές όπως είναι η γεωγραφική κάλυψη που παρέχει που είναι μεγαλύτερη λόγω ήδη εγκατεστημένου δικτύου LTE που εξυπηρετεί κυρίως ανάγκες κινητής τηλεφωνίας. Όμως μπορεί να δημιουργηθούν και ζητήματα που αφορούν την ασφάλεια των δεδομένων μιας και το δίκτυο LTE δεν ανήκει και δεν το διαχειρίζεται το ευφυές δίκτυο ενέργειας, με αποτέλεσμα να υπάρχει η περίπτωση διαρροής δεδομένων. Η παραπάνω περίπτωση υπάρχει η δυνατότητα να περιοριστεί με χρήση vpn δικτύων που βασίζονται στο δίκτυο LTE, έτσι τα δεδομένα που ανήκουν σε ένα ευφυές δίκτυο ενέργειας, δεν συγκεντρώνονται μαζί με δεδομένα που καλύπτουν άλλες ανάγκες(κινητής τηλεφωνίας). Από την άλλη μεριά το κόστος χρήσης ενός έτοιμου δικτύου LTE θεωρείται μεγάλο, λόγω εκτεταμένης χρήσης του δικτύου, οπότε χρειάζεται ανάλυση κόστους ώστε να αποφασισθεί ποια περίπτωση χρήση θα προτιμηθεί. Η επιλογή, επηρεάζεται από πολλούς παράγοντες, όπως είναι η γεωγραφική περιοχή, ο αριθμός των συνδρομητών που εξυπηρετούνται, ο όγκος των δεδομένων που ανταλλάσσονται, τα ελάχιστα χαρακτηριστικά του δικτύου που απαιτούνται(bandwidth, καθυστέρηση κτλ) ώστε να προσδιοριστεί το συνολικό κόστος χρήσης του δικτύου LTE. (Ericsson)

Να αναφερθεί ότι στα ευφυή δίκτυα ενέργειας γίνονται προσπάθειες εφαρμογής της τεχνολογίας LTE βασιζόμενη στην έκδοση 8(Release 8), στο μέλλον με την υλοποίηση της τελευταίας έκδοσης της τεχνολογίας LTE-Advances που τελειοποιήθηκε το Μάρτιου του 2011 και προσφέρει μέχρι 1Gbps download , 500Mbps upload, και καθυστέρηση κάτω από 5ms, υπερκαλύπτονται ακόμα και οι απαιτήσεις καθυστέρησης κάτω των 10ms που θεωρούνται κρίσιμες για την λειτουργία του ευφυές δικτύου ενέργειας. Ακόμη, στην πραγματικότητα επικοινωνίες τέταρτης γενιάς(4G), θεωρούνται η LTE-Advanced και η τεχνολογία 802.16m ή WirelessMan-Advanced που σπάνε το φράγμα του 1Gbps για download δεδομένων.

3.5 ΚΥΨΕΛΟΕΙΔΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΕΥΤΕΡΗΣ ΚΑΙ ΤΡΙΤΗΣ ΓΕΝΙΑΣ

Οι κυψελοειδείς επικοινωνίες δεν είναι μια πρόσφατη ασύρματη τεχνολογία, ήδη χρησιμοποιούνται αρκετά χρόνια στην κινητή τηλεφωνία και από την δεύτερη γενιά τους υποστηρίζουν ανταλλαγή δεδομένων. Αρχικά, στην δεύτερη γενιά με την χρήση του General Packet Radio Service(GPRS),ενός πρωτοκόλλου μεταφοράς πακέτων με ταχύτητα από 56 μέχρι 114Kbps. Με την εξέλιξη των κυψελωτών δικτύων και την ανάγκη ανταλλαγής μεγαλύτερου όγκου δεδομένων σχεδιάστηκαν τεχνολογίες και πρότυπα που ανήκουν στην τρίτη γενιά κυψελωτών δικτύων υποστηρίζοντας ταχύτητες μεγαλύτερες από 200Kbps. Η χρήση των κυψελωτών επικοινωνιών μπορούν να χρησιμοποιηθούν για την κάλυψη των απαιτήσεων στα δίκτυα επικοινωνίας σύμφωνα με την χαρακτηριστικά που προσφέρει η κάθε τεχνολογία. Τα πλεονεκτήματα χρήσης των κυψελωτών τεχνολογιών δεύτερης και τρίτης γενιάς είναι: (Qualcomm, 2012)

1. Υψηλή αξιοπιστία

Τα σημερινά κυψελωτά δίκτυα δεύτερης και τρίτης γενιάς προσφέρουν υψηλή αξιοπιστία και συγκεκριμένα διαθεσιμότητα δικτύου μεγαλύτερη από 99%. Βρίσκονται σε χρήση αρκετά χρόνια και οι πάροχοι έχουν δοκιμάσει και βελτιώσει την ποιότητα των υπηρεσιών.

2. Μεγάλη γεωγραφική κάλυψη

Τα κυψελωτά δίκτυα δεύτερης και τρίτης γενιάς καλύπτουν τις μεγαλύτερες περιοχές σε όλες τις χώρες από οποιοδήποτε άλλο δίκτυο με την χρήση τους στην κινητή τηλεφωνία.

3. Ασφάλεια

Παρέχουν ασφάλεια με χρήση κρυπτογράφησης των δεδομένων που ανταλλάσσονται και αυθεντικοποίησης. Ακόμη, μπορούν να εφαρμοσθούν πρόσθετές τεχνικές για βελτιστοποίηση της ασφάλειας των δεδομένων.

4. Μεγάλη επεκτασιμότητα

Κάθε κυψέλη με τον σταθμό βάσης της μπορεί να υποστηρίξει πολλές συσκευές ταυτόχρονα και σε περίπτωση που αυτές αυξηθούν μπορεί να τοποθετηθεί νέος σταθμός βάσης.

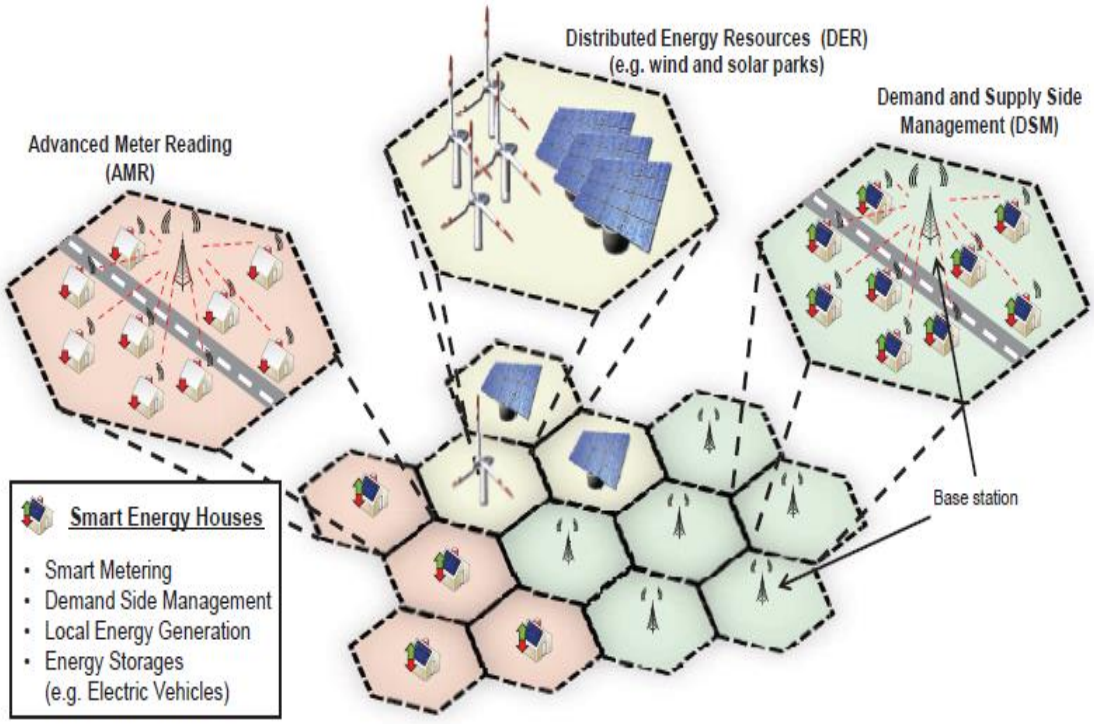
5. Διαλειτουργικότητα

Οι κυψελωτές τεχνολογίες χρησιμοποιούνται σε όλο τον κόσμο, με την χρήση τους διασφαλίζεται η συμβατότητα ανάμεσα σε συσκευές, όπως είναι οι έξυπνοι μετρητές και ανάμεσα σε διαφορετικά ευφυή δίκτυα ενέργειας.

Το Global System for Mobile(GSM) είναι το πιο γνωστό δίκτυο κυψελών σε όλο τον κόσμο, λειτουργεί σε συχνότητες 900MHz και 1800MHz με ρυθμό μετάδοσης δεδομένων μέχρι 270Kbps. Αποτελείται από τέσσερα βασικά τμήματα: Mobile handset, Base Station Subsystem, Network Switching Substation και Operation Support Substation. (Ahmad Usman, 2013)

Το GPRS είναι ένα πρωτόκολλο μεταφοράς δεδομένων με την μορφή πακέτων με την τεχνική circuit switched πάνω σε GSM δίκτυα. Με αυτό τον τρόπο υπάρχει η δυνατότητα, να χρησιμοποιηθούν εφαρμογές βασιζόμενες στο IP και με ρυθμό μετάδοσης δεδομένων μεγαλύτερο από το GSM. Στα ευφυή δίκτυα ενέργειας, χρησιμοποιείται συνήθως για απομακρυσμένη παρακολούθηση και καταγραφή. Ένα τέτοιο σύστημα απομακρυσμένης παρακολούθησης υποσταθμών με την χρήση του GPRS παρουσιάζεται στο (Lee P, 2007). Το GPRS μπορεί να έχει εφαρμογή και σε ένα HAN δίκτυο για απομακρυσμένη παρακολούθηση και καταγραφή μέσω του έξυπνου μετρητή και με την τοποθέτηση κάρτας Subscriber Identity Module(SIM). Με αυτόν τον τρόπο ο καταναλωτής μπορεί να λαμβάνει πληροφορίες για την λειτουργία του δικτύου HAN ακόμη και με Short Message Service(SMS). (Wasi-ur-Rahman, 2009) Από την άλλη μεριά υπάρχουν θέματα όπως η ταχύτητα που είναι χαμηλή για την υποστήριξη των επικοινωνιών ενός WAN αλλά και η καθυστέρηση.

Για την υποστήριξη QoS στο GRPS είναι απαραίτητο να πραγματοποιηθεί δέσμευση καναλιών από τα συνολικά κανάλια που είναι διαθέσιμα προς χρήση. Αυτό έχει ως αποτέλεσμα να μειωθεί η χωρητικότητα του δικτύου σε κίνηση και έχει αρνητική επίδραση στην απόδοση του δικτύου. Συνεπώς η χρήση του GPRS περιορίζεται για συγκεκριμένους σκοπούς απομακρυσμένης παρακολούθησης, και σε σημεία όπου δεν απαιτείται χαμηλή καθυστέρηση ή ο όγκος των δεδομένων που ανταλλάσσονται δεν είναι μεγάλος. Οπότε, η χρήση του GRPS για την εξολοκλήρου επικοινωνία σε WAN δεν είναι εφικτή. (Ahmad Usman, 2013)



Εικόνα 25 Κυψελοειδές δίκτυο σε ευφυή δίκτυο ενέργειας" (Christian Muller, 2012)

Το GSM μαζί με το GPRS θεωρούνται η δεύτερη γενιά κυψελωτών δικτύων. Η εξέλιξη των δικτύων αυτών θεωρούνται τα δίκτυα τρίτης γενιάς, όπου υποστηρίζουν μεγαλύτερο ρυθμό μετάδοσης δεδομένων με καλύτερα χαρακτηριστικά δικτύου. Τα δίκτυα τρίτης γενιάς έχουν ορισθεί από το International Mobile Telecommunications 2000(IMT 2000) του οργανισμού International Telecommunication Union(ITU). Ο οργανισμός 3GPP καθορίζει όμως τα τεχνικά χαρακτηριστικά και την πορεία εξέλιξης των τεχνολογιών τρίτης γενιάς. Οι συχνότητες λειτουργίας ενός 3G δικτύου είναι από 1.92-1.98MHz και 2.11-2.17(Licensed). (Piyush Ghune, 2013) Ενώ η ταχύτητα είναι από 384Kbps μέχρι 2Mbps, και σε συνδυασμό με το High Speed Data Packet Access(HSDPA) οι ταχύτητες φτάνουν τα 22Mbps, η απόσταση επικοινωνίας από τον σταθμό βάσης φτάνει από 1 έως 10 χιλιόμετρα. Στο (Qualcomm, 2012) η καθυστέρηση υπολογίζεται σε μικρότερη από 1 δευτερόλεπτο, από τις απαιτήσεις όμως της καθυστέρησης ενός ευφυούς δικτύου ενέργειας που είναι στην τάξη των μερικών ms, είναι κατανοητό πως η 3G τεχνολογία δεν μπορεί να χρησιμοποιηθεί αποκλειστικά για την υποστήριξη του δικτύου ενός ευφυούς δικτύου ενέργειας. Σύμφωνα με το IEC 61850 οι απαιτήσεις των αυτοματισμών των υποσταθμών του δικτύου ενέργεια απαιτούν καθυστέρηση μικρότερη από 20ms, και τα αυστηρότερα όρια θέτονται ακόμα και κάτω από 10ms. Από την άλλη μεριά, η 3G τεχνολογία μπορεί να έχει εφαρμογές στα ευφυή δίκτυα ενέργειας σε σημεία που δεν απαιτείται τόσο μικρή καθυστέρηση, όπως είναι η συλλογή δεδομένων από έξυπνους μετρητές, αλλά και για απομακρυσμένη παρακολούθηση του δικτύου και συλλογή πληροφοριών, μονάδες παραγωγής ενέργειας, ανανεώσιμες πηγές. Επίσης με την χρήση ήδη υπαρχόντων δικτύων 3G και μίσθωση τους από άλλους παρόχους το κόστος της υποδομής μεταβιβάζεται από το ευφυή δίκτυο ενέργειας, και αναλαμβάνει μόνο το κόστος χρήσης της υποδομής του δικτύου 3G.

3.6 WIRELESS MESH

Ένα ασύρματο δίκτυο mesh, είναι το δίκτυο εκείνο που η σύνδεση των κόμβων βασίζεται στην τοπολογία mesh. Με τον όρο multi-hop χαρακτηρίζονται τα δίκτυα εκείνα που για την επικοινωνία ανάμεσα σε δύο κόμβους, τα δεδομένα διέρχονται από ενδιάμεσους κόμβους που τα προωθούν προς τον παραλήπτη. Κάθε κόμβος που λειτουργεί σε κατάσταση relay, προωθεί τα δικά του δεδομένα μαζί με τα δεδομένα που έχει λάβει. Η εφαρμογή των ασύρματων mesh δικτύων, προσφέρει πολλά πλεονεκτήματα στα ευφυή δίκτυα ενέργειας και έχουν υπάρξει πολλές προτάσεις για την εφαρμογή τους στο HAN και NAN κυρίως. Ακόμη, θεωρούνται ιδανική λύση για την επικοινωνία στο NAN στο κομμάτι του ‘’last mile’’ και την συλλογή δεδομένων από έξυπνους μετρητές. Ένα multi-hop ασύρματο δίκτυο, παρέχει πολλαπλά μονοπάτια επικοινωνίας ανάμεσα σε δύο κόμβους ενός δικτύου mesh. Αυτό ελαχιστοποιεί την πιθανότητα αποτυχίας μιας σύνδεσης ανάμεσα σε δύο κόμβους και μειώνει κατά πολύ την περίπτωση δημιουργίας bottleneck στις ενεργές συνδέσεις. Με αυτόν τον τρόπο, αυξάνεται η αξιοπιστία του δικτύου σε συνδυασμό με τις ασύρματες τεχνολογίες που χρησιμοποιούνται

στο mesh δίκτυο. Ακόμη, με την χρήση πολλαπλών μονοπατιών επιτυγχάνεται καλύτερη ισορροπία στην κίνηση των δεδομένων στο δίκτυο μειώνοντας τον φόρτο που έχουν να διαχειριστούν συσκευές που συγκεντρώνουν δεδομένα σε περίπτωση μιας point to point σύνδεσης. Η υλοποίηση ενός mesh δικτύου μπορεί να γίνει με διάφορες τεχνολογίες ασύρματης δικτύωσης όπως είναι, το IEEE 802.11s, το IEEE 802.16j, το IEEE 802.15. (Emilio Ancillotti, 2013). Ένα από τα κρίσιμα τμήματα του δικτύου που απαιτούν αξιοπιστία είναι το τμήμα εκείνο που χαρακτηρίζεται από τον όρο “last mile”, και αφορά την επικοινωνία ανάμεσα σε έναν έξυπνο μετρητή και το σημείο(συσκευή) που συγκεντρώνονται τα δεδομένα από τα HAN και από εκεί προωθούνται στο WAN του ευφυούς δικτύου ενέργειας. Η αξιοπιστία στην επικοινωνία είναι βασικό χαρακτηριστικό που απαιτείται λόγω, ότι σε περίπτωση αποτυχίας δημιουργούνται σοβαρά προβλήματα στην λειτουργία του δικτύου επικοινωνιών. (Arabyat, 2013) Επιπλέον, τα κύρια χαρακτηριστικά από την υλοποίηση ενός δικτύου mesh για τις ανάγκες της “last-mile” επικοινωνίας είναι:

1. Χαμηλό κόστος διαχείρισης και συντήρησης

Τα mesh δίκτυα χαρακτηρίζονται από τον όρο “self-organizing” και δεν απαιτούν χειροκίνητες ρυθμίσεις στην δρομολόγηση του δικτύου, στην διευθυνσιοδότηση και στα κανάλια επικοινωνίας. Είναι εύκολη η διαχείριση χιλιάδων συσκευών του δικτύου με το ελάχιστον κόστος.

2. Υψηλή αξιοπιστία

Οι μηχανισμοί και τα πρωτόκολλα δρομολόγησης παρέχουν δευτερεύοντα μονοπάτια επικοινωνίας ανάμεσα στον αποστολέα και στον παραλήπτη του ασύρματου mesh δικτύου. Η αξιοπιστία αυξάνεται κατά μεγάλο βαθμό με την μείωση της πιθανότητας αποτυχίας επικοινωνίας σε σχέση με μια “point to point” σύνδεση.

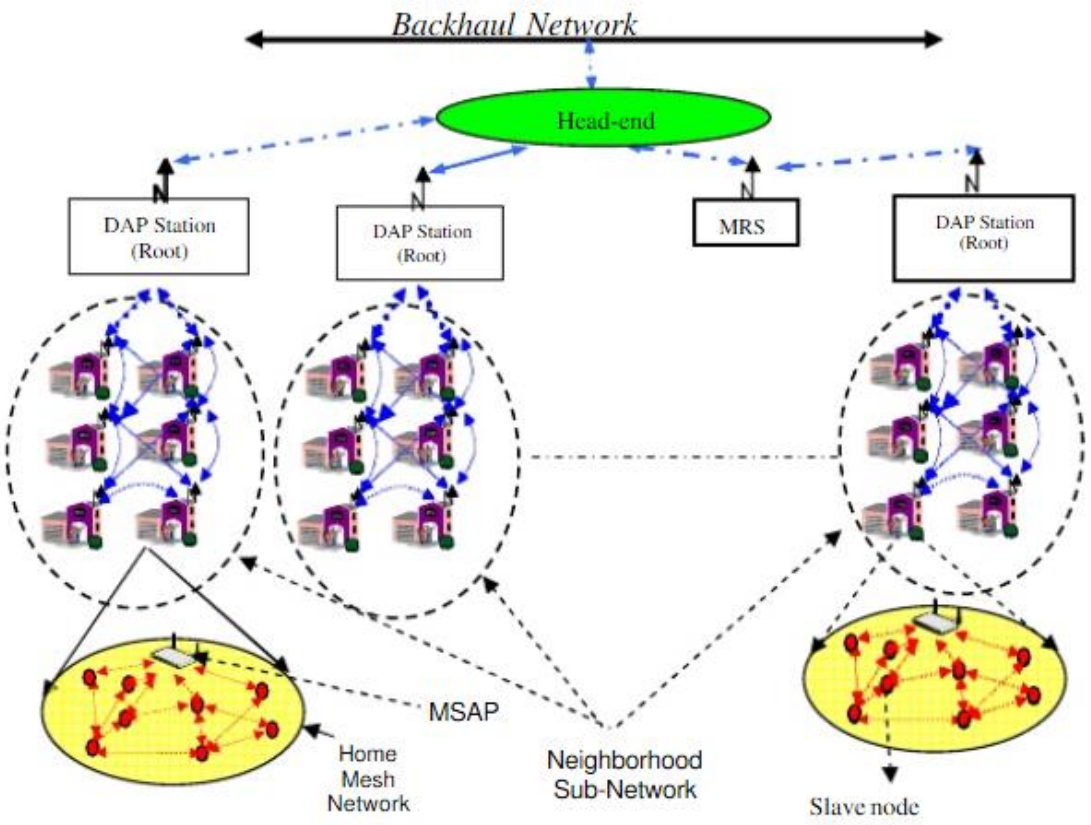
3. Επεκτασιμότητα και ευελιξία

Τα mesh δίκτυα χαρακτηρίζονται από τον όρο “self-organizing”. Οι κόμβοι που στην προκειμένη περίπτωση είναι οι έξυπνοι μετρητές και οι πύλες(gateways) που είναι οι συλλέκτες δεδομένων(data concentrators) διαθέτουν ευελιξία στις συνδέσεις. Μπορεί να προστεθεί μεγάλος αριθμός έξυπνων μετρητών και συλλεκτών δεδομένων και υποστηρίζεται μεγάλος αριθμός έξυπνων μετρητών ανά συλλέκτη δεδομένων.

4. Υψηλή ασφάλεια

Η επικοινωνία ανάμεσα στους έξυπνους μετρητές και τους συλλέκτες χαρακτηρίζεται από αυθεντικοποίηση των έξυπνων μετρητών αλλά και κρυπτογράφηση των δεδομένων με χρήση του αλγόριθμου AES. Με αυτόν τον τρόπο, παρέχεται αυθεντικοποίηση αλλά και εμπιστευτικότητα και ακεραιότητα των δεδομένων που ανταλλάσσονται. (Philip Huu Huynh, 2013)

Στο (Hamid Gharavi, Multigate Communication Network for Smart Grid , 2011) παρουσιάζεται μια τοπολογία δικτύου mesh υλοποιημένη με το 802.11s. Ως πύλη δικτύου για το HAN είναι οι έξυπνοι μετρητές που είναι εγκατεστημένοι σε κάθε οικία που επικοινωνούν με συλλέκτες δεδομένων(Data Aggregation Point στην εικόνα) που βρίσκονται σε σημεία που ανήκουν στο δίκτυο διανομής ηλεκτρικής ενέργειας(όπως είναι οι πυλώνες μεταφοράς ηλεκτρισμού). Επίσης να αναφερθεί ότι οι έξυπνοι μετρητές λειτουργούν ως δρομολογητές για να μπορούν να λειτουργήσουν σωστά και να προωθούν τα δεδομένα που αποστέλλουν και λαμβάνουν. Η ομάδα σχεδίασης και ανάπτυξης του 802.11s επέκτεινε τις τεχνικές multi-hop για να καθορίσει τις ίδιες λειτουργίες για την διασύνδεση συσκευών που λειτουργούν με το 802.11. Ακόμη, ένα σημαντικό χαρακτηριστικό του 802.11s είναι υποστηρίζει προώθηση frame και επιλογή μονοπατιού στο δεύτερο επίπεδο του OSI(media access control layer), εκτός από το τρίτο(network layer). Ειδικότερα, τα πρωτόκολλα δρομολόγησης χρησιμοποιούν την MAC διεύθυνση και υποστηρίζουν unicast, multicast αλλά και broadcast παράδοση δεδομένων. Επίσης, έχει συμβατότητα με πρωτόκολλα υψηλότερου επιπέδου και η υλοποίηση του βασίζεται στο ίδιο φυσικό επίπεδο με το 802.11. Το προεπιλεγμένο πρωτόκολλο δρομολόγησης του 802.11s είναι το Hybrid Wireless Mesh Protocol (HWMP).



Εικόνα 26 "Αρχιτεκτονική mesh για last-mile επικοινωνία" (Hamid Gharavi, Multigate Communication Network for Smart Grid , 2011)

Στην παραπάνω αρχιτεκτονική υπάρχουν τέσσερα είδη κόμβων:

1. Mesh Relay Station(MRS)

Αναλαμβάνει να προωθεί τα δεδομένα που λαμβάνει προς το ευφυές δίκτυο

2. Mesh Station Access Point

Είναι ο έξυπνος μετρητής που λειτουργεί ως πύλη δικτύου για το HAN. Προωθεί τα δεδομένα που λαμβάνει προς το DAP που είναι συνδεμένος. Στην εικόνα παραπάνω, οι συσκευές που είναι σε slave mode είναι οι συσκευές που είναι εγκατεστημένες μέσα στο HAN.

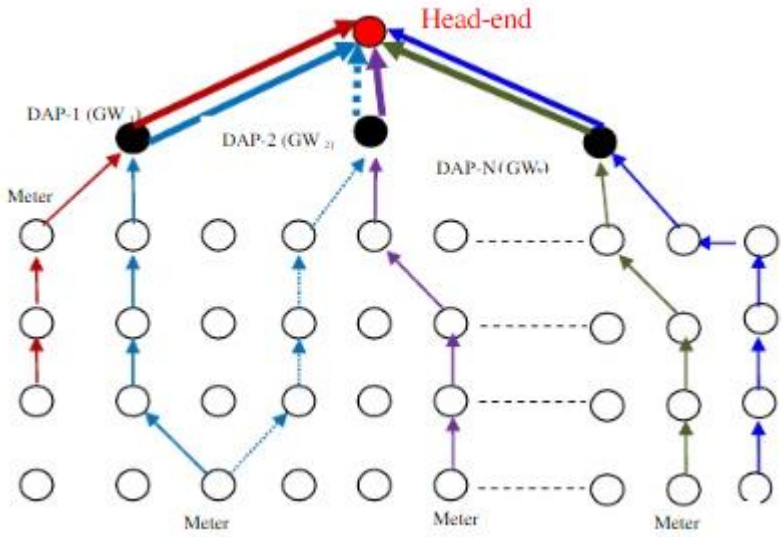
3. DAP Station

Λειτουργεί ως πύλη δικτύου για τους έξυπνους μετρητές που είναι συνδεμένοι πάνω του. Είναι ο root κόμβος που δέντρου που δημιουργείται.

4. Master Gateway Station

Είναι συνδεμένο με το δίκτυο κορμού και είναι το σημείο που συγκεντρώνονται τα δεδομένα από τους έξυπνους μετρητές.

Ο DAP περιοδικά στέλνει μηνύματα δηλώνοντας ότι είναι ο root του δέντρου, όταν ένας έξυπνος μετρητής λάβει το μήνυμα αποθηκεύει την MAC address του DAP και πριν προωθήσει το μήνυμα σε κάποιον άλλον έξυπνο μετρητή(broadcast) που είναι συνδεμένος περιμένει ένα συγκεκριμένο χρονικό διάστημα μήπως ληφθεί κάποιο άλλο μήνυμα δήλωσης. Όταν λήξει το χρονικό όριο ο έξυπνος μετρητής γνωρίζει την MAC address του DAP και μπορεί να στείλει ένα μήνυμα Path Request(PREQ) μέσα από τον κόμβο (έξυπνο μετρητή) που θεωρείται ως parent. Το PREQ χρησιμοποιείται για την επαλήθευση του μονοπατιού μέσου του parent προς το DAP. Ο DAP απαντάει με unicast ένα Path Replay(PREP) στον έξυπνο μετρητή. Η διαδικασία που οι έξυπνοι μετρητές μαθαίνουν την διεύθυνση και το μονοπάτι προς το DAP είναι σημαντική για το χαρακτηρισμό που έχει δοθεί στο mesh δίκτυο self-organization και self-healing, που σε περίπτωση δυσλειτουργίας ενός έξυπνου μετρητή, με την διαδικασία παραπάνω μπορεί να ενημερωθεί ο πίνακας δρομολόγησης όλων των έξυπνων μετρητών ώστε να παρακαμφθεί το προβληματικός έξυπνος μετρητής. Ανάμεσα στα πρωτόκολλα δρομολόγησης αυτά που είναι περισσότερο δοκιμασμένα και γνωστά είναι το Ad-hoc On Demand Distance Vector(AODV) και το Dynamic Source Routing(DSR). Οι διαφορές τους μεταξύ τους είναι ότι κάθε πακέτο DSR περιέχει όλες τις διευθύνσεις IP των κόμβων του μονοπατιού ανάμεσα στον αποστολέα και στο παραλήπτη. Σε αντίθεση με το AODV που περιέχει μόνο την διεύθυνση του παραλήπτη. Είναι φανερό, ότι σε ένα μεγάλο mesh δίκτυο, που ανάμεσα στον αποστολέα και στον παραλήπτη υπάρχουν πολλά hops, το DSR αυξάνει κατά πολύ το επιπλέον φόρτο(overhead).



Εικόνα 27 "Mesh αρχιτεκτονική με N αριθμό DAP" (Hamid Gharavi, Multigate Mesh Routing for Smart Grid Last Mile, 2011)

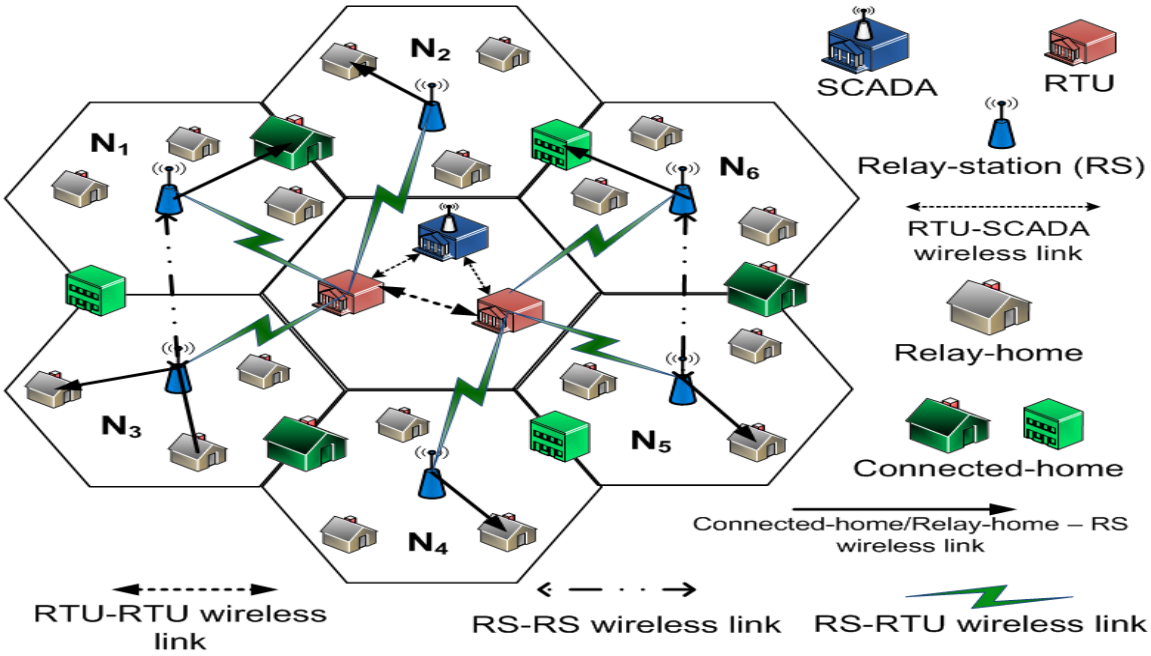
Στην αρχιτεκτονική που παρουσιάστηκε υπάρχει ένα σοβαρό μειονέκτημα ως προς την λειτουργία του mesh δικτύου. Κάθε DAP λειτουργεί ως πύλη δικτύου για τους έξυπνους μετρητές, που βρίσκονται στο δέντρο κάτω από αυτόν. Σε περίπτωση που ένας DAP εξυπηρετεί πολλούς έξυπνους μετρητές ενδέχεται να παρουσιαστεί συμφόρηση στο DAP λόγου του όγκου των δεδομένων ενώ σε ενδεχόμενη δυσλειτουργία του οι έξυπνοι μετρητές αποκόπτονται από το υπόλοιπο δίκτυο. Την ίδια στιγμή, ένας άλλος διπλανός DAP ενδέχεται να μην έχει τόσο μεγάλο φόρτο. Οπότε, οι ιδανικές συνθήκες θα ήταν να μπορούν οι έξυπνοι μετρητές να επικοινωνούν και με τους άλλους DAP του δικτύου δημιουργώντας μονοπάτια για την δρομολόγηση των δεδομένων τους. Το παραπάνω απαιτεί η δρομολόγηση με τέτοιον τρόπο ώστε να μπορούν οι μετρητές σύμφωνα με τα root announcements που λαμβάνουν να επιλέγουν το καλύτερο μονοπάτι για κάθε DAP. Στο (Hamid Gharavi, Multigate Mesh Routing for Smart Grid Last Mile, 2011) παρουσιάζεται η λύση στον πρόβλημα της δρομολόγησης σε αυτό το mesh δίκτυο.

Κάθε DAP στέλνει με broadcast μηνύματα με την διεύθυνση του ώστε να κατασκευαστεί το δέντρο από κάθε έξυπνο μετρητή. Όταν ένας έξυπνος μετρητής λάβει το μήνυμα αυτό, ελέγχει το πίνακά του για να δει ένα υπάρχει κάποιο δέντρο με το ίδιο root(DAP). Εάν δεν υπάρχει, τότε δημιουργεί ένα δέντρο με τις πληροφορίες(root και parent κόμβος) που έχει λάβει από τον root(DAP) και αποθηκεύεται στον πίνακα του. Σε περίπτωση που υπάρχει δέντρο με το ίδιο (root)DAP, τότε ενημερώνει το δέντρο αν υπάρχει κάποιος DAP με καλύτερο μονοπάτι ή νεότερος. Σε αντίθετη περίπτωση, τότε οι πληροφορίες απορρίπτονται.

Η δρομολόγηση στην αρχιτεκτονική αυτή περιγράφεται ως multigate routing, και ως στόχο έχει κάθε έξυπνος μετρητής να έχει ευελιξία στην δρομολόγηση για την επιλογή του καλύτερου μονοπατιού μέσω των γειτονικών κόμβων για κάθε DAP. Και εναλλακτικά μονοπάτια σε περίπτωση που χρειασθούν. Η δρομολόγηση αυτή

όμως έχει και αρνητικά σημεία και ειδικότερα το ότι επειδή τα root announcements από τα DAP γίνονται broadcast στο mesh δίκτυο, υπάρχει αυξημένος όγκος δεδομένων στο δίκτυο. Στο (Tadashige Iwao, Dynamic Data Forwarding in Wireless Mesh, 2010) παρουσιάζεται ένα άλλο τύπος δρομολόγησης το Distributed Autonomous Depth-First Routing(DADR) που δεν χρησιμοποιεί μηνύματα ενημέρωσης των κόμβων για την δημιουργία των μονοπατιών άλλα, ο πίνακας δρομολόγησης ενημερώνεται βασιζόμενος στην προώθηση των δεδομένων κατά την διαδικασία του αρχικής επικοινωνίας ανάμεσα σε γειτονικούς κόμβους(Hello message). Σε περίπτωση που ένα μονοπάτι δεν είναι προσβάσιμο, χρησιμοποιείται ένα μηχανισμός που παρέχει τα διαθέσιμα μονοπάτια προς κάθε προορισμό και βασίζεται στον πίνακα δρομολόγησης και στον αλγόριθμο Depth First Search. Για την ανίχνευση και αποφυγή δημιουργίας loop σε κάθε frame προστίθεται ένα μοναδικό αναγνωριστικό που ονομάζεται Unique Frame Id(FID). (Nico Saputro, 2012).

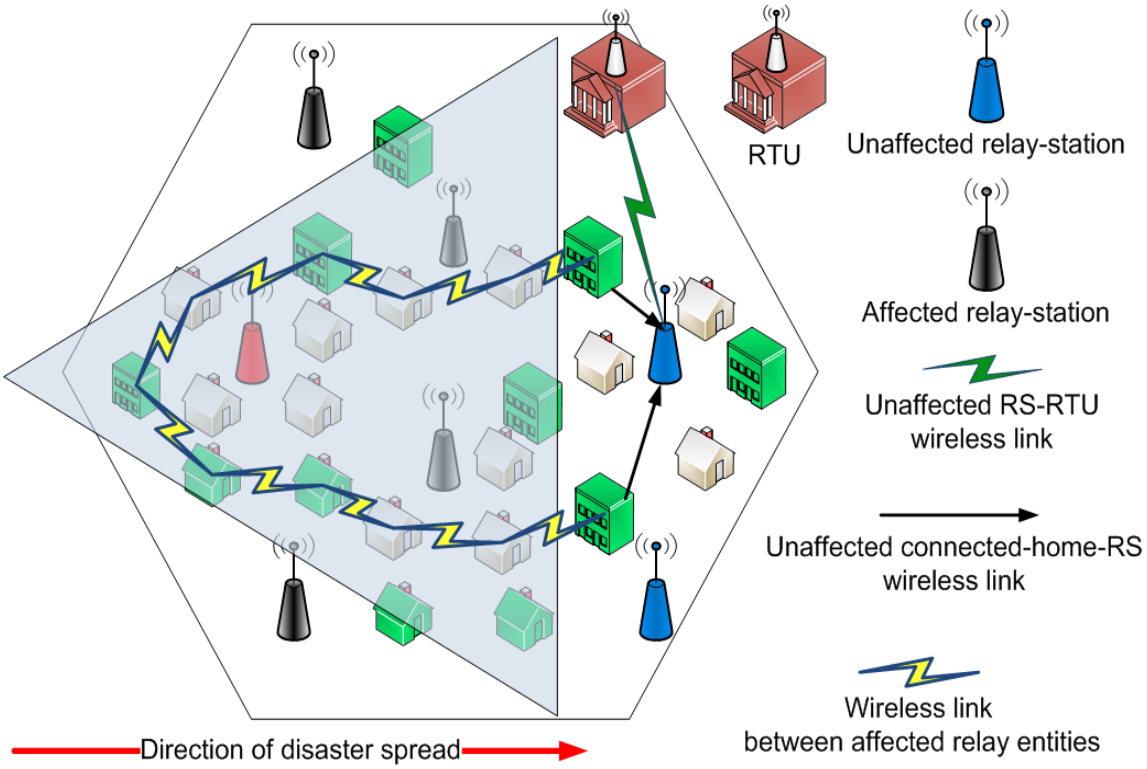
Ακόμη στο (Hamid Gharavi, Multigate Communication Network for Smart Grid , 2011) μελετάτε ότι η multigate δρομολόγηση σε συνδυασμό με την τεχνική back pressure packet scheduling βελτιώνει την απόδοση δρομολογώντας τα δεδομένα στα DAP με μικρότερο overload. Έχει αναφερθεί ότι το δίκτυο επικοινωνιών ενός ευφυούς δικτύου ενέργειας παίζει καθοριστικό ρόλο στην λειτουργία του δικτύου, από την άλλη όμως δεν είναι δυνατόν να αποφευχθούν πάντα ενδεχόμενα προβλήματα επικοινωνίας ή καταστροφές σε κρίσιμες συσκευές(συλλέκτες δεδομένων, relay κτλ). Είναι απαραίτητο οι παραπάνω περιπτώσεις να ληφθούν υπόψη κατά στην σχεδίαση του δικτύου ώστε να προβλεφτούν ενδεχόμενες τέτοιου είδους καταστάσεις. Στο (Arjun Athreya, 2012) μελετάται η χρήση ενός δικτύου mesh όπου παρέχει αξιόπιστη επικοινωνία σε περιπτώσεις προβλημάτων επικοινωνίας στο δίκτυο. Το δίκτυο παρουσιάζεται στην εικόνα 28.



Εικόνα 28 "Το NAN χωρίζεται σε μικρότερες περιοχές που συνδέονται με συλλέκτες δεδομένων/relay stations" (Arjun Athreya, 2012)

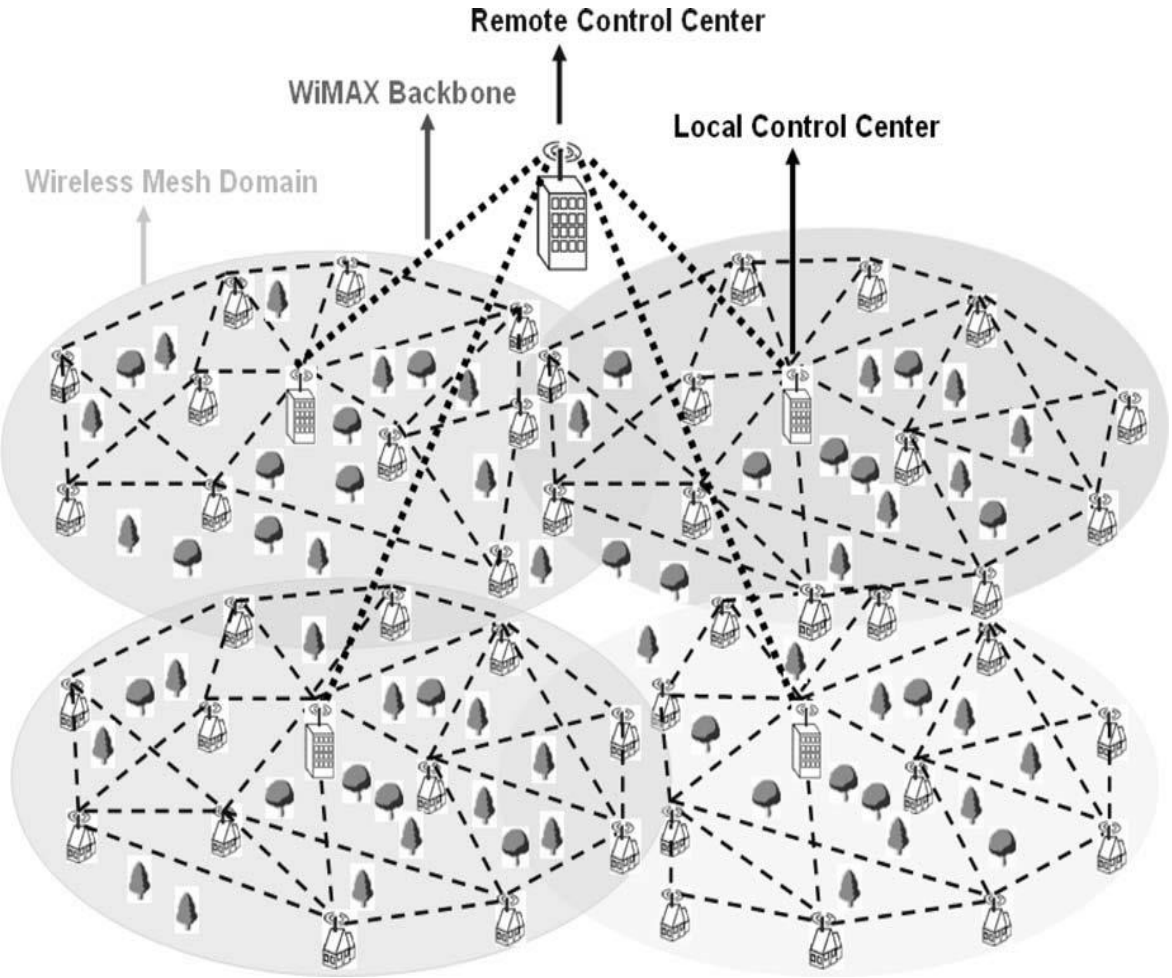
Στο παραπάνω δίκτυο, οι Relay Station(RS), συγκεντρώνουν τα δεδομένα των μετρήσεων από τα HAN και τα HAN συνδέονται μεταξύ τους μέσω των μετρητών ώστε να προωθούν τα δεδομένα στα RS. Σε ενδεχόμενη παρουσίαση βλάβης ή καταστροφής ενός RS τα HAN δίκτυα που συνδέονται θα έχουν αποκοπεί από το υπόλοιπο δίκτυο. Η λύση στο πρόβλημα αυτό έρχεται να δοθεί ως εξής, κάθε έξυπνος μετρητής έχει την δυνατότητα να επικοινωνεί με την γειτονικό του έξυπνο μετρητή(one hop), όπου λειτουργεί ως relay για τον γειτονικό έξυπνο μετρητή. Οι έξυπνοι μετρητές περιοδικά ενημερώνουν τις συνδέσεις που διατηρούν με τους γειτονικούς αλλά και μπορούν να πραγματοποιήσουν συνδέσεις με RS που είναι γειτονικοί(one hop). Οι RS έχουν την δυνατότητα να συνδέονται με γειτονικούς RS αλλά και με τα Remote Terminal Units(RTU) για την συγκέντρωση των δεδομένων.

Η ενδεχόμενη περίπτωση βλάβης ή καταστροφής ενός ή περισσοτέρων RS παρουσιάζεται ως εξής, ένας έξυπνος μετρητής λειτουργεί ως relay για τον γειτονικό έξυπνο μετρητή μέχρι να πραγματοποιηθεί σύνδεση με ένα RS ή με ένα RTU. Επίσης, όταν ανιχνευτεί ένα πρόβλημα σύνδεσης, ένας έξυπνος μετρητής έχει την δυνατότητα να στείλει ένα μήνυμα ειδοποίησης broadcast ώστε να ενημερωθούν όλοι οι έξυπνοι μετρητές του δικτύου. Στην παρακάτω εικόνα παρουσιάζεται το δίκτυό mesh σε κατάσταση προβληματικής λειτουργίας μερικών RS.



Εικόνα 29 "Δίκτυο mesh σε περίπτωση βλάβης ή καταστροφής RS" (Arjun Athreya, 2012)

Η χρήση mesh δικτύων για το NAN μπορεί να συνδυαστεί και με άλλες ασύρματες τεχνολογίες δικτύωσης δημιουργώντας ένα υβριδικό σύστημα επικοινωνίας αποτελούμενο από δύο ή και περισσότερες τεχνολογίες, εκμεταλλευόμενοι τα πλεονεκτήματα που προσφέρει η καθεμιά. Στο (V.C. Gungor, 2006) παρουσιάζεται ένα δίκτυο mesh σε συνδυασμό με την ασύρματη τεχνολογία WiMAX. Το δίκτυο mesh χρησιμοποιείται για την επικοινωνία στο κομμάτι του NAN ανάμεσα στους έξυπνους μετρητές και στους συλλέκτες δεδομένων που χρησιμοποιούν και τις δύο ασύρματες τεχνολογίες. Συνεπώς το mesh δίκτυο μπορεί να υλοποιηθεί με το 802.11s ή κάποια άλλη ασύρματη τεχνολογία mesh. Το δίκτυο κορμού που αναφέρεται στο δίκτυο που ενώνει τους συλλέκτες δεδομένων με το κέντρο διαχείρισης υλοποιείται με την τεχνολογία WiMAX. Στην εικόνα παρακάτω παρουσιάζεται η εφαρμογή του υβριδικού αυτού συστήματος.

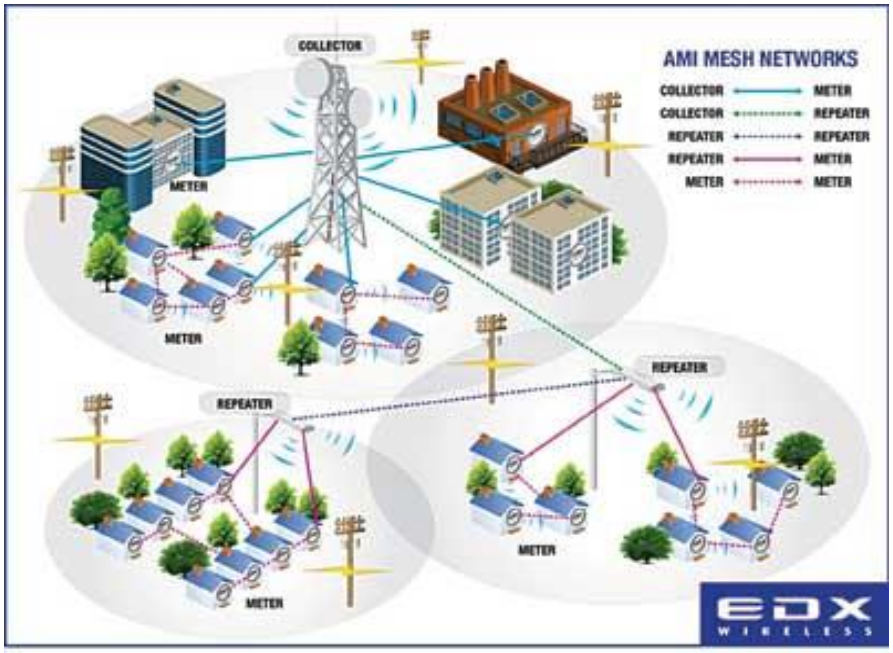


Εικόνα 30 "Δίκτυο mesh σε συνδυασμό με την τεχνολογία WiMAX" (V.C. Gungor, 2006)

Τα πλεονεκτήματα που προσφέρει η υβριδική αυτή σχεδίαση είναι, υψηλή αξιοπιστία λόγω mesh δικτύου, χαμηλό κόστος εγκατάστασης λόγω ότι χρησιμοποιούνται Access Points(AP) βασισμένα στο 802.11s, αλλά και μεγάλη γεωγραφική κάλυψη, λόγω χρήσης της τεχνολογίας WiMAX.

Εκτός από τα πλεονεκτήματα όμως εμφανίζονται θέματα προς επίλυση από την χρήση αυτού του μοντέλου που έχουν να κάνουν με την χρήση των τεχνολογιών αυτών αλλά και στα σημεία στα οποία υλοποιούνται. Ειδικότερα, σε σημεία που υπάρχουν παρεμβολές όπως είναι οι υποσταθμοί λόγω γραμμών μεταφοράς ηλεκτρικής ενέργειας. Το 802.11s λειτουργεί σε συχνότητα 2.4GHz, όπου η συχνότητα αυτή είναι ελεύθερη προς χρήση από διάφορες συσκευές. Οι WiMAX πύργοι επικοινωνιών πρέπει να τοποθετούνται σε σημεία ώστε να καλύπτουν όσο καλύτερα γίνεται το δίκτυο mesh, αυτό πάντα δεν είναι εύκολο να πραγματοποιηθεί. Επίσης, η ασφάλεια του δικτύου και των δεδομένων που ανταλλάσσονται είναι καθοριστικά σημεία για την αξιόπιστη λειτουργία του ευφυούς δικτύου ενέργειας. Είναι απαραίτητο, να σχεδιαστεί με τέτοιο τρόπο το δίκτυο, ώστε να εξασφαλίζεται η φυσική ασφάλεια των υποδομών αλλά και των δεδομένων με την χρήση κρυπτογράφησης και αυθεντικοποίησης των συσκευών.

Μια άλλη διαφορετική περίπτωση, έκτος από την υλοποίηση δικτύων mesh με το 802.11s, mesh δίκτυα για την συλλογή δεδομένων από τους έξυπνους μετρητές μπορούν να υλοποιηθούν και με Radio Frequency(RF) mesh δίκτυα. Στο (Christian Muller, 2012) μελετάται μια αρχιτεκτονική δικτύου mesh βασισμένη σε RF και η απόδοση της. Η RF επικοινωνία γίνεται σε συχνότητα 902-928 MHz και με ρυθμούς μετάδοσης 9.6Kbps ανά κανάλι. Βασίζεται στην γεωγραφική δρομολόγηση, ο μέγιστος αριθμός hops είναι 40 και η απόσταση φτάνει σε ιδανικές συνθήκες μέχρι τα 150 μέτρα. Παρόμοιο σύστημα παρουσιάζεται στο (Leon, 2011) αναφέροντας ότι ένα τυπικό δίκτυο mesh διαθέτει από 5 έως 15 hops και κάθε συλλέκτης δεδομένων εξυπηρετεί από 1000 έως 10000 έξυπνους μετρητές.



Εικόνα 31 "Δίκτυο RF mesh" (Leon, 2011)

Η εφαρμογή mesh δικτύων στα ευφυή δίκτυα ενέργειας πέραν από τα πλεονεκτήματα που προσφέρει που έχουν αναφερθεί παραπάνω, έχει και αρνητικά επιπτώσεις κυρίως στον όγκο των δεδομένων που διακινούνται. Τα θέματα που δημιουργούνται είναι απαραίτητο να καθοριστούν ώστε να βρεθούν τρόποι για βελτίωση των επιπτώσεων που έχουν στο δίκτυο επικοινωνιών. Τα ενδεχόμενα προβλήματα είναι: (Tadashige Iwao, Dynamic Data Forwarding in Wireless Mesh Networks, 2010) (Arabyat, 2013)

1. Παρεμβολές

Τα mesh δίκτυα αναλόγως πως είναι υλοποιημένα(802.11s, 802.15) λειτουργούν στην ελεύθερη μπάντα των 2.4GHz. Στην μπάντα αυτή λόγω της ελεύθερης χρήσης της λειτουργούν παρά πολλές συσκευές που χρησιμοποιούνται καθημερινά όπως είναι Wi-Fi routers στις οικίες για πρόσβαση στο διαδίκτυο, δίκτυο HAN με χρήση του ZigBee κτλ. Οπότε με την χρήση πολλών συσκευών στην ίδια περίπου ακτίνα λειτουργίας, ενδέχεται να παρουσιαστούν φαινόμενα παρεμβολών(interference). Αυτό έχει ως αποτέλεσμα, πολλά πακέτα να χάνονται(dropped) ή να καθυστερούν και έτσι να υπάρχει αύξηση του όγκου των δεδομένων αλλά και καθυστέρηση στην παράδοση των δεδομένων επειδή πρέπει να ξανασταλθούν.

2. Αυξημένο Overload

Η χρήση πρωτοκόλλων δρομολόγησης mesh δικτύων παρέχει μειωμένη καθυστέρηση από άκρη σε άκρη και βελτιώνει την αξιοπιστία αλλά για τα επιτευχθούν τα παραπάνω σε ένα δίκτυο που αποτελείται από χιλιάδες συσκευές ο επιπλέον φόρτος(overload) πακέτων διαχείρισης δικτύου(control packets) είναι μεγάλος λόγω των πληροφοριών που αποθηκεύονται για τα πολλαπλά μονοπάτια. Υπάρχουν όμως και το DADR όπου δεν υπάρχει επιπλέον overload για την διαχείριση των μονοπατιών.

3. Ασφάλεια δεδομένων

Η εφαρμογή του 802.11s ενδέχεται να αποτελέσει στόχο σε ενδεχόμενες επιθέσεις από κακόβουλους χρήστες μιας και πρόκειται από τις πιο γνωστές τεχνολογίες δικτύωσης. Ακόμη, από την στιγμή που ο τρόπος λειτουργίας ενός δικτύου mesh περιλαμβάνει ότι τα δεδομένα που ανταλλάσσονται ανάμεσα στους έξυπνους μετρητές και το ευφυές δίκτυο ενέργειας, διέρχονται από τρίτους έξυπνους μετρητές, ενδέχεται να παρουσιαστούν φαινόμενα υποκλοπών των δεδομένων αυτών ή παραποίηση τους. Τα παραπάνω αποτελούν σοβαρό πρόβλημα λειτουργίας σε περίπτωση που πραγματοποιηθούν. Είναι απαραίτητο λοιπόν να εφαρμοστούν αποτελεσματικές τεχνικές κρυπτογράφησης δεδομένων, αυθεντικοποίησης συσκευών, ώστε να διασφαλιστεί η ακεραιότητα των δεδομένων. Επίσης, είναι απαραίτητο να αναπτυχθούν συστήματα έγκυρης προειδοποίησης και πρόβλεψης κακόβουλων ενεργειών αλλά και να βρεθούν τρόποι προστασίας των έξυπνων μετρητών για διασφάλιση της φυσικής ασφάλειας του εξοπλισμού.

ΕΠΙΛΟΓΟΣ

Μέχρι στιγμής έχουμε μελετήσει την εφαρμογή των γνωστότερων ασύρματων τεχνολογιών στα ευφυή δίκτυα ενέργειας. Η επιλογή της κατάλληλης τεχνολογίας για την κάλυψη των αναγκών στο WAN, NAN, HAN δεν είναι εύκολη υπόθεση, ούτε από την άλλη μεριά δεν μπορούν να καλυφθούν οι ανάγκες με την χρήση μιας μόνο τεχνολογίας. Η επιλογή επηρεάζεται εκτός από την κάλυψη των απαιτήσεων καθυστέρησης και ρυθμού μετάδοσης και από παραμέτρους όπως είναι η αρχιτεκτονική που θα υλοποιηθεί, το οικονομικό κόστος της υλοποίησης, η ασφάλεια των δεδομένων αλλά και η φυσική ασφάλεια των υποδομών. Στο WAN οι ασύρματες τεχνολογίες τέταρτης γενιάς(WiMAX, LTE), φαίνεται να είναι μονόδρομος για το δίκτυο κορμού, εάν και σε κάποιες περιπτώσεις χρειάζονται περεταίρω εξέλιξη για την καλύτερη υλοποίηση δικτύου βασιζόμενες σε αυτές. Σε τμήματα όπως είναι το εσωτερικό δίκτυο επικοινωνιών των υποσταθμών του δικτύου ενέργειας, υπάρχει η δυνατότητα και άλλων ασύρματων τεχνολογιών όπως είναι το Wi-Fi που ταιριάζουν καλύτερα στα χαρακτηριστικά του δικτύου αυτού.

Στο NAN, υπάρχουν περισσότερες επιλογές, εκτός από τις τεχνολογίες τέταρτης γενιάς, εμφανίζεται η χρήση του Wi-Fi σε point to point ή σε mesh αρχιτεκτονική, που χαρακτηρίζεται από σχετικά μικρό κόστος υλοποίησης, με περιορισμένο όμως εύρος λειτουργίας, οπότε υλοποιείται για το last-mile. Επίσης εμφανίζεται σε περιορισμένο βαθμό η χρήση RF mesh και δικτύου βασισμένου στο 802.15.4. Αντίθετα στο HAN, το ZigBee, φαίνεται να κερδίζει έδαφος σε σχέση με άλλες ασύρματες τεχνολογίες όπως είναι το Wi-Fi, ή το PLC. Στο επόμενο κεφάλαιο μελετιούνται οι ενσύρματες τεχνολογίες που έχουν εφαρμογή στα ευφυή δίκτυα ενέργειας, ώστε να μπορέσουμε να βγάλουμε ασφαλή συμπεράσματα συνολικά σε σχέση με τις ασύρματες. Οι κυριότερες ενσύρματες τεχνολογίες που βρίσκουν εφαρμογή είναι οι οπτικές είναι και οι PLC τεχνολογίες.

ΚΕΦΑΛΑΙΟ 4

ΤΕΧΝΟΛΟΓΙΕΣ ΕΝΣΥΡΜΑΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΕΙΣΑΓΩΓΗ

Η χρήση ασύρματων τεχνολογιών σε αρκετές περιπτώσεις ενδέχεται να μην καλύπτει τις ανάγκες επικοινωνίας σε τμήματα των ευφυών δικτύων ενέργειας. Οι ενσύρματες τεχνολογίες έρχονται να καλύψουν τέτοια κενά και ειδικότερα οι οπτικές ίνες και η Powerline. Στο κεφάλαιο αυτό, μελετιούνται η χρήση των δύο αυτών ενσύρματων τεχνολογιών στα ευφυή δίκτυα ενέργειας και σε περιοχές όπου μπορούν να χρησιμοποιηθούν. Μέχρι στιγμή οι οπτικές ίνες χρησιμοποιούνταν αποκλειστικά στο WAN, αλλά με την εισχώρηση τους στα ευφυή δίκτυα ενέργειας, δημιουργήθηκε η ανάγκη σχεδίασης δικτύου επικοινωνιών σε συνδυασμό με δίκτυο παροχής ενέργειας, για την επέκταση τους και στο NAN. Από την άλλη, το ήδη υπάρχον δίκτυο ηλεκτρικής ενέργειας δεν θα μπορούσε να μείνει ανεκμετάλλευτο από την στιγμή, που μπορούν να μεταφερθούν δεδομένα. Έτσι, και εδώ σχεδιάστηκαν νέα πρότυπα και πρωτόκολλα κατάλληλα για την μεταφορά δεδομένων εστιάζοντας την εφαρμογή τους στα ευφυή δίκτυα ενέργειας και τις ιδιαιτερότητες που παρουσιάζουν.

4.1 ΟΠΤΙΚΕΣ ΙΝΕΣ

Οι οπτικές ίνες είναι το πιο γρήγορο μέσο επικοινωνίας στα πλαίσια ενός ευφυούς δικτύου ενέργειας. Η χρήση των οπτικών ινών δεν είναι κάτι καινούριο στις σημερινές επικοινωνίες. Χρησιμοποιούνται ήδη πολλά χρόνια από παρόχους διαδικτύου, αλλά και σε ιδιόκτητα δίκτυα καλύπτοντας τις ανάγκες του δικτύου κορμού παρέχοντας υψηλό ρυθμό μετάδοσης, μικρή καθυστέρηση και με μεγάλη αξιοπιστία. Υπάρχουν δύο τύποι οπτικών ινών, η single mode και multi mode. Στην single mode ο ρυθμός μετάδοσης είναι μεγαλύτερος όπως και η απόσταση που φτάνει το σήμα(δέσμη φωτός). Από την άλλη μεριά η single mode οπτικές ίνες κοστίζουν περισσότερο. Η multi mode, έχουν μεγαλύτερη διάμετρο και παρέχουν υψηλό ρυθμό απόδοσης για μεσαίες αποστάσεις(χρήση σε εσωτερικό κτηρίων και μεταξύ κοντινών κτηρίων). Η χρήση των οπτικών ινών στο δίκτυο επικοινωνιών ενός ευφυούς δικτύου ενέργειας μέχρι στιγμής δεν έχει εισχωρήσει σε μεγάλο βαθμό. Αυτό οφείλεται κατά κύριο λόγο στο αυξημένο κόστος που απαιτείται για την εγκατάσταση των οπτικών ινών. Ο τρόπος λειτουργίας τους και τα χαρακτηριστικά τους καθιστούν τις οπτικές ίνες ιδανικές για συγκεκριμένα τμήματα του δικτύου επικοινωνιών. Όπως έχει αναφερθεί, οι οπτικές ίνες μεταδίδουν τα δεδομένα μέσω φωτός, αυτό τις καθιστά ιδανικές για σημεία του ευφυούς δικτύου που παρουσιάζονται φαινόμενα ηλεκτρομαγνητικών παρεμβολών όπως είναι οι υποσταθμοί του δικτύου ενέργειας, όπου λόγω γραμμών, μετασχηματιστών και άλλων συσκευών επηρεάζουν την λειτουργία των ασύρματων τεχνολογιών. Τα πλεονεκτήματα από την χρήση των οπτικών ινών είναι:

1. Υψηλός ρυθμός μετάδοσης δεδομένων

Επιτυγχάνονται πολύ υψηλοί ρυθμοί μετάδοσης δεδομένων μέχρι και 10Gbps για μία κυματομορφή, ενώ με τη εφαρμογή πολλαπλών κυματορφών στην ίδια οπτικά ίνα (Wavelength Division Multiplexing) ο ρυθμός μετάδοσης δεδομένων φτάνει από 40Gbps και πάνω.

2. Μικρός αριθμός λαθών
3. Προστασία και ανεξαρτησία από παρεμβολές

Η οπτικές ίνες λόγω ότι χρησιμοποιούν φως για την μετάδοση του σήματος δεν επηρεάζονται από ηλεκτρομαγνητικές παρεμβολές.

4. Χαμηλή ενεργειακή κατανάλωση

Οι ακροδέκτες και οι αναμεταδότες που χρησιμοποιούνται καταναλώνουν μικρές ποσότητες ενέργειας.

Εκτός από τα παραπάνω πλεονεκτήματα, δεν υπάρχουν μειονεκτήματα από τα χαρακτηριστικά τους για ενδεχόμενη χρήση τους στα ευφυή δίκτυα ενέργειας. Το κύριο μειονέκτημα έχει να κάνει με το αυξημένο κόστος υλοποίηση του δικτύου. Άρα, ένα δίκτυο οπτικών ινών, για χρήση αυστηρά στα πλαίσια ενός ευφυούς δικτύου ενέργειας κρίνεται ασύμφορο προς το παρόν. Αυτό όμως δεν καταργεί την δυνατότητα χρήσης του σε συγκεκριμένες περιοχές που απαιτούν υψηλούς ρυθμούς μετάδοσης και μικρή καθυστέρηση.

Έχει αναφερθεί επίσης σε προηγούμενα κεφάλαια ότι σύμφωνα με το πρότυπο IEC 61850 οι αυτοματισμοί που υπάρχουν στους υποσταθμούς απαιτούν πολύ μικρή καθυστέρηση, η χρήση οπτικών ινών με το απαραίτητο QoS καλύπτει τις ανάγκες αυτές. (V.C. Gungor, 2006). Στο (WEI Yong, 2012) χρησιμοποιείται παθητικό δίκτυο οπτικών ινών ώστε να επιτυγχάνονται οι απαιτήσεις καθυστέρησης των μηνυμάτων GOOSE που χρησιμοποιούνται στους υποσταθμούς. Υποστηρίζεται QoS και παρέχεται μεγαλύτερη αξιοπιστία λόγω ότι οι οπτικές ίνες είναι προστατευμένες από το ισχυρό προστατευτικό περίβλημα τους. Γίνεται σύγκριση με συμβατικό δίκτυο Ethernet και προκύπτει ότι το κόστος δεν είναι μεγάλο για την υλοποίηση ενός εσωτερικού δικτύου βασισμένο σε Ethernet Passive Optical Network(EPON).

Για την υλοποίηση ενός δικτύου οπτικών ινών που καλύπτει το κομμάτι του “last-mile” για την επικοινωνία με τους έξυπνους μετρητές, η χρήση των οπτικών ινών υπερκαλύπτει κατά πολύ τις ανάγκες με τον ρυθμό μετάδοσης δεδομένων που προσφέρει. Όμως, με την υλοποίηση ενός τέτοιου δικτύου που μοιάζει με δίκτυα που ήδη έχουν εφαρμοσθεί, όπως είναι το Fiber-To-The-Home, για παροχή διαδικτύου, καλωδιακής τηλεόρασης, σε περίπτωση που χρησιμοποιηθεί ένα τέτοιο δίκτυο για την επικοινωνία ανάμεσα στους έξυπνους μετρητές και σημείων όπου ανήκουν στο ευφυές δίκτυο, το κόστος υλοποίησης και χρήσης του δικτύου μειώνεται δραματικά. Προς το παρόν το κόστος για την κατασκευή ενός τέτοιου δικτύου ανέρχεται σε ποσά μέχρι 2000 € ανά οικία για απομακρυσμένες περιοχές

σε αντίθετη με την υλοποίηση δικτύου ασύρματων επικοινωνιών που έχει μικρότερο κόστος κατασκευής. (Sörries, 2013)

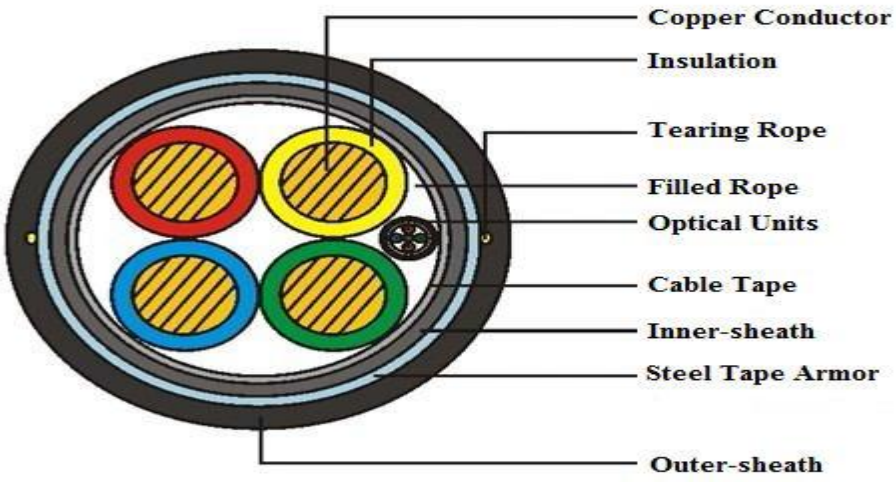
Οι οπτικές ίνες λόγω ότι παρέχουν επικοινωνία σε μεγάλες αποστάσεις και μένουν ανεπηρέαστες από παρεμβολές μπορούν να χρησιμοποιηθούν σε συνδυασμό με το δίκτυο διανομής ηλεκτρικής ενέργειας για μείωση του κόστους εγκατάστασης σε ενδεχόμενη κατασκευή νέου δικτύου διανομής. Στο (Xie Shu-Hong, 2011) μελετάται μια νέα αρχιτεκτονική δικτύου με την ονομασία Power Fiber To The Home(PFTTH) όπου σχεδιάζεται να υλοποιηθεί παρέχοντας ηλεκτρική ενέργειας και επικοινωνία με χρήση οπτικών ινών σε ένα κοινό καλώδιο. Το μέσο αυτό είναι γνωστό ως Optical Fiber Composite Low Voltage Cable(OPLC). Ειδικότερα το OPLC είναι ένας νέος τύπος καλωδίου ο οποίος αποτελείται από κοινά καλώδια μεταφοράς χαμηλής τάσης και οπτική ίνα για μεταφορά δεδομένων. Τα πλεονεκτήματα χρήσης ενός δικτύου που προκύπτουν από την χρήση του μέσου αυτού είναι: (Xie Shu-Hong, 2011)

1. Κοινό μέσο

Οι οπτικές ίνες παρέχουν υψηλούς ρυθμούς μετάδοσης δεδομένων, οπότε η συγκεκριμένη υποδομή μπορεί να χρησιμοποιηθεί για παροχή υπηρεσιών διαδικτύου, καλωδιακής τηλεόρασης κτλ. Με την υλοποίηση αυτή μειώνεται το κόστος κατασκευής ανεξάρτητων υποδομών για κάθε παροχή υπηρεσίας που ζητάει ο πελάτης και αποφεύγονται καινούριες κατασκευές που ενδέχεται να παρουσιάσουν νέα προβλήματα εγκατάστασης. Ως αποτέλεσμα το κόστος μειώνεται σημαντικά.

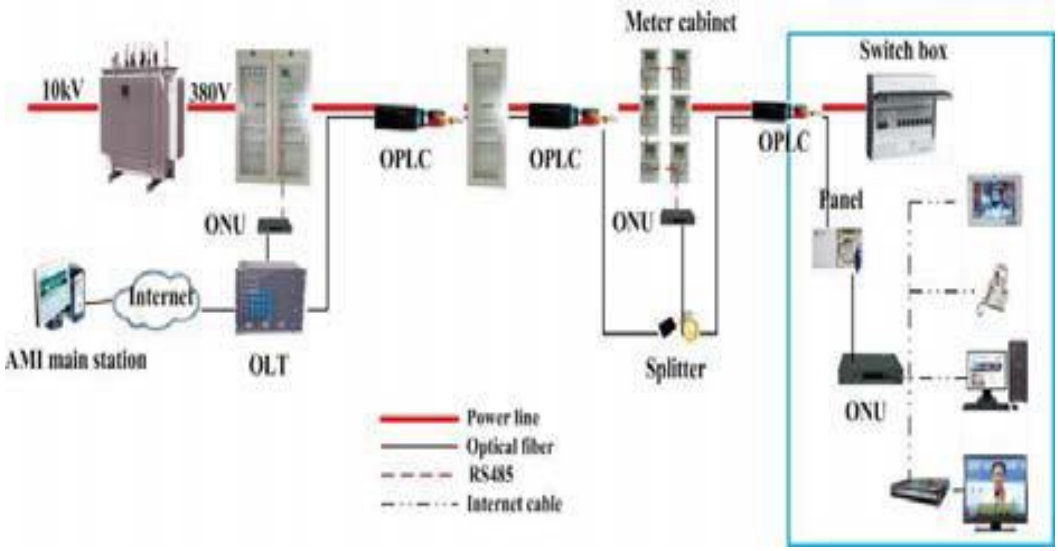
2. OPLC και παθητικά οπτικά δίκτυα

Το OPLC και οι τεχνολογίες Passive Optical Networks(xPON) αν συνδυαστούν προσφέρουν point to multi point συνδέσεις μειώνοντας ο κόστος κατασκευής του δικτύου. Με την χρήση xPON και εξαρτημάτων που χρειάζονται για την κατασκευή του δικτύου όπως είναι τα optical line terminals για τον τερματισμό των οπτικών ινών το ίδιο μέσο χρησιμοποιείται για πολλές οικίες παρέχοντας διαφορετικές υπηρεσίες όπως αναφέρθηκαν προηγουμένως.



Εικόνα 32 "Καλώδιο OPLC" (Liu Jianming W. J., 2011)

Ακόμη, αναφέρεται ότι το συνολικό κόστος εξοικονόμησης σε σχέση με την υλοποίηση ενός δικτύου διανομής ενέργειας και ενός ανεξάρτητου δικτύου οπτικών ινών είναι 40%. Η υλοποίηση ενός τέτοιου δικτύου πραγματοποιείται στην Κίνα και μέχρι στιγμή εξυπηρετεί 62000 οικίες με συνολικό μήκος καλωδίων 10000 χιλιόμετρα. Συνεπώς, η χρήση οπτικών ινών για το δίκτυο επικοινωνιών ενός ευφυούς δικτύου ενέργειας δεν είναι αδύνατη αλλά το μόνο που απαιτείται είναι να συνδυαστεί μαζί με το δίκτυο ενέργειας για μείωση του κόστους εγκατάστασης.



Εικόνα 33 "Δίκτυο βασισμένο στο OPLC" (Liu Jianming W. J., 2011)

4.2 POWER LINE COMMUNICATION

Η ιδέα να χρησιμοποιηθεί το δίκτυο μεταφοράς ηλεκτρικής ενέργειας για επικοινωνιακούς σκοπούς δεν είναι κάτι πρόσφατο λόγω της μεγάλης γεωγραφικής κάλυψης του δικτύου ηλεκτρικής ενέργειας. Το μεγάλο πλεονέκτημα ως προς την χρήση για επικοινωνιακούς σκοπούς είναι ότι το δίκτυο ηλεκτρικής ενέργειας προϋπάρχει και το μόνο που απαιτείται είναι ο κατάλληλο εξοπλισμός για την μετάδοση των δεδομένων, την κωδικοποίηση και την αποκωδικοποίηση τους. Στην λειτουργία των ευφυών δικτύων ενέργειας το δίκτυο επικοινωνιών με το δίκτυο ηλεκτρικής ενέργειας συνεργάζονται σε μεγάλο βαθμό και με αυτόν τον τρόπο η χρήση της τεχνολογίας Power Line Communication(PLC) δεν μπορεί να περάσει απαρατήρητη. Από πλευράς απόδοσης, ο ρυθμός μετάδοσης δεδομένων και η ακτίνα λειτουργίας διαφέρει αναλόγως του προτύπου που υλοποιείται και την συχνότητα μετάδοσης των δεδομένων πάνω στο μέσο, που στην προκειμένη περίπτωση είναι το δίκτυο ηλεκτρικής ενέργειας. Σημαντικό ρόλο παίζουν ενδεχόμενες παρεμβολές στο μέσο μιας και λόγω του τύπου του επηρεάζεται από ηλεκτρομαγνητικές παρεμβολές. Οι PLC τεχνολογίες μπορούν να χωριστούν σε τρείς τύπους: (Emilio Ancillotti, 2013) (Fahad Khan, 2012)

1. Ultra Narrow Band(UNB)

Λειτουργούν σε πολύ χαμηλές συχνότητες (0.3-3 KHz) ή στο εύρος 30-300Hz) και ο ρυθμός μετάδοσης δεδομένων που υποστηρίζουν είναι περίπου 100bps. Ακόμη, έχουν πολύ μεγάλη ακτίνα λειτουργίας που φτάνει μέχρι και 150 χιλιόμετρα και ή και περισσότερο. Αυτό οφείλεται ακόμη στο ότι το σήμα του διέρχεται μέσα από τους μετασχηματιστές μεσαίας και χαμηλής τάσης και ως αποτέλεσμα χρειάζονται λιγότεροι αναμεταδότες σήματος.

2. Narrowband(NB)

Οι τεχνολογίες αυτές λειτουργούν σε συχνότητες VLF/LF/MF (3-500 KHz) και χωρίζονται σε τεχνολογίες χαμηλού ρυθμού μετάδοσης(μερικών kbps) όπως είναι το IEC 61334, X10, και το HomePlug και σε υψηλού ρυθμού μετάδοσης τέτοιες τεχνολογίες είναι το IEEE 1901.2, G3-PLC, PRIME, ITU-T G.hnem και παρέχουν από 10kbps μέχρι 500kbps. Στην Ευρώπη οι συχνότητες λειτουργίας καθορίζονται από τον οργανισμό European Committee for Electrotechnical Standardization(CENELEC) και βασίζονται στο πρότυπο EN 50065. Οι συχνότητα χωρίζονται σε τέσσερα εύρη τα οποία είναι: (Lars Torsten Berger, 2013)

- A μπάντα, 3-95KHz, για χρήση στο WAN και NAN
- B μπάντα, 95-125KHz, για οποιαδήποτε χρήση
- C μπάντα, 125-140KHz, για χρήση στο HAN αποκλειστικά
- D μπάντα, 140-148.5KHz, για χρήση σε συστήματα ασφαλείας

3. Broadband(BB)

Οι τεχνολογίες αυτές λειτουργούν σε συχνότητες HF/VHF (1.8-250 MHz) και παρέχουν ρυθμό μετάδοσης μέχρι και 200Mbps. Παραδείγματα τέτοιων τεχνολογιών είναι, HomePlug 1.0 και οι επόμενες εκδόσεις του, το IEEE 1901. Οι BB-PLC τεχνολογίες καθίστανται ιδανικές για οικιακή χρήση. Στο (Gharbaoui M, 2012) αναφέρεται ότι οι κατασκευαστές έχουν καταφέρει την χρήση τεχνολογιών BB-PLC να φτάσουν σε ακτίνα 8 χιλιομέτρων και με ρυθμό μετάδοσης στα 10Mbps. Με την χρήση TCP/IP ο ρυθμός μετάδοσης ξεπερνάει τα 80Mbps. Οι τεχνολογίες της κατηγορίας αυτής ακόμη είναι γνωστές ως Broadband Power Line(BPL) γιατί έχουν την δυνατότητα να παρέχουν ακόμη και πρόσβαση στο διαδίκτυο με το ρυθμό μετάδοσης δεδομένων που επιτυγχάνουν.

Για την καλύτερη μελέτη των τεχνολογιών PLC και των προτύπων που σχετίζονται με αυτές είναι απαραίτητο να γίνει ένας διαχωρισμός του δικτύου ηλεκτρικής ενέργειας, μιας και το δίκτυο αυτό είναι ταυτόχρονα και το δίκτυο επικοινωνίας με την χρήση PLC. Ειδικότερα το δίκτυο ηλεκτρικής ενέργειας μπορεί να διαχωριστεί σε τρεις ομάδες: (Hrasnica Halid, 2004)

1. Δίκτυο χαμηλής τάσης

Είναι το δίκτυο διανομής που φτάνει μέχρι και τις οικίες και παρέχει ηλεκτρική ενέργειας στους οικιακούς καταναλωτές. Στην Αμερική για παράδειγμα το δίκτυο λειτουργεί σε τάση 120 volt, ενώ στην Ευρώπη σε τάση 220/230 Volt. Σημαντικό είναι και πρέπει να αναφερθεί ότι η σχεδίαση του δικτύου ηλεκτρικής ενέργειας διαφέρει, και σε κοντινές αποστάσεις εμφανίζονται φαινόμενα παρεμβολών αλλά και εξασθένισης του σήματος.

2. Δίκτυο μεσαίας τάσης

Είναι το δίκτυο παρέχει ενέργεια σε ολόκληρες περιοχές, με τάση μεγαλύτερη από το δίκτυο χαμηλή τάσης. Επίσης χρησιμοποιείται για την ηλεκτροδότηση βιομηχανικών μονάδων κτλ

3. Δίκτυο υψηλής τάσης

Είναι το δίκτυο κορμού του δικτύου ηλεκτρικής ενέργειας και χρησιμοποιείται για την μεταφορά ενέργειας από τους σταθμούς παραγωγής προς τους υποσταθμούς αλλά και για μεταφορά ενέργειας ανάμεσα σε διαφορετικές χώρες ή ηπείρους.

Με την χρήση τεχνολογιών PLC στα ευφυή δίκτυα ενέργειας καλύπτεται ένα ευρύ φάσμα υπηρεσιών που απαιτούν επικοινωνία ανάμεσα σε διάφορα τμήματα του ευφυούς δικτύου ενέργειας. Συνεπώς οι τεχνολογίες PLC μπορούν να εφαρμοσθούν και στα τρία δίκτυα(WAN,NAN,HAN) που απαρτίζουν ένα ευφυές δίκτυο ενέργειας. Ειδικότερα στο HAN η χρήση των PLC, φαίνεται μια εναλλακτική της χρήση ασύρματων τεχνολογιών όπως είναι το ZigBee που έχει μελετηθεί σε προηγούμενο κεφάλαιο. Αυτό συμβαίνει γιατί σε κάθε οικία και σε κάθε δωμάτιο υπάρχουν ηλεκτρικές πρίζες για την παροχή ηλεκτρικού ρεύματος και με την χρήση κατάλληλων μετατροπέων(adapter) μεταδίδονται δεδομένα μέσω του ηλεκτρικού δικτύου της οικίας. Σε ένα HAN ενδέχεται να υπάρχει συνδεμένο και κάποιο ηλεκτρικό όχημα το οποίο φορτίζει με την χρήση ηλεκτρικής ενέργειας από

την οικία. Με την χρήση PLC μπορεί να πραγματοποιηθεί η επικοινωνία του οχήματος με το HAN δίκτυο για την ανταλλαγή πληροφοριών(κατανάλωση ενέργειας, χρόνος φόρτισης) χωρίς την χρήση ασύρματων τεχνολογιών. Στο NAN, υπάρχει η δυνατότητα χρήσης του για αναφορά προβλημάτων από τους υποσταθμούς, την κατάσταση του δικτύου ενέργειας με πληροφορίες που λαμβάνονται από τα IED. Ακόμη, υπάρχει η δυνατότητα να χρησιμοποιηθεί plc τεχνολογία για συλλογή δεδομένων από τους έξυπνους μετρητές(smart metering). Τέτοια δίκτυα υπάρχουν ήδη υλοποιημένα κυρίως στην Ευρώπη.

Ένα πρότυπο τεχνολογίας PLC που χρησιμοποιείται κυρίως για την συλλογή δεδομένων από τους έξυπνους μετρητές είναι το PoweRLine Intelligent Metering Evolution(PRIME) το οποίο έχει αναπτυχθεί από τον οργανισμό PRIME Alliance. Το PRIME ανήκει στη κατηγορία Narrowband PLC και χρησιμοποιεί την τεχνική OFDM σε συχνότητες λειτουργίας στην Ευρώπη που ανήκουν στην κατηγορία CENELEC A (42-89 KHz). Το PRIME στην Ευρώπη, έχει χρησιμοποιηθεί σε μεγάλος εύρος από την Ισπανική εταιρία ηλεκτρικής ενέργειας Iberdola για την συλλογή δεδομένων από τους έξυπνους μετρητές. Ο μέγιστος ρυθμός μετάδοσης δεδομένων που επιτυγχάνεται φτάνει τα 128Kbps για δίκτυα χαμηλής τάσης. Μέχρι στιγμής υποστηρίζονται μόνο τα δίκτυα χαμηλής τάσης, δηλαδή η περιοχή του “last-mile” για το κομμάτι των επικοινωνιών. Να αναφερθεί ότι το PRIME υλοποιείται με βάση ένα μοντέλο αναφοράς που βασίζεται στο πρότυπο IEEE 802.16 (Project P. , 2008). Για την αντιμετώπιση των παρεμβολών, παρέχεται προς υλοποίηση τεχνική Automatic Retransmission Request(ARQ) βασιζόμενη στην επιλεκτική επανάποστολή. Για την υλοποίηση του PRIME ορίζονται δύο είδη κόμβων, ο Base Node και ο Service Node. Ο Base Node, είναι το κεντρικό σημείο που δικτύου και ονομάζεται συλλέκτης δεδομένων (Concentrator) και είναι υπεύθυνος για την διαχείριση του υποδικτύου του. Ως Service Nodes είναι οι έξυπνοι μετρητές όπου συνδέονται με τον συλλέκτη δεδομένων. Ακόμη οι Service Nodes λειτουργούν σε τρεις καταστάσεις:

1. Αποσυνδεμένη κατάσταση

Στην κατάσταση αυτή είναι αποσυνδεμένος και δεν επικοινωνεί με το συλλέκτη δεδομένων.

2. Τερματική κατάσταση

Στην κατάσταση αυτή, ο έξυπνος μετρητής έχει συνδεθεί στο υποδίκτυο και επικοινωνεί με τον συλλέκτη δεδομένων.

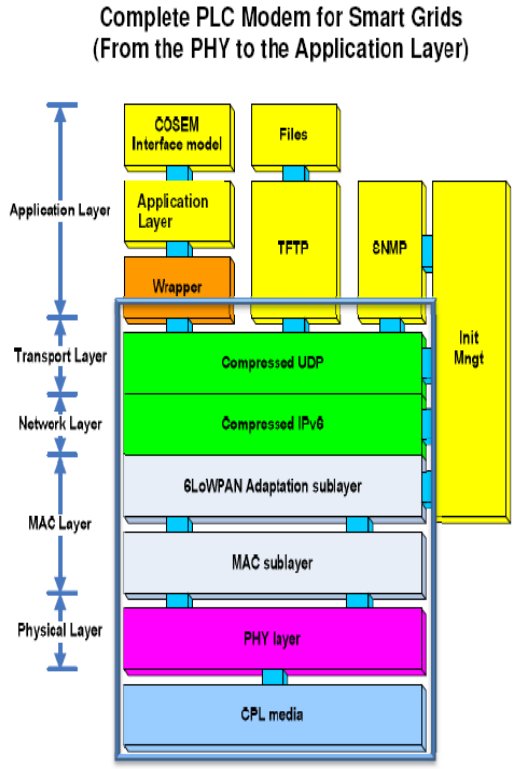
3. Κατάσταση διακοπής

Στην κατάσταση αυτή ο έξυπνος μετρητής, έχει την δυνατότητα να παρέχει επικοινωνία και σε άλλους έξυπνους μετρητές που βρίσκονται στην τερματική κατάσταση ή στην ίδια κατάσταση με τον ίδιο.

Σύμφωνά με τα παραπάνω το υποδίκτυο λειτουργεί σε κατάσταση Master/Slave και οι καταστάσεις αλλάζουν σύμφωνα με την κατάσταση του ηλεκτρικού δικτύου(θόρυβος, εξασθένιση).

Το PRIME έχει την δυνατότητα να υποστηρίξει προτόκολλα όπως είναι το IPv4, και με αυτόν τον τρόπο ένας έξυπνος μετρητής μπορεί να προωθήσει πακέτα ipv4 στον συλλέκτη δεδομένων ή σε κάποιον άλλον έξυπνο μετρητή. Από πλευράς διευθυνσιοδότησης, μπορεί να γίνει χρήση στατικών ip διευθύνσεων ή να αποδίδονται δυναμικά στους έξυπνους μετρητές με χρήση Dynamic Host Configuration Protocol (DHCP). Οι έξυπνοι μετρητές εκτός από διευθύνσεις τρίτου επιπέδου OSI, έχουν και MAC διευθύνσεις στο δεύτερο επίπεδο με την μετάφραση των διευθύνσεων να γίνεται από τον συλλέκτη δεδομένων(Base Node). Επιπλεόν υποστηρίζεται και η χρήση broacasting αλλά και multicasting σε κάθε υποδίκτυο. Στην τελευταία έκδοση του προτύπου, παρέχεται η δυνατότητα υλοποίησης του δικτύου στην τελευταία έκδοση του προτοκόλου IP, το IPv6, κερδίζοντας όλα τα πλεονεκτήματα που προσσφέρει έναντι της προηγούμενης έκδοσης. Για την ασφάλεια των δεδομένων που ανταλλάσονται και επειδή δεν είναι υποχρεωτικό να εφαρμοσθεί κάποια τεχνική κρυπτογράφησης για την χρήση του PRIME, είναι όμως υποχρεωτικό, να κρυπτογραφούνται να μυνήματα ελέγχου στο επίπεδο MAC που ανταλλάσονται μεταξύ των συσκευών. Η τεχνική κρυπτογράφησης που υποστηρίζεται από το PRIME είναι η AES 128 bit. (Group P. A., 2012)

Στην ίδια κατηγορία ανήκει και ένα ακόμη πρότυπο plc τεχνολογίας το G3-PLC. Το G3-PLC αναπτύχτηκε από τον οργανισμό G3-PLC Alliance και δημοσιεύθηκε τον Αύγουστο του 2009. Ο κύριος στόχος του είναι παροχή αξιόπιστης επικοινωνίας με υψηλή ασφάλεια, σε μακρινές αποστάσεις. Ένα μεγάλο πλεονέκτημα του είναι, ότι έχει την δυνατότητα να διέρχεται το σήμα μέσα από τους μετασχηματιστές του δικτύου μεσαίας και χαμηλής τάσης και με αυτόν τον τρόπο να υποστηρίζει και τα δύο αυτά δίκτυα με εύρος περίπου τα 8 χιλιόμετρα. Το παραπάνω έχει ως αποτέλεσμα να απαιτείται μικρότερος αριθμός συλλεκτών δεδομένων, ενώ σε διαφορετική περίπτωση πριν κάθε μετασχηματιστή του δικτύου ενέργειας θα απαιτούνταν να υπάρχει συλλέκτης δεδομένων. Στην Ευρώπη λειτουργεί στις συχνότητες που καθορίζονται από τον CENELEC και ειδικότερα στις συχνότητες κατηγορίας CENELEC A και CENELEC B. Ο μέγιστος ρυθμός μετάδοσης που επιτυγχάνεται φτάνει τα 300Kbit/sec και βασίζεται στην τεχνική OFDM. Επίσης στο επίπεδο MAC το πρότυπο αυτό βασίζεται στο IEEE 802.15.4 και χρησιμοποιείται το 6LoWPAN για την υλοποίηση του IPv6 στο IEEE 802.15.4. Να αναφερθεί ότι από την στιγμή που υποστηρίζεται το IP πρωτόκολλο και με την υλοποίηση των ANSI C12.22 και κατά προέκταση του ANSI C12.19 στο επίπεδο εφαρμογών του OSI επιτυγχάνεται οι επικοινωνία με έξυπνους μετρητές για συλλογή των δεδομένων των HAN. Ακόμη η ασφάλεια εξασφαλίζεται μέσω του ANSI C12.22 που παρέχει υψηλή ασφάλεια με χρήση της αλγόριθμου κρυπτογράφησης AES. Συνοπτικά το ANSI C12.19 περιγράφει την δομή των δεδομένων που ανταλλάσσονται μεταξύ ενός έξυπνου μετρητή και ενός συλλέκτη δεδομένων, ενώ το ANSI C12.22 περιγράφει την ασφαλή και αξιόπιστη μεταφορά των δεδομένων όπως καθορίζονται από το ANSI C12.19. (Lars Torsten Berger, 2013) (Integrated)



- **Application layer**
  - Compliant with ANSI C12.19/C12.22, IEC 62056-61/62 (DLMS/COSEM), and other international standards
- **Transport and network layers**
  - IPv6 enables potential services: SNMP, TFPT, etc.
  - 6LoWPAN adaptation layer associates the IEEE 802.15.4-based MAC layer to IPv6
    - Compression of IP header, fragmentation, routing, and authentication
- **MAC layer**
  - Plug-and-play network management chooses "the best path" (full mesh support)
  - Time-domain and collision management
  - IEEE 802.15.4-2006 MAC layer
  - CSMA/ARQ
- **Physical layer**
  - Support of internationally accepted bands from 10kHz to 490kHz (FCC, CENELEC, ARIB)
  - Multilayer error encoding/decoding
    - Viterbi, convolutional, Reed Solomon, and CRC16
  - 8PSK,QPSK, BPSK, ROBO, and Messaging modes
  - Adaptive tone mapping, notching, and modulation

Εικόνα 34 "Στοίβα πρωτοκόλλων του G3-PLC" (Sanz, 2010)

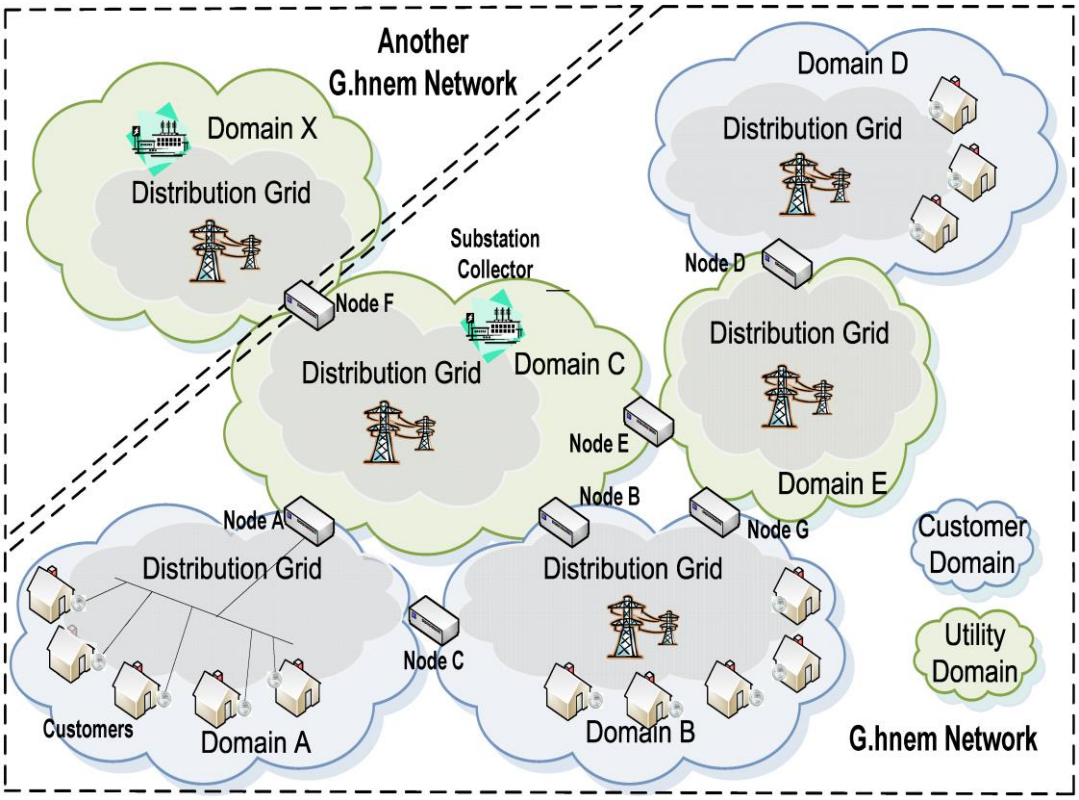
Τα παραπάνω δύο πρότυπα, όπως αναφέρθηκε ανήκουν στην κατηγορία NB-PLC και λειτουργούν στα δίκτυα χαμηλής και μεσαίας τάσης. Τα δύο όμως αυτά πρότυπα είναι διαφορετικά ως προς τα χαρακτηριστικά τους και τον τρόπο λειτουργίας τους. Για να διασφαλιστεί η διαλειτουργικότητα μεταξύ διαφορετικών προτύπων στις χαμηλές αυτές συχνότητες απαιτείται να καθοριστούν προδιαγραφές αυτές. Ένα τέτοιο πρότυπο που βρίσκεται σε εξέλιξη είναι το IEEE P1901.2 το οποίο καθορίζει την επικοινωνία σε χαμηλές συχνότητες (μικρότερες των 500KHz) σε NB-PLC. Υποστηρίζει επικοινωνία για εσωτερικούς, εξωτερικούς χώρους και μέσα από μετασχηματιστές του ηλεκτρικού δικτύου για μεγάλες αποστάσεις. Εκτός από την επικοινωνία με έξυπνους μετρητές για την συλλογή δεδομένων, υποστηρίζεται και η επικοινωνία άλλων συσκευών ή τμημάτων ενός ευφυούς δικτύου ενέργειας, όπως είναι μονάδες φωτοβολταικών, ηλεκτρικά οχήματα κτλ. Ο ρυθμός μετάδοσης δεδομένων είναι επεκτάσιμος μέχρι 500Kbps και εξαρτάται από τις απαιτήσεις του υπάρχουν. Το πρότυπο αυτό σχεδιάζεται για να είναι πλήρως συμβατό με πρωτόκολλα δικτύου όπως είναι το IPv4 και IPv6 αλλά και με τα γνωστότερα πρωτόκολλα μεταφοράς όπως το Transmission Control Protocol (TCP) και το User Datagram Protocol (UDP). Για την ασφάλεια των δεδομένων που ανταλλάσσονται υποστηρίζεται ο αλγόριθμος AES 128bit. Να

αναφερθεί ότι για να είναι πλήρως συμβατό το πρότυπο αυτό, με το PRIME αλλά και το G3-PLC υιοθετεί χαρακτηριστικά και από τα δύο, όπως είναι η χρήση της τεχνικής OFDM, αλλά και το χαρακτηριστικό του G3-PLC να διέρχεται μέσα από μετασχηματιστές ηλεκτρισμού για δίκτυα χαμηλής και μεσαίας τάσης δεδομένων. Οι συχνότητες λειτουργίας καθορίζονται από διεθνείς οργανισμούς όπως είναι για την Ευρώπη ο CENELEC, για την Ιαπωνία ο ARIB και για τις Ηνωμένες Πολιτείες ο FCC. Το πρότυπο περιγράφει την δομή και την λειτουργία των δύο κατώτερων επιπέδων, του φυσικού επιπέδου αλλά και του επιπέδου MAC. Ειδικότερα, στο MAC επίπεδο η πρόσβαση στο μέσο γίνεται με την γνωστή τεχνική CSMA/CA παρέχοντας ενημέρωση στα παραπάνω επίπεδα μέσω θετικών ή αρνητικών απαντήσεων(ACK και NACK) αλλά και πραγματοποιείται το fragmentation και το reassembly των frames. Ένα κύριο πρόβλημα που μελετάται είναι οι παρεμβολές που παρουσιάζονται ανάμεσα σε τεχνολογίες PLC που λειτουργούν σε κοντινές συχνότητες. Το αποτέλεσμα είναι να μειώνεται η απόδοση του δικτύου στην μετάδοση δεδομένων. Η ομάδα ανάπτυξης του P1901.2, έχει επιλέξει την τεχνική Preamble-based csma mechanism η οποία καλύπτει και τις προδιαγραφές του θέτονται από το NIST PAP15. Ο μηχανισμός αυτός χρησιμοποιείται για την πρόσβαση στο μέσο από διαφορετικές συσκευές που λειτουργούν σε κοντινές συχνότητες. Τέλος να αναφερθεί ότι ο NIST στο PAP15 έχει πιστοποιήσει ως πρόταση την υλοποίηση του παραπάνω μηχανισμού για συσκευές που λειτουργούν κάτω από 500KHz σύμφωνα με το IEEE P1901.2 (Su, 2013) (Jim LeClare, 2012) (Lars Torsten Berger, 2013)

Ένα ακόμη πρότυπο που σχετίζεται με την επικοινωνία στην κατηγορία των NB-PLC, έχει δημιουργήσει ο οργανισμός ITU με την ονομασία G.hnem. Το πρότυπο ITU G.hnem αποτελείται στην πραγματικότητα από δύο άλλα πρότυπα που καθορίζουν τα χαρακτηριστικά του. Αυτά είναι, τα ITU-T G.9955 και ITU-T G.9956. Το πρώτο σχετίζεται με τα χαρακτηριστικά στο φυσικό επίπεδο (PHY), ενώ το δεύτερο σχετίζεται με το δεύτερο επίπεδο (MAC). Παραπάνω αναφέρθηκε ότι το NIST με το PAP15 καθορίζει τις απαιτήσεις για φυσικό και MAC επίπεδο, το G.hnem έχει λάβει υπόψη τις προτάσεις αυτές και τις έχει συμπεριλάβει στην σχεδίαση του προτύπου. Το G.hnem, λειτουργεί σε συχνότητες από 35 μέχρι 143KHz για την Ευρώπη, οι οποίες καθορίζονται από τον CENELEC και από 34-475KHZ για συχνότητες που καθορίζονται από τον FCC. Ο ρυθμός μετάδοσης δεδομένων φτάνει το 1Mbps, ενώ υποστηρίζει πρωτόκολλα δικτύου όπως είναι το IPv4 και IPv6. Στο φυσικό επίπεδο χρησιμοποιείται η τεχνική OFDM όπως στο PRIME και στο G3-PLC. Η χρήση του ITU G.hnem αφορά την συλλογή δεδομένων από έξυπνους μετρητές και λειτουργίες DR. Στο (Rossello-Busquet, 2012) μελετάται η εφαρμογή του προτύπου G.hnem για συλλογή δεδομένων από τους έξυπνους μετρητές. Ένα δίκτυο G.hnem χωρίζεται σε ένα ή περισσότερα domains και κάθε domain είναι ένα λογικό σύνολο από κόμβους. Επίσης ένα domain μπορεί να καλύπτει ένα άλλο κατά ένα μέρος ή ολόκληρο. Κάθε domain έχει ένα μοναδικό στοιχείο ταυτότητας το domain id. Συνολικά ένα δίκτυο G.hnem έχει την δυνατότητα να έχει 65535 domain, και κάθε domain να έχει 32768 κόμβους. Κάθε

κόμβος είναι μοναδικός με στοιχείο ταυτότητας το id του. Σε κάθε δίκτυο G.hnem οι κόμβοι μπορούν να επικοινωνούν μεταξύ τους άμεσα ή μέσω άλλον κόμβων. Όπως αναφέρθηκε προηγουμένως, το ITU-T G.9955 περιγράφει το φυσικό επίπεδο και καθορίζει τις παραμέτρους, ενώ οι λειτουργίες αφορούν την μετάδοση σήματος με την τεχνική OFDM. Το ITU-T G.9956, καθορίζει τις παραμέτρους και την δημιουργία των frames, για την ενσωμάτωση τους σε πρωτόκολλα δικτύου. Ακόμη, υποστηρίζεται σε επίπεδο MAC QoS, αυτό με την ταξινόμηση των frames στα τέσσερα είδη προτεραιοτήτων που υπάρχουν. Να σημειωθεί ότι η μέγιστη προτεραιότητα χρησιμοποιείται μόνο για μετάδοση πληροφοριών σε έκτακτη ανάγκη, όπως είναι μια βλάβη στο ηλεκτρικό δίκτυο.

Η παρακάτω εικόνα παρουσιάζει το δίκτυο επικοινωνιών ενός ευφυούς δικτύου ενέργειας βασισμένο στο πρότυπο G.hnem, όμως λόγω ότι δεν μπορεί να σχεδιαστεί μια ακριβής εικόνα του ηλεκτρικού δικτύου γιατί διαφέρει από χώρα σε χώρα, η διάταξη γίνεται στις λογικές ομάδες που καθορίζονται από τα πρότυπα σχεδιασμού που υπάρχουν. Στην εικόνα, παρουσιάζεται ένα domain που είναι ξεχωριστό από τα υπόλοιπα, αυτό είναι το domain x, το οποίο με την χρήση του Node F, ο οποίος λειτουργεί ως γέφυρα, ενώνει δύο διαφορετικά δίκτυα G.hnem. Τέλος, γίνεται ένας διαχωρισμός με βάση την λειτουργικότητα που καθορίζεται σε κάθε περιοχή, έτσι διακρίνουμε τα domain Customer και Utility.



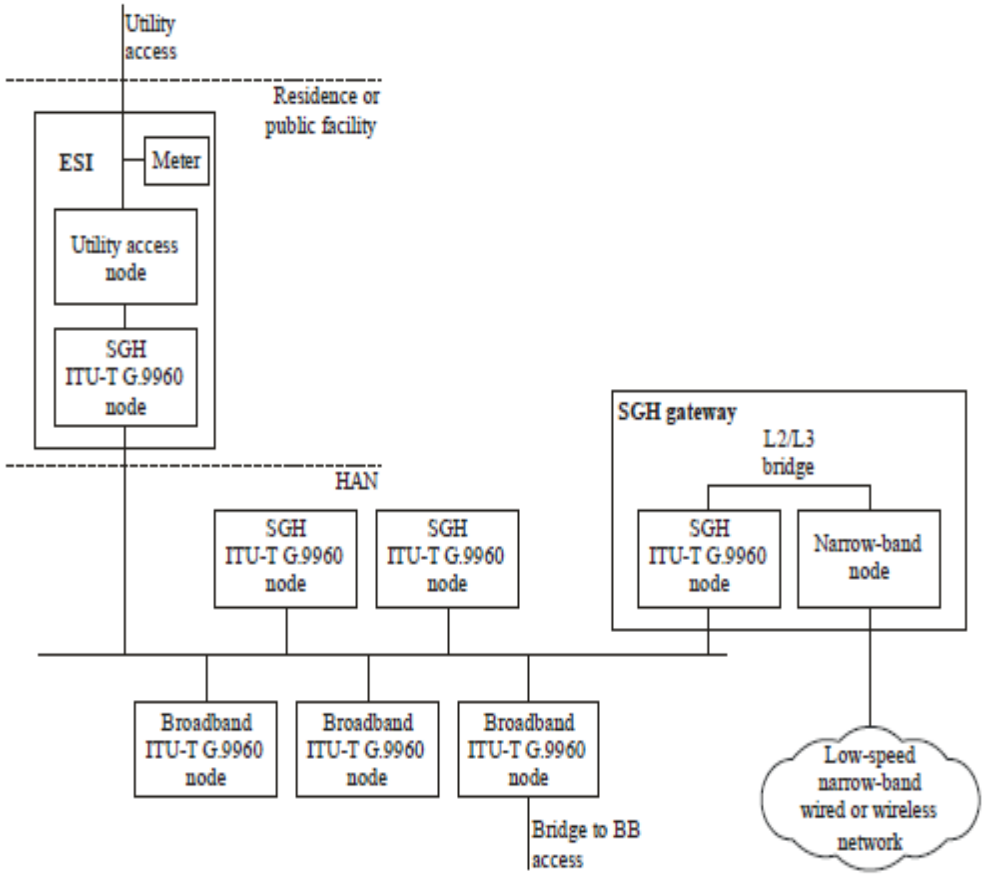
Εικόνα 35 "Δίκτυο βασισμένο στο πρότυπο G.hnem" (Rossello-Busquet, 2012)

Οι τεχνολογίες που παρουσιάστηκαν όπως είδαμε και ανήκουν στην κατηγορία των NB-PLC και παρουσιάζουν σχετικά μικρούς ρυθμούς μετάδοσης δεδομένων, στην κατηγορία των BB-PLC, υπάρχουν πρότυπα που έχουν σχεδιαστεί να προσφέρουν ρυθμούς μετάδοσης της τάξης αρκετών mbps και η χρήση τους αφορά κυρίως εσωτερική χρήση. Στην προσπάθεια προτυποποίησης αυτή ενεργό ρόλο έχουν η IEEE και ITU. Η πρώτη με το πρότυπο IEEE 1901 και η δεύτερη με το ITU-T G.hn. Το IEEE 1901, λειτουργεί σε δίκτυα χαμηλής και μεσαίας τάσης σε συχνότητες από 2 μέχρι 30MHz. Για την πρόσβαση στο φυσικό μέσο υπάρχουν δύο τρόποι, ο πρώτος είναι με χρήση της τεχνικής OFDM και ο άλλος είναι με την χρήση τεχνικής διαμόρφωσης Wavelet, η οποία έχει αναπτυχθεί από τον οργανισμό HomePlug Powerline Alliance για την μετάδοση δεδομένων κάτω από 100MHz. (Galli S, 2011)

Με τον πρώτο τρόπο παρέχεται υποστήριξη για συμβατότητα με συσκευές που ακολουθούν της προδιαγραφές του HomePlug AV, ενώ με τον δεύτερο για συσκευές που ακολουθούν τις προδιαγραφές του οργανισμού HD-PLC Alliance. Στο (Rahman M.M, 2011) παρουσιάζονται αναλυτικά και γίνεται σύγκριση των χαρακτηριστικών ανάμεσα στα δύο πρότυπα το IEEE P1901 και το ITU-T G.hn. Η οργάνωση του δικτύου και στα δύο πρότυπα μοιάζει, ειδικότερα το IEEE P1901, καθορίζει υποδίκτυα που αναφέρονται ως Basic Service Set(BSS) και διαχειριστής είναι ο BSS Manager, που συνδέεται με τους σταθμούς/Stations. Όπως αναφέρθηκε το IEEE P1901 υποστηρίζει δύο τρόπους πρόσβασης στο μέσο, για την σωστή ταυτόχρονη λειτουργία και των δύο υπάρχει ένας μηχανισμός που χρησιμοποιούν οι συσκευές που υποστηρίζουν το πρότυπο αυτό το οποίο ονομάζεται Inter-System Protocol(ISP). (Lars Torsten Berger, 2013). Τέλος, να αναφερθεί ότι ο ρυθμός μετάδοσης δεδομένων ανέρχεται το λιγότερο σε 100Mbps με την υλοποίηση του ISP μηχανισμού, ενώ με κατάλληλες παραμετροποιήσεις στο MAC και φυσικό επίπεδο μπορεί να φτάσει τα 200Mbps. (Galli S, 2011). Το δεύτερο πρότυπο με την ονομασία ITU-T G.hn, μοιάζει αρκετά με το πρότυπο της IEEE. Έχει σχεδιαστεί, για την broadband επικοινωνία για το HAN. Λειτουργεί σε συχνότητες από 2MHz μέχρι 100MHz και χρησιμοποιεί την τεχνική OFDM. Η αρχιτεκτονική και χαρακτηριστικά του ITU-T G.hn καθορίζονται από άλλα δύο πρότυπα του οργανισμού ITU, το G.9960/G.9961. Παρόμοιο μηχανισμό με τον ISP του IEEE P1901 διαθέτει και το G.hn ο οποίος έχει πιστοποιηθεί από το ITU G.9972. Λειτουργεί μοιάζοντας τον χρόνο σε ίσα τμήματα για τον τρόπο πρόσβασης στο ίδιο μέσο.

Και οι δύο αυτοί μηχανισμοί αναφέρονται ως μηχανισμοί συνύπαρξης. Με το G.9960 καθορίζεται το φυσικό επίπεδο και η πρόσβαση σε αυτό ενώ με το G.9961 καθορίζεται το δεύτερο επίπεδο(Data Link). Η αρχιτεκτονική δικτύου του G.hn βασίζεται στην λογική των domain. Ειδικότερα, κάθε δίκτυο αποτελείται από ένα ή και περισσότερα domain και κάθε ένα από αυτά διαχειρίζεται από τον Domain Master(DM). Επιπλέον, οι κόμβοι μπορούν να επικοινωνούν μεταξύ τους ακόμη και εάν ανήκουν σε διαφορετικό domain με την χρήση γεφυρών, που ονομάζονται InterDomain Bridge(IDB) με την χρήση πρωτοκόλλων τρίτου επιπέδου και πάνω.

Αριθμητικά, ένα domain έχει την δυνατότητα να υποστηρίξει από 32 κόμβους μέχρι 250. Ο κύριος λόγος σχεδίασης του προτύπου αυτού είναι η παροχή επικοινωνίας μέσα από υφιστάμενα μέσα όπως είναι ενσύρματα οικιακά δίκτυα, δικτύου ηλεκτρικής ενέργειας αλλά και τηλεφωνικά καλώδια. (Rahman M.M, 2011) Ο οργανισμός ITU-T στο (ITU, Unified high-speed wireline-based home networking transceivers – System architecture and physical layer specification, Recommendation ITU-T G.9960, 2011) παρουσιάζει περισσότερες πληροφορίες σχετικά με την εφαρμογή του G.9960 στα ευφυή δίκτυα ενέργειας, όπως την δυνατότητα διασύνδεσης ενός HAN που βασίζεται στο G.hn με ένα δίκτυο που βασίζεται σε NB-PLC προς το NAN. Το πλεονέκτημα της εφαρμογής ενός τέτοιου δικτύου διαφορετικής τεχνολογίας, είναι ότι οι τεχνολογίες NB-PLC προσφέρουν μεγάλη ακτίνα λειτουργίας. Ακόμη, το ενδεχόμενο παρεμβολών μειώνεται δραματικά μιας και το G.hn λειτουργεί σε συχνότητες μεγαλύτερες των 2MHz, ενώ πολλές τεχνολογίες NB-PLC λειτουργούν κάτω από τα 500KHz.



Εικόνα 36 "Διασύνδεση HAN βασισμένου στο G.hn πρότυπο με δίκτυο Narrowband" (ITU, Unified high-speed wireline-based home networking transceivers – System architecture and physical layer specification, Recommendation ITU-T G.9960, 2011)

Ένα από τα γνωστότερα πρότυπα που ανήκουν στην κατηγορία των BB-PLC, είναι το HomePlug, με τις διάφορες εκδόσεις του, που έχουν αναπτυχθεί από τον οργανισμό HomePlug Powerline Alliance. (Zyren, 2011) Ο οργανισμός αυτός βλέποντας, την ανάπτυξη των ευφυών δικτύων ενέργειας και την εισχώρηση των PLC τεχνολογιών, σχεδίασε και ανέπτυξε μια νέα έκδοση HomePlug το 2010 για την κάλυψη των επικοινωνιακών απαιτήσεων των HAN με μειωμένο κόστος και κατανάλωσης ενέργειας. Το νέο πρότυπο με την ονομασία HomePlug Green PHY, παρέχει μείωση κόστους εγκατάστασης και κατανάλωσης μέχρι 75% σε σχέση με το πρότυπο HomePlug AV/IEEE 1901, παρέχοντας συμβατότητα, τον ίδιο βαθμό αξιοπιστίας αλλά και κάλυψη.

Οι απαιτήσεις ενός HAN καλύπτονται με ρυθμούς μετάδοσης μικρότερους από τους ευρυζωνικούς των 200Mbps, άρα συσκευές ενός HAN, όπως θερμοστάτες, οικιακές συσκευές, αλλά και ηλεκτρικά οχήματα που υποστηρίζει για σύνδεση το πρότυπο αυτό, καλύπτονται από το ρυθμό μετάδοσης που παρέχει το HomePlug Green PHY μέχρι 10Mbps. Το πρότυπο αυτό καθορίζει τα δύο χαμηλότερα επίπεδα, δηλαδή το φυσικό επίπεδο το MAC επίπεδο, ενώ τα υψηλότερα επίπεδα δικτύου και μεταφοράς, καλύπτονται από πρωτόκολλα όπως είναι το TCP/IP. Η συχνότητα λειτουργία του προτύπου καλύπτει το εύρος από 1.8 μέχρι 30MHz και χρησιμοποιείται η τεχνική OFDM, ενώ για την ανίχνευση και την διόρθωση των λαθών που δημιουργήθηκαν κατά την μετάδοση εφαρμόζεται η τεχνική Turbo Code, ένα είδος Forward Error Correction (FEC) και ως αποτέλεσμα περιορίζονται οι περιπτώσεις που απαιτείται επαναποστολή των δεδομένων από τον αποστολέα.

Ακόμη, για την καλύτερη αξιοπιστία και μικρό ρυθμό μετάδοσης δεδομένων χρησιμοποιείται η τεχνική Robust OFDM, η οποία είναι μια τεχνική προαποστολής για την υποστήριξη του ρυθμού μετάδοσης που επιτυγχάνει το πρότυπο αυτό. Με την τεχνική αυτή, ο ρυθμός μετάδοσης επιτυγχάνεται σε σχέση με το βαθμό που απαιτείται για επαναποστολή δεδομένων. Είναι όμως κατανοητό όμως ότι η επαναποστολή δεδομένων εισάγει ένα βαθμό αναποτελεσματικότητας, αλλά από την άλλη μεριά η εφαρμογή της διαδικασίας αυτής προσφέρει πλεονεκτήματα. Λόγω παρεμβολών υπάρχει περίπτωση το σήμα, να φτάνει στον παραλήπτη και με αυτό τον τρόπο να μην λαμβάνονται δεδομένα χωρίς να δημιουργείται σφάλμα παράδοσης, ώστε να ενημερωθεί ο αποστολέας. Η τεχνική αυτή έχει αποδειχθεί αποτελεσματική κάτω από τις περισσότερες συνηθισμένες συνθήκες εφαρμογής. Στο MAC επίπεδο, χρησιμοποιεί την τεχνική CSMA/CA και η διαχείριση γίνεται με beacon frame. Κάθε δίκτυο διαθέτει ένα συντονιστή(Coordinator), ένα σταθμό ο οποίος είναι υπεύθυνος για την αρχικοποίηση και την διαχείριση του δικτύου. Για την μείωση της κατανάλωσης ενέργειας των συσκευών το οποίο αποτελεί σημαντικό παράγοντα σε ένα ευφυές δίκτυο ενέργειας, έχει αναπτυχθεί μια διαδικασία κατάστασης εξοικονόμησης ενέργειας/αναμονής με την ονομασία Power Saving Mode. Κάθε συσκευή, βρίσκεται στην κατάσταση αυτή, και όταν θέλει να αποστείλει ή να λάβει δεδομένα, διέρχεται σε μια άλλη κατάσταση κατά την οποία είναι πλήρως λειτουργική, η κατάσταση αυτή ονομάζεται Awake State.

Για την καλύτερη διαχείριση των εναλλαγών αυτών των καταστάσεων και το συγχρονισμό μεταξύ αποστολέα και παραλήπτη, πριν κάθε εισαγωγή σε κατάσταση αναμονής στέλνεται ένα μήνυμα αιτήματος προς το διαχειριστή του δικτύου(Coordinator), ώστε να απαντήσει θετικά ή αρνητικά για την αλλαγή της κατάστασης. Η διαδικασία αυτή, είναι απαραίτητη, γιατί σε περίπτωση που ένας σταθμός ήθελε να στείλει δεδομένα και ο παραλήπτης ήταν σε κατάσταση αναμονής, τότε δεν θα λάμβανε ποτέ τα δεδομένα αυτά. (Alliance H. P., HomePlug Green PHY 1.1, The Standard for In-Home Smart Grid Powerline Communications: An application and technology overview, 2012)

ΕΠΙΛΟΓΟΣ

Οι δύο κυρίαρχες ενσύρματες τεχνολογίες στα ευφυή δίκτυα ενέργειας είναι οι οπτικές ίνες και τα PLC. Και οι δύο τεχνολογίες παρουσιάζουν τις ιδιαιτερότητες τους αλλά έχουν αρκετές προοπτικές εφαρμογής στα ευφυή δίκτυα ενέργειας. Η πρώτη, με την υλοποίηση δικτύου βασισμένο στο PFTTH και η δεύτερη με την χρήση του δικτύου μεταφοράς ηλεκτρικής ενέργειας σε συνδυασμό με τα πρότυπα και πρωτόκολλα που έχουν σχεδιασθεί με γνώμονα την εφαρμογή στα ευφυή δίκτυα ενέργειας. Μέχρι στιγμής, έχουμε μελετήσει τις ασύρματες και ενσύρματες τεχνολογίες επικοινωνίας που μπορούν να χρησιμοποιηθούν στα ευφυή δίκτυα ενέργειας για την κάλυψη των αναγκών στο WAN, NAN και HAN. Για την αξιόπιστη λειτουργία ενός ολοκληρωμένου δικτύου επικοινωνιών απαιτείται η προστασία των υποδομών, των επικοινωνιών και των δεδομένων που διακινούνται. Κάθε μεγάλου εύρους υποδομές, παρουσιάζουν ευπάθειες και απειλές, συνεπώς η ασφάλεια στα ευφυή δίκτυα ενέργειας είναι ιδιαίτερα σημαντική, μιας και σχετίζεται με την παροχή ενέργειας. Στα επόμενα κεφάλαια θα μελετήσουμε, τα ευφυή δίκτυα ενέργειας από την σκοπιά της ασφάλειας με στόχο όλα τα μέτρα που πρέπει να ληφθούν για την προστασία τους και σύμφωνα με τις τελευταίες εξελίξεις στο χώρο.

ΚΕΦΑΛΑΙΟ 5

ΑΣΦΑΛΕΙΑ ΣΤΑ ΕΥΦΥΗ ΔΙΚΤΥΑ ΕΝΕΡΓΕΙΑΣ

ΕΙΣΑΓΩΓΗ

Τα ευφυή δίκτυα ενέργειας εισάγουν νέες λειτουργίες στα υπάρχον δίκτυα παραγωγής, μεταφοράς και διανομής ηλεκτρικής ενέργειας. Από την άλλη μεριά, εισάγονται και νέες προκλήσεις από την μεριά της ασφάλειας, γιατί είναι γνωστό ότι η παροχή ηλεκτρικής ενέργειας μέσω ενός δικτύου είναι κρίσιμης σημασίας. Με αυτό τον τρόπο η ασφάλεια ως γενικός όρος στα ευφυή δίκτυα ενέργειας αποτελεί καθοριστική σημασία. Τα θέματα που σχετίζονται με την ασφάλεια αφορούν καίρια σημεία όπως είναι οι απαιτήσεις επικοινωνίας, οι αυτοματισμοί συστημάτων, οι νέες τεχνολογίες που χρησιμοποιούνται αλλά και τα δεδομένα που ανταλλάσσονται στα δίκτυα επικοινωνιών που διαθέτει κάθε ευφυής δίκτυο ενέργειας. Η δικτύωση διαφορετικών υποσυστημάτων, αυξάνει την πολυπλοκότητα και ως αποτέλεσμα αυξάνεται ο βαθμός των πιθανών ευπαθειών που ενδέχεται να εμφανιστούν κατά την λειτουργία. Σε αυτό συμβάλει και ο μεγάλος αριθμός πυλών πρόσβασης στο δίκτυο επικοινωνιών (ένας έξυπνος μετρητής). Επιπλέον, η εφαρμογή διαφορετικών τεχνολογιών επικοινωνίας, αυξάνει και αυτή τον αριθμό των πιθανών ευπαθειών συνολικά. Στα προηγούμενα κεφάλαια έχει αναφερθεί ότι ο παράγοντας καθυστέρηση έχει πολύ σημαντικό ρόλο στην λειτουργία κάποιων υποδομών που απαιτούν real time επικοινωνία. Οπότε, ενδεχόμενα προβλήματα που μπορούν να δημιουργηθούν από κακόβουλες ενέργειες, έχουν ως στόχο την δημιουργία καθυστέρησης αλλά και παραποίησης δεδομένων που διακινούνται στο δίκτυο επικοινωνιών ενός ευφυούς δικτύου ενέργειας. Υπάρχουν όμως και απειλές που σχετίζονται εκτός από τα δεδομένα που διακινούνται και με την φυσική ασφάλεια των υποδομών, που έχουν ως αποτέλεσμα μέχρι και την μερική ή ολική διακοπή της λειτουργίας ενός ευφυούς δικτύου ενέργειας. Μια άλλη κατηγορία απειλών, είναι η κυβερνό-απειλές που εμφανίζονται στην βιβλιογραφία ως ένα αντικείμενο μελέτης για τα ευφυή δίκτυα ενέργειας. Οι κυβερνό-απειλές, έχουν ως στόχο την απόκτηση προσβασιμότητας από κακόβουλους χρήστες κυρίως στα δίκτυα NAN και HAN, ώστε να θέσουν σε έλεγχο συσκευές, για την υποκλοπή δεδομένων, την παραποίηση δεδομένων αλλά και γενικότερα την δημιουργία ανεπιθύμητων καταστάσεων στα παραπάνω δίκτυα ώστε να εμφανιστούν προβλήματα στις λειτουργία τους. Όπως, κάθε κρίσιμη υποδομή ένα ευφυές δίκτυο ενέργειας, αναμένεται να είναι ένας δελεαστικός στόχος για κακόβουλους χρήστες. Είναι απαραίτητο να ληφθούν μέτρα αντιμετώπισης, ώστε να διαφυλαχθεί σε όσο μεγαλύτερο βαθμό γίνεται η λειτουργία ενός ευφυούς δικτύου ενέργειας.

5.1 ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΕΥΦΥΩΝ ΔΙΚΤΥΩΝ ΕΝΕΡΓΕΙΑΣ

Οι κύριοι στόχοι της ασφάλειας στα ευφυή δίκτυα ενέργειας, διαφέρουν από αντίστοιχές μεγάλης κλίμακας υποδομές. Είναι σημαντικό, ότι για κάθε μέτρο προστασίας που λαμβάνεται, ο όρος της διαθεσιμότητας είναι καθοριστικός. Ειδικότερα, υπάρχουν τρεις όροι που σχετίζονται με τους γενικούς στόχους που θέτονται για την ασφάλεια στα ευφυή δίκτυα ενέργειας. Αυτοί είναι, η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Να σημειωθεί ότι ο NIST, παρέχει οδηγίες για την προστασία των ευφυών δικτύων ενέργειας, βασιζόμενος πάνω σε αυτούς τους όρους. (Group h. S.–C., 2010) Στις περισσότερες μεγάλου μεγέθους υποδομές παροχής υπηρεσιών, όπως είναι ένα ευφυές δίκτυο ενέργειας, το οποίο παρέχει εξελιγμένες υπηρεσίες στους καταναλωτές, η εμπιστευτικότητα και η ακεραιότητα υπερέχουν σε σχέση με την διαθεσιμότητα. Το αντίθετο συμβαίνει όμως σε συστήματα τα οποία σχετίζονται με την παροχή ενέργειας, όπως είναι ένα ευφυές δίκτυο ενέργειας, όπου ο όρος διαθεσιμότητα υπερέχει έναντι των άλλων δύο. Από την άλλη μεριά, το παραπάνω δεν είναι ο γενικός κανόνας, γιατί ενδέχεται σε κάποια σημεία εντός ενός ευφυούς δικτύου ενέργειας, η εμπιστευτικότητα να υπερέχει έναντι των άλλων βασικών αρχών.

1. Διαθεσιμότητα δικτύου

Η διαθεσιμότητα του δικτύου αναφέρεται στην διασφάλιση ότι μη εξουσιοδοτημένα πρόσωπα ή ενέργειες δεν θα περιορίσουν την πρόσβαση στο δίκτυο σε εξουσιοδοτημένους χρήστες. Ο όρος αυτός συσχετίζεται με όλο τον εξοπλισμό και τις υπηρεσίες που ανήκουν στο κομμάτι του IT. Κακόβουλές ενέργειες έχουν ως στόχο να πλήξουν την διαθεσιμότητα του δικτύου επικοινωνιών με σκοπό την δημιουργία λειτουργικών προβλημάτων σε μέρος ή σε ολόκληρο τμήμα ενός ευφυούς δικτύου ενέργειας. Αυτού του τύπου οι ενέργειες μπορούν να καθοριστούν ως επιθέσεις άρνησης υπηρεσιών(Denial Of Service) ώστε να καθυστερήσουν, ή να μπλοκάρουν πληροφορίες να φτάσουν στο παραλήπτη τους αλλά και να θέσουν εκτός λειτουργίες λόγου φόρτου πόρους δικτύου(συσκευές). Στα προηγούμενα κεφάλαια έχει αναφερθεί πόσο σημαντικός είναι ο παράγοντας καθυστέρηση στην επικοινωνία ανάμεσα στα διάφορα τμήματα ενός ευφυούς δικτύου ενέργειας. Με αυτό τον τρόπο μπορεί να συνδεθεί ο όρος διαθεσιμότητα και με τις απαιτήσεις καθυστέρησης που πρέπει να ικανοποιούνται ώστε να χαρακτηρίζεται το δίκτυο με τον όρο αυτό. Συνεπώς, πληροφορίες που φτάνουν καθυστερημένες πολλές φορές θεωρούνται άχρηστες. (Ye Yan, A Survey on Cyber Security for Smart Grid Communications, 2012)

2. Ακεραιότητα δεδομένων

Η ακεραιότητα ως όρος αναφέρεται στην πρόληψη ανεπιθύμητης παραποίησης δεδομένων ή πληροφοριών από μη εξουσιοδοτημένους χρήστες ή συστήματα. Για τα ευφυή δίκτυα ενέργειας η ακεραιότητα σχετίζεται με όλα τα δεδομένα που διακινούνται στο δίκτυο επικοινωνιών, αλλά και τα δεδομένα όπως αυτά λαμβάνονται από συσκευές όπως είναι οι έξυπνοι μετρητές, συλλέκτες δεδομένων

στα NAN, αλλά και δεδομένα που συλλέγονται από αισθητήρες και διάφορες συσκευές που σχετίζονται με την κατάσταση του δικτύου ενέργειας. Παραβίαση της ακεραιότητας επηρεάζει την λειτουργία του δικτύου, και οδηγεί σε λανθασμένες αποφάσεις σχετικά με την πραγματική κατάσταση του δικτύου ή μέρους του δικτύου. Συνήθως, επίκεντρο για την παραβίαση του όρου αυτού είναι τα δεδομένα που σχετίζονται με την τιμή της ενέργειας, μια δεδομένη χρονική στιγμή.

3. Εμπιστευτικότητα

Η εμπιστευτικότητα αναφέρεται στην προστασία των δεδομένων από πρόσβαση σε μη-εξουσιοδοτημένους χρήστες ακόμη και μέσα στο ίδιο ευφυές δίκτυο ενέργειας. Χαρακτηριστικό παράδειγμα, είναι τα δεδομένα κάθε HAN, που συλλέγονται από τους έξυπνους μετρητές ενέργειας και αφορούν μετρήσεις και κόστος κατανάλωσης ενέργειας. Στα δεδομένα αυτά, δεν θα πρέπει να έχει πρόσβαση κάποιος χρήστης από άλλο HAN. (Wenye Wang Z. L., 2013) (Emiliano Pallotti, 2011)

Η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα είναι οι τρεις υψηλού επιπέδου κύριοι στόχοι της ασφάλειας στα ευφυή δίκτυα ενέργειας. Ο NIST στο (Group h. S.–C., 2010) προτείνει συγκεκριμένες απαιτήσεις ασφαλείας που χωρίζονται σε δύο κατηγορίες. Μία της φυσικής ασφάλειας των υποδομών, που αναφέρεται στην προστασία του υλικού, δηλαδή το σύνολο του εξοπλισμού που χρησιμοποιείται σε ένα ευφυές δίκτυο ενέργειας για την επικοινωνία, αλλά δεύτερον στην κυβερνό-ασφάλεια. Η κυβερνό-ασφάλεια, εστιάζει στην προστασία των δεδομένων αλλά και των επικοινωνιακών συστημάτων. Συνοψίζοντας τις παραπάνω οδηγίες έχουμε:

1. Ανίχνευση απειλών

Τα ευφυή δίκτυα ενέργειας διαθέτουν μεγάλης γεωγραφικής έκτασης δίκτυο επικοινωνιών που καλύπτει σχεδόν ολόκληρο το δίκτυο παροχής ενέργειας. Συνεπώς, είναι αδύνατον να υπάρξει η διασφάλιση ότι κάθε σημείο του δικτύου είναι προστατευμένο από δικτυακές επιθέσεις. Στο δίκτυο επικοινωνίας είναι απαραίτητο να πραγματοποιούνται έλεγχοι, δοκιμές και παρακολούθηση της κίνησης του δικτύου σχετικά με την κίνηση του δικτύου ώστε να ανιχνεύονται και να αναγνωρίζονται εγκαίρως μη φυσιολογικά περιστατικά. Συνήθως, τα παραπάνω αναγνωρίζονται ως αυξημένη κίνηση δεδομένων στο δίκτυο επικοινωνιών ή σε κάποιο συγκεκριμένο τμήμα αυτού. Επιπλέον, κάθε δίκτυο επικοινωνιών είναι απαραίτητο να διαθέτει την ικανότητα της αυτό-ανάρρωσης(self-healing) σε περίπτωση επίθεσης λόγω της κρισιμότητας που έχει η παροχή ενέργειας, εξασφαλίζοντας της διαθεσιμότητα σε όλο το δίκτυο.

2. Ταυτοποίηση, αυθεντικοποίηση και έλεγχος πρόσβασης

Η συνολική υποδομή σε κάθε ευφυές δίκτυο ενέργειας διαθέτει εκατομμύρια ηλεκτρονικές συσκευές που διαθέτουν ικανότητα επικοινωνίας. Η ταυτοποίηση και η εξουσιοδότηση είναι τα δύο βασικά χαρακτηριστικά για την αναγνώριση κάθε συσκευής ή χρήστη για την πρόσβαση στο δίκτυο επικοινωνιών. Ο έλεγχος

πρόσβασης εστιάζει στην διασφάλιση ότι πρόσβαση σε συγκεκριμένους πόρους έχουν μόνο οι συσκευές ή οι χρήστες που έχουν αναγνωριστεί μέσω συγκεκριμένων διαδικασιών. Αυστηρός έλεγχος πρόσβασης είναι απαραίτητος να υλοποιηθεί ώστε να υπάρχει πρόληψη για τον περιορισμό ένας μη-εξουσιοδοτημένος χρήστης να έχει πρόσβαση σε δεδομένα και συστήματα. Για να καλυφθούν οι παραπάνω απαιτήσεις, κάθε συσκευή που είναι συνδεδεμένη στο δίκτυο επικοινωνιών είναι απαραίτητο να διαθέτει τουλάχιστον κάποιες βασικές λειτουργίες κρυπτογράφησης, όπως είναι συμμετρική ή ασύμμετρη κρυπτογράφηση, για κρυπτογράφηση δεδομένων και αυθεντικοποίηση.

3. Ασφαλή και αποτελεσματικά πρωτόκολλα επικοινωνιών

Διαφέροντας από τα κοινά δίκτυα επικοινωνιών, η παράδοση μηνυμάτων θεωρείται κρίσιμη ως προς τον χρόνο και την ασφάλεια. Ένα δίκτυο επικοινωνιών ή μέρος αυτού, δεν μπορεί πάντα να είναι προστατευμένο από κάθε απειλή, ούτε μπορεί να είναι υψηλού ρυθμού μετάδοσης σε κάθε σημείο του. Είναι απαραίτητο, να βρεθεί η ισορροπία ανάμεσα στην απόδοση του δικτύου και στην ασφάλεια που απαιτείται κατά την σχεδίαση του δικτύου και το πρωτοκόλλων που υλοποιούνται. (Wenye Wang Z. L., 2013) (Yilin Mo, 2012)

5.2 ΑΠΕΙΛΕΣ ΣΤΑ ΕΥΦΥΗ ΔΙΚΤΥΑ ΕΝΕΡΓΕΙΑΣ

Τα ευφυή δίκτυα ενέργειας λόγω της κρισιμότητας της υποδομής τους και του σκοπού λειτουργίας τους, να παρέχουν ενέργεια, όπως είναι φυσικό εστιάζουν την προσπάθεια κακόβουλων χρηστών για τέτοιου είδους ενέργειες. Ένα ευφυές δίκτυο ενέργεια όπως είναι κατανοητό διαθέτει ένα περίπλοκο δίκτυο επικοινωνιών με εκατομμύρια συσκευές οι οποίες επικοινωνούν μεταξύ τους. Η προσπάθεια κατηγοριοποίησης των επιθέσεων είναι μια μεγάλη πρόκληση λόγου του μεγέθους και της πολυπλοκότητας του δικτύου επικοινωνιών. Είναι όμως απαραίτητη για την κατανόηση και την πρόληψη με τους απαραίτητους μηχανισμούς ώστε να αποφευχθούν απρόβλεπτες συνέπειες στην λειτουργία των ευφυών δικτύων ενέργειας. Οι απειλές λόγω της πολυπλοκότητας που παρουσιάζουν οι υποδομές των ευφυών δικτύων ενέργειας, μπορούν να ταξινομηθούν σε διάφορες κατηγορίες αναλόγως από την πλευρά που μελετιούνται. Ο γενικότερος διαχωρισμός τους είναι σε φυσικές απειλές και κυβερνό-απειλές. Η πρώτη κατηγορία, σχετίζεται με τις απειλές στην δικτυακή υποδομή ενός ευφυούς δικτύου ενέργεια από παράγοντες όπως είναι επικίνδυνα καιρικά φαινόμενα (σεισμοί, πλημμύρες κτλ), όπου δεν συμμετέχει ο ανθρώπινος παράγοντας. Στην δεύτερη κατηγορία, οι απειλές σχετίζονται με την εκμετάλλευση αδυναμιών των υποδομών και των τεχνολογιών που χρησιμοποιούνται από κακόβουλους χρήστες. Έκτος από το παραπάνω διαχωρισμό, στο (Daojing He, 2012) οι επιθέσεις χωρίζονται σε δύο κατηγορίες τις ενεργές επιθέσεις και τις παθητικές επιθέσεις. Στις παθητικές επιθέσεις, ανήκουν οι επιθέσεις που απειλούν της εμπιστευτικότητα των δεδομένων που διακινούνται στο δίκτυο. Ενώ, στην δεύτερη κατηγορία ανήκουν οι επιθέσεις που απειλούν την διαθεσιμότητα, την εξουσιοδότηση και την

ακεραιότητα των δεδομένων που θεωρούνται κρισιμότερες. Είναι κατανοητό ότι υπάρχουν πολλές διαφορετικές κατηγοριοποιήσεις αναλόγως την σκοπιά που μελετιούνται. Από την άλλη μεριά, με το καθορισμό των τριών βασικών αρχών από το NIST, έμφαση δίνεται στην κατηγοριοποίηση με βάση την αρχή που προσβάλει κάθε επίθεση, μιας και ένα τύπος επίθεσης μπορεί να προσβάλει πολλά διαφορετικά σημεία σε ένα ευφυές δίκτυο ενέργειας, παραβιάζοντας την ίδια βασική αρχή. Παρακάτω, η κατηγοριοποίηση γίνεται με βάση τις τρείς βασικές αρχές που αναφέρθηκαν στο προηγούμενο υποκεφάλαιο.

1. Επιθέσεις που έχουν στόχο την διαθεσιμότητα, είναι επιθέσεις τύπου DoS, με στόχο να καθυστερήσουν, να μπλοκάρουν ή να διακόψουν κάποιο κανάλι επικοινωνίας.
2. Επιθέσεις που έχουν στόχο την ακεραιότητα των δεδομένων στοχεύουν στην παραποίηση των δεδομένων που διακινούνται στο δίκτυο.
3. Επιθέσεις που στοχεύουν στην εμπιστευτικότητα επικεντρώνονται στην μη-εξουσιοδοτημένη πρόσβαση σε δικτυακούς πόρους και δεδομένα.

Όπως έχει αναφερθεί στα προηγούμενα κεφάλαια, το δίκτυο επικοινωνιών καλύπτει το μεγαλύτερο τμήμα λειτουργίας ενός ευφυούς δικτύου, που αποτελείται κυρίως από τα συστήματα παραγωγής ενέργειας, το δίκτυο μεταφοράς, το δίκτυο διανομής και τέλος τους καταναλωτές. Για την καλύτερη μελέτη των ευπαθειών και των απειλών είναι καλό κάθε τμήμα να μελετηθεί ξεχωριστά βασιζόμενοι πάντα στις τρεις παραπάνω βασικές αρχές. (Wenye Wang Z. L., 2013) Το τελευταίο διάστημα οι ερευνητικές προσπάθειες εστιάζουν στις επιθέσεις τύπου DoS για κάθε επίπεδο του OSI ξεχωριστά.

Για το φυσικό επίπεδο, το Channel Jamming, είναι ένας από τους αποδοτικότερους τρόπους για DoS επιθέσεις, ειδικότερα για ασύρματα δίκτυα. Το μόνο που απαιτείται είναι ο κακόβουλος χρήστης να συνδεθεί και να εκπέμπει στο κανάλι που θέλει να μπλοκάρει, χωρίς να έχει εξουσιοδοτηθεί για πρόσβαση στο δίκτυο. Στο κανάλι δημιουργείται θόρυβο, και όταν ένα κόμβος πραγματοποιήσει έλεγχο σήματος πριν εκπέμψει ένα πακέτο το κανάλι φαίνεται σε χρήση. Αντίστοιχα ένα άλλος κόμβος δεν θα έχει την δυνατότητα για λήψη πακέτων. Αυτού του είδους η επίθεση έχει στόχο να πλήξει την διαθεσιμότητα ενός ασύρματου δικτύου. (Eun-Kyu Lee, Physical Layer Security in Wireless Smart Grid, 2012) Τα τοπικά ασύρματα δίκτυα έχουν μια ευρεία χρήση στα ευθεία δίκτυα ενέργειας και ειδικά σε κεντρικές υποδομές ύψιστης σημασίας για την παραγωγή ενέργειας, είναι κατανοητό ότι το παραπάνω μπορεί να οδηγήσει σε απρόβλεπτες καταστάσεις.

Στο MAC επίπεδο, ένας κακόβουλος χρήστης έχει την δυνατότητα να παραποιήσει στοιχεία ενός frame που μεταδίδεται, έχοντας με αυτό τον τρόπο μεγαλύτερες πιθανότητες για πρόσβαση στο δίκτυο. Η τεχνική του Spoofing, χρησιμοποιεί την δυνατότητα να χρησιμοποιήσει στο πεδίο διεύθυνσης της MAC διεύθυνσης ότι επιθυμεί, και ως αποτέλεσμα πραγματοποιεί μια επίθεση προσποίησης άλλης συσκευής ώστε να στείλει ψεύτικα δεδομένα σε άλλες

δικτυακές συσκευές. Παράδειγμα, σε ένα τοπικό δίκτυο μιας μονάδας παραγωγής ενέργειας ή ενός κέντρου διαχείρισης, ένας μολυσμένος κόμβος, μπορεί να κάνει broadcast Automatic Repeat Request(ARP) πακέτα ώστε να απενεργοποιήσει συσκευές τύπου IED που είναι υπεύθυνες για έλεγχο της κατάστασης του δικτύου ενέργειας μέσω αισθητήρων.

Αντίστοιχα στα επίπεδα δικτύου και μεταφοράς, το πιο γνωστό πρότυπο που χρησιμοποιείται είναι το TCP/IP, συνδυασμένο με το IEC 61850, που είναι το πιο ευρέως αποδεκτό πρότυπο για τα ευφυή δίκτυα ενέργειας. Το TCP/IP είναι γνωστό από την χρήση του σε τοπικά δίκτυα αλλά και το διαδίκτυο ότι είναι ευάλωτο σε επιθέσεις DoS. Στα ευφυή δίκτυα ενέργειας, μια τέτοιου είδους επίθεση μας ενδιαφέρει από την ζημιά που προκαλεί στην καθυστέρηση παράδοσης των μηνυμάτων και όχι από την μείωση του ρυθμού μετάδοσης δεδομένων λόγω του φόρτου στο δίκτυο. Να σημειωθεί, ότι οι απαιτήσεις καθυστέρησης για το IEC 61850, είναι της τάξεως κάτω των 8ms και ότι ο παράγοντας χρόνος είναι πολύ κρίσιμος για την σωστή λειτουργία του δικτύου.

Στο (Zhuo Lu, 2010) δίνεται έμφαση στην μελέτη των DoS επιθέσεων σε κεντρικές υποδομές παραγωγής ενέργειας και μέσω δοκιμών παρουσιάζονται τα αποτελέσματα. Το πρωτόκολλο που χρησιμοποιείται είναι το DNP3, ένα από τα πιο διαδεδομένα σε χρήση για επικοινωνία σε υποσταθμούς των ευφυών δικτύων ενέργειας. Λειτουργεί σε αρχιτεκτονική Master-Slave και χρησιμοποιείται για την επικοινωνία ανάμεσα στα κέντρα διαχείρισης και IED. Το κέντρο διαχείρισης εκκινεί την σύνδεση και στέλνει εντολές στις IED, και αυτές με την σειρά τους απαντούν. Για την μέτρηση απόδοσης στο συγκεκριμένο σενάριο χρησιμοποιείται η καθυστέρηση round-trip, που ορίζεται ως ο χρόνος από την στιγμή που το κέντρο διαχείρισης θα στείλει ένα πακέτο DNP3, μέχρι να λάβει ένα πακέτο ACK. Ο στόχος της επίθεσης δεν είναι να αποκοπεί τελείως η επικοινωνία, αλλά να περιέλθει το δίκτυο σε τέτοια κατάσταση όπου η καθυστέρηση παράδοσης των μηνυμάτων να ξεπερνά τις προκαθορισμένες απαιτήσεις.

Τα συμπεράσματα που προκύπτουν είναι ότι όσο μικρότερο είναι το μέγεθος του πακέτου DNP3 τόσο το δίκτυο είναι ανθεκτικότερο σε επιθέσεις. Επιπλέον, με τα ίδια δεδομένα ένα δίκτυο βασισμένο στο Wi-Fi στα 54Mbps σε σχέση με ένα Ethernet 100Mbps, παρουσιάζει ελαφρώς μεγαλύτερη καθυστέρηση. Οι επιθέσεις DoS, στα κατώτερα επίπεδα έχουν ως στόχο κυρίως να πλήξουν το διαθέσιμο εύρος σε συγκεκριμένα κανάλια επικοινωνίας και δικτυακές συσκευές, ενώ στο επίπεδο εφαρμογών, αντίστοιχα στόχο έχουν να απασχολούν μεγάλο αριθμό υπολογιστικών πόρων(μνήμη ram, πόροι cpu κτλ) (Wenye Wang Z. L., 2013)

Συμπερασματικά, στα ευφυή δίκτυα ενέργειας, ο επιτιθέμενος που χρησιμοποιεί την τεχνική DoS, λόγω τις ευαισθησίας των λειτουργιών στο χρόνο δεν χρειάζεται να θέσει το δίκτυο εκτός λειτουργίας, αρκεί απλά να δημιουργήσει μια κατάσταση κατά την οποία παραβιάζονται οι απαιτήσεις που θέτονται από τα πρότυπα και τα πρωτόκολλα που χρησιμοποιούνται. Το παραπάνω, είναι κατανοητό πως είναι καταστροφικό για την λειτουργία ενός ευφυούς δικτύου ενέργειας.

Έκτος από τις επιθέσεις DoS που αναφέρθηκαν παραπάνω, υπάρχουν επιθέσεις που έχουν ως στόχο να πλήξουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Αυτού του είδους οι επιθέσεις στοχεύουν στην παραποίηση των δεδομένων χωρίς να γίνει αντιληπτό για να πετύχουν κυρίως την διακοπή συγκεκριμένων λειτουργιών σε ένα ευφυές δίκτυο ενέργειας. Ο στόχος μπορεί να είναι είτε δεδομένα που έχουν σχέση με τους καταναλωτές(κόστος ενέργειας, χρεώσεις καταναλωτών) είτε δεδομένα που έχουν σχέση με την λειτουργία του δικτύου ενέργειας(IED για την κατάσταση του δικτύου). Μία τέτοιου είδους επίθεση ανακαλύφθηκε με την ονομασία False Data Injection Attack. Η επίθεση αυτή σχεδιάστηκε με στόχο την εφαρμογή της πάνω σε κεντρικές υποδομές ενέργειας.

Στο (Wenye Wang Z. L., 2013) παρουσιάστηκε για πρώτη φορά η επίθεση αυτού του είδους και μελετάται η δυνατότητα ένας επιτιθέμενος αφού εισάγει λανθασμένα δεδομένα σε έξυπνους μετρητές, να καταφέρει να παραπλανήσει τα κεντρικά συστήματα που είναι υπεύθυνα για τις χρεώσεις ενέργειας των καταναλωτών. Επιπλέον, εκτός από δεδομένα σχετικά με το κόστος ενέργειας, οι επιθέσεις αυτού του είδους στοχεύουν και στην παραπλάνηση του δικτύου σχετικά με την κατάσταση του δικτύου μεταφοράς και διανομής ενέργειας, με σκοπό την δημιουργία διακοπών παροχής ενέργειας ή δημιουργία βλαβών σε τμήματα ή υποδομές του δικτύου ενέργειας. (Jie Lin, 2012) Αυτού του είδους οι επιθέσεις βρίσκονται ακόμα υπό μελέτη. Σε σχέση με τις παραπάνω επιθέσεις που έχουν ως στόχο να πλήξουν την ακεραιότητα, οι επιθέσεις που στοχεύουν στην εμπιστευτικότητα δεν έχουν σκοπό να παραποιήσουν τα δεδομένα, αλλά να τα υποκλέψουν. Όσο η εμπιστευτικότητα γίνεται σημαντικότερη ως στόχος για τα δεδομένα των καταναλωτών τόσο θα εξελίσσονται αυτού του είδους οι επιθέσεις.

Παραπάνω παρουσιάστηκαν οι απειλές και ευπάθειες στα ευφυή δίκτυα ενέργειας εστιάζοντας στα συστήματα παραγωγής ενέργειας και τις κεντρικές υποδομές διαχείρισης ενός ευφυούς δικτύου ενέργειας, που ανήκουν στο κομμάτι του WAN. Έκτος από τα παραπάνω τμήματα ένα ευφυές δίκτυο ενέργειας, διαθέτει και το κομμάτι του δικτύου μεταφοράς και διανομής ενέργειας με αντίστοιχο δίκτυο επικοινωνιών που εκφράζεται ως NAN, αλλά και το κομμάτι που ανήκει στα HAN με τους έξυπνους μετρητές ενέργειας.

Στο (Wenye Wang Z. L., 2013) μελετιούνται οι επιθέσεις που ανήκουν στο δίκτυο μεταφοράς και διανομής. Τα πρωτόκολλα που χρησιμοποιούνται εδώ συνήθως είναι το IEC 61850 σε συνδυασμό με TCP/IP και το DNP3. Διαχωρίζοντας τις επιθέσεις, έχουμε τις εσωτερικές επιθέσεις και τις εξωτερικές επιθέσεις. Στην πρώτη κατηγορία ανήκουν οι επιθέσεις που προέρχονται από την εσωτερική περίμετρο ενός υποσταθμού ενώ οι δεύτερη κατηγορία οι επιθέσεις προέρχονται εκτός του υποσταθμού. Οι επιθέσεις που ξεκινούν από το εσωτερικό συνήθως προέρχονται από κακόβουλο λογισμικό το οποίο έχει μολύνει υπολογιστικά συστήματα του υποσταθμού με στόχο την διαθεσιμότητα του δικτύου και την ακεραιότητα των δεδομένων που διακινούνται. Λόγω, το ότι οι επιθέσεις

αυτές συνήθως περνάνε απαρατήρητες μέχρι να εμφανισθούν οι πρώτες ενδείξεις είναι ιδιαίτερα επικίνδυνες.

Οι DoS επιθέσεις και εδώ θεωρούνται μία από της ευκολότερες να παρουσιαστούν, γιατί όπως αναφέρθηκε προηγουμένως συνήθως χρησιμοποιείται το πρωτόκολλο TCP/IP με την χρήση τεχνικών flooding tcp πακέτων. DoS επιθέσεις όμως ενδέχεται να εμφανιστούν και ως εξωτερικές επιθέσεις, προσβάλλοντας την πύλη-gateway του υποσταθμού με σκοπό να υπολειτουργεί ως προς τις ανάγκες του δικτύου. Είναι απαραίτητο να εφαρμόζονται αυστηρά ισχυρός έλεγχος πρόσβασης και πολιτικές ασφαλείας ώστε να προλαμβάνονται αυτού του είδους οι επιθέσεις.

Σε περίπτωση χρήσης ασύρματων τεχνολογιών είναι απαραίτητο να ληφθούν μέτρα για την αντιμετώπιση επιθέσεων με την τεχνική jamming. Να σημειωθεί ότι σε περίπτωση που υπάρχουν IED για την παρακολούθηση του δικτύου ενέργειας, εκτός περιμέτρου ενός υποσταθμού, έμφαση πρέπει να δοθεί και στην φυσική ασφάλεια των συσκευών αυτών, γιατί σε διαφορετική περίπτωση ενδεχόμενη πρόσβαση και σε συνδυασμό με την τεχνική false data attack, μπορεί το δίκτυο να οδηγηθεί σε λανθασμένες αποφάσεις από αποστολή παραπλανητικών δεδομένων που έχουν σταλεί από την συσκευή αυτή.

Παρουσιασθήκαν οι απειλές που αντιμετωπίζουν οι κεντρικές υποδομές και το δίκτυο διανομής ενέργειας με τους υποσταθμούς του, έκτος όμως από αυτά τα τμήματα, ένα ευφυές δίκτυο ενέργειας περιλαμβάνει έξυπνους μετρητές αλλά και τους συλλέκτες δεδομένων που συλλέγουν τα δεδομένα από κάθε έξυπνο μετρητή. Η ασφάλεια όμως δεν περιορίζεται μόνο στην επικοινωνία ανάμεσα στα δύο αυτά μέρη αλλά, περιλαμβάνει την ασφάλεια των δεδομένων που ανταλλάσσονται ανάμεσα στο ευφυές δίκτυο ενέργειας και στους έξυπνους μετρητές, την φυσικά ασφάλεια των έξυπνων μετρητών ενέργειας, αλλά και την επικοινωνία του έξυπνου μετρητή ενέργειας με συσκευές που υπάρχουν σε κάθε HAN. Η ακεραιότητα των δεδομένων που ανταλλάσσονται όπως και η εμπιστευτικότητα υπερτερεί σε σχέση με την διαθεσιμότητα του δικτύου, που στα υπόλοιπα τμήματα είναι πρώτη. Η αυθεντικοποίηση και η κρυπτογράφηση είναι βασικά στοιχεία που απαιτούνται για την κάλυψη των αναγκών αυτών. Στο (Sophia Kaplantzis, 2012) γίνεται καθορισμός των υποδομών που αποτελούν στόχο επιθέσεων για το Smart Metering, και τα οποία είναι:

1. Έξυπνοι μετρητές
2. Συλλέκτες δεδομένων
3. Δίκτυο επικοινωνίας
4. Κεντρικό σύστημα συλλογής δεδομένων

Έκτος από το τελευταίο τμήμα, το οποίο είναι υπεύθυνο για την συλλογή των δεδομένων από τους έξυπνους μετρητές και ανήκει στο κέντρο διαχείρισης του ευφυούς δικτύου ενέργειας, τα υπόλοιπα ανήκουν στα δίκτυα NAN και HAN και συνεπώς το ενδιαφέρον από πλευράς ασφάλειας που σχετίζεται με έξυπνους μετρητές και την συλλογή δεδομένων αφορά τα τρία πρώτα τμήματα. Η

κατηγοριοποίηση των επιθέσεων γίνεται κυρίως με βάση το στόχο που έχει, άλλα μια άλλη πιθανή κατηγοριοποίηση είναι με βάση το είδος της ασφάλειας. Έτσι έχουμε:

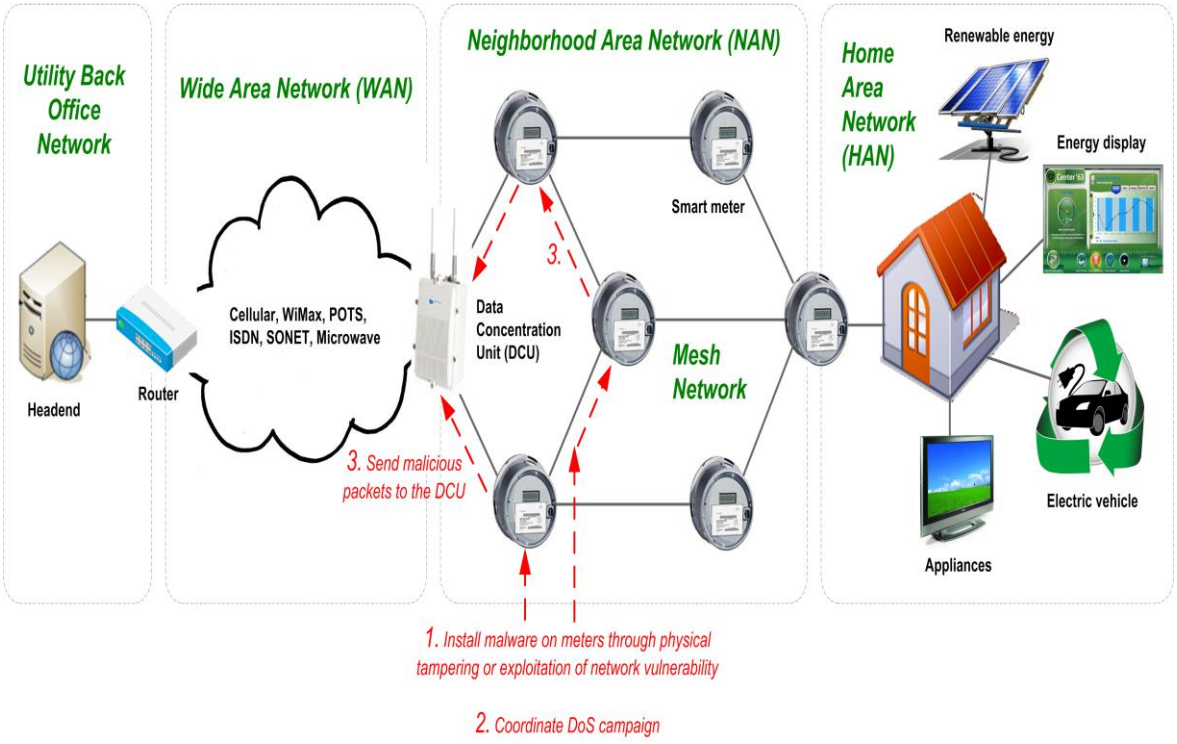
1. Φυσική ασφάλεια
2. Ασφάλεια επικοινωνιών
3. Ασφάλεια δεδομένων και λογισμικού

Η φυσική ασφάλεια σχετίζεται με την πρόσβαση που υπάρχει στο εξοπλισμό, είτε αυτός είναι ένας έξυπνος μετρητής είτε είναι ένας συλλέκτης δεδομένων. Οι έξυπνοι μετρητές θα πρέπει να βρίσκονται σε περιβάλλον ελεγχόμενης πρόσβασης, όπου δεν θα μπορεί ο οποιοσδήποτε να έχει πρόσβαση, λόγω ότι πλέον είναι ένα μικρό υπολογιστικό σύστημα, το οποίο τρέχει λογισμικό. Σε περίπτωση, που κάποιος κακόβουλος αποκτήσει πρόσβαση μέσω κάποιας θύρας που υπάρχει ενσωματωμένη στο έξυπνο μετρητή, υπάρχει η δυνατότητα να εγκαταστήσει κακόβουλο λογισμικό, που μπορεί να προσβάλει και άλλους έξυπνους μετρητές. Σε αυτή την περίπτωση είναι απαραίτητη η αυθεντικοποίηση των συσκευών που έχουν πρόσβαση σε έναν έξυπνο μετρητή. Το ίδιο ισχύει και για συλλέκτες δεδομένων όπου είναι υπεύθυνοι για την συλλογή δεδομένων από ένα συγκεκριμένο πλήθος έξυπνων μετρητών σε ένα NAN. Είναι αναγκαίο η υποδομή αυτή να βρίσκεται σε ασφαλές σημείο και όχι σε κοινόχρηστο χώρο. Σε ενδεχόμενη καταστροφή, ένας μεγάλος αριθμός έξυπνων μετρητών αποκόπτονται από το υπόλοιπο δίκτυο επικοινωνιών. Επιπλέον, και εδώ, είναι απαραίτητη η αυθεντικοποίηση για την σύνδεση μιας συσκευής μέσω θύρας, ή ασύρματης δικτύωσης με έναν συλλέκτη δεδομένων, γιατί σε ενδεχόμενη προσβολή του από κακόβουλο λογισμικό, οι έξυπνοι μετρητές που βρίσκονται συνδεμένοι έχουν μεγάλη πιθανότητα να προσβληθούν. Η κύρια λύση που υιοθετείται είναι να τοποθετούνται οι έξυπνοι μετρητές σε σημεία που ανήκουν στο ευφυές δίκτυο ενέργειας, ή σε υποσταθμούς του δικτύου, όπου μπορεί να παρέχεται η φυσική ασφάλεια που απαιτείται. (Gilbert N. Sorebo, 2011)

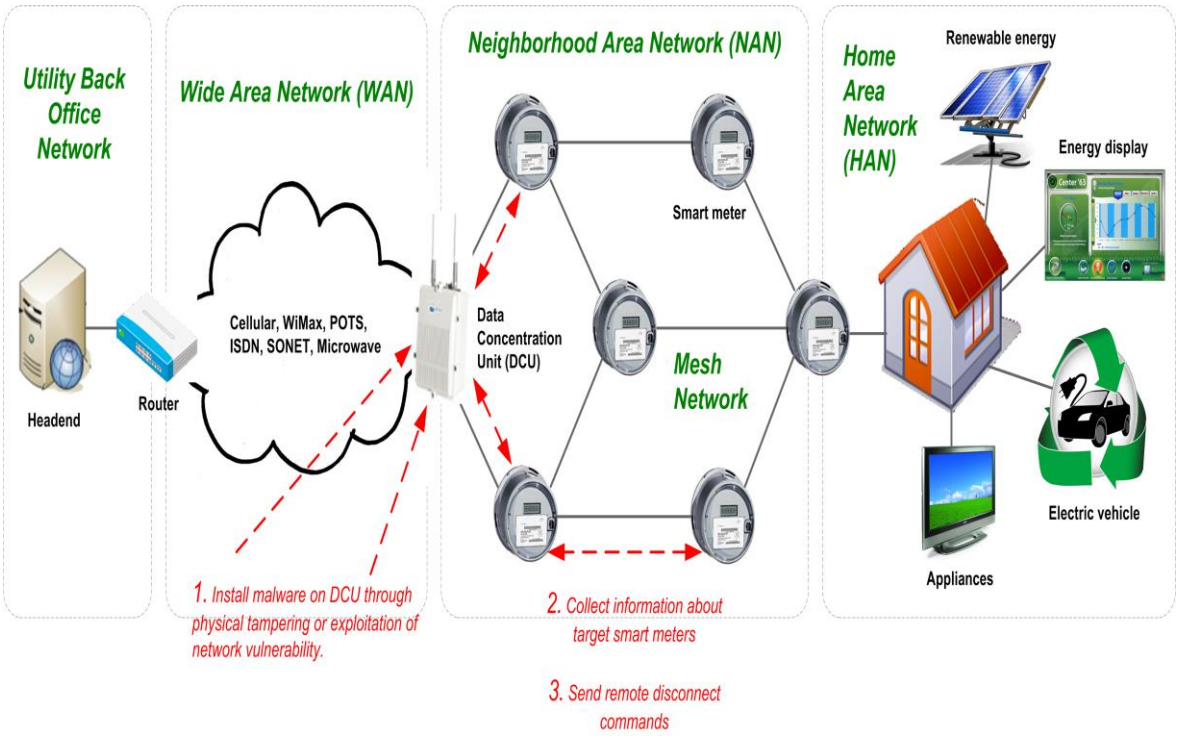
Για την επικοινωνία των έξυπνων μετρητών με το ευφυές δίκτυο ενέργειας, και συγκεκριμένα η επικοινωνία με συλλέκτες δεδομένων κατά κύριο λόγω γίνεται μέσω ασύρματων τεχνολογιών . Η ευκολία που παρέχουν όμως οι ασύρματες τεχνολογίες αντικρούονται από την ευπάθεια που παρουσιάζουν. Σε φυσικό επίπεδο υπάρχουν επιθέσεις που στόχο έχουν να παρεμβάλουν την επικοινωνία ανάμεσα στους έξυπνους μετρητές και στους συλλέκτες δεδομένων. Οι επιθέσεις αυτές χαρακτηρίζονται ως Jamming attacks και στόχο έχουν την δημιουργία θορύβου σε ένα κανάλι επικοινωνίας. Ένα πακέτο θεωρείται ότι έχει παραδοθεί επιτυχώς όταν αποκωδικοποιηθεί από τον δέκτη. Όταν εφαρμόζονται αυτού του είδους οι επιθέσεις, έχουν στόχο να φαίνεται στο αποστολέα ότι το κανάλι είναι σε χρήση, ή σε περίπτωση που εκπέμπει ο αποστολέας να αλλοιωθεί το σήμα ώστε ο δέκτης να λάβει κατεστραμμένα πακέτα. Μια μορφή τέτοιας επίθεσης είναι να στέλνει ο επιτιθέμενος, μια συνεχόμενη σειρά από πακέτα(stream) με υψηλότερο ρυθμό μετάδοσης από την κανονική εκπομπή δεδομένων, αφού έχει αποκτήσει την προτεραιότητα εκπομπής σύμφωνα με το πρωτόκολλο πρόσβασης στο μέσο.

(Vinod Namboodiri, 2013) Στο (Eun-Kyu Lee, Physical Layer Security in Wireless Smart Grid, 2012) οι επιθέσεις Jamming διαχωρίζονται σε δύο κατηγορίες, σε proactive jamming, είναι η επίθεση όπου συνεχόμενα εκπέμπεται σήμα, όπου είναι εύκολα αντιληπτή, ενώ η reactive jamming, πρώτα ο επιτιθέμενος παρακολουθεί και όταν αντιληφθεί ότι υπάρχει μετάδοση παρεμβάλει με θόρυβο. Η δεύτερη περίπτωση φυσικά είναι δυσκολότερο να ανιχνευθεί. Ενδιαφέρον παρουσιάζουν και οι επιθέσεις DoS στους έξυπνους μετρητές και στους συλλέκτες δεδομένων. Σε προηγούμενο κεφάλαιο μελετήθηκαν τα πλεονεκτήματα που προσφέρουν οι ασύρματες τεχνολογίες mesh από πλευράς επικοινωνιών. Οι παραπάνω αρχιτεκτονικές τύπου mesh, επειδή λειτουργούν ως relay, για την προώθηση των δεδομένων γειτονικών έξυπνων μετρητών, παρουσιάζουν μια ευπάθεια ως προς τι επιθέσεις DoS. Με αυτό τον τρόπο, εάν ένας έξυπνος μετρητής έχει μολυνθεί από κακόβουλο λογισμικό, θα επηρεάσει αλυσιδωτά όλους τους κόμβους με αποτέλεσμα να παρουσιασθούν προβλήματα επικοινωνίας σε ένα υποδίκτυο που εξυπηρετεί ένας συλλέκτης δεδομένων. Αυτού του είδους η επίθεση παρουσιάζεται στο (David Grochocki, 2012) σε τρία στάδια:

1. Προσβολή ενός έξυπνου μετρητή
2. Αντιγραφή του κακόβουλου λογισμικού μέσω του δικτύου mesh, σε άλλους έξυπνους μετρητές με σκοπό να μολυνθεί ο συλλέκτης δεδομένων
3. Εκκίνηση της επίθεσης με σκοπό την επίθεση σε όλο το υποδίκτυο που εξυπηρετεί ο συλλέκτης δεδομένων



Εικόνα 37 "DoS επίθεση σε έξυπνους μετρητές ενέργειας" (David Grochocki, 2012)



Εικόνα 38 "Επίθεση Remote Disconnect" (David Grochocki, 2012)

Στην ίδια πηγή παρουσιάζεται και μια νέα επίθεση διαφορετική από τις DoS επιθέσεις, με την ονομασία Remote Disconnect. Αυτή η επίθεση έχει στόχο, να αποκόψει την επικοινωνία έξυπνων μετρητών με το συλλέκτη δεδομένων, με στόχο να πλήξει την διαθεσιμότητα του δικτύου. Στην παραπάνω εικόνα παρουσιάζεται η επίθεση αυτή, ενώ τα τρία στάδια της επίθεσης είναι:

1. Εγκατάσταση κακόβουλου λογισμικού σε συλλέκτη δεδομένων, εκμεταλλευόμενοι την φυσική ή δικτυακή ευπάθεια
2. Συλλογή πληροφοριών σχετικά με την τοπολογία του δικτύου(έξυπνων μετρητών) και επιλογή στόχων
3. Αποστολή εντολών αποσύνδεσης από το δίκτυο προς τους έξυπνους μετρητές εκμεταλλευόμενοι τις λειτουργίες σύνδεσης/αποσύνδεσης που προσφέρει το λογισμικό των έξυπνων μετρητών ενέργειας.

Έκτος από τις επιθέσεις που έχουν στόχο να πλήξουν την διαθεσιμότητα του δικτύου, υπάρχουν επιθέσεις που έχουν ως στόχο την υποκλοπή δεδομένων κυρίως από ασύρματα κανάλια επικοινωνίας. Αυτού του είδους οι επιθέσεις ονομάζονται Eavesdropping attacks. (Wenye Wang Z. L., 2013) Στο (Craig Valli, 2013) δοκιμάζεται σε πειραματικό στάδιο η υποκλοπή δεδομένων από ασύρματο δίκτυο ZigBee, ενός έξυπνου μετρητή ενέργειας.

Στην τελευταία κατηγορία, ανήκουν οι επιθέσεις και απειλές που σχετίζονται με τα δεδομένα που ανταλλάσσονται ανάμεσα στους έξυπνους μετρητές ενέργειας και το ευφυές δίκτυο ενέργειας αλλά και ανάμεσα στους έξυπνους μετρητές ενέργειας και τις συσκευές που ανήκουν στο HAN. Κύριος στόχος των επιθέσεων

είναι η παραποίηση των δεδομένων και κυρίως αυτών που σχετίζονται με την κατανάλωση ενέργειας και το κόστος της, παραβιάζοντας το κριτήριο της ακεραιότητας Το κύριο πρωτόκολλο που χρησιμοποιείται για την ανταλλαγή δεδομένων ανάμεσα στους έξυπνους μετρητές και το ευφυές δίκτυο ενέργειας είναι το ANSI C12.22. Το συγκεκριμένο πρωτόκολλο όμως παρουσιάζει ευπάθειες που εάν εκμεταλλευτούν από κακόβουλους χρήστες, μπορούν να χρησιμοποιηθούν σε επιθέσεις. Ανάλυση των ευπαθειών του πρωτοκόλλου και ενδεχόμενες επιθέσεις που προκύπτουν αναλύονται στο (Shehla Rana, 2012).

Η κύρια επίθεση που σχετίζεται με το ANSI C12.22 είναι η DoS με σκοπό την δυσλειτουργία του δικτύου με περιορισμό του διαθέσιμου εύρους ζώνης. Αυτό συμβαίνει με εκμετάλλευση λειτουργιών του ANSI C12.22 όπως είναι η Trace Service, που δίνει την δυνατότητα εντοπισμού του μονοπατιού για τον προορισμό. Ένας κακόβουλος χρήστης μπορεί να δημιουργήσει επίθεση τύπου DoS, με συνεχή αιτήματα για την εύρεση πολλαπλών μονοπατιών. (Zach Yordy) Κάτι αντίστοιχο συμβαίνει με μια ακόμα λειτουργία του ANSI C12.22 την Resolve Service που χρησιμοποιείται για την εύρεση κόμβων(έξυπνων μετρητών) και της διεύθυνσης τους. Σε περίπτωση που ένας αριθμός κόμβων έχει προσβληθεί από κακόβουλο λογισμικό μπορούν να δημιουργού απαντήσεις σε ψεύτικα αιτήματα που στέλνονται broadcast στο δίκτυο προς ένα συγκεκριμένο κόμβο που λειτουργεί σε relay. Εάν οι απαντήσεις αυτές έχουν παραλήπτη έναν συγκεκριμένο κόμβο, ο κόμβος αυτός από την πολλαπλή λήψη τέτοιων μηνυμάτων θα εμφανίσει προβλήματα επικοινωνίας και λειτουργίας. Η επίθεση αυτή εκμεταλλεύεται την συγκεκριμένη λειτουργία του ANSI C12.22 και την δυνατότητα των κόμβων που λειτουργούν σε κατάσταση relay, να στέλνουν broadcast μηνύματα.

Η τελευταία ευπάθεια του πρωτοκόλλου, παρουσιάζεται στα μηνύματα που γίνονται tag, με ένα συγκεκριμένο bit, και στόχο έχουν την προώθηση τους με επισήμανση επείγον. Τα μηνύματα αυτά έχουν προτεραιότητα στην δρομολόγηση τους, γιατί σχετίζονται με την κατάσταση του δικτύου ενέργειας ή εντολών που πρέπει να εκτελεστούν άμεσα. Η εκμετάλλευση των μηνυμάτων αυτών γίνεται από κακόβολους χρήστες, ώστε μηνύματα ή εντολές που θέλουν να εκτελεστούν να επισημαίνονται με το tag αυτό. Η επίθεση αυτή χαρακτηρίζεται από προσποίηση(spoofing) ως προς την προέλευση του μηνύματος και την αποστολή του.

ΕΠΙΛΟΓΟΣ

Στο κεφάλαιο αυτό μελετήθηκαν οι επιθέσεις που εμφανίζονται σε όλο το εύρος των ευφυών δικτύων ενέργειας, εκμεταλλευόμενες τις αδυναμίες που ενδέχεται να υπάρχουν σε δικτυακές υποδομές αλλά και λογισμικό. Λόγω του μεγέθους και τις σημαντικότητας των ευφυών δικτύων ενέργειας συγκεντρώνουν την προσοχή κακόβουλων ατόμων. Επίσης, πολλές επιθέσεις είναι κοινές και σε άλλες υποδομές μεγάλης εμβέλειας όπως το διαδίκτυο, όμως στα ευφυή δίκτυα ενέργειας, οι απαιτήσεις είναι διαφορετικές, όπως και οι βασικές αρχές που είναι

απαραίτητο να ικανοποιούνται. Ο κύριος στόχος είναι η διαθεσιμότητα του δικτύου επικοινωνιών, μη διαθέσιμο δίκτυο δημιουργεί τεράστια προβλήματα επικοινωνίας. Ειδικά στο WAN των ευφυών δικτύων ενέργειας, η διαθεσιμότητα έχει το πρώτο ρόλο σε αντίθεση με άλλα τμήματα. Εκτός όμως από την διαθεσιμότητα, η ακεραιότητα και η ιδιωτικότητα των δεδομένων είναι βασικοί στόχοι στο NAN και στο HAN.

Όπως είδαμε επιθέσεις DoS, false data injection, remote disconnect, αλλά και flooding, με την εκμετάλλευση κενών ασφάλειας σε πρωτοκόλλα και λογισμικό είναι ιδιαίτερα επικίνδυνες. Συνεπώς, κάθε ευφυές δίκτυο ενέργειας, για την προστασία του, και την ασφαλή λειτουργία του, πρέπει να υλοποιεί αντίμετρα στις επιθέσεις που ενδέχεται να δεχθεί δίνοντας βάρος στην πρόληψη αλλά και στην αντιμετώπιση των επιθέσεων σε περίπτωση που συμβούν. Η έγκαιρη ανίχνευση επιθέσεων μπορεί να είναι σωτήρια για την λειτουργία του δικτύου επικοινωνιών, ενώ η αντιμετώπιση τους με τεχνικές περιορίζουν σημαντικά την εμφάνιση ενδεχόμενων προβλημάτων. Στο επόμενο κεφάλαιο γίνεται αναλυτική μελέτη των μέτρων ασφάλειας που είναι απαραίτητο να ληφθούν για την προστασία ενός ευφυούς δικτύου ενέργειας, σύμφωνα με τις τελευταίες εξελίξεις στο τομέα τις ασφάλειας. Έμφαση δίνεται στην ασφάλεια των επικοινωνιών αλλά και στην ασφάλεια των δεδομένων που διακινούνται στο δίκτυο επικοινωνιών.

ΚΕΦΑΛΑΙΟ 6

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΕΥΦΥΩΝ ΔΙΚΤΥΩΝ ΕΝΕΡΓΕΙΑΣ

ΕΙΣΑΓΩΓΗ

Η ασφάλεια είναι από τις μεγαλύτερες προκλήσεις στην εξέλιξη των ευφυών δικτύων ενέργειας. Οι ευπάθειες, η αδυναμίες, του λογισμικού και του υλικού που χρησιμοποιούνται στα ευφυή δίκτυα ενέργειας εάν αξιοποιηθούν κατάλληλα από κακόβολους χρήστες οδηγούν σε επιθέσεις. Οι επιθέσεις αυτές έχουν στόχο να πλήξουν πρώτα την διαθεσιμότητα του δικτύου, που είναι ο πρωταρχικός παράγοντας λειτουργίας, την ακεραιότητα των δεδομένων και την ιδιωτικότητα. Κατά την σχεδίαση και την υλοποίηση του δικτύου επικοινωνιών ενός ευφυούς δικτύου ενέργειας, η ασφάλεια πρέπει να λαμβάνεται υπόψη εξ αρχής. Στο κεφαλαίο αυτό, η μελέτη των συστημάτων και τεχνικών ασφαλείας γίνεται με βάση τις τρεις περιοχές από τις οποίες αποτελείται ένα ευφυές δίκτυο, μιας και κάθε περιοχή έχει διαφορετικές ανάγκες προστασίας.

6.1 ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ WAN

Το WAN στα ευφυή δίκτυα ενέργειας καλύπτει τις ανάγκες επικοινωνίας για τις κεντρικές υποδομές, όπου περιλαμβάνονται τα κέντρα διαχείρισης του δικτύου, μονάδες παραγωγής ηλεκτρικής ενέργειας, μονάδες αποθήκευσης ηλεκτρικής ενέργειας και υποσταθμοί. Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο η διαθεσιμότητα προηγείται σε σχέση με τις δύο άλλες βασικές αρχές στο WAN. Η κύρια απειλή για το WAN είναι οι επιθέσεις DoS. Η πρώτη αντιμετώπιση για την προστασία από αυτού του είδους τις επιθέσεις είναι η έγκαιρη ανίχνευση. Να σημειωθεί ότι στην κατηγορία αυτήν, οι τεχνική που μπορεί να χρησιμοποιηθεί διαφέρει αναλόγως το σκοπό του επιτιθέμενου ή με βάση το επίπεδο του OSI, που ανήκει. Στο, (Wenye Wang Z. L., 2013) οι διάφορες λύσεις που υπάρχουν στην βιβλιογραφία ταξινομούνται σε δύο μεγάλες κατηγορίες. Αυτές είναι:

1. Ανίχνευσης σήματος

Στην κατηγορία αυτή ανήκουν οι τεχνικές που ανιχνεύουν το σήμα που εκπέμπεται σε φυσικό επίπεδο, και αφορούν επιθέσεις βασισμένες στο Jamming. Οι τεχνικές βασίζονται στο Received Signal Strength Information(RSSI). Εάν ο αριθμός RSSI για πολλά πακέτα είναι μεγαλύτερος από το threshold (που σημαίνει ότι σε φυσιολογικές συνθήκες θα λάβει τα πακέτα), αλλά κατά την αποκωδικοποίηση των πακέτων παράγονται λάθη, αναλόγως την τεχνική ανίχνευσης που χρησιμοποιείται τότε, θεωρείται ότι υπάρχει απειλή. Οι τεχνικές αυτές, μπορούν εύκολα να αναπτυχθούν σε κεντρικές υποδομές ενός ευφυούς δικτύου ενέργειας, και ειδικότερα σε ασύρματες κεραίες που χρησιμοποιούνται για παρακολούθηση της κατάστασης του δικτύου.

2. Ανίχνευσης πακέτων

Οι λύσεις που ανήκουν στην κατηγορία αυτήν, έχουν στόχο τον έλεγχο των πακέτων που μεταδίδονται σε ένα δίκτυο. Ειδικότερα, παρακολουθούν τον ρυθμό των αποτυχημένων αποστολών και λήψεων πακέτων και ένα διαπιστώσουν μεγάλο αριθμό αποτυχημένων προσπαθειών ανιχνεύεται ως απειλή η κατάσταση αυτή. Οι τεχνικές αυτές θεωρούνται αποτελεσματικές.

3. Προληπτική μέθοδος ανίχνευσης

Η κύρια ιδέα των τεχνικών αυτών είναι η σχεδίαση αλγορίθμων που προσπαθούν να ανιχνεύσουν μια DoS επίθεση σε πρώιμο στάδιο. Για να γίνει αυτό, ανά τακτά χρονικά διαστήματα στέλνουν πακέτα για να εντοπίσουν ενδεχόμενες απειλές. Να σημειωθεί ότι οι τεχνικές που ανήκουν στην κατηγορία αυτήν, αποφεύγονται να χρησιμοποιηθούν σε κρίσιμες υποδομές όπως είναι αυτές σε ένα WAN, λόγω ότι προσθέτουν επιπλέον φόρτο στο δίκτυο επικοινωνιών.

4. Υβριδική μέθοδος ανίχνευσης

Οι τεχνικές αυτές συνδυάζουν ιδέες από τις παραπάνω κατηγορίες για καλύτερη ακρίβεια στην ανίχνευση επιθέσεων.

Ένα σύστημα ανίχνευσης επιθέσεων που ανήκει στην κατηγορία ανίχνευσης πακέτων παρουσιάζεται στο (Upeka Kanchana Premaratne, 2010). Το σύστημα αυτό σχεδιάστηκε για να αναλύει επιθέσεις που βασίζονται στο IEC 61850, που χρησιμοποιείται σε υποσταθμούς και συλλέγει δεδομένα από IED. Τα συστήματα έγκαιρης ανίχνευσης είναι ένα αποτελεσματικό μέτρο αντιμετώπισης επιθέσεων στο WAN. Είναι ικανά να αντιμετωπίζουν τις επιθέσεις ενεργητικά και όχι παθητικά όπως ένα τοίχος προστασίας που προστατεύει την περίμετρο. Ενώ τα τείχη προστασίας μπορούν να προστατέψουν από μη-εξουσιοδοτημένη πρόσβαση, δεν μπορούν να προστατέψουν από ευπάθειες που βασίζονται στα πρωτόκολλα που χρησιμοποιούνται. Τα συστήματα έγκαιρης ανίχνευσης ταξινομούνται σε: (Emilio Ancillotti, 2013)

1. Ανίχνευσης υπογραφών(Signature detection)

Στην κατηγορία αυτήν ανήκουν τα συστήματα που ανιχνεύουν τις υπογραφές, δηλαδή τα ψηφιακά αποτυπώματα που αφήνει μια επίθεση. Αυτό γίνεται με δεδομένα που διαθέτει το σύστημα, από εξομοιώσεις επιθέσεων ή από προηγούμενες πραγματικές επιθέσεις. Το πλεονέκτημα το συστημάτων που ανήκουν στην κατηγορία αυτή, είναι ότι έχουν υψηλή ακρίβεια και μικρό αριθμό λάθος συναγερμών.

2. Ανίχνευσης ανωμαλιών(Anomaly detection)

Στην κατηγορία αυτή ανήκουν τα συστήματα που ανιχνεύουν εισβολές με βάση την παραβίαση της φυσιολογικής λειτουργίας πρωτοκόλλων, προγραμμάτων, λειτουργιών. Για την ανίχνευση χρησιμοποιούνται στατιστικά μοντέλα, ενώ το πλεονέκτημα τους είναι ότι έχουν την δυνατότητα να ανιχνεύουν άγνωστες επιθέσεις. Το μειονέκτημα τους, είναι ότι έχουν μεγάλο αριθμό λάθος συναγερμών.

3. Ανίχνευσης προδιαγραφών(Specification detection)

Στην κατηγορία αυτή ανήκουν τα συστήματα που ανιχνεύουν εισβολές με βάση ένα σύνολο κανόνων τα οποία ορίζουν ποια είναι η φυσιολογική συμπεριφορά/λειτουργία. Παραβίαση αυτών των κανόνων, θεωρείται παραβίαση της ασφάλειας. Έχουν την δυνατότητα, να ανιχνεύουν άγνωστες επιθέσεις όπως τα συστήματα ανίχνευσης ανωμαλιών, ενώ το μειονέκτημα τους είναι ότι απαιτούν αρκετό χρόνο για το καθορισμό των κανόνων. Να σημειωθεί, ότι τα συστήματα αυτά είναι καταλληλότερα για εφαρμογές όπου είναι καθορισμένα τα πρωτόκολλα που χρησιμοποιούνται.

Μια διαφορετική μορφή ενός συστήματος προστασίας με επίπεδα παρουσιάζεται στο (Dong Wei Y. L., 2010), η εφαρμογή του καλύπτει το κέντρο διαχείρισης, τους υποσταθμούς αλλά κα συσκευές που είναι υπεύθυνες για την συλλογή δεδομένων(IED). Το σύστημα αυτό, αποτελείται από τρία κύρια μέρη:

i. Security agents

Είναι λογισμικό, το οποίο εγκαθίσταται σε IED και σκοπός του είναι να καταγράφει δεδομένα που λαμβάνονται και να τα αναλύει ώστε να τα αποστείλει στο Security Manager. Επίσης, αναλαμβάνει την επικοινωνία ανάμεσα σε διαφορετικά πρωτόκολλα, και εγκαθιστά και τρέχει τις πιο πρόσφατες διορθώσεις-ενημερώσεις που στέλνονται από το Security Manager.

ii. Managed Security Switch

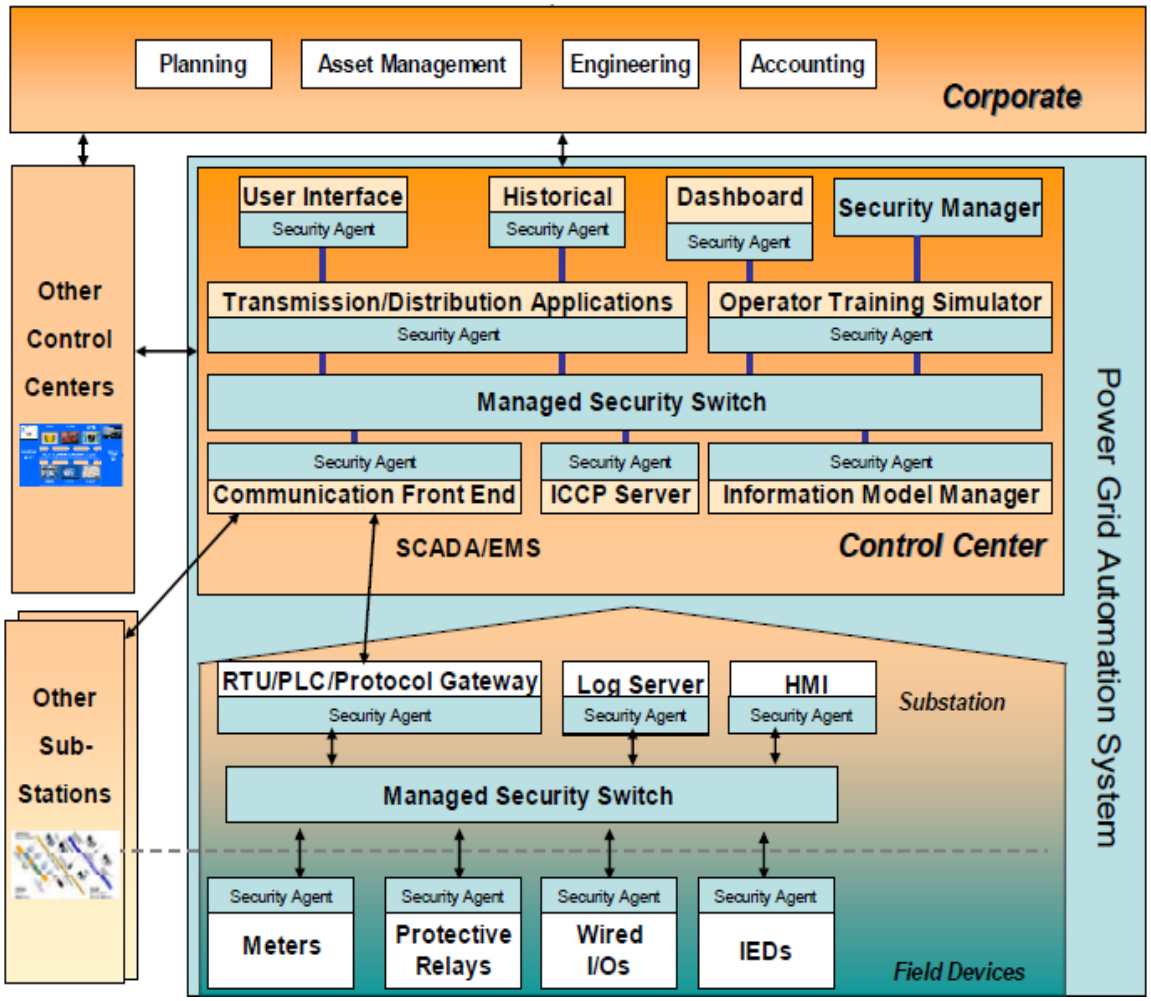
Το τμήμα αυτό, αναφέρεται σε ένα σύνολο από δικτυακές τύπου switch/router, που συνδέουν συσκευές σε έναν υποσταθμό και στόχο έχουν τον έλεγχο του εύρους ζώνης και τον έλεγχο της προτεραιότητας των δεδομένων. Επίσης, ξεχωρίζουν το εσωτερικό δίκτυο του υποσταθμού από το εξωτερικό, δημιουργώντας περίμετρο και πραγματοποιώντας λειτουργίες Network Address Translation(NAT). Για την διαχείριση του εύρους ζώνης και της προτεραιότητας των δεδομένων, εκτελούν εντολές που δέχονται από το Security Manager. Στο εσωτερικό δίκτυο του υποσταθμού, δίνεται η δυνατότητα διαχωρισμού του δικτύου σε Virtual Lans(VLANS), για καλύτερη διαχείριση και μεγαλύτερη ασφάλεια ως προς την πρόσβαση σε επιμέρους τμήματα με την χρήση κανόνων.

iii. Security Manager

Το τμήμα αυτό βρίσκεται στο κέντρο διαχείρισης του ευφυούς δικτύου ενέργειας, και είναι υπεύθυνο για την διαχείριση των παραπάνω τμημάτων. Επικοινωνεί με τους Security Agents και Managed Security Switch, συνήθως μέσο Virtual Printed Network(VPN), συλλέγει τα δεδομένα από τους Security Agents, στέλνει ενημερώσεις για τις πιο πρόσφατες διορθώσεις ασφαλείας στο λογισμικό και διαχειρίζεται τις συνδέσεις μέσω VPN. Ακόμη, λειτουργεί ως Authentication, Authorization, Accounting (AAA) server, για την πιστοποίηση των χρηστών που έχουν πρόσβαση σε λειτουργίες ή υποδομές και παρέχει δικαιώματα πρόσβασης, όπως και καταγραφή των κινήσεων κάθε χρήστη. Τέλος, ο έλεγχος και η εκχώρηση δικαιωμάτων πρόσβασης γίνεται δυναμικά, βασισμένη σε λίστες

πρόσβασης, αναλόγως σε τι κατάσταση λειτουργεί το κάθε επί μέρους τμήμα. Χαρακτηριστικό παράδειγμα είναι, ότι διαφορετικά δικαιώματα εκχωρούνται σε έναν υποσταθμό σε κατάσταση κανονικής λειτουργίας και διαφορετικά σε περίπτωση έκτακτης ανάγκης ή εργασιών συντήρησης. Πάνω στο μοντέλο αυτό προτείνεται και η υλοποίηση ενός συστήματος έγκαιρης ανίχνευσης απειλών, το οποίο θεωρείται υβριδικό, δηλαδή ανήκει και στις δύο κατηγορίες συστημάτων έγκαιρης ανίχνευσης που παρουσιαστήκαν. Οπότε, η ανίχνευση απειλών από το σύστημα αυτό γίνεται σε τρία επίπεδα: (Dong Wei Y. L., 2011)

1. Οι Security Agents, πραγματοποιούν το πρώτο επίπεδο ελέγχου, Καταγράφουν τα δεδομένα που συλλέγουν και αποστέλλουν αναφορές σχετικά με αυτά. Επίσης , εκτελούν λειτουργίες κρυπτογράφησης-αποκρυπτογράφησης. Μια σημαντική λειτουργία τους είναι ο έλεγχος πρόσβασης, βασιζόμενος σε λίστες, Access Control List(ACL). Πραγματοποιούν έλεγχο σε πακέτα, ελέγχοντας την διεύθυνση αποστολέα και παραλήπτη, τον αριθμό της θύρας ή του πρωτοκόλλου εάν ταιριάζει με κάποια εγγραφή στην ACL. Εάν ταιριάζει, το πακέτο προωθείται, αλλιώς απορρίπτεται. Λόγω, των στενών απαιτήσεων από πλευράς απαιτήσεων καθυστέρησης, ο έλεγχος πρόσβασης πραγματοποιείται μόνο στο τρίτο και τέταρτο επίπεδο του OSI. Έλεγχος σε υψηλότερο επίπεδο, όπως είναι το επίπεδο εφαρμογών, απαιτεί βαθύτερο έλεγχο των πακέτων και προσθέτει επιπλέον καθυστέρηση στις επικοινωνίες.
2. Τα Managed Security Switch, πραγματοποιούν το δεύτερο στάδιο ανίχνευσης, βασιζόμενα σε στοιχεία της απόδοσης του δικτύου, όπως είναι καθυστέρηση πακέτων, χρήση του εύρους ζώνης, πρωτοκόλλων που χρησιμοποιούνται.
3. Ο Security Manager πραγματοποιεί έλεγχο του δικτύου και παρακολούθηση των δύο προηγούμενων επιπέδων, καταγράφοντας τα δεδομένα που λαμβάνει Είναι υπεύθυνος για την αποστολή ενημερώσεων ασφαλείας στους Security Agents, όπως και των λιστών πρόσβασης που εκτελούν. Οι λίστες πρόσβασης δημιουργούνται βασιζόμενες στα δεδομένα που συλλέγονται αλλά και από αυτά που ορίζει ο διαχειριστής του συστήματος.



Εικόνα 39 "Προτεινόμενο μοντέλο ασφαλείας βασισμένο σε τρία επίπεδα" (Upeka Kanchana Premaratne, 2010)

Ένα διαφορετικό σύστημα ανίχνευσης και αντιμετώπισης επιθέσεων παρουσιάζεται στο (Y. Yang, 2014), το οποίο δεν βασίζεται στην αντιμετώπιση ήδη γνωστών επιθέσεων όπως στο (Upeka Kanchana Premaratne, 2010), το οποίο αν και μπορεί να αντιμετωπίσει αποτελεσματικά επιθέσεις, δεν προστατεύει από όλους τους κινδύνους. Το μοντέλο που προτείνεται, προσφέρει προστασία από εξωτερικές απειλές αλλά και εσωτερικές. Δηλαδή, οι απειλές δεν είναι μόνο εκτός των υποδομών του ευφυούς δικτύου ενέργειας, αλλά μπορούν να προκύψουν και εσωτερικά, για παράδειγμα με εγκατάσταση κακόβουλου λογισμικού. Επίσης, για την εφαρμογή του μοντέλου αυτού απαιτείται και καθορισμός της περιμέτρου των υποδομών για την πραγματοποίηση των ελέγχων. Το σύστημα αυτό από πλευράς κατηγοριοποίησης εντάσσεται στην κατηγορία των υβριδικών και ο έλεγχος πρόσβασης γίνεται βασιζόμενος σε:

1. Λίστες πρόσβασης δευτέρου, τρίτου επιπέδου και τετάρτου του OSI

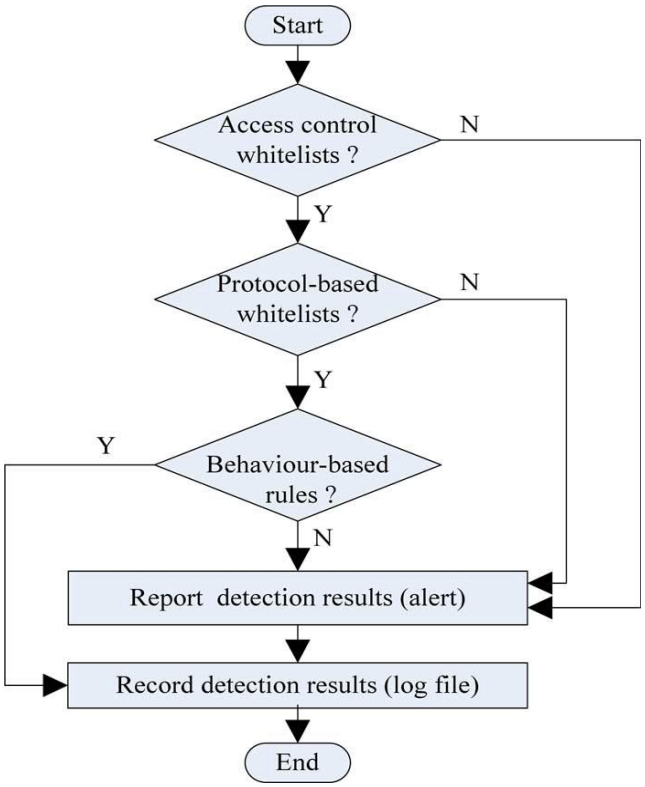
Με βάσης τις λίστες πρόσβασης, ο έλεγχος γίνεται σε διευθύνσεις MAC και IP και port. Εάν υπάρχουν τα στοιχεία στην λίστα εκχωρούνται τα κατάλληλα δικαιώματα, αλλιώς απορρίπτονται και καταγράφονται.

2. Λίστες ελέγχου πρόσβασης βασισμένες σε πρωτόκολλα

Ο έλεγχος σε αυτές τις λίστες σε υψηλότερα επίπεδα από τον προηγούμενο έλεγχο, και φτάνει μέχρι το έβδομο επίπεδο του OSI, το επίπεδο εφαρμογών. Ο έλεγχος πραγματοποιείται σε πρωτόκολλα όπως είναι το DNP3, IEC 61850 κτλ.

3. Κανόνες ψηφιακών ιχνών(υπογραφών) και συμπεριφοράς

Ο έλεγχος γίνεται με βάση κανόνες που βασίζονται στο Deep Packet Inspection(DPI) για τον έλεγχο των πακέτων. Οι κανόνες μπορεί να διαφέρουν αναλόγως το σημείο το οποίο καλούνται να προστατέψουν. Οι έλεγχοι του βασίζονται στο DPI, να αναφερθεί ότι αποκρούουν αποτελεσματικά τις περισσότερες γνωστές επιθέσεις όπως είναι οι DoS.



Εικόνα 40 "Διαδικασία ελέγχου πρόσβασης για το προτεινόμενο μοντέλο" (Y. Yang, 2014)

Εκτός από την προστασία ενάντια σε επιθέσεις που έχουν σκοπό να πλήξουν την διαθεσιμότητα του δικτύου, είναι απαραίτητο να ληφθούν μέτρα προστασίας ενάντια σε παραβιάσεις τις ακεραιότητας και της εμπιστευτικότητας των δεδομένων που διακινούνται στο WAN και στις υποδομές που περιλαμβάνει. Η επιθέσεις τύπου DoS, αντιμετωπίζονται με συστήματα έγκαιρης ανίχνευσης ώστε να διασφαλίζεται η διαθεσιμότητα του δικτύου επικοινωνιών. Εκτός όμως από την διαθεσιμότητα και η αυθεντικοποίηση είναι σημαντική παράμετρο στα ευφυή δίκτυα ενέργειας για την αντιμετώπιση απειλών που έχουν στόχο την ακεραιότητα των δεδομένων. Κάθε χρήστης για να έχει πρόσβαση σε συστήματα διαχείρισης του ευφυούς δικτύου ενέργειας πρέπει να έχει αναγνωρισθεί, ότι είναι αυτός που ισχυρίζεται ότι είναι. Ακόμη, υπάρχουν και συσκευές που χρειάζεται να έχουν αναγνωρισθεί ώστε να μην θεωρούνται απειλή για το ευφυές δίκτυο ενέργειας. Είναι κατανοητό λοιπόν, ότι απαιτείται η εφαρμογή πρωτοκόλλων αυθεντικοποίησης για την αναγνώριση χρηστών και συσκευών, ώστε να προστατευτεί η ακεραιότητα των δεδομένων. Για την καλύτερη κατανόηση των μοντέλων αυθεντικοποίησης θα αναφερθούν οι δύο βασικές μορφές κρυπτογράφησης: (Wenye Wang Z. L., 2013)

1. Ασύμμετρη κρυπτογράφηση

Απαιτεί περισσότερους υπολογιστικούς πόρους σε σχέση με την συμμετρική κρυπτογράφηση για μεγάλου μήκους κλειδιού και συνεπώς μεγαλύτερη ασφάλεια.

2. Συμμετρική κρυπτογράφηση

Οι υπολογιστικοί πόροι που απαιτούνται είναι ανεξάρτητοι από το μήκους κλειδιού, αλλά απαιτείται ασφαλή ανταλλαγή του κλειδιού ανάμεσα στον αποστολέα και στον παραλήπτη. Συνεπώς, καθιστά την διαχείριση των κλειδιών περισσότερο πολύπλοκη και ιδιαίτερα σημαντική.

Η κύρια μορφή αυθεντικοποίησης στο WAN, βασίζεται σε αυθεντικοποίηση σε συνδυασμό με την multicast επικοινωνία. Η multicast επικοινωνία έχει ευρεία χρήση στις υποδομές του WAN και επίσης η επικοινωνία είναι ευαίσθητη ως προς το χρόνο και την χρήση του διαθέσιμου εύρους ζώνης. Είναι καλύτερο να γίνεται η αυθεντικοποίηση σε ένα σύνολο συσκευών ή χρηστών από ότι ξεχωριστά. Στην ασφάλεια των επικοινωνιών γενικότερα η χρήση ασύμμετρης κρυπτογράφησης ή κρυπτογράφησης δημοσίου κλειδιού σε συνδυασμό με multicast επικοινωνία είναι από τα πιο γνωστά μοντέλα που σχετίζονται με την αυθεντικοποίηση. Στα μοντέλα αυτά, όλοι οι παραλήπτες μοιράζονται το ίδιο δημόσιο κλειδί και ο αποστολέας κρυπτογραφεί το μήνυμα με το δικό του προσωπικό κλειδί, ενώ οι παραλήπτες το αποκρυπτογραφούν. (Yacine Challal, 2004) Τα μοντέλα αυτά, μπορεί να είναι αποδοτικά ως προς τον τρόπο λειτουργίας τους, όμως δημιουργούνται νέες προκλήσεις η εφαρμογή τους στα ευφυή δίκτυα ενέργειας μιας και απαιτούν από τους παραλήπτες να έχουν αυξημένες υπολογιστικές ικανότητες.

Μια άλλη διαφορετική λύση είναι η χρήση συμμετρικής κρυπτογράφησης. Στα μοντέλα αυτά, ο αποστολέας κρυπτογραφεί το μήνυμα με το δικό του κλειδί, το

οποίο μοιράζεται στους παραλήπτες για να μπορούν να αποκρυπτογραφήσουν το μήνυμα. Η διαδικασία αυτή, ενώ απαιτεί μικρότερο υπολογιστικό κόστος, εισάγει το πρόβλημα, ότι το κλειδί μπορεί να υποκλαπεί και τα δεδομένα να διαβαστούν από κάποιον κακόβουλο. Σε αυτήν την περίπτωση εισάγεται το πρόβλημα της διαχείρισης του κλειδιού αλλά και του τρόπου διαμοιρασμού τους στους παραλήπτες. Λόγω των απαιτήσεων για πολύ μικρή καθυστέρηση στις επικοινωνίες στα ευφυή δίκτυα ενέργειας, τα κοινά μοντέλα που υπάρχουν για αυθεντικοποίηση βασισμένα σε multicast επικοινωνία δεν καλύπτουν τις απαιτήσεις καθυστέρησης.

Η ανάγκη αυτή οδήγησε στην σχεδίαση νέων μοντέλων αυθεντικοποίησης με μικρή επιπρόσθετη πληροφορία(overhead) αλλά και μικρή καθυστέρηση στην συνολική επικοινωνία. Τα μοντέλα αυτά ανήκουν στην υβριδική κατηγορία από τις κατηγορίες των μοντέλων αυθεντικοποίησης για multicast επικοινωνία. Η υβριδική κατηγορία συνδυάζει χαρακτηριστικά μοντέλων με στόχο το όσο το δυνατό μειωμένο υπολογιστικό κόστος, το οποίο είναι πολύ σημαντικό για συσκευές που έχουν περιορισμένες υπολογιστικές ικανότητες. Τα μοντέλα αυτά συνδυάζουν ασύμμετρη κρυπτογράφηση με one-way συναρτήσεις. Το αποτέλεσμα που προκύπτει είναι η δημιουργία μιας ψηφιακής υπογραφής για κάθε μήνυμα. Το σχήμα αυτό ενώ είναι γρήγορο στην λειτουργία του, δεν είναι εύκολα διαχειρίσιμο από πλευράς, ιδιωτικού και δημοσίου κλειδιού μιας και για κάθε μήνυμα χρειάζεται ένα ζευγάρι κλειδιών. Ακόμη, το μέγεθος του μηνύματος με την χρήση ψηφιακής υπογραφής είναι μεγάλο. Το σχήμα αυτό έχει ονομαστεί one-time signature(OTS). (Qinghua Li, 2011)

Για τον περιορισμό των αδυναμιών του σχήματος αυτού, οι ερευνητές το εξέλιξαν ώστε με την χρήση ενός ζευγαριού κλειδιών και μιας hash συνάρτησης, να γίνεται χρήση της ψηφιακής αυτής υπογραφής σε πολλαπλά μηνύματα. Το αποτέλεσμα είναι να περιορίζεται σημαντικά το υπολογιστικό κόστος αλλά και το κόστος διαχείρισης των κλειδιών που απαιτούνται. Από την άλλη μεριά όμως, τα μηνύματα που υπογράφονται ψηφιακά με την ίδια υπογραφή, χρειάζεται να αποθηκεύονται προσωρινά σε buffers, στον αποστολέα ή στον παραλήπτη, μέχρι να συγκεντρωθούν όλα μαζί. Αυτό προσθέτει επιπλέον καθυστέρηση στην συνολική επικοινωνία με αποτέλεσμα και πάλι να μην καλύπτονται οι ανάγκες καθυστέρησης των ευφυών δικτύων ενέργειας.

Το πιο γρήγορο υπολογιστικά σχήμα που ανήκει στην κατηγορία αυτή είναι το HORS όπου έχει μικρό υπολογιστικό κόστος και μέγεθος υπογραφής περίπου 130 bytes. Όμως δεν μπορεί να αξιοποιηθεί στα ευφυή δίκτυα ενέργειας επειδή το μέγεθος δημοσίου κλειδιού απαιτεί αποθηκευτικό χώρο και δημιουργείται το θέμα διαχείρισης και διανομής του κλειδιού αυτού στους παραλήπτες.

Η κύρια βελτίωση του σχήματος HORS, είναι το σχήμα Time-Valid HORS (TV-HORS) που στόχο έχει την μείωση της καθυστέρησης σε σχέση με άλλα σχήματα αυθεντικοποίησης. (Qiyan Wang, 2009). Το TV-HORS, συνδυάζει σχήματα TV-OTS, όπου το ζεύγος κλειδιών είναι σε ισχύ για ένα μικρό χρονικό διάστημα, κατά

το οποίο απαιτείται συγχρονισμό από αποστολέα και δέκτη, αλλά και του HORS όπου με το ίδιο ζεύγος κλειδιών, υπογράφονται ψηφιακά πολλά μηνύματα. Συνολικά, η καθυστέρηση και το overhead στην επικοινωνία είναι πολύ μικρότερα σε σχέση με σχήματα OTS. Επίσης, γρηγορότερες υπολογιστικά είναι και οι διαδικασίες του signing και του verification. (Carl H. Hauser, 2012) Δηλαδή του χρόνου που απαιτείται για να υπογραφεί ένα μήνυμα και του χρόνου για να πιστοποιηθεί με το δημόσιο κλειδί του παραλήπτη. Το μειονέκτημα του είναι όμως είναι το μέγεθος του δημοσίου κλειδιού που είναι ανάμεσα σε 8KB με 10KB.

Στο (Qiyan Wang, 2009) γίνεται ανάλυση του TV-HORS κάτω από διαφορετικά είδη επιθέσεων όπως είναι η επίθεση Brute Force αλλά και DoS με την τεχνική flooding. Τα αποτελέσματα που προκύπτουν είναι ιδιαίτερα ενθαρρυντικά για την ασφάλεια του σχήματος αυτού. Τέλος, να σημειωθεί ότι η χρήση των σχημάτων αυτών δεν έχει εφαρμοσθεί σε μεγάλη κλίμακα σε ευφυή δίκτυα ενέργειας μια και ακόμα βρίσκονται σε εξέλιξη η βελτιστοποίηση τους.

Εκτός από την επιλογή του σχήματος αυθεντικοποίησης που χρειάζεται να εφαρμοσθεί στο WAN η διαχείριση των κλειδιών που χρησιμοποιούνται για την κρυπτογράφηση αποτελεί σημαντικό στοιχείο για την ασφαλή λειτουργία του δικτύου και των υποδομών του. Εάν η διαχείριση και ο διαμοιρασμός των κλειδιών δεν γίνεται με ασφαλή τρόπο, κανένα σχήμα αυθεντικοποίησης δεν μπορεί να λειτουργήσει αποτελεσματικά. Να σημειωθεί ότι στο κέντρο διαχείρισης του ευφυούς δικτύου ενέργειας, εκτός από την διαχείριση των κλειδιών του WAN και των υποδομών που ανήκουν σε αυτά, πραγματοποιείται και η διαχείριση των κλειδιών του NAN, ειδικότερα των έξυπνων μετρητών και των συλλεκτών δεδομένων.

Επίσης, ένα σύστημα κρυπτογράφησης δεν μπορεί να καλύψει τις απαιτήσεις ολόκληρου δικτύου, λόγω τις πληθώρας διαφορετικών συσκευών που υπάρχουν, των διαφορετικών απαιτήσεων που πρέπει να καλυφθούν αλλά της απόδοσης όταν τα μοντέλα αυτά εφαρμόζονται σε πολύ μεγάλη κλίμακα. Τα συστήματα διαχείρισης κλειδιών διακρίνονται δύο γενικές κατηγορίες: (Wenye Wang Z. L., 2013) (Group h. S.–C., 2010)

1. Υποδομή δημοσίου κλειδιού

Η Υποδομή δημοσίου κλειδιού ή Public Key Infrastructure(PKI) είναι ένας μηχανισμός που αποτελείται από ένα σύνολο λειτουργιών που αντιστοιχούν τα δημοσία κλειδιά σε χρήστες ή γενικότερα οντότητες κάτω από τον έλεγχο της αρχή πιστοποίησης ή Certificate Authority(CA). Οι χρήστες που χρειάζονται ένα δημόσιο κλειδί το ζητούν από την αρχή πιστοποίησης για την δημιουργία ενός ασφαλούς καναλιού επικοινωνίας.

2. Διαχείριση συμμετρικών κλειδιών

Στην κατηγορία αυτήν ανήκουν τα συστήματα που διαχειρίζονται τα κλειδιά από μοντέλα συμμετρικής κρυπτογράφησης και παρέχουν λειτουργίες όπως είναι η δημιουργία, διανομή, αποθήκευση και ενημέρωση κλειδιών. Τα συστήματα αυτά

απαιτούν καλύτερο συντονισμό μεταξύ των δύο οντοτήτων που μοιράζονται το ίδιο κλειδί σε σχέση με τις υποδομές δημοσίου κλειδιού.

Στο (Wenye Wang Z. L., 2013) γίνεται μια παρουσίαση των συστημάτων διαχείρισης κλειδιών για το WAN και τις υποδομές που περιλαμβάνει όπως είναι το κέντρο διαχείρισης αλλά και ο υποσταθμοί του δικτύου ενέργειας. Συνοπτικά τα συστήματα διαχείρισης κλειδιών είναι:

1. Διαχείριση συμμετρικών κλειδιών

Τα συστήματα αυτά είναι υπεύθυνα για την δημιουργία, διανομή, αποθήκευση και ανανέωση των συμμετρικών κλειδιών. Η χρήση όμως του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση, βασίζεται σε μεγάλο βαθμό στην ασφαλή διανομή του κλειδιού. Για παράδειγμα, σε έναν υποσταθμό που περιλαμβάνει αρκετές IED, η χρήση του ίδιου κλειδιού δημιουργεί προβλήματα όπως στην περίπτωση που διαρρεύσει ένα κλειδί, το κενό ασφαλείας που δημιουργείται είναι τεράστιο. Υπάρχει όμως και η αντίθετη άποψη ότι ένα σύστημα διαχείρισης συμμετρικών κλειδιών με την κατάλληλη σχεδίαση μπορεί να λειτουργήσει αποτελεσματικά και με ασφάλεια. Στο (Fangming Zhao, 2012) παρουσιάζεται ένα σύστημα αυθεντικοποίησης και διαχείρισης συμμετρικών κλειδιών, θεωρώντας την εφαρμογή ασύμμετρης κρυπτογράφησης ως ακατάλληλη και μη πρακτική για την εφαρμογή σε υποδομές που είναι κρίσιμες και με μικρές απαιτήσεις καθυστέρησης. Το σύστημα αυτό ακόμη έχει πρόβλεψη για ανάκληση του κλειδιού σε περίπτωση που μια IED συσκευή που έχει αυθεντικοποιηθεί έχει προσβληθεί.

2. ASKMA

Το ASKMA είναι ένα σύστημα διαχείρισης κλειδιών σχεδιασμένο για τα κέντρα διαχείρισης ευφυών δικτύων ενέργειας, ενώ βασίζεται στην λογική ιεραρχία κλειδιών. Το σύστημα αυτό έχει δύο πλεονεκτήματα: υποστηρίζει multicast και broadcast επικοινωνία, επιπλέον, θεωρείται υπολογιστικά αποδοτικό. Να σημειωθεί, ότι σε επικοινωνία broadcast είναι περισσότερο αποδοτικό σε σχέση με multicast.

3. ASKMA+

Το ASKMA+ είναι ένα σύστημα που σχεδιάστηκε για να βελτιώσει την απόδοση του ASKMA. Στο ASKMA+ έχει μειωθεί ο αριθμός των κλειδιών που διατηρούνται χωρίζοντας την λογική ιεραρχία κλειδιών σε δύο τμήματα. Όπως και το ASKMA υποστηρίζει και broadcast και multicast επικοινωνία. (Donghyun Choi, 2010)

4. WAKE

Το WAKE είναι ένα σύστημα διαχείρισης κλειδιών με στόχο την δημιουργία ασφαλών καναλιών επικοινωνία ανάμεσα σε συσκευές και το κέντρο διαχείρισης. Το σύστημα αυτό είναι υπεύθυνο για την συλλογή δεδομένων σχετικά με την κατάσταση του δικτύου ηλεκτρικής ενέργειας και το WAKE έχει ως στόχο να καλύψει τις απαιτήσεις ασφαλείας του συστήματος παρακολούθησης του δικτύου

ενέργειας που ανήκει στο WAN. Το WAKE χρησιμοποιεί υποδομή δημοσίου κλειδιού και μια ιεραρχία από αρχές πιστοποίησης με την κορυφή να είναι η αρχή πιστοποίησης που ανήκει στο ευφυές δίκτυο ενέργειας. Κάθε IED συσκευή διαθέτει ένα ζευγάρι private/public κλειδί. Στο ίδιο σύστημα περιλαμβάνεται και ένα IDS, για την ανίχνευση απειλών και σε περίπτωση που μια IED συσκευή θεωρεί ως μη-έμπιστη ανακαλείται το ψηφιακό πιστοποιητικό μέσω μια λίστας ανακλήσεων που διατηρείται και γίνεται broadcast στο υπόλοιπο δίκτυο η αλλαγή αυτή. Να σημειωθεί, ότι το σύστημα αυτό για multicast αυθεντικοποίηση υιοθετεί το TV-HORS, ως το αποδοτικότερο σχήμα για multicast αυθεντικοποίηση και με της μεγαλύτερες προοπτικές για ευρεία χρήση. (Yee Wei Law, 2013)

6.2 ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ NAN

Η ασφάλεια στο NAN είναι από τους κυριότερους παράγοντες για την λειτουργία των ευφυών δικτύων ενέργειας λόγω της πολυπλοκότητας που παρουσιάζει για αυτό και αποτελεί το επίκεντρο της μελέτης. Ένα NAN συνδέει χιλιάδες έξυπνους μετρητές και συλλέκτες δεδομένων σε μεγάλες γεωγραφικές αποστάσεις και το οποίο το καθιστά ιδιαίτερα ευπαθές. Οι έξυπνοι μετρητές συλλέγουν δεδομένα που σχετίζονται με την κατανάλωση από τα HAN των καταναλωτών και μεταφέρουν τις μετρήσεις μέσω του NAN στο WAN. Δέχονται όμως και πληροφορίες από το ευφυές δίκτυο ενέργειας, με την επικοινωνία να είναι αμφίδρομη. Επίσης, το NAN αποτελεί το last-mile τμήμα του AMI το οποίο είναι το πλήρες σύστημα συλλογής δεδομένων σε ένα ευφυές δίκτυο ενέργειας και αποτελεί το ενδιάμεσο δίκτυο ανάμεσα στο WAN και στο HAN όπου και επικοινωνεί με το WAN μέσω του backhaul δικτύου. Με την συλλογή των δεδομένων διαφορετικών HAN, η ιδιωτικότητα είναι ένας σημαντικός παράγοντας όπου είναι απαραίτητο με τις κατάλληλες τεχνικές αλλά και την σχεδίαση του δικτύου να διασφαλίζεται. Εκτός όμως από την ιδιωτικότητα των δεδομένων που διακινούνται λόγω ότι στο NAN περιλαμβάνονται εκατοντάδες ή ακόμα και χιλιάδες συσκευές είναι απαραίτητη η αυθεντικοποίηση και η κρυπτογράφηση των καναλιών επικοινωνίας ανεξάρτητα της τεχνολογίας που χρησιμοποιείται.

Στην συνολική ασφάλεια σημαντικό ρόλο παίζει η αρχιτεκτονική του δικτύου γιατί αναλόγως την αρχιτεκτονική και την τεχνολογία του χρησιμοποιείται οι απειλές ενδέχεται να διαφέρουν. Χαρακτηριστικά, η εφαρμογή mesh αρχιτεκτονικών όπου οι έξυπνοι μετρητές επικοινωνούν μεταξύ τους εκτός από τα πλεονεκτήματα που προσφέρει ως προς την διαθεσιμότητα του δικτύου, αυξάνει τους κινδύνους και δημιουργεί διαφορετικές απειλές γιατί σε μια ενδεχόμενη επίθεση μπορούν εύκολα να προσβληθούν οι υπόλοιποι έξυπνοι μετρητές ή οι συλλέκτες δεδομένων. Συνολικά, η ασφάλεια στο NAN εστιάζει στους παρακάτω τρεις τομείς της ασφάλειας: (Weixiao Meng, 2014)

1. Συστήματα έγκαιρης ανίχνευσης επιθέσεων
2. Κρυπτογράφηση και αυθεντικοποίηση
3. Προστασία της ιδιωτικότητας

Η ανίχνευση εισβολών μέσω ενός IDS σε ένα δίκτυο δεν είναι καινούρια ιδέα. Η σχεδίαση και η εφαρμογή ενός IDS στα ευφυή δίκτυα ενέργειας και ειδικότερα στο NAN διαφέρει από την εφαρμογή των κοινών IDS. Για την σχεδίαση ενός IDS ο κύριος στόχος είναι η αναγνώριση των απειλών του δικτύου και των συσκευών που καλείται να προφυλάξει όπως και των δεδομένων που απαιτούνται για την ανίχνευση των απειλών αυτών. Εκτός από τους δύο παραπάνω στόχους, προκλήσεις στην σχεδίαση είναι, η ακρίβεια στην ανίχνευση καινούριων επιθέσεων, το μικρότερο δυνατό overhead αλλά και το μικρότερο διαχειριστικό και υπολογιστικό κόστος. (Robin Berthier W. S., 2010). Στο (David Grochocki, 2012) περιγράφονται οι πληροφορίες που απαιτούνται για την ανίχνευση απειλών από ένα IDS που καλείται να προστατέψει ένα σύστημα AMI:

1. Πληροφορίες συστήματος

Είναι οι πληροφορίες σχετικά με την κατάσταση(κατανάλωση πόρων κτλ) των έξυπνων μετρητών, των συλλεκτών δεδομένων αλλά και η κατάσταση σχετικά με το λογισμικό το οποίο διαθέτουν.

2. Πληροφορίες δικτύου

Είναι οι πληροφορίες σχετικά με την κατάσταση του δικτύου επικοινωνιών, όπως είναι το packet loss, response time ενός έξυπνου μετρητή, το collision rate, αλλά και η ακεραιότητα των πινάκων δρομολόγησης σε περίπτωση υλοποίησης μιας mesh αρχιτεκτονικής.

3. Πληροφορίες πολιτικής

Είναι οι πληροφορίες σχετικά με τα πρωτόκολλα που χρησιμοποιούνται για το σύστημα AMI, τους τύπους των συσκευών, εξουσιοδοτημένες ενημερώσεις δρομολόγησης, εξουσιοδοτημένες αναβαθμίσεις λογισμικού σε συσκευές.

Εκτός από τον καθορισμό των πληροφοριών που απαιτούνται για την ανίχνευση επιθέσεων, σημαντικός παράγοντας είναι η αρχιτεκτονική ενός IDS. Ένα κοινό IDS βασίζεται σε ένα κεντρικό σύστημα διαχείρισης που συγκεντρώνει δεδομένα από τους ονομαζόμενους sensors ή agents. Στα ευφυή δίκτυα ενέργειας λόγω των ιδιαιτεροτήτων που έχουν ένα τέτοιο σύστημα δεν μπορεί να λειτουργήσει αποτελεσματικά. Εάν η λήψη των δεδομένων που απαιτούνται γίνεται στο head-end του AMI συστήματος, όπου συλλέγονται τα δεδομένα από όλους τους έξυπνους μετρητές ενέργειας, επιθέσεις που θα πλήξουν έναν έξυπνο μετρητή ή έναν συλλέκτη δεδομένων δεν θα γίνουν αντιληπτές.

Τέτοιες επιθέσεις είναι η εγκατάσταση κακόβουλου λογισμικού σε έξυπνους μετρητές ή σε συλλέκτες δεδομένων, υποκλοπή δεδομένων, όπως και επιθέσεις που στόχο έχουν την ακεραιότητα των δεδομένων(επίθεση false data injection). Επίσης, επιθέσεις που έχουν στόχο χαμηλότερα επίπεδα δικτύωσης δεν θα μπορούν να ανιχνευτούν, μιας και ο έλεγχος γίνεται σε επίπεδο εφαρμογών για την συγκέντρωση των δεδομένων. Είναι κατανοητό, πως ένα τέτοιο κεντρικό σύστημα δεν μπορεί να εφαρμοσθεί στα ευφυή δίκτυα ενέργειας και πως το σύστημα που

πρέπει να σχεδιασθεί πρέπει να είναι κατανεμημένο σε όλο το εύρος του ευφυούς δικτύου ενέργειας.

Η δεύτερη αρχιτεκτονική IDS, βασίζεται στην ενσωμάτωση sensor ή agent σε κάθε έξυπνο μετρητή ενέργειας δημιουργώντας ένα κατανεμημένο IDS σε όλο το εύρος του ευφυούς δικτύου ενέργειας. Τα δεδομένα που συγκεντρώνουν σχετίζονται με την κατάσταση λειτουργίας του έξυπνου μετρητή, όπως πόροι που καταναλώνονται(μνήμη, cpu usage), κατάσταση λογισμικού. Από την άλλη μεριά, οι έξυπνοι μετρητές γίνονται περιπλοκότεροι στην κατασκευή και πιθανόν ξεπερνώντας περιορισμούς κατασκευαστικούς όπως είναι το όριο των 5watt που καθορίζεται από τα πρότυπα ANSI C12.1 και IEC 62053-61. Επιπλέον, αυξάνεται το συνολικό overhead στην επικοινωνία προς το ευφυές δίκτυο ενέργειας, και απαιτείται η εφαρμογή QoS. Πάνω στην ίδια κατανεμημένη αρχιτεκτονική έχει προταθεί η εφαρμογή sensor ή agent σε επιλεγμένους έξυπνους μετρητές για δίκτυα που βασίζονται στην αρχιτεκτονική mesh.

Οι συγκεκριμένοι έξυπνοι μετρητές ενσωματώνουν παραπάνω λειτουργίες ανίχνευσης των δεδομένων, μιας και σε ένα mesh δίκτυο, μερικοί σταθμοί λειτουργούν σε κατάσταση relay, προωθώντας τα δεδομένα που δέχονται από τους γειτονικούς τους σταθμούς που είναι συνδεμένοι. Με αυτό τον τρόπο επιτυγχάνεται η έγκαιρη ανίχνευση απειλών που ξεκινούν από τους έξυπνους μετρητές ή μέσα από το ίδιο το HAN και στόχο έχουν την επέκταση τους στο υπόλοιπο mesh δίκτυο ή στους συλλέκτες δεδομένων. Με την τοποθέτηση sensor ή agent μονό στους έξυπνους μετρητές, επιθέσεις που θα πραγματοποιηθούν με στόχο ένα συλλέκτη δεδομένων δεν θα γίνουν αντιληπτές. Με την επικοινωνία στο AMI να είναι κρυπτογραφημένη από άκρο σε άκρο, για την διασφάλιση των ενδιάμεσων επιθέσεων, για να λειτουργήσει σωστά αυτό το κατανεμημένο IDS, χρειάζεται να αποκρυπτογραφεί τα δεδομένα για να εξετάζει το περιεχόμενο των πακέτων που διακινούνται στο δίκτυο. Η διαδικασία αυτή, κοστίζει και σε υπολογιστικό κόστος, καθυστέρηση, αλλά και σε επίπεδο διαχειρισμού των κλειδιών. Οι παραπάνω περιορισμοί οδηγούν στην ανάγκη ανάπτυξης μιας νέας αρχιτεκτονικής σχεδιασμένη με γνώμονα την κάλυψη των απαιτήσεων αυτών.

Η τρίτη αρχιτεκτονική, βασίζεται στην τοποθέτηση των sensor ή agent, σε καίρια σημεία της δικτυακής υποδομής. Ένα τέτοιο σημείο είναι οι συλλέκτες δεδομένων όπου συγκεντρώνουν τα δεδομένα από τους έξυπνους μετρητές. Το πρόβλημα που προκύπτει από την προηγούμενη αρχιτεκτονική σχετικά με την διαχείριση των κλειδιών για την εξέταση πακέτων στους έξυπνους μετρητές, μπορεί να καλυφθεί από την αποκρυπτογράφηση των δεδομένων στους συλλέκτες δεδομένων για την εξέταση των πακέτων που διακινούνται στο δίκτυο μιας και ο αριθμός των συλλεκτών δεδομένων είναι μικρότερος και ευκολότερα διαχείρισιμος. Επιπλέον, οι υπολογιστικές ικανότητες των συλλεκτών δεδομένων είναι μεγαλύτερες. Όμως επιθέσεις που ενδέχεται να παρουσιαστούν στους έξυπνους μετρητές, όπως η εγκατάσταση κακόβουλου λογισμικού για DoS επιθέσεις δεν θα μπορούν να ανιχνευτούν εγκαίρως. Αντίστοιχα, επιθέσεις που ξεκινούν από το HAN,

βασισμένες στην παραβίαση της ακεραιότητας των δεδομένων, όπως είναι η επίθεση false data Injection, δεν θα μπορούν να ανιχνευτούν.

Η τέταρτη αρχιτεκτονική έρχεται να καλύψει τα κενά που δημιουργούνται από τις προηγούμενες, και εκτός από την τοποθέτηση sensor ή agent σε επιλεγμένους έξυπνους μετρητές ενέργειας, τοποθετούνται αντίστοιχα σε άλλες συσκευές , όπως είναι οι συλλέκτες δεδομένων. Ακόμη, εξέταση των δεδομένων και σύγκριση σε σχέση με αυτά που λαμβάνονται από τους έξυπνους μετρητές ενέργειας γίνεται και στο head-end του AMI, και έτσι διασφαλίζεται η ακεραιότητα των δεδομένων από άκρο σε άκρο. Με αυτό τον τρόπο, η παρακολούθηση του δικτύου γίνεται από άκρο σε άκρο με αποτέλεσμα να ανιχνεύονται απειλές έγκαιρα και χωρίς να αφήνονται σημεία του δικτύου που δεν έχουν καλυφθεί. Συνεπώς, η τελευταία αυτή αρχιτεκτονική που περιγράφηκε δείχνει να είναι η πιο κατάλληλη για εφαρμογή στα ευφυή δίκτυα ενέργειας, καλύπτοντας επαρκώς το NAN και συνδυάζοντας σε μα υβριδική αρχιτεκτονική τα πλεονεκτήματα των υπολοίπων. (David Grochocki, 2012) (Alvaro A. Cárdenas, 2014)

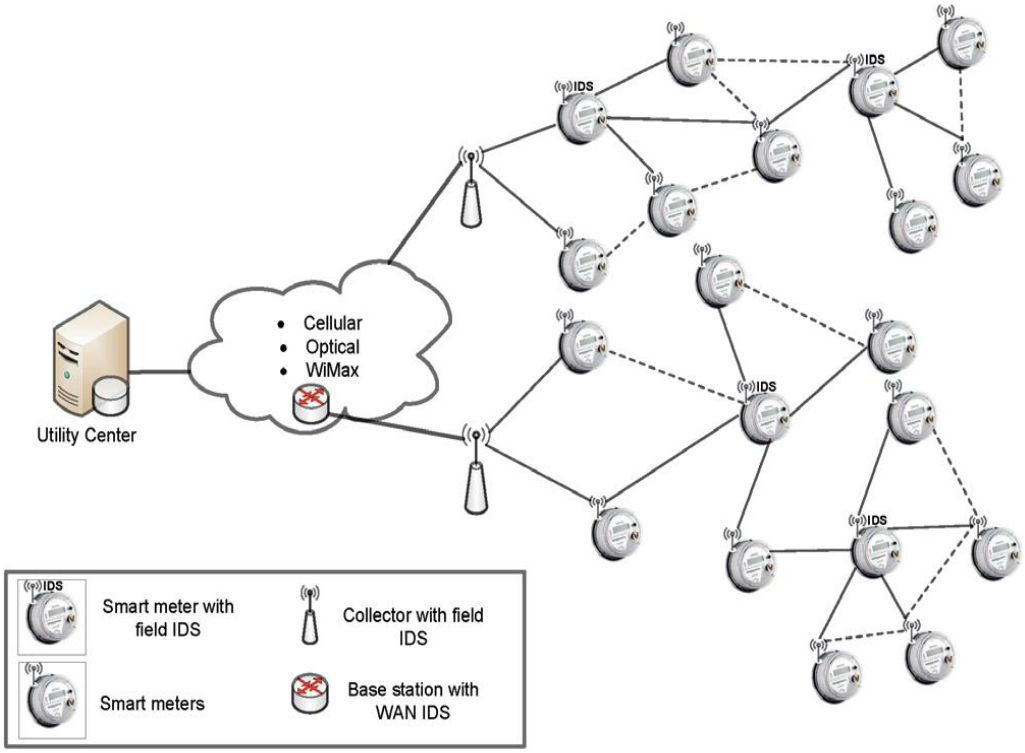
Ένα IDS που ανήκει στην τελευταία αυτήν υβριδική κατηγορία παρουσιάζεται στο (Beigi-Mohammadi, 2012), το οποίο έχει στόχο την προστασία του AMI από επιθέσεις. Το IDS αυτό ανήκει στην κατηγορία των IDS ανίχνευσης ανωμαλιών, έχει σχεδιασθεί για δίκτυο στο NAN που ακολουθεί την αρχιτεκτονική mesh και τέλος αποτελείται από τρεις τύπους κόμβων:

1. Field IDS
2. Wan IDS
3. Central IDS

Τα Field IDS είναι εγκατεστημένα σε επιλεγμένους έξυπνους μετρητές ενέργειας στο δίκτυο mesh του NAN, όπως και σε συλλέκτες δεδομένων. Για την εγκατάσταση τους στους έξυπνους μετρητές ενέργειας, απαιτείται μεγαλύτερη υπολογιστική ισχύ αλλά και αποθηκευτική δυνατότητα σε σχέση με τους υπολοίπους έξυπνους μετρητές. Κάθε έξυπνος μετρητής που δεν έχει εγκατεστημένο ένα Field IDS, είναι απαραίτητο να επικοινωνεί με ένα.

Ο σκοπός εγκατάστασης των Field IDS είναι η παθητική παρακολούθηση της κίνησης του δικτύου mesh και συχνά στέλνουν μηνύματα συγχρονισμού και ανίχνευσης προς το WAN IDS. Το WAN IDS βρίσκεται εγκατεστημένο σε κάποιο σημείο, όπου το WAN ενώνεται με το NAN, με το ονομαζόμενο back haul δίκτυο και είναι υπεύθυνο για την αποστολή και λήψη δεδομένων από τους συλλέκτες δεδομένων. Σε περίπτωση που έχει ανιχνευθεί επίθεση και έχει σημάνει συναγερμός, το WAN IDS ενημερώνει στο Central IDS που βρίσκεται στο κέντρο διαχείρισης του ευφυούς δικτύου ενέργειας. Επίσης, το Central IDS είναι υπεύθυνο για την διαχείριση ολόκληρου του IDS και είναι αυτό που με βάση τα στοιχεία που συλλέγονται από το NAN και WAN, λαμβάνει τις τελικές αποφάσεις. Η λειτουργία του IDS παρουσιάζεται σε τρεις φάσεις:

1. Συλλογή δεδομένων από Field IDS όπου αναλύουν τα δεδομένα που λαμβάνουν από τους γειτονικούς έξυπνους μετρητές. Οι WAN IDS, ελέγχουν και οι ίδιοι τα δεδομένα σε δεύτερο βαθμό, εάν υπάρχει μη-φυσιολογική κατάσταση ενώ, το Central IDS ελέγχει την κατάσταση ολόκληρου του IDS, και εάν η επικοινωνία με τα WAN IDS λειτουργεί απρόοπτα.
2. Ανάλυση δεδομένων που έχουν συγκεντρωθεί ώστε να διαπιστωθεί εάν οι συμπεριφορά του δικτύου είναι σε φυσιολογική κατάσταση
3. Η ανάλυση των δεδομένων αποστέλλεται στο Central IDS, για την τελική απόφαση ένα υπάρχει μια μη-φυσιολογική κατάσταση και ένα απαιτείται λήψη μέτρων προστασίας. Για καλύτερη αποτελεσματικότητα και ακρίβεια είναι απαραίτητο να κρατείται στο Central IDS, ιστορικό με προηγούμενες αναλύσεις του δικτύου, ώστε να γίνεται σύγκριση ένα υφίσταται επίθεση ή κάποιο πρόβλημα στην λειτουργία του δικτύου επικοινωνιών.



Εικόνα 41 "Δομή του IDS στο NAN" (Beigi-Mohammadi, 2012)

Τα IDS που ανήκουν στην κατηγορία Specification-based, πραγματοποιούν την ανίχνευση των επιθέσεων βασιζόμενα σε κανόνες που έχουν προκαθοριστεί σε σχέση με τα IDS άλλων κατηγοριών που βασίζονται στην ανίχνευση ιχνών(υπογραφών) των επιθέσεων. Επίσης, στο ίδιο IDS περιγράφεται ο τρόπος ορισμού των κανόνων με βάση την επίθεση. Χαρακτηριστικό παράδειγμα είναι για την πρόληψη μιας επίθεσης DoS βασιζόμενη στην τεχνική του flooding, απαιτείται η δημιουργία ενός κανόνα που ορίζει ένα όριο στο μέγεθος των δεδομένων. Το μέγεθος των δεδομένων που διακινούνται είναι περίπου σταθερό, με τον ορισμό ενός κανόνα που έχει ένα αριθμητικό μέγεθος μπορούν να ανιχνευτούν επιθέσεις flooding, που έχουν στόχο την δημιουργία περιττής κίνησης στο δίκτυο. Ένας άλλος κανόνας για την αντιμετώπιση επιθέσεων τύπου jamming, μπορεί να δημιουργηθεί με βάση το κανάλι επικοινωνίας και την συχνότητα που επικοινωνούν δύο έξυπνοι μετρητές. Σε περίπτωση που ανιχνευτούν υψηλά επίπεδα θορύβου το IDS, έχει την δυνατότητα να σημάνει συναγερμό. Η ανίχνευση επιθέσεων DoS, δεν περιορίζεται μόνο σε έναν κανόνα ή σε ένα συγκεκριμένο τμήμα. Η καθυστέρηση στην επικοινωνία μπορεί με την χρήση κανόνα να χρησιμοποιηθεί για ανίχνευση απειλών. Ειδικότερα, το κέντρο διαχείρισης αποστείλει μια συγκεκριμένη εντολή προς έναν έξυπνο μετρητή και αυτός καθυστερήσει να απαντήσει μέσα σε ένα συγκεκριμένο χρονικό διάστημα, μπορεί να επισημανθεί ως ύποπτος για να παρακολουθηθεί η κατάσταση από το IDS. Οι επιθέσεις DoS αυξάνουν την καθυστέρηση στην επικοινωνία, οπότε με αυτό τον τρόπο είναι εύκολο να ανιχνευτούν. Επιπλέον, για την ανίχνευση DoS επίθεσης στο mesh δίκτυο, με την δημιουργία ενός κανόνα στα Field IDS, και από την στιγμή που κάθε έξυπνος μετρητής επικοινωνεί με έναν μόνο Field IDS, είναι εύκολο να διαπιστωθεί αν ένας μολυσμένος έξυπνος μετρητής προσπαθεί να δημιουργήσει συνδέσεις με άλλους, όπου δεν επιτρέπεται. Τέλος, κανόνας μπορεί να δημιουργηθεί και με βάση την προέλευση των request/response. Ειδικότερα, το Central IDS είναι το μόνο που ζητάει δεδομένα από τα WAN και Field IDS, ενώ τα δύο τελευταία απαντούν στα ερωτήματα. Εάν ένας έξυπνος μετρητής προσπαθήσει να αποστείλει δεδομένα σε διαφορετικό παραλήπτη από το προκαθορισμένο, χρειάζεται να σημάνει συναγερμός για αναγνώριση του περιστατικού. Να σημειωθεί ότι τα IDS που χρησιμοποιούν κανόνες για την ανίχνευση έχουν το μεγαλύτερο ρυθμό αποτυχημένων συναγερμών, μιας και οτιδήποτε δεν έχει προκαθοριστεί από κανόνα θεωρείται ως ύποπτο.

Ένα IDS που ανήκει σε διαφορετική κατηγορία από το προηγούμενο που μελετήθηκε παρουσιάζεται στο (Robin Berthier W. H., 2011). Ειδικότερα, το IDS που παρουσιάζεται ανήκει στην κατηγορία των Specification-based IDS. Τα Specification-based IDS μοιάζουν με τα Anomaly-based IDS, στο ότι και τα δύο βασίζονται στην ανίχνευση επιθέσεων ως προς την αλλαγή της κατάστασης από την κανονική-φυσιολογική λειτουργία του ευφυούς δικτύου ενέργειας που καλούνται να προστατέψουν. Επίσης τα Specification based IDS, για την ανίχνευση των επιθέσεων τους βασίζονται σε κανόνες που έχουν προκαθοριστεί με σκοπό να φιλτράρουν την φυσιολογική συμπεριφορά του δικτύου. Σε σχέση με

τα IDS που ανήκουν στην κατηγορία των Anomaly-based, έχουν μικρότερο ρυθμό λανθασμένων συναγερμών λόγω άγνωστων καταστάσεων που δεν έχουν προκαθοριστεί από κανόνες ενώ δεν αποτελούν απειλή. Τα μειονεκτήματα της κατηγορίας αυτής εστιάζουν στο ότι είναι το κόστος καθορισμού των κανόνων είναι μεγάλο και αποτελεί μια χρονοβόρα διαδικασία. Ένα ακόμη μειονέκτημα είναι η δυσκολία αναγνώρισης εάν οι κανόνες που έχουν προκαθοριστεί καλύπτουν όλες οι απειλές που καλούνται να αντιμετωπίσουν.

Οι ίδιοι συγγραφείς και σε προηγούμενη μελέτη τους στο (Robin Berthier W. S., 2010) θεωρούν τα specification based IDS τα καταλληλότερα σε σχέση με τα υπόλοιπα για τους λόγους που μόλις αναφέρθηκαν. Το συγκεκριμένο IDS βασίζεται σε sensors που βρίσκονται σε έξυπνους μετρητές και συλλέκτες δεδομένων και εξετάζουν το επίπεδο δικτύου, μεταφορά και εφαρμογών του OSI. Για την υλοποίηση του AMI, χρησιμοποιείται το ANSI C12.22 και πάνω στο πρωτόκολλο αυτό, προκαθορίζονται όλοι οι κανόνες ώστε σε ενδεχόμενη παραβίαση του να υπάρξει έγκαιρη ανίχνευση. Ορίζονται τρία καταστάσεις λειτουργίας και σύμφωνα με τις καταστάσεις αυτές καθορίζονται και για το καθένα διαφορετικές λειτουργίες και δικαιώματα. Τα τρία επίπεδα είναι, in use, to configure, offline. Η φυσιολογική κατάσταση λειτουργίας είναι το in use, ενώ στην κατάσταση to configure, ο έξυπνος μετρητής έχει περιορισμένες δυνατότητες, μόνο να λαμβάνει πληροφορίες ρυθμίσεων και δεν αλληλεπιδρά με άλλους έξυπνους μετρητές. Τέλος, στην κατάσταση off line, ο έξυπνος μετρητής, δεν αναγνωρίζεται από το IDS και αποκόπτεται από το δίκτυο. Για παράδειγμα, ένας έξυπνος μετρητής, που δεν έχει αναγνωρίζεται από το IDS, σε ενδεχόμενη επίθεση spoofing, μπαίνει σε κατάσταση to configure, για να λάβει τις ρυθμίσεις, να γίνει προσπάθεια αναγνώρισης και να διερευνηθεί το περιστατικό.

Σημαντικό σημείο στο IDS αυτό είναι και η οργάνωση των κανόνων που δημιουργούνται. Οι κανόνες χωρίζονται σε τρείς κατηγορίες, network based, device based, application based ενώ για κάθε κατηγορία ορίζονται και τύποι κανόνων οι οποίοι είναι, data, access, timing, resource usage και operational. Οι κατηγορίες και οι τύποι αυτοί έχουν καθοριστεί με βάση τις γνωστές επιθέσεις που υπάρχουν, όπως και την κατηγοριοποίηση των δεδομένων που διακινούνται. Η κύρια ιδέα του IDS, είναι ελέγχονται οι συνδέσεις-μονοπάτια ανάμεσα στους έξυπνους μετρητές στο δίκτυο mesh, ώστε να μην παραβιάζεται κανένας κανόνας. Οι προσπάθειες καθορισμού των κανόνων εστιάζονται σε 4 γενικούς κανόνες:

1. Μόνο σωστά ορισμένα αιτήματα και απαντήσεις του πρωτοκόλλου ANSI C12.22 επιτρέπονται στο επίπεδο εφαρμογών.
2. Μόνο το κεντρικό σύστημα διαχείρισης του IDS επιτρέπεται να δημιουργεί αιτήματα προς τους έξυπνους μετρητές.
3. Αιτήματα που χαρακτηρίζονται ως ευαίσθητα, όπως είναι για την δημιουργία συνδέσεων-αποσυνδέσεων(remote disconnect) επιτρέπονται να πραγματοποιούνται με έναν συγκεκριμένο ρυθμό Y ανά ώρα. Με αυτό, τον τρόπο προλαμβάνονται remote disconnect επιθέσεις στο δίκτυο mesh.

4. Σωστά παραμετροποιημένοι και σε κατάσταση in use έξυπνοι μετρητές, πρέπει να απαντούν σε αιτήματα μέσα σε ένα προκαθορισμένο χρονικό διάστημα.

Ο πρώτος κανόνας έχει καθοριστεί για την ανίχνευση επιθέσεων παραβίασης της ακεραιότητας των δεδομένων που διακινούνται στο δίκτυο. Ο δεύτερος κανόνας αντίστοιχα για την αναγνώριση μολυσμένων έξυπνων μετρητών, ενώ ο τρίτος, για την αποτροπή ένας μολυσμένος έξυπνος μετρητής να μολύνει γειτονικούς. Τέλος, ο τέταρτος κανόνας, για την έγκαιρη ανίχνευση DoS επιθέσεων. Τέλος, στο πάνω στο συγκεκριμένο IDS γίνεται προσομοίωση εφαρμογής των κανόνων αυτών στο ANSI C12.22 και παρουσίαση των αποτελεσμάτων. Να σημειωθεί ότι στο συγκεκριμένο IDS, το οποίο βρίσκεται σε εξέλιξη, δεν έχει ληφθεί υπόψη η κρυπτογράφηση των δεδομένων, η διαχείριση κλειδιών και το overhead που προκύπτει.

Όπως και στο WAN έτσι και στο NAN, η αυθεντικοποίηση των έξυπνων μετρητών και των συλλεκτών δεδομένων είναι απαραίτητη. Επίσης, πάνω στην αυθεντικοποίηση στηρίζονται η ακεραιότητα και η εμπιστευτικότητα των δεδομένων που διακινούνται. Οι τρεις αυτοί όροι, ενώ είναι ανεξάρτητοι είναι απαραίτητο να συνδυαστούν αποτελεσματικά για την επίτευξη ενός ασφαλούς δικτύου επικοινωνιών στα ευφυή δίκτυα ενέργειας. Να σημειωθεί ότι η κύρια πρόκληση εκτός από την ανάπτυξη σχημάτων αυθεντικοποίησης είναι και η διαχείριση των κλειδιών από το ευφυές δίκτυο ενέργειας, μιας και το NAN χαρακτηρίζεται από μεγάλο πλήθος συσκευών και πολυπλοκότητα.

Για την αυθεντικοποίηση, κατά κύριο λόγο υλοποιούνται αρχιτεκτονικές που βασίζονται στην υποδομή δημοσίου κλειδιού αλλά εκτός από αυτές υπάρχουν και άλλες που βασίζονται σε αυθεντικοποίηση με αναγνωριστικό ή ακόμη και χωρίς την χρήση αρχής πιστοποίησης. (Mohamad Badra, 2013) Για την ακριβή μελέτη των σχημάτων αυθεντικοποίησης, είναι απαραίτητος ο καθορισμός των απειλών από τους οποίους καλούνται να προστατέψουν το ευφυές δίκτυο ενέργειας αλλά και του τρόπου που διαχειρίζονται τα κρυπτογραφικά κλειδιά. Στο (Himanshu Khurana, 2010) καθορίζονται μερικές βασικές αρχές που πρέπει να καλύπτουν τα σχήματα αυθεντικοποίησης όχι μόνο στο NAN, αλλά για ολόκληρο το σύστημα του AMI. Έμφαση κατά την σχεδίαση ενός σχήματος χρειάζεται να δίνεται στην απόδοση του σχήματος, στο μικρότερο δυνατό υπολογιστικό κόστος, με το μικρότερο δυνατό overhead, αλλά και με το μικρότερο δυνατό οικονομικό κόστος για την εφαρμογή του σχήματος στους έξυπνους μετρητές(ανάγκη για hardware). Τέλος, αναφέρεται ότι κοινό λάθος είναι η εφαρμογή ενός σχήματος αυθεντικοποίησης σε ένα περιβάλλον με απειλές τις οποίες το σχήμα δεν είναι κατάλληλο και απαιτούνται σημαντικές αλλαγές πάνω στο ίδιο σχήμα.

Μια κατηγορία αυθεντικοποίησης δημοσίου κλειδιού είναι η ID-based PKI που μειώνει την ανάγκη αρχής πιστοποίησης. Στην κατηγορία αυτή τα σχήματα χρησιμοποιούν για την αυθεντικοποίηση δημόσιο και ιδιωτικό κλειδί, άλλα το δημόσιο κλειδί ορίζεται ως μια πληροφορία που είναι μοναδική για κάθε χρήστη ή

συσκευή. Αυτό μπορεί να είναι ένα όνομα, ή ακόμη και μια διεύθυνση δικτύου. Ένα σχήμα αυθεντικοποίηση και διαχείρισης κλειδιών μελετάται στο (Hasen Nicanfar, Smart grid authentication and key management for unicast and multicast communications, 2011) όπου οι υποχρεώσεις της αρχής πιστοποίησης μεταφέρονται σε έναν server(Security Associate) στο κέντρο διαχείρισης. Το σχήμα αυτό έχει δύο κρυφές τιμές, όπου στο SA αποθηκεύεται η κύρια, ενώ στους έξυπνους μετρητές αποθηκεύονται οι δευτερεύοντες(η οποία είναι ένας αθροιστής, ένας τυχαίος αριθμός που έχει δημιουργηθεί από το SA). Ακόμη, ο SA διατηρεί μια συνάρτηση(one way hash) η οποία εφαρμόζεται στο αναγνωριστικό(στο σχήμα αυτό είναι η IP διεύθυνση) του κάθε έξυπνου μετρητή και η οποία αποδίδει το δημόσιο κλειδί. Ο SA είναι υπεύθυνος για την παροχή του ιδιωτικού κλειδιού στον έξυπνο μετρητή το οποίο υπολογίζεται από το τυχαίο αθροιστή στο SA σε συνδυασμό με το αναγνωριστικό του έξυπνου μετρητή και την κρυφή τιμή του SA.

Επίσης, κατά την εγκατάσταση ενός νέου έξυπνου μετρητή πραγματοποιείται η διαδικασία της αυθεντικοποίησης με τον SA. Για να γίνει αυτό, ο καινούριος έξυπνος μετρητής που εγκαθίσταται στο δίκτυο, διαλέγει ένα ήδη αυθεντικοποιημένο έξυπνο μετρητή, ο οποίο αναφέρεται Authentication Agent. Κατά την διαδικασία αυτή, ο SA στέλνει το ιδιωτικό κλειδί στο έξυπνο μετρητή, αφού έχει ήδη υπολογίσει το δημόσιο κλειδί του AG και το δικό του για τον αντίστοιχο έξυπνο μετρητή. Σε περίπτωση που αποτύχει η αυθεντικοποίηση του καινούριο έξυπνου μετρητή ενημερώνεται ο SA, και η διαδικασία ξεκινάει από την αρχή με τον ίδιο ή άλλο AG. Με την χρήση του AG, ως ενδιάμεσου κατά την διαδικασία αυτή, εξασφαλίζεται η αυθεντικοποίηση του έξυπνου μετρητή στο SA, αλλά και ο SA στον έξυπνο μετρητή, με αποτέλεσμα οι δύο συσκευές να αναγνωρίζονται. Για την ανανέωση των κλειδιών ο SA, ανανεώνει τις κρυφές τιμές και μηδενίζει τον αθροιστή, ώστε η διαδικασία να ξεκινάει από την αρχή. Το σχήμα αυτό αν και είναι περίπλοκο, παρέχει μικρό overhead. Από την άλλη μεριά υπάρχουν όμως αντιθέσεις ως προς την χρήση του AG, μιας και σε περίπτωση που ο AG, είναι ήδη αυθεντικοποιημένος έχει μολυνθεί από κακόβουλο λογισμικό, ενδέχεται να διαρρεύσει σημαντικά στοιχεία της διαδικασίας αυθεντικοποίησης.

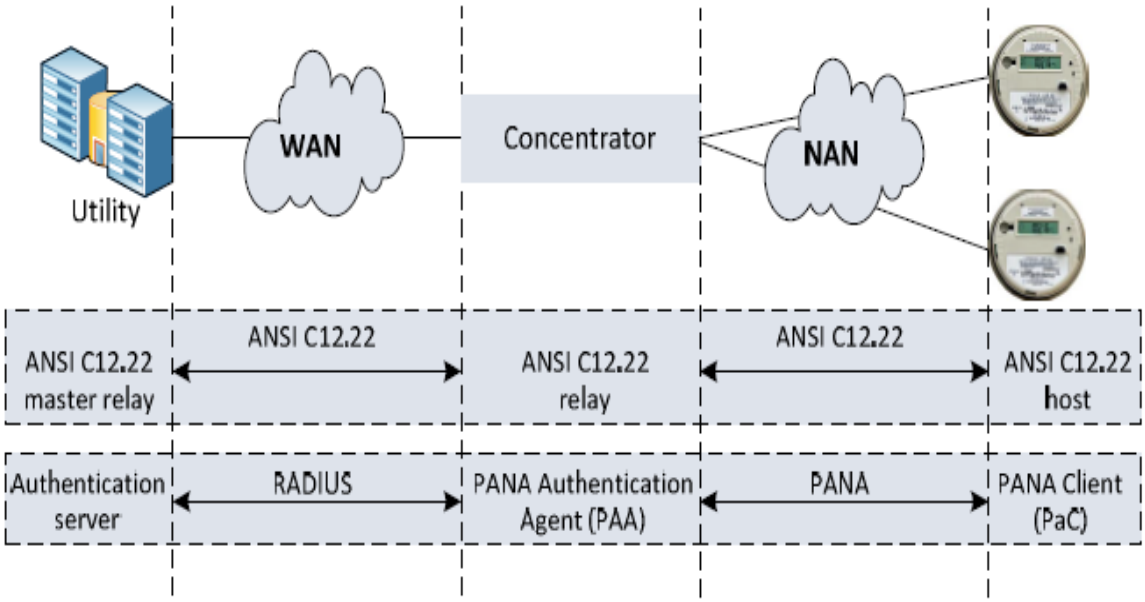
Αντίστοιχα ένα σχήμα που ανήκει στην ίδια κατηγορία των ID based PKI, το οποίο προσφέρει και κρυπτογράφηση των δεδομένων που διακινούνται και αυθεντικοποίηση αναλύεται στο (Hayden K.-H. So, 2010). Αρχικά, κάθε συσκευή πρέπει να αιτηθεί από κεντρικό σύστημα διαχείρισης κλειδιών το ιδιωτικό κλειδί της αν θέλει να έχει δυνατότητα τα αποκρυπτογραφεί τα δεδομένα που λαμβάνει ή για να υπογράφει τα δεδομένα που θέλει να στείλει. Επίσης κάθε συσκευή διαθέτει ένα μοναδικό αναγνωριστικό(μπορεί να καθοριστεί εύκολα κατά την κατασκευή της συσκευής). Το κεντρικό σύστημα διαχείρισης διαθέτει ένα κύριο κλειδί του σχήματος αυτού, το οποίο απαιτείται για την δημιουργία των ιδιωτικών κλειδιών κάθε συσκευής. Όταν μιας συσκευή διαθέτει το ιδιωτικό της κλειδί μπορεί να επικοινωνήσει με άλλες συσκευές χωρίς να παρεμβληθεί ξανά το κεντρικό σύστημα διαχείρισης. Συνεπώς, το overhead είναι πολύ μικρότερο σε σχέση με την εφαρμογή απλά μιας υποδομής δημοσίου κλειδιού με χρήση αρχής

πιστοποίησης. Όταν μια συσκευή θέλει να στείλει δεδομένα πρώτα, υπολογίζει το δημόσιο κλειδί του παραλήπτη με βάση το μοναδικό χαρακτηριστικό του, κρυπτογραφεί τα δεδομένα με ένα μοναδικό κλειδί που δημιουργείται από το δημόσιο κλειδί του παραλήπτη και τα επισημάνει με το ιδιωτικό της πριν τα αποστέλλει. Μόλις ο παραλήπτης, δεχθεί τα δεδομένα τα αποκρυπτογραφεί με το ιδιωτικό του κλειδί και στην συνέχεια με το δημόσιο κλειδί του αποστολέα. Το συγκεκριμένο σχήμα χρησιμοποιεί των αλγόριθμο AES.

Στο κεντρικό σύστημα διαχείρισης των κλειδιών υποστηρίζει και ανάκληση κλειδιών(key revocation), σε περίπτωση που το ιδιωτικό κλειδί κάποιας συσκευής διαρρεύσει. Η συσκευή αυτή πρέπει να δηλώσει την απώλεια όπως και να αλλάξει το μοναδικό αναγνωριστικό της. Το κεντρικό σύστημα διαχείρισης υπολογίζει ένα καινούριο ιδιωτικό κλειδί για την συσκευή και τοποθετεί σε έναν πίνακα που διαθέτει το παλιό αναγνωριστικό και το στέλνει broadcast στο δίκτυο για ενημερωθούν και οι υπόλοιπες συσκευές. Ο έλεγχος του πινάκα ανακλήσεων γίνεται ακόμη και όταν μια συσκευή θέλει να επικοινωνήσει με μια άλλη. Πρώτα ελέγχεται ο πίνακας και αν δεν υπάρχει το αναγνωριστικό τότε η διαδικασία συνεχίζεται κανονικά.

Τα προηγούμενα δύο σχήματα έχουν σχεδιασθεί για την αυθεντικοποίηση σε δίκτυα αρχιτεκτονικής mesh. Εκτός από mesh αρχιτεκτονική, προτείνεται και η χρήση point-to point συνδέσεων ανάμεσα σε έξυπνους μετρητές και συλλέκτες δεδομένων με χρήση ασύρματων τεχνολογιών όπως είναι το WiMAX. Όπως είναι κατανοητό τα προηγούμενα σχήματα που δεν μπορούν να λειτουργήσουν πάνω σε μια τέτοια αρχιτεκτονική.

Στο (David Famolari, 2012) περιγράφεται η υλοποίηση ενός σχήματος αυθεντικοποίησης βασισμένο στο Extensible Authentication Protocol(EAP), το οποίο είναι ένα ευρέως γνωστό σχήμα αυθεντικοποίησης για point to point ασύρματες συνδέσεις. Χαρακτηριστικό παράδειγμα είναι ότι το 802.11 και τα πρότυπα WPA και WPA2 χρησιμοποιούν το EAP. Επίσης, από πλευράς πρωτοκόλλου εφαρμογών για την συλλογή δεδομένων από τους έξυπνους μετρητές ενέργειας, προτείνεται η χρήση του ANSI C12.22. Για την αυθεντικοποίηση των έξυπνων μετρητών στους συλλέκτες δεδομένων προτείνεται η χρήση του Protocol for Carrying Authentication for Network Access(PANA) . Στο σχήμα αυτό, οι συλλέκτες δεδομένων λειτουργούν ως relay και το PANA χρησιμοποιείται για την μεταφορά των πακέτων του EAP.



Εικόνα 42 "Αρχιτεκτονική και αντιστοίχιση του EAP και ANSI C12.22" (Mohamad Badra, 2013)

Αφού έχει ολοκληρωθεί η αυθεντικοποίηση EAP, οι έξυπνοι μετρητές έχουν ην δυνατότητα να επικοινωνήσουν με το Meter Data Management System(MDMS) με το ANSI C12.22. Τέλος, ένα κλειδί που έχει δημιουργηθεί από το EAP, μοιράζεται ανάμεσα σε κάθε έξυπνο μετρητή, συλλέκτη δεδομένων και το ευφυές δίκτυο ενέργειας.

Στο (Seung-Hyun Seo, 2013) προτείνεται ένα σχήμα που ανήκει σε μια ειδική κατηγορία των ID based PKI με την ονομασία CertificateLess Public Key Cryptography(CL-PKC). Στο σχήμα αυθεντικοποίησης αυτό, το κέντρο διαχείρισης διαθέτει υποδομή δημοσίου κλειδιού με ψηφιακά πιστοποιητικά, αλλά όχι οι έξυπνοι μετρητές στο NAN. Αντί για την χρήση πιστοποιητικών χρησιμοποιείται το προτεινόμενο σχήμα για την διαχείριση των κλειδιών. Στα CL-PLC σχήματα, κάθε χρήστης διαθέτει ένα partial ιδιωτικό κλειδί και μια κρυφή τιμή ως το κανονικό του ιδιωτικό του κλειδί. Η κρυφή αυτή τιμή και το δημόσιο του κλειδί δημιουργούνται από το χρήστη. Το partial ιδιωτικό του κλειδί, δημιουργείται από το κέντρο διαχείρισης και προκύπτει ως συνδυασμός του κυρίως κλειδιού του κέντρου διαχείρισης, του μοναδικού αναγνωριστικού του κάθε χρήστη και μια τυχαία τιμή. Από την στιγμή, που το κέντρο διαχείρισης δεν έχει γνώση της κρυφής τιμής του κάθε χρήστη, δεν μπορεί να αποκρυπτογραφήσει τα δεδομένα ή να δημιουργήσει αντίστοιχα μια ψηφιακή υπογραφή. Με αυτό τον τρόπο, ο χρήστης έχει την δυνατότητα να κρυπτογραφήσει ένα μήνυμα χωρίς την ανάγκη πιστοποίησης του δημοσίου κλειδιού. Το κέντρο διαχείρισης των κλειδιών μεταφέρεται πλέον στους

συλλέκτες δεδομένων, οι οποίοι ο καθένας του διευθύνουν ένα σύνολο από έξυπνους μετρητές και δημιουργούν τα partial ιδιωτικά τους κλειδιά.

Πρόσφατα παρουσιάστηκε ένα σχήμα αυθεντικοποίησης το οποίο ανήκει στην κατηγορία των Mutual authentication σχημάτων και εστιάζει στην αμφίδρομη αυθεντικοποίηση ανάμεσα σε έξυπνους μετρητές και συλλέκτες δεδομένων. (Soohyun Oh, 2012) Οι συγγραφείς θεωρούν ότι τα σχήματα που ανήκουν στην κατηγορία των ID based PKI, με προκαθορισμένο ID, παρουσιάζουν ευπάθειες, έναντι επιθέσεων dictionary, επειδή το ID αυτό χρησιμοποιείται συνήθως για συγκεκριμένο χρονικό διάστημα και το μέγεθος των ID είναι συνήθως μικρό. Το προτεινόμενο σχήμα παρουσιάζεται στα παρακάτω βήματα:

1. Ο έξυπνος μετρητής στέλνει αίτημα αυθεντικοποίησης στο συλλέκτη δεδομένων.
2. Ο συλλέκτης δεδομένων, απαντάει με το δημόσιο πιστοποιητικό του.
3. Ο έξυπνος μετρητής λαμβάνει το πιστοποιητικό του και ανακτά το δημόσιο κλειδί.
4. Ο έξυπνος μετρητής δημιουργεί ένα τυχαίο προσωρινό κλειδί, το οποίο το κρυπτογραφεί με το δημόσιο κλειδί του συλλέκτη δεδομένων.
5. Ο έξυπνος μετρητής αποστέλλει το κρυπτογραφημένο μήνυμα στο συλλέκτη δεδομένων.
6. Ο συλλέκτης δεδομένων, αποκρυπτογραφεί το προσωρινό κλειδί με το δικό του ιδιωτικό κλειδί.
7. Ο συλλέκτης δεδομένων δημιουργεί έναν τυχαίο αριθμό και υπολογίζει μια hash κρυπτογραφική συνάρτηση με βάση το προσωπικό κλειδί που έλαβε και ένα κλειδί long-term κλειδί που υπάρχει ανάμεσα σε συλλέκτη και έξυπνο μετρητή. Επιπλέον, υπολογίζει μια συνάρτηση που βασίζεται σε συμμετρικό κλειδί με βάση, το αποτέλεσμα που προέκυψε από την προηγούμενη hash κρυπτογραφική συνάρτηση αλλά και το τυχαίο αριθμό που δημιούργησε στην αρχή.
8. Ο συλλέκτης δεδομένων αποστέλλει στον έξυπνο μετρητή το αποτέλεσμα της τελευταίας συνάρτηση.
9. Ο έξυπνος μετρητής αποκρυπτογραφεί το μήνυμα και με βάση το προσωρινό κλειδί που και το long-term κλειδί, υπολογίζει την hash κρυπτογραφική συνάρτηση.
10. Εάν το αποτέλεσμα είναι σωστό, Ο έξυπνος μετρητής δημιουργεί, έναν νέο τυχαίο αριθμό και υπολογίζει με βάση το προσωρινό κλειδί ,το long-term κλειδί, τον καινούριο τυχαίο αριθμό αλλά το τυχαίο αριθμό που δημιουργήθηκε από το συλλέκτη, την hash κρυπτογραφική συνάρτηση. Επίσης, υπολογίζει την συνάρτηση συμμετρικού κλειδιού, με βάση το προηγούμενο αποτέλεσμα, και του δύο τυχαίους προηγούμενους αριθμούς.
11. Ο έξυπνος μετρητής αποστέλλει το αποτέλεσμα της συνάρτησης συμμετρικού κλειδιού στο συλλέκτη δεδομένων.
12. Με βάση το προσωρινό κλειδί και τους δύο τυχαίους αριθμούς, ο έξυπνος μετρητής υπολογίζει μέσω μια ψευδοτυχαίας συνάρτησης τρεις νέες τιμές

MIK, το οποίο είναι ένα κλειδί για τον έλεγχο της ακεραιότητας των δεδομένων, το TK, το οποίο είναι ένα προσωρινό κλειδί και το KEK που είναι ένα κλειδί για χρησιμοποιείται για την κρυπτογράφηση ενός συνόλου κλειδιών.

13. Ο συλλέκτης δεδομένων αποκρυπτογραφεί, το αποτέλεσμα της συνάρτησης από το βήμα 11 και με βάση το προσωρινό, το long-term κλειδί, και τους δύο τυχαίους αριθμούς που έχουν δημιουργηθεί σε προηγούμενα βήματα υπολογίζει την hash κρυπτογραφική συνάρτηση για να ελέγχει ένα είναι σωστό.
14. Εάν το προηγούμενο βήμα είναι σωστό, το προσωρινό κλειδί, μαζί με τους δύο τυχαίους αριθμούς εφαρμόζεται η ψευδοτυχαία συνάρτηση με αποτέλεσμα τα κλειδιά MIK, TK και KEK.
15. Ο συλλέκτης δεδομένων κρυπτογραφεί το group key(GK) με το KEK.
16. Ο συλλέκτης δεδομένων αποστέλλει το κρυπτογραφημένο μήνυμα στον έξυπνο μετρητή.
17. Ο έξυπνος μετρητής με βάση το KEK κλειδί, αποκρυπτογραφεί το μήνυμα και ανακτά το GK.

Όπως και στο προηγούμενο σχήμα έτσι και στο (Sangji Lee, 2014) παρουσιάζεται ένα σχήμα που ανήκει στην κατηγορία των Mutual Authentication σχημάτων. Το συγκεκριμένο σχήμα χρησιμοποιεί υποδομή δημοσίου κλειδιού σε συνδυασμό με αυθεντικοποίηση αναγνωριστικού (ID-based PKI). Έμφαση δίνεται στο overhead, δηλαδή στην μείωση του πλήθους των μηνυμάτων που απαιτούνται για να ολοκληρωθεί η διαδικασία. Επίσης, γίνεται χρήση πιστοποιητικών από μια αρχή πιστοποίησης η οποία χορηγεί λειτουργίες στο σύστημα διαχείρισης της διαδικασίας της αυθεντικοποίησης αλλά και την λίστα που διαθέτει η αρχή πιστοποίησης. Στο σχήμα αυτό επίσης συμμετέχουν και οι συσκευές που συνδέονται με τους έξυπνους μετρητές ενέργειας.

Εκτός από την αυθεντικοποίηση στα ευφυή δίκτυα ενέργειας, σημαντικό είναι και η εξασφάλιση της ιδιωτικότητας των δεδομένων που διακινούνται στο δίκτυο επικοινωνιών, και ειδικά των δεδομένων που σχετίζονται σχετικά με την χρήση της ενέργειας από τους καταναλωτές. Η συλλογή δεδομένων από τους έξυπνους μετρητές ενέργειας, πέρα από την καταγραφή της κατανάλωσης ενέργειας, βοηθάει το ευφυές δίκτυο ενέργειας, στην συλλογή δεδομένων σχετικά με την ζήτηση/προσφορά και διαχείρισης της ενέργειας. Οι έξυπνοι μετρητές συλλέγουν εκτός από την κατανάλωση ενέργειας, και άλλες πληροφορίες όπως είναι διάρκεια λειτουργίας, πια συσκευή λειτουργεί κτλ. Τα προσωπικά αυτά δεδομένα των καταναλωτών σχετίζονται με την συμπεριφορά των καταναλωτών και την καθημερινότητα τους. Συνεπώς, είναι απαραίτητο να δημιουργηθούν οι κατάλληλες συνθήκες ότι αυτά τα δεδομένα δεν θα διοχετεύονται στο ευφυές δίκτυο ενέργειας και δεν θα τα γνωρίζει κάποιος άλλος εκτός από τους ίδιους. Η αξία των δεδομένων αυτών που σχετίζεται με την καθημερινότητα των χρηστών είναι πολύ σημαντική γιατί συλλέγοντας

δεδομένα που σχετίζονται με την συμπεριφορά των χρηστών δημιουργείται το αίσθημα ότι παραβιάζεται η ιδιωτικότητα τους. Χαρακτηριστικό παράδειγμα, τι θα γινόταν εάν διέρρεαν πληροφορίες σχετικά με το αν στην οικία υπάρχουν πολλές οικιακές συσκευές σε λειτουργία, ώστε να προκύψουν συμπεράσματα σχετικά με τις ώρες που βρίσκονται εκεί ή πόσες έξυπνες συσκευές συγκεκριμένου κατασκευαστή λειτουργούν μια συγκεκριμένη χρονική στιγμή.

Το αποτέλεσμα θα ήταν να υπάρχει η αίσθηση ότι η καθημερινότητα καταγράφεται χωρίς οι καταναλωτές να γνωρίζουν ποιοι κατέχουν τις πληροφορίες αυτές και πως τις διαχειρίζονται. Η αξία αυτών των πληροφοριών τα τελευταία χρόνια έχει αυξηθεί δραματικά, μιας και αυτές οι πληροφορίες χρησιμοποιούνται κατά κύριο λόγω για επιχειρηματικές δραστηριότητες, προώθηση στοχευόμενων πωλήσεων κτλ. Σε μια τέτοια περίπτωση, πλήττεται η αξιοπιστία του ευφυούς δικτύου ενέργειας, και δημιουργούνται απρόβλεπτες συνέπειες για την λειτουργία του. Στο (Zhong Fan, 2013) υποστηρίζεται ότι είναι δύσκολος ο ακριβής ορισμός των συνεπειών της παραβίασης της ιδιωτικότητας στα ευφυή δίκτυα ενέργειας και αυτό γιατί:

1. Δεν γνωρίζουμε τις συνέπειες από την εξαγωγή πληροφοριών από τα δεδομένα που διακινούνται.
2. Ο ακριβής ορισμός της ιδιωτικότητας στα ευφυή δίκτυα ενέργειας μέχρι στιγμή δεν έχει ορισθεί-προτυποποιηθεί.

Στην ίδια πηγή επισημαίνεται και ένα νέο πρόβλημα σχετικά με την ιδιωτικότητα το οποίο αναφέρεται ως Non-intrusive Appliance Load Monitoring (NALM) και εστιάζει στην ανάλυση των μετρήσεων ενέργειας για την εξαγωγή πληροφοριών σχετικά με την χρήση συσκευών.

Για την διασφάλιση της ιδιωτικότητας των δεδομένων που διακινούνται στο δίκτυο έχει προταθεί από πολλούς ερευνητές η χρήση data anonymization. Με τον όρο αυτό, ορίζεται μια τεχνολογία που μετατρέπει δεδομένα σε μια μορφή μη-αναγνωρίσιμη από το άνθρωπο και μη αναστρέψιμη. Η εφαρμογή της τεχνολογίας αυτή προτείνεται και από μια ομάδα εργασίας που έχει ορισθεί από την Ευρωπαϊκή Ένωση, με την ονομασία Smart Grid Task Force, για μελέτη της διαχείρισης των δεδομένων που διακινούνται σε ένα ευφυές δίκτυο ενέργειας. (Zhong Fan, 2013). Ένα γνωστό σχήμα που βασίζεται στην τεχνολογία αυτή και υλοποιείται για την προστασία δεδομένων των έξυπνων μετρητών έχει σχεδιασθεί στο (Costas Efthymiou, 2010). Ο στόχος του σχήματος αυτού είναι να περιέλθουν τα δεδομένα σε μια μορφή όπου δεν θα μπορούν να συνδεθούν με έναν έξυπνο μετρητή, συνεπώς και με έναν συγκεκριμένο χρήστη, αλλά θα μπορούν να χρησιμοποιηθούν από το ευφυές δίκτυο ενέργειας. Τα δεδομένα που παράγονται από έναν έξυπνο μετρητή ενέργειας διακρίνονται σε δύο τύπους:

1. High-Frequency, δηλαδή δεδομένα υψηλής συχνότητας
2. Low-Frequency, δηλαδή δεδομένα χαμηλής συχνότητας

Στην πρώτη κατηγορία ανήκουν τα δεδομένα που μεταδίδονται από έναν έξυπνο μετρητή ενέργειας αρκετά συχνά(συνήθως κάθε μερικά λεπτά) και περιλαμβάνουν πληροφορίες σχετικά με την διαχείριση και την κατανάλωση ενέργειας από το καταναλωτή. Στην δεύτερη κατηγορία ανήκουν τα δεδομένα που ένας έξυπνος μετρητής μεταδίδει όχι αρκετά συχνά(κάθε βδομάδα ή μήνα) προς το κέντρο διαχείρισης και χρησιμοποιούνται για χρέωση της κατανάλωσης ενέργειας. Το κύριο πρόβλημα εστιάζεται στο πως μπορούν τα δεδομένα που ανήκουν στην πρώτη κατηγορία να μεταποιηθούν σε μια μορφή, όπου δεν θα μπορούν να συνδεθούν με έναν συγκεκριμένο έξυπνο μετρητή χωρίς να επηρεαστεί η λειτουργία του δικτύου ή διαθεσιμότητα των δεδομένων. Ακόμη, κάθε έξυπνος μετρητής διαθέτει δύο μοναδικά αναγνωριστικά(ID):

1. HFID, High-Frequency ID
2. LFID, Low-Frequency ID

Κάθε μήνυμα έχει σήμανση με ένα από τα δύο παραπάνω αναγνωριστικά. Ο κύριος στόχος εδώ είναι η απόκρυψη της συσχέτισης του HFID από τα αντίστοιχα μηνύματα. Το HFID, εύκολα μπορεί να βρίσκεται αποθηκευμένο στον έξυπνο μετρητή από τον κατασκευαστή της συσκευής αυτής. Εδώ όμως προκύπτει το πρόβλημα πως το ευφυές δίκτυο ενέργειας θα αναγνωρίζει το μοναδικό αναγνωριστικό αυτό. Αυτό, γεννά την ανάγκη να χρησιμοποιηθεί μια τρίτη αρχή, συνδεμένη με το ευφυές δίκτυο ενέργειας, η οποία φυσικά θεωρείται έμπιστή από το ευφυές δίκτυο ενέργειας και είναι η μόνη που γνωρίζει το κάθε ζευγάρι HFID και LFID. Επίσης, η τρίτη αυτή αρχή χορηγεί σε κάθε έξυπνο μετρητή δύο ζευγάρια δημόσια//ιδιωτικά κλειδιά.

Στο σχήμα αυτό δίνεται έμφαση στην διαδικασία εγγραφής ενός έξυπνου μετρητή, δηλαδή η εισαγωγή του στο NAN. Η κύρια ιδέα της εγγραφής χωρίζεται σε δύο βήματα. Στο πρώτο βήμα, ο έξυπνος μετρητής ενημερώνει το κέντρο διαχείρισης για το LFID και το δημόσιο κλειδί του LFID. Στο δεύτερο βήμα, ο έξυπνος μετρητής αποστέλλει το HFID και το δημόσιο κλειδί του HFID στην τρίτη αυτή ανεξάρτητη αρχή, η οποία αναλαμβάνει να τα προωθήσει στο κέντρο διαχείρισης. Οι δύο αυτές διαδικασίες προτείνεται να γίνονται με μια χρονική καθυστέρηση για να μην υπάρχει δυνατότητα συσχετισμού. Εκτός από την τρίτη αρχή, χρησιμοποιούνται στο σχήμα και συλλέκτες δεδομένων που εξυπηρετούν ο καθένας ένα σύνολο έξυπνων μετρητών. Η διαδικασία συνεχίζεται με την αυθεντικοποίηση του έξυπνου μετρητή και του συλλέκτη δεδομένων, και σε δεύτερη φάση ενημερώνεται το κέντρο διαχείρισης ώστε να απαντήσει με μια συγκεκριμένη διαδικασία. Τέλος, η διαδικασία συνεχίζεται με την αποστολή των High frequency δεδομένων στην Τρίτη αρχή κάτω από μια σειρά διαδικασιών, ενώ τα Low Frequency αποστέλλονται στο συλλέκτη δεδομένων που συνδέεται ο έξυπνος μετρητής. (Xu Li, 2012).

Συμπερασματικά, το σχήμα αυτό, βασίζεται σε μεγάλο βαθμό στην τρίτη αρχή, για την σύνδεση των αναγνωριστικών με τα δεδομένα High-Frequency, εξίσου

σημαντικό είναι και το χρονικό διάστημα ανάμεσα στην αποστολή του αναγνωριστικού HFID και του δημοσίου κλειδιού στην Τρίτη αρχή πιστοποίησης.

Η χρήση data anonymization είναι μια πρόταση για την διασφάλιση της ιδιωτικότητας στα δεδομένα των καταναλωτών. Μια άλλη λύση στο πρόβλημα αυτό έρχεται να δοθεί με την χρήση τεχνικών data aggregation, που θεωρείται ως αποδοτικότερη μιας και η προηγούμενη με την εισαγωγή της τρίτης αρχής γίνεται περίπλοκη. Το data aggregation υλοποιείται για την συλλογή δεδομένων από τους έξυπνους μετρητές ενέργειας, κατά κύριο λόγω σε NAN που βασίζεται σε αρχιτεκτονική δικτύου mesh. Τα δεδομένα κάθε έξυπνου μετρητή, συγκεντρώνονται σε συλλέκτες δεδομένων ακολουθώντας ένα μονοπάτι μέσα από το δίκτυο mesh και από εκεί προωθούνται προς το κέντρο διαχείρισης. Η ιδιωτικότητα χρειάζεται να διασφαλιστεί μιας και τα προσωπικά δεδομένα μέχρι να φτάσουν στους συλλέκτες δεδομένων διέρχονται από ένα πλήθος άλλων έξυπνων μετρητών.

Για την προστασία των δεδομένων γίνεται χρήση σχημάτων κρυπτογράφησης, ένα τέτοιο σχήμα έχει σχεδιασθεί και παρουσιασθεί στο (Fengjun Li B. L., 2010). Αναφέρεται αρχικά ότι η υπολογιστική ικανότητα των έξυπνων μετρητών δεν αποτελεί πρόβλημα αλλά το εύρος ζώνης σε περιπτώσεις που η συγκέντρωση δεδομένων είναι συχνή. Η λειτουργία του σχήματος βασίζεται στην δημιουργία μιας δενδρικής δομής(aggregation tree), όπου κάθε κόμβος του δέντρου συλλέγει τα δεδομένα των κόμβων που θεωρούνται παιδιά του και υπολογίζει ένα σύνολο το οποίο το προωθεί στον κόμβο όπου βρίσκεται από πάνω του στην δενδρική δομή(κόμβος πατέρας). Ο Συλλέκτης βρίσκεται στην κορυφή του δέντρου όπου συλλέγει τα δεδομένα ολόκληρου του δέντρου. Για την κατασκευή του δεντρικής αυτής δομής, υπάρχουν δύο παράμετροι όπου χρειάζεται να ληφθούν υπόψη:

1. Το ύψος του δέντρου πρέπει να είναι μικρό, για υπάρχει μικρός αριθμός βημάτων ανάμεσα στο τελευταίο κόμβο και το συλλέκτη, με σκοπό να διατηρείται σε όσο χαμηλά επίπεδα γίνεται ο χρόνος συγκέντρωσης των δεδομένων από άκρο σε άκρος(aggregation time).
2. Ένας κόμβος στο εσωτερικό του δέντρου, δεν πρέπει να έχει πολλούς κόμβους παιδιά, για την αποτροπή υψηλού υπολογιστικού κόστους και φόρτου στο δίκτυο επικοινωνιών.

Για την αποτροπή των δύο αυτών θεμάτων γίνεται χρήση η τεχνική breadth-first traversal. Αφού έχει σχεδιασθεί η δομή, έρχεται η σειρά για κρυπτογράφηση των δεδομένων, όπου χρησιμοποιείται ομομορφική κρυπτογράφηση(homomorphic encryption) σε κάθε έξυπνο μετρητή. Το είδος αυτής της κρυπτογράφησης επιτρέπει την διενέργειας πράξεων πάνω στο κρυπτογράφημα(ciphertext), χωρίς να χρειάζεται να αποκρυπτογραφηθεί. Το αποτέλεσμα μπορεί να συγκριθεί με την ίδια διενέργεια πράξεων στο plaintext. Αυτό επιτρέπει στους έξυπνους μετρητές να συμμετέχουν στην διενέργεια των συγχωνεύσεων χωρίς να γνωρίζουν πληροφορίες από άλλους έξυπνους μετρητές. Το σχήμα αυτό βασίζεται στον αλγόριθμό του Paillier. Όπου χρησιμοποιείται ένα δημόσιο κλειδί από κάθε έξυπνο

μετρητή, ενώ το ιδιωτικό κλειδί το γνωρίζει μόνο ο συλλέκτης δεδομένων για την αποκρυπτογράφηση των δεδομένων. Αυτό σημαίνει ότι οι συλλέκτες δεδομένων είναι απαραίτητο να έχουν ικανή υπολογιστική δύναμη για την αποκρυπτογράφηση των δεδομένων. Επίσης, στην δεντρική δομή που έχει δημιουργηθεί σε περίπτωση όπου ένας κόμβος έχει κάποιο λειτουργικό πρόβλημα, ενημερώνεται αμέσως ο κόμβος πατέρας, ο οποίος το προωθεί στο συλλέκτη για ενημέρωση του δέντρου.

Η μόνη περίπτωση που παρουσιάζεται πρόβλημα, αφορά την περίπτωση να δημιουργηθούν τέτοιες συνθήκες όπου η δεντρική δομή διασπαστεί σε τμήματα. Τέλος, η ευπάθειες στο σχήμα ιδιωτικότητας που παρουσιάστηκε αφορά την εισαγωγή λανθασμένων δεδομένων, δηλαδή σε επιθέσεις false data injection ή σε επιθέσεις προσποίησης ενός έξυπνου μετρητή. Αυτό συμβαίνει γιατί κάθε έξυπνος μετρητής δημιουργεί το κρυπτογράφημα και γνωρίζει το δημόσιο κλειδί συνεπώς μπορεί να δημιουργήσει ένα παραποιημένο κρυπτογράφημα.

Για να λυθούν οι ευπάθειες, οι ίδιοι ερευνητές προτείνουν βελτίωση του σχήματος που παρουσιάζεται στο (Fengjun Li B. L., 2012) με την χρήση ψηφιακής υπογραφής, μιας μορφής επιβεβαίωσης με στόχο την διασφάλιση της ακεραιότητας των δεδομένων. Να σημειωθεί ότι η ομομορφική κρυπτογράφηση δεν παρέχει επιβεβαίωση, ούτε σε ενδιάμεσους κόμβους, ούτε στον τελικό παραλήπτη, όπως είναι για παράδειγμα ένας συλλέκτης δεδομένων. Ο στόχος πάνω στο σχήμα αυτό, είναι η ανίχνευση παραβιάσεων της ακεραιότητας στο σημείο όπου συλλέγονται τα δεδομένα, όπως είναι ένας συλλέκτης δεδομένων, μέσω ανίχνευσης ανωμαλιών.

Η χρήση ψηφιακής υπογραφής σε ένα σχήμα που εφαρμόζει τεχνική data aggregation, παραβιάζει την αρχή λειτουργίας του σχήματος, δηλαδή την συλλογή των δεδομένων, και την παρουσίαση σου σε μια συνοπτική μορφή. Η λύση στο θέμα αυτό έρχεται με την χρήση ψηφιακής υπογραφής, όπου αποθηκεύεται μέσα στο μονοπάτι, δηλαδή, κάθε κόμβος αποστέλλει το Ciphertext, μαζί με την ψηφιακή υπογραφή στο κόμβο πατέρα, ενώ αυτός την ελέγχει και την αποθηκεύει. Ο έλεγχος και η αποθήκευση γίνεται για συγκεκριμένο χρονικό διάστημα στη μνήμη του κόμβου και όταν ξεπεραστεί το διάστημα αυτό, η ψηφιακή υπογραφή διαγράφεται. Η υπογραφή αποστέλλεται στο συλλέκτη δεδομένων, On-demand, όταν ζητηθεί, εάν ο συλλέκτης διαπιστώσει ανωμαλία στα δεδομένα που συγκεντρώνονται, δηλαδή παραποίηση. Η διαδικασία που ακολουθείται είναι συγκεκριμένη και ξεκινάει από το συλλέκτη δεδομένων αρχικά με σκοπό τον εντοπισμό του μολυσμένου/προβληματικού κόμβου. Η διαδικασία επιβεβαίωσης αυτή, με την ονομασία Incremental Verification, εισάγει μια διαφορετική λειτουργία στο παρόν σχήμα.

Σε περίπτωση που ένας κόμβος θεωρηθεί μολυσμένος ή προβληματικός, η δεντρική δομή, μπορεί να ξανακατασκευαστεί από την αρχή, ώστε τα παιδιά που προβληματικού κόμβου να μετακινηθούν σε έναν λειτουργικό κόμβο, ενώ ο προβληματικός αυτός κόμβος αποσυνδέεται από τον κόμβο πατέρα που ανήκει.

Αναλόγως την επίθεση μπορεί απαιτηθεί η ανανέωση των κλειδιών και η διανομή τους. Σημαντικό είναι ότι με την τεχνική αυτή, το υπολογιστικό κόστος γίνεται κατανεμημένο, δηλαδή οι συλλέκτες δεδομένων ελαφρύνονται από το φόρτο της συλλογής όλων των ψηφιακών υπογραφών από όλους τους έξυπνους μετρητές, αποφεύγοντας την διακίνηση μεγάλου όγκου δεδομένων. Σε περίπτωση ανίχνευσης ανωμαλίας, ο έλεγχος και εδώ γίνεται επιλεκτικά, οπότε το συνολικό overhead είναι μικρό.

Πρόσφατα παρουσιάσθηκε ένα πλαίσιο (Joseph Kamto, 2012) που προσφέρει συγκέντρωση δεδομένων όπως το προηγούμενο σχήμα, αυθεντικοποίηση και διαχείριση των κλειδιών. Και σε αυτό το σχήμα γίνεται χρήση της ομομορφικής κρυπτογράφησης για την προστασία της ιδιωτικότητας των δεδομένων που συγκεντρώνονται από έξυπνους μετρητές. Τα δεδομένα εδώ διαχωρίζονται σε τύπους, αυτά που σχετίζονται με την ζήτηση ενέργειας που αποστέλλονται πολύ συχνά, στους συλλέκτες και από εκεί προς το ευφυές δίκτυο ενέργειας, αλλά και αυτά που συλλέγονται σε μικρότερη συχνότητα με σκοπό, την χρέωση της καταναλωμένης ενέργειας.

Δίνοντας βαρύτητα και στην αυθεντικοποίηση των έξυπνων μετρητών, για τη πρόληψη επιθέσεων η αυθεντικοποίηση γίνεται ως εξής. Κάθε καινούριος έξυπνος μετρητής που θέλει να συνδεθεί στο NAN, αναζητά το ισχυρότερο σήμα(hello message) που εκπέμπεται από συλλέκτη δεδομένων ή από κάποιον έξυπνο μετρητή, και λαμβάνει το αντίστοιχο πιστοποιητικό, για επιβεβαίωση της νομιμότητας του και λήψης του δημοσίου κλειδιού. Με το δημόσιο κλειδί κρυπτογραφεί ένα κλειδί το οποίο προκύπτει από μια hash συνάρτηση που δέχεται ως είσοδο το δημόσιο κλειδί. Με την λήψη το μηνύματος, αφού έχει πραγματοποιήσει τον έλεγχο, απαντά στο έξυπνο μετρητή με ένα μήνυμα επιβεβαίωσης, το οποίο το κρυπτογραφεί με το δημόσιο κλειδί του έξυπνου μετρητή. Το session key που δημιουργήθηκε από την hash συνάρτηση χρησιμοποιείται για την ασφαλή επικοινωνία μεταξύ τους. Η ομομορφική κρυπτογράφηση στο σχήμα αυτό χρησιμοποιείται, για δεδομένα που στέλνονται συχνά και μπορούν να φανερώσουν την συμπεριφορά του καταναλωτή, ενώ για τα δεδομένα που σχετίζονται με την τιμολόγηση της καταναλωμένης ενέργειας, επειδή δεν απαιτείται κάποιου είδους συγχρονισμός, εφαρμόζεται στα δεδομένα μια hash συνάρτηση(SHA-1, MD5). Υπολογίζεται ένα κλειδί που προκύπτει από την συνάρτηση αυτή, το οποίο χρησιμοποιείται για κρυπτογράφηση των δεδομένων και αποστέλλεται στο κόμβο πατέρα μαζί με τον τυχαίο αριθμό που αντιστοιχεί στον έξυπνο μετρητή.

Πάνω στο (Fengjun Li B. L., 2010) που μελετήθηκε προηγουμένως, βασίζεται και το (Pan Deng, 2012) οποίο χρησιμοποιεί ομομορφική κρυπτογράφηση για προστασία της ακεραιότητας, αυθεντικοποίηση μέσω ID based PKI και προστασία της ακεραιότητας των δεδομένων με χρήση ψηφιακής υπογραφής. Κάθε έξυπνος μετρητής, έχει από την κατασκευή του αποθηκευμένο το ιδιωτικό του κλειδί και ένα μοναδικό αναγνωριστικό ID. Το δημόσιο κλειδί, και το αναγνωριστικό το γνωρίζει

το κέντρο διαχείρισης. Η αυθεντικοποίηση κάθε έξυπνου μετρητή γίνεται με τα παρακάτω βήματα:

1. Κάθε καινούριος έξυπνος μετρητής, αποστέλλει ένα αίτημα για εγγραφή στο δίκτυο, το οποίο περιλαμβάνει το αναγνωριστικό του σε μια προκαθορισμένη μορφή. Το μήνυμα αυτό κρυπτογραφήθηκε με το ιδιωτικό κλειδί.
2. Το αίτημα αυτό φτάνει στο συλλέκτη δεδομένων, μέσα από ένα μονοπάτι έξυπνων μετρητών και από εκεί προωθείται στο κέντρο διαχείρισης
3. Το αίτημα φτάνει στο κέντρο διαχείρισης, όπου διατηρείται ένας εξυπηρετητής αυθεντικοποίησης. Σύμφωνα με το αναγνωριστικό που περιλαμβάνεται στο μήνυμα, βρίσκει το δημόσιο κλειδί που αντιστοιχεί στο αναγνωριστικό αυτό και το ελέγχει το μήνυμα. Εάν είναι ο έλεγχος είναι θετικός, απαντάει στο με ένα θετικό μήνυμα και το δημόσιο κλειδί του έξυπνου μετρητή, σε διαφορετική περίπτωση απλά απαντάει αρνητικά.
4. Ο συλλέκτης δεδομένων μόλις λάβει την απάντηση, ένα είναι θετική στέλνει ένα μήνυμα επιβεβαίωσης και το δικό του δημόσιο κλειδί στον έξυπνο μετρητή, αφού έχει εισάγει σε έναν πίνακα που διατηρεί, μια νέα εγγραφή, με το δημόσιο κλειδί του έξυπνου μετρητή και το αναγνωριστικό του. Σε διαφορετική περίπτωση δίνει αρνητική απάντηση.

Αφού έχουν ολοκληρωθεί τα παραπάνω βήματα, ο έξυπνος μετρητής και ο συλλέκτης δεδομένων ξέρουν ο καθένας τα δημόσια κλειδιά του αλλού και με αυτό τον τρόπο ανά πάσα στιγμή, μπορεί να δημιουργηθεί ένα ασφαλές κανάλι. Επίσης, με βάση το πίνακα που αποθηκεύει ο συλλέκτης τις πληροφορίες για κάθε έξυπνο μετρητή, έχει την δυνατότητα να δημιουργήσει ένα εικονικό σχέδιο με την τοπολογία του δικτύου. Κάθε έξυπνος μετρητής γνωρίζει τις παρακάτω πληροφορίες:

1. Τα αναγνωριστικά και τα δημόσια κλειδιά των έξυπνων μετρητών που είναι παιδιά του(children node).
2. Το αναγνωριστικό και την δικτυακή διεύθυνση του έξυπνου μετρητή που είναι κόμβος πατέρας.

Η διαδικασία του aggregation, συμβαίνει σε σταθερή συχνότητα κάθε μέρα. Θεωρούμε ότι όλοι οι έξυπνοι μετρητές είναι εξοπλισμένοι με ένα ρολόι για συγχρονισμό της διαδικασίας με στόχο την μείωση του χρόνου αναμονής λήψης των δεδομένων. Η διαδικασία για κάθε έξυπνο μετρητή είναι η εξής:

1. Κρυπτογράφηση των δεδομένων με το δημόσιο κλειδί του συλλέκτη.
2. Αναμονή για λήψη δεδομένων από τους κόμβους παιδιά, ένα υπάρχουν. Όταν ληφθούν τα δεδομένα, ελέγχεται η ακεραιότητα τους με βάση το δημόσιο κλειδί του κάθε κόμβου παιδί.
3. Υπολογισμό του συνόλου των δεδομένων πολλαπλασιάζοντας τα δεδομένα του με τα δεδομένα που έλαβε, εάν έλαβε.
4. Δημιουργία ψηφιακής υπογραφής με τα συγκεντρωμένα δεδομένα και με χρονοσφραγίδα(timestamp). Η χρονοσφραγίδα, είναι μια αλληλουχία από

bit, που ορίζουν τον χρόνο που έγινε το aggregation και συνεπώς είναι διαφορετική, για κάθε διεργασία aggregation.

5. Αποστολή του συνόλου των δεδομένων μαζί με την ψηφιακή υπογραφή, στο κόμβο πατέρα.

Όταν φτάσει η προκαθορισμένη στιγμή για την διαδικασία, πραγματοποιούνται οι παρακάτω διαδικασίες:

1. Οι κόμβοι στα χαμηλότερα επίπεδα, κρυπτογραφούν τα δεδομένα με το δημόσιο κλειδί του συλλέκτη δεδομένων όπου ανήκουν και δημιουργούν την ψηφιακής τους υπογραφή με βάση το δικό τους ιδιωτικό κλειδί.
2. Αποστέλλουν τα δεδομένα υπογεγραμμένα με την ψηφιακής τους υπογραφή στο κόμβο πατέρα τους.
3. Μόλις τα λάβει ο κόμβος πατέρας, τα ελέγχει με βάση τα δημόσια κλειδιά του καθενός, που ήδη γνωρίζει. Εάν, οι υπογραφές είναι αληθής, πολλαπλασιάζει τα δεδομένα και τα υπογράφει ψηφιακά.
4. Προωθεί τα δεδομένα στο συλλέκτη δεδομένων. Ο συλλέκτης δεδομένων την ίδια στιγμή μπορεί να δέχεται δεδομένα από άλλες μέρος του δεντρικής δομής. Εάν λάβει δεδομένα, ελέγχει την ακεραιότητα τους, τα συγκεντρώνει(aggregate) και τα αποκρυπτογραφεί με βάση το ιδιωτικό του κλειδί.

Συμπερασματικά, οι παραπάνω διαδικασίες στο σχήμα αυτό, εκτός από την ιδιωτικότητα, παρέχουν αυθεντικοποίηση και εξασφάλιση της ακεραιότητας των δεδομένων καθώς διέρχονται από τα μονοπάτια του δικτύου του NAN.

6.3 ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ HAN

Μέχρι στιγμής έχουμε μελετήσει τα απαραίτητα μέτρα προστασίας για το WAN και το NAN με σκοπό την απρόοπτη λειτουργία τους. Το WAN και το NAN, αποτελούν το μεγαλύτερο τμήμα του συστήματος AMI και τον κεντρικών υποδομών ενός ευφυούς δικτύου ενέργειας(υποσταθμοί, μονάδες παραγωγής ενέργειας, δίκτυο μεταφοράς ενέργειας κτλ). Από την άλλη μεριά η λειτουργία ενός ευφυούς δικτύου ενέργειας βασίζεται και στην ενεργή συμμετοχή των καταναλωτών με σκοπό την σωστή διαχείρισης της ενέργειας. Με τους έξυπνους μετρητές, να θεωρούνται η πύλη δικτύου(gateway) του HAN προς το NAN, δεν πρέπει να αγνοηθούν και τα μέτρα ασφαλείας που απαιτούνται για την ασφαλή λειτουργία του HAN και των έξυπνων μετρητών όπου συλλέγονται τα δεδομένα.

Μέχρι στιγμής, η ερευνητική κοινότητα έχει εστιάσει το ενδιαφέρον της στην προστασία του WAN και NAN, με το HAN μην έχει εξελιχθεί σημαντικά από πλευράς ασφάλειας. Να σημειωθεί ότι η προστασία του HAN, διαφέρει από τα παραδοσιακά οικιακά δίκτυα των αποκαλούμενων έξυπνων σπιτιών. Αυτό συμβαίνει, γιατί στο HAN ενός ευφυούς δικτύου ενέργειας ο καταναλωτής δεν είναι μόνη οντότητα που συμμετέχει στην επωφελείται από την προστασία του, αλλά και το ίδιο το ευφυές δίκτυο ενέργειας μιας και απειλές και επιθέσεις που μπορούν να

έχει ως σημείο εκκίνησης το HAN, υπάρχει ο κίνδυνος να επεκταθούν στο NAN, επιφέρουν προβλήματα στην λειτουργία του.

Όπως στο WAN και NAN, έτσι και στο HAN, τα μέτρα προστασίας εστιάζουν στην διαθεσιμότητα του HAN, στην ακεραιότητα και εμπιστευτικότητα των δεδομένων που διακινούνται αλλά επιπλέον και στην αυθεντικοποίηση των συσκευών που επικοινωνούν με τον έξυπνο μετρητή. Στο δεύτερο κεφάλαιο, μελετήθηκε η χρήση του ZigBee στο HAN για την επικοινωνία των οικιακών συσκευών με των έξυπνο μετρητή ενέργειας. Να ξαναθυμίσουμε ότι η προώθηση για την χρήση του ZigBee βασίζεται στα χαρακτηριστικά που διαθέτει, μέσα στο οποίο είναι και η χαμηλή κατανάλωση ενέργειας και το χαμηλό κόστος κατασκευής από πλευράς υλικού(hardware). Στο (Paria Jokar, 2011) έχει σχεδιασθεί ένα σύστημα ανίχνευσης απειλών που βασίζεται στην χρήση του ZigBee για στο HAN με σκοπό την ανίχνευση γνωστών αλλά και αγνώστων απειλών που έχουν σκοπό να πλήξουν το HAN. Ειδικότερα, έχει σχεδιασθεί για το φυσικό επίπεδο και το MAC επίπεδο του 802.15.4 που βασίζεται το ZigBee, ενώ ανήκει στην κατηγορία των specification-based IDS.

Τα IDS που ανήκουν στην κατηγορία αυτή, ανιχνεύουν τις επιθέσεις με βάση την παρεκτροπή από μια κατάσταση που θεωρείται φυσιολογική και χρησιμοποιούν ορισμένους κανόνες για να το πετύχουν. Η επιλογή της χρήσης ενός τέτοιου συστήματος βασίζεται στο ότι τα Signature-based IDS, έχουν μεγάλο αριθμό λάθος συναγερμών στην ανίχνευση επιθέσεων και επιπλέον αδυνατούν να ανιχνεύσουν άγνωστες επιθέσεις. Τα Anomaly-based IDS, από την άλλη μεριά, έχουν και αυτά μεγάλο αριθμό λάθος συναγερμών και κοστίζουν σε χρόνο για την δημιουργία των κανόνων για ανίχνευση γνωστών και άγνωστων απειλών. Ως αποτέλεσμα, θεωρείται η χρήση των Specification-based IDS ως η καταλληλότερη, γιατί στο HAN που η χρήση πρωτοκόλλων και προτύπων είναι σχετικά μικρή σε αριθμό, είναι ευκολότερος ο καθορισμός των κανόνων για την ανίχνευση των επιθέσεων. Επίσης αναφέρεται ότι η προώθηση των αποτελεσμάτων από ανιχνεύσεις επιθέσεων σε ένα IDS υψηλότερου επιπέδου που πιθανόν να ανήκει στο NAN ή σε ένα κατανεμημένο IDS του AMI αυξάνει το επίπεδο ασφαλείας.

Από πλευράς υλοποίησης, το IDS εφαρμόζεται στην συσκευή που λειτουργεί ως PAN Coordinator, όπου διαθέτει υπολογιστικές ικανότητες, συγκεντρώνει τα δεδομένα από συσκευές RFD και τα συγκρίνει σύμφωνα με τους προκαθορισμένους κανόνες. Χαρακτηριστικά, η ανίχνευση βασίζεται στο αριθμό των λανθασμένων Frame Check Sequences(FCS), το οποίο χρησιμοποιείται για την ανίχνευση λαθών κατά την μετάδοση στο επίπεδο MAC. Ένας προκαθορισμένος μέσος αριθμός λάθος υπολογισμών, μπορεί να σημάνει ανίχνευση επίθεσης τύπου Jamming.

Το IDS γνωρίζει των αριθμό των συσκευών που είναι συνδεμένες στον Coordinator, οποιαδήποτε άγνωστη συσκευή προσπαθήσει να συνδεθεί χωρίς να έχει αυθεντικοποιηθεί στο δίκτυο μπορεί να θεωρηθεί ως απειλή. Ο καθορισμός προτύπων για τα δεδομένα που διακινούνται δίνει την δυνατότητα την έγκαιρης

ανίχνευσης επιθέσεων DoS, και χαρακτηριστικά με την τεχνική flooding. Οι συσκευές στο HAN, αποστέλλουν τα δεδομένα τους σε συγκεκριμένα χρονικά διαστήματα, οποιαδήποτε ανίχνευση αποστολής δεδομένων με ρυθμό μεγαλύτερο από το συνηθισμένο μπορεί να σημάνει συναγερμό για την ανίχνευση επίθεσης. Στο παραπάνω έρχεται να προστεθεί και η εξέταση των ACK, για την ανίχνευση DoS επιθέσεων, υψηλός ρυθμός σε μικρό χρονικό διάστημα μπορεί να θεωρηθεί απειλή.

Αναφερθήκαμε στην επίθεση Jamming που αντιμετωπίζει το HAN, σε αυτό δεν πρέπει να παραλείψουμε ότι λόγω τις φύσεως του HAN(έλλειψη φυσικής ασφάλειας εξωτερικού χώρου) εκτός από την πρόληψη και την έγκαιρη ανίχνευση απαιτείται και αντιμετώπιση σε περίπτωση που συμβεί. Στο (Visvakumar Aravinthan, 2011) μελετούνται οι επιθέσεις που έχουν πολλές πιθανότητες να εμφανιστούν σε ένα HAN και αναφέρεται ότι οι επιθέσεις που βασίζονται στο Jamming είναι από τις πιο επικίνδυνες από αυτές που ανήκουν στην κατηγορία DoS. Για την αντιμετώπιση της επίθεσης αυτής, η καλύτερη λύση είναι χρήση εναλλακτικών πολλαπλών καναλιών εάν το τρέχον κανάλι που χρησιμοποιείται παρουσιάζει σε μεγάλο βαθμό παρεμβολές όπου οδηγούν σε απώλεια πακέτων(packet loss).

Ο έξυπνος μετρητής, αλλά και οι συσκευές μπορούν κατά την κατασκευή τους, να έχουν προκαθορισμένα κανάλια που σε περίπτωση που παρουσιαστούν παρεμβολές στο κύριο κανάλι να έχουν εναλλακτική λύση. Για λόγους διαχείρισης, αυτό που μπορεί να γίνει είναι, όταν μια νέα συσκευή αυθεντικοποιηθεί στο HAN στο προκαθορισμένο κανάλι επικοινωνίας, να γίνεται καθορισμός των εναλλακτικών καναλιών επικοινωνίας. Σε ενδεχόμενη υλοποίηση του HAN με ZigBee, την ενέργεια αυτή μπορεί να την αναλάβει ο ZigBee Coordinator, ώστε να έχει τον έλεγχο και την διαχείριση όλων των καναλιών που έχουν συμφωνηθεί με κάθε συσκευή. Αντίστοιχη αντιμετώπιση επιθέσεων που βασίζονται στο Jamming προτείνεται και στο (Punith K. Neelam), όπου σε προσομοίωση υπολογίζεται ότι το δίκτυο μπορεί να διατηρηθεί σε λειτουργία κατά 60%.

Προηγουμένως αναφερθήκαμε και στην αυθεντικοποίηση, κάθε συσκευή που συνδέεται στο HAN, είναι απαραίτητο να έχει αυθεντικοποιηθεί, επιπλέον δεν αρκεί μόνο η σχεδίαση ενός σχήματος αυθεντικοποίησης αλλά και η διαχείριση των κλειδιών. Στο (Hasen Nicanfar, Smart grid authentication and key management for unicast and multicast communications, 2011) μελετάται η αυθεντικοποίηση συσκευών στο HAN με χρήση δημοσίου/ίδιωτικού κλειδιού σε συνδυασμό με ID-based κρυπτογράφηση και η αποτελεσματική διαχείριση των κλειδιών για τις συσκευές. Υποστηρίζεται ότι παρέχει ασφαλή unicast, multicast και broadcast επικοινωνία με μικρό overhead.

Στο συγκεκριμένο σχήμα, ένας Trust Agent(TA) επιλέγει τυχαία μια κρυφή τιμή s και υπολογίζει το ιδιωτικό κλειδί για κάθε συσκευή με βάση ένα μοναδικό αναγνωριστικό και μια κρυπτογραφική συνάρτηση. Το δημόσιο κλειδί είναι αποτέλεσμα της κρυπτογραφικής συνάρτησης με είσοδο το αναγνωριστικό ID, ενώ

το ιδιωτικό κλειδί, είναι το αποτέλεσμα της συνάρτησης με είσοδο το αναγνωριστικό πολλαπλασιαζόμενη με την κρυφή τιμή s. Για την ανανέωση των ιδιωτικών κλειδιών, ο ΤΑ απλά ανανεώνει την s, και επαναυπολογίζει το ιδιωτικό κλειδί κάθε συσκευής και τις ενημερώνει. Επίσης, κάθε HAN έχει ένα μοναδικό αναγνωριστικό HID και ο ΤΑ λειτουργεί ο γεννήτρια ιδιωτικών κλειδιών, ενώ είναι ο μόνος που έχει το ιδιωτικό κλειδί του HAN και έχει την ικανότητα να αποκρυπτογραφεί δεδομένα που είναι κρυπτογραφημένα με το δημόσιο κλειδί του HAN. Κάθε συσκευή στο δίκτυο, γνωρίζουν μια κρυπτογραφική συνάρτηση που αν δεχτεί ως είσοδο το αναγνωριστικό μιας άλλης, υπολογίζει το δημόσιο κλειδί της συσκευής αυτής. Όταν μια καινούρια συσκευή συνδέεται στο δίκτυο, υπολογίζει το δημόσιο κλειδί του HAN, δίνοντας ως είσοδο στην συνάρτηση το αναγνωριστικό του HAN και στέλνει broadcast, ένα μήνυμα που περιλαμβάνει το αναγνωριστικό της συσκευής αυτής και ένα συμμετρικό κλειδί που έχει δημιουργήσει το οποίο έχει περιορισμένη χρονική ισχύ, ενώ ξεκινάει έναν χρονομετρητή για την λήξη.

Όλες συσκευές λαμβάνουν το μήνυμα αυτό, αλλά μόνο ο ΤΑ μπορεί να το αποκρυπτογραφήσει. Ο ΤΑ με την σειρά του, απαντάει στη συσκευή αυτή, με το δικό του αναγνωριστικό, δικό της και έναν τυχαίο αριθμό. Το αποτέλεσμα είναι, ότι από την στιγμή που ο ΤΑ, έχει αποκρυπτογραφήσει το μήνυμα να έχει αυθεντικοποιηθεί, ενώ χρησιμοποιώντας το συμμετρικό κλειδί που δημιουργήθηκε από την συσκευή, να έχει αυθεντικοποιηθεί στην συσκευή αυτή. Από την στιγμή αυτή, ο ΤΑ έχει ξεκινήσει έναν χρονομετρητή για την λήψη του επόμενου μηνύματος, ενώ αν δεν ληφθεί μέσα στο διάστημα αυτό, απορρίπτει την διαδικασία. Αυτό γίνεται για πρόληψη έναντι σε επιθέσεις DoS. Δηλαδή, ο ΤΑ δέχεται περιορισμένο αριθμό αυθεντικοποιήσεων σε ένα μικρό χρονικό διάστημα. Από την άλλη πλευρά, η συσκευή, αποκρυπτογραφεί με το συμμετρικό κλειδί το μήνυμα και ανακτά το αναγνωριστικό του ΤΑ και τον τυχαίο αριθμό. Ακόμη, η συσκευή στέλνει στον ΤΑ έναν τυχαίο κωδικό του έχει δημιουργήσει μαζί με το τυχαίο αριθμό που παράχθηκε προηγουμένως, ενώ έχει κρυπτογραφήσει το μήνυμα αυτό με το συμμετρικό κλειδί. Ο ΤΑ από την πλευρά του, ελέγχει το κωδικό που δέχτηκε με μια βάση δεδομένων που διατηρεί για την συγκεκριμένη συσκευή. Απαντάει στην συσκευή με ένα μήνυμα επιβεβαίωσης και το ιδιωτικό της κλειδί.

Υποστηρίζεται ότι το συγκεκριμένο σχήμα αυθεντικοποίησης είναι ανθεκτικό έναντι σε επιθέσεις DoS, Brute-Force, Man In The Middle και Replay. Ένα διαφορετικό σε φιλοσοφία σχήμα αυθεντικοποίησης αναπτύσσεται στο (Erman Ayday, 2011) το οποίο για την διαχείριση των κλειδιών στο HAN, εισάγει την έννοια της τρίτης αρχής, όπου μπορεί να είναι ένας πάροχος Cloud ή κάποια άλλη έμπιστη αρχή. Εισάγοντας από την άλλη μεριά μια τρίτη αρχή για την επίτευξη της αυθεντικοποίησης των συσκευών, ξεφεύγουμε από τα όρια του ευφυούς δικτύου ενέργειας, ενώ δημιουργούνται καινούρια προβλήματα.

ΕΠΙΛΟΓΟΣ

Στο κεφάλαιο αυτό μελετήθηκαν όλα τα απαραίτητα μέτρα ασφαλείας που χρειάζονται να ληφθούν για την απρόοπτη λειτουργία ενός ευφυούς δικτύου ενέργειας. Μελετήθηκαν συστήματα ανίχνευσης επιθέσεων για το WAN, NAN και HAN που στόχο έχουν την έγκαιρη ανίχνευση επιθέσεων. Έμφαση δόθηκε στα κατανεμημένα συστήματα μιας και θεωρούνται καταλληλότερα για τα ευφυή δίκτυα ενέργειας, λόγω της αρχιτεκτονικής τους και του μεγάλου πλήθους συσκευών. Επιπλέον μελετήθηκαν τα σχήματα αυθεντικοποίησης που είναι κατάλληλα σχεδιασμένα για εφαρμογή σε ένα ευφυές δίκτυο ενέργειας, δίνοντας βαρύτητα στην διαχείριση των κλειδιών και το overhead που προσθέτουν.

Η εφαρμογή τεχνικών αυθεντικοποίησης είναι απαραίτητο συστατικό για την προστασία ενάντια σε επιθέσεις προσποίησης χρηστών ή συσκευών. Λόγω της φύσης των ευφυών δικτύων ενέργειας, και την δυσκολία εξασφάλισης της φυσικής ασφάλειας συσκευών όπως είναι οι έξυπνοι μετρητές, η αυθεντικοποίηση αποκτά μεγάλη βαρύτητα. Μια άλλη βασική απαίτηση είναι η εξασφάλιση της ιδιωτικότητας των δεδομένων που συγκεντρώνονται από τους έξυπνους μετρητές ενέργειας στο NAN, η οποία καλύφθηκε με την υλοποίηση εξειδικευμένων τεχνικών κρυπτογράφησης, τεχνικών συγκέντρωσης δεδομένων, ανωνυμίας δεδομένων και χρήση τρίτης αρχής. Η ιδιωτικότητα είναι πολύ σημαντικός στόχος, εδικά για τα δεδομένα που συγκεντρώνονται από τους έξυπνους μετρητές, μιας και όπως έχουν αναφέρει ορίζουν την συμπεριφορά των χρηστών. Η πρόταση χρήσης όμως τρίτης αρχής, δημιουργεί νέα προβλήματα πρόσβασης στα δεδομένα, ενώ οι πρόσφατες τεχνικές εστιάζουν σε εξελιγμένες τεχνικές κρυπτογράφησης με στόχο το μικρό overhead στην συνολική επικοινωνία. Όμως, οι τεχνικές κρυπτογράφησης, παρουσιάζουν ευπάθειες έναντι σε νέες επιθέσεις που εμφανίζονται στα ευφυή δίκτυα ενέργειας, συνεπώς απαιτείται ακόμα χρόνος για την βελτίωση της απόδοσης των τεχνικών αυτών.

Μέχρι στιγμής, έχουν προταθεί αρκετές λύσεις στα προβλήματα ασφαλείας των ευφυών δικτύων ενέργειας, όμως, η καθολική εφαρμογή τεχνικών σε τόσο μεγάλο εύρος δεν είναι εύκολη υπόθεση και απαιτεί χρόνο, δοκιμές και βελτιστοποιήσεις μέχρι την πραγματική υλοποίηση. Όπως και στις τεχνολογίες δικτύων έτσι και στην ασφάλεια απαιτείται καθορισμός απαιτήσεων, ορισμός προδιαγραφών, και προτάσεις για την εφαρμογή τεχνικών. Στο επόμενο κεφάλαιο, παρουσιάζονται εκτός από πρότυπα και πρωτόκολλα επικοινωνιών, πρότυπα και πρωτόκολλα που σχετίζονται με την ασφάλεια στα ευφυή δίκτυα ενέργειας. Μερικά χαρακτηριστικά παραδείγματα είναι, το IEC 62351, το IEEE 1686 και το Nistir 7628.

ΚΕΦΑΛΑΙΟ 7

ΠΡΟΤΥΠΟΠΟΙΗΣΗ-ΠΡΩΤΟΚΟΛΛΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΣΤΑ ΕΥΦΥΗ ΔΙΚΤΥΑ ΕΝΕΡΓΕΙΑΣ

ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό πραγματοποιείται παρουσίαση των προτύπων και πρωτοκόλλων που έχουν σχεδιασθεί από διεθνείς οργανισμούς και σχετίζονται με τις επικοινωνίες και την ασφάλεια στα ευφυή δίκτυα ενέργειας. Στο τέλος του κεφαλαίου γίνεται συνοπτική παρουσίαση σε πίνακα.

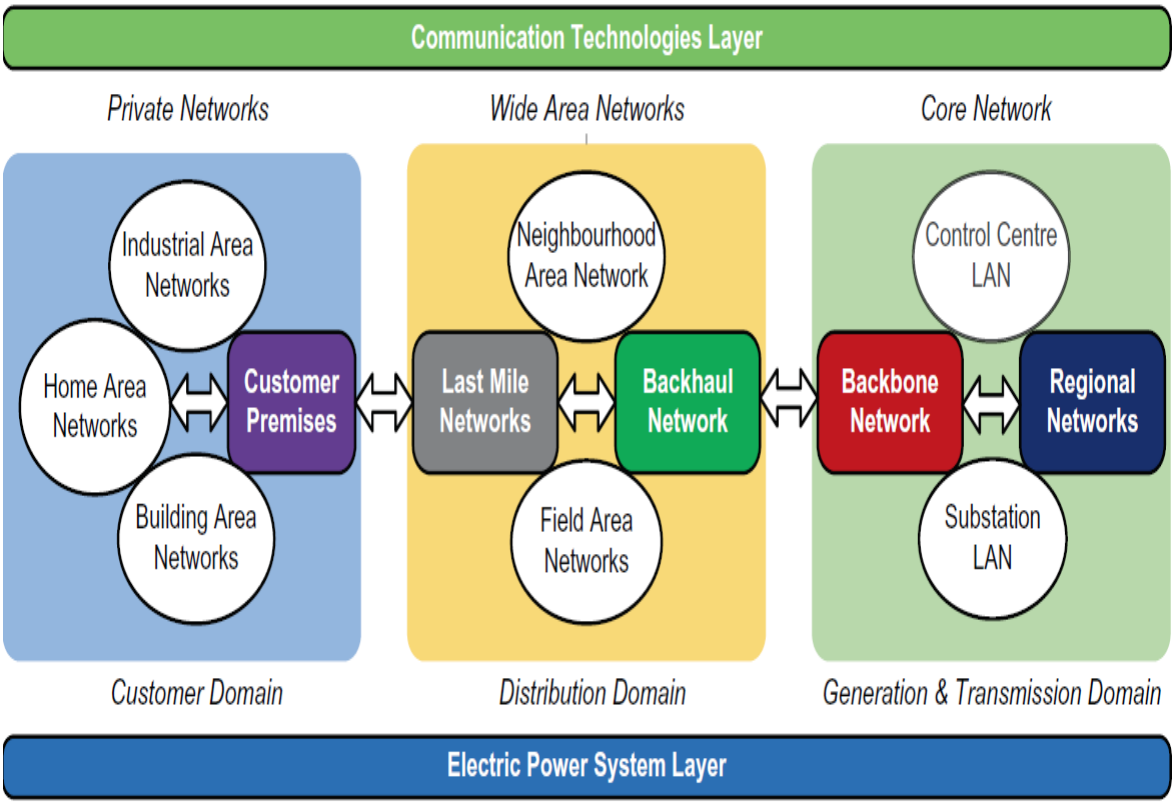
7.1 IEEE

IEEE 2030

Το IEEE 2030 με την ονομασία, IEEE Guide for Smart Grid Interoperability of Energy technology and Information Technology Operation with the Electric Power System(EPS), End-Use Application and Loads, είναι ένα πρότυπο που έχει σχεδιασθεί για να παρέχει οδηγίες σχετικά με την κατανόηση και ορισμό της διαλειτουργικότητας. Ορίζει το Smart Grid Interoperability Reference Model(SGIRM) το οποίο είναι ένα μοντέλο που παρουσιάζει αφαιρετικά την αρχιτεκτονική ενός ευφυούς δικτύου ενέργειας που αποτελείται από τρία τμήματα:

- Power Systems
- Communications
- Information Technology

Ο στόχος του είναι η ανάπτυξη της συνεργασίας μεταξύ διαφόρων ομάδων ή οργανισμών που ασχολούνται με την ανάπτυξη των ευφυών δικτύων ενέργειας, ενώ το μοντέλο που προτείνει στόχο έχει την βελτίωση της διαλειτουργικότητας στα τμήματα που αποτελείται ένα ευφυές δίκτυο ενέργειας. Για παράδειγμα, για κάθε περιοχή ενός ευφυούς δικτύου ενέργειας, διαφορετικοί σχεδιαστές μπορούν να δώσουν διαφορετικές ονομασίες, όπως είναι το HAN, BAN, WAN. Το HAN μπορεί να αναφερθεί ως Customer Premises Network(CPS) αλλά επίσημα αναφέρεται ως Home Area Network. Επίσης, αναφέρεται η χρήση του διαδικτύου για την κάλυψη των αναγκών επικοινωνίας ως εναλλακτική λύση. (Leccese, 2012)



Εικόνα 43 "Αρχιτεκτονική δικτύου επικοινωνιών σύμφωνα με το IEEE 2030" (Reduan H. Khan, A comprehensive review of the application characteristics and traffic, 2013)

IEEE 1815

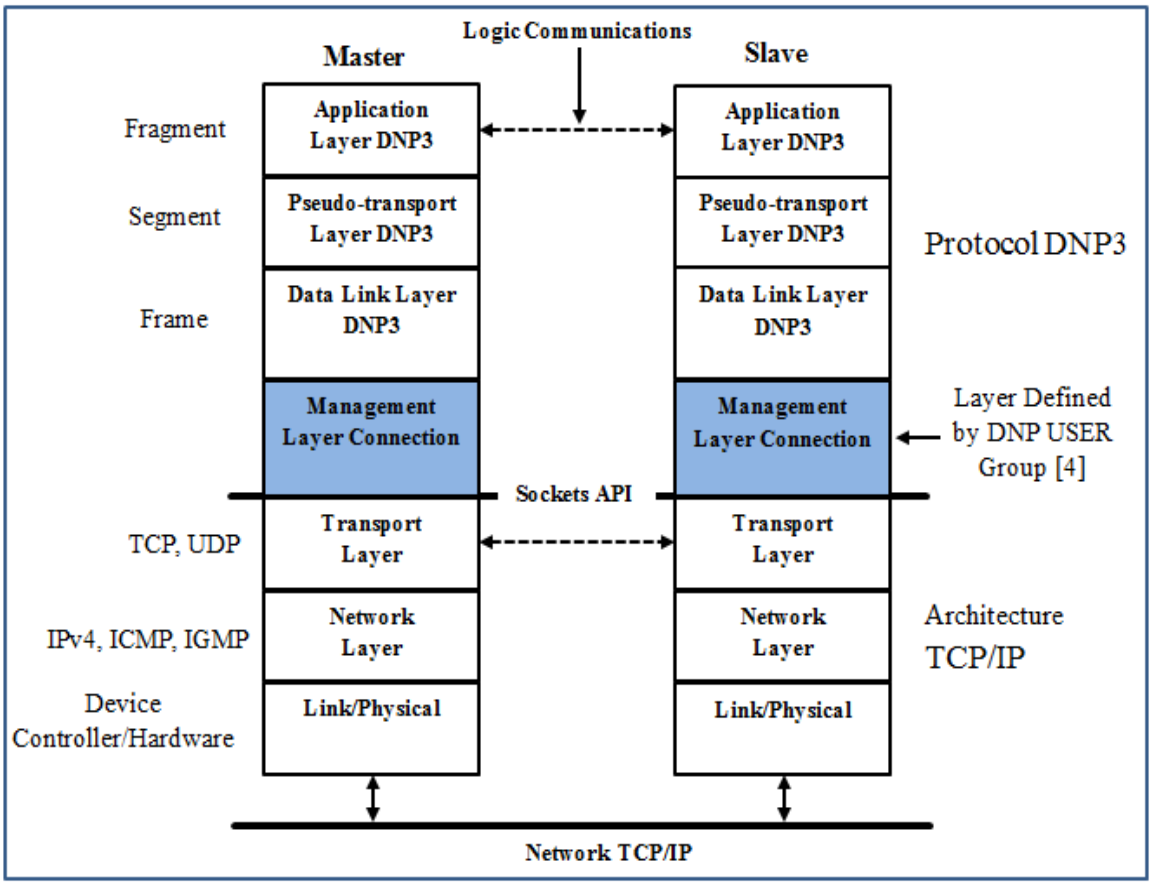
Το 2011 η IEEE ανακοίνωσε ότι το πρωτόκολλο Distributed Network Protocol(DNP3) ανήκει πλέον στην λίστα των προτύπων της IEEE που αφορούν τις επικοινωνίες στα ευφυή δίκτυα ενέργειας. Το DNP3, είναι ένα σύνολο πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται σε συστήματα αυτοματισμού για τον απομακρυσμένο έλεγχο συσκευών IED που υπάρχουν στο δίκτυο ηλεκτρικής ενέργειας. Επιτυγχάνεται η επικοινωνία ανάμεσα σε IED και υποσταθμούς αλλά και κέντρα διαχείρισης. Οι κύριες λειτουργίες που παρέχονται αφορούν την πολυπλεξία, τον έλεγχο σφαλμάτων, κατακερματισμό δεδομένων, αλλά και εφαρμογή προτεραιοτήτων. Σημαντικό, είναι ότι παρέχει και δυνατότητα συγχρονισμού των συσκευών που υλοποιούν το DNP3.

Η IEEE έχει επεκτείνει τις λειτουργίες του DNP3, ώστε να καλύπτονται οι ανάγκες στα ευφυή δίκτυα ενέργειας με τον καλύτερο δυνατό τρόπο και αυτό γίνεται με το πρότυπο IEEE P1815-2010 αλλά και την τελευταία έκδοση που είναι η IEEE P1815-2012. Η πρώτη έκδοση δημιουργήθηκε σε συνδυασμό με το DNP User Group, ενώ η δεύτερη μόνο από την IEEE. Η δεύτερη έκδοση περιλαμβάνει βελτιώσεις όπως είναι αυθεντικοποίηση βασιζόμενη σε υποδομή δημοσίου κλειδιού. Επίσης, το DNP3 λόγω τις ευελιξίας που διαθέτει μπορεί να υλοποιηθεί και σε συνδυασμό με IP δίκτυα με TCP ή UDP πακέτα. (Society I. P., 2010) Το DNP3 έχει δύο κατηγορίες συσκευών, Central Stations(Masters), όπου οι

συσκευές αυτές έχουν υπολογιστικές και αποθηκευτικές δυνατότητες. Οι Masters, συνδέονται με τις συσκευές με την ονομασία Stations(Outstations), όπου συγκεντρώνουν τα δεδομένα που συλλέγουν οι δεύτερες για την κατάσταση του δικτύου ηλεκτρικής ενέργειας. Να σημειωθεί ότι οι δύο αυτές συσκευές στο επίπεδο εφαρμογών.

Από πλευράς υλοποίησης στα ευφυή δίκτυα ενέργειας προωθείται η εφαρμογή του σε συνδυασμό με το TCP/IP, ενώ το DNP user group προτείνει τα παρακάτω:

- Τα μηνύματα ACK του DNP3 link layer θα πρέπει να απενεργοποιηθούν, γιατί το TCP, αναλαμβάνει την δημιουργία καναλιού επικοινωνίας.
- Προτείνεται η εφαρμογή του σε Ethernet.
- Όλες οι συσκευές που το υλοποιούν είναι απαραίτητο να υποστηρίζουν TCP και UDP.
- Το TCP πρέπει να χρησιμοποιείται στο WAN, γιατί είναι connection-oriented.



Εικόνα 44 "DNP3 σε TCP/IP δίκτυο" (Alcides Ortega, 2013)

Τα ψευδό-επίπεδα transport και data link, χρησιμοποιούνται για ανίχνευση λαθών(error detection). Η δημιουργία ενός μηνύματος DNP3, ξεκινάει από πάνω προς τα κάτω στην στοίβα. Το frame του DNP3, με μέγιστο μέγεθος 292 bytes, ενθυλακώνεται σε ένα tcp segment, με 20 bytes μέγεθος κεφαλίδας(header). Ενώ το μέγιστο μέγεθος του tcp segment είναι 556 bytes(536 bytes και 20 το μέγεθος της κεφαλίδας). Στην συνέχεια ενθυλακώνεται σε ένα IP πακέτο. (Alcides Ortega, 2013)

IEEE 1588

Ένα ακόμη πρότυπο που έχει σχεδιασθεί από την IEEE που σχετίζεται με το συγχρονισμό και χρησιμοποιείται σε υποσταθμούς κυρίως των ευφυών δικτύων ενέργειας είναι το IEEE 1588. Το IEEE 1588 ή Precision Time Protocol (PTP) είναι ένα πρωτόκολλο που χρησιμοποιείται για το συγχρονισμό ανάμεσα σε υπολογιστικές συσκευές. Στους υποσταθμούς των ευφυών δικτύων ενέργειας, αλλά και στο δίκτυο διανομής υπάρχουν IED ή phasor measurement unit(PMU), που συγκεντρώνουν δεδομένα που σχετίζονται με την κατάσταση του δικτύου ενέργειας. Έτσι, απαιτείται συγχρονισμός μεταξύ των συσκευών αυτών και αυτό επιτυγχάνεται με το IEEE 1588. Να αναφερθεί πως το συγκεκριμένο πρωτόκολλο, δεν έχει σχεδιασθεί για αποκλειστική χρήση στα ευφυή δίκτυα ενέργειας, αλλά και για ευρύτερη χρήση συγχρονισμού αυτοματισμών. Για την καλύτερη εφαρμογή του στα ευφυή δίκτυα ενέργειας και την κάλυψη των απαιτήσεων καθυστέρησης όπως ορίζονται από πρότυπα όπως είναι το IEC, η IEEE παρέχει οδηγίες υλοποίησης μέσω του IEEE C37.238. (Bernhard Baumgartner, 2013)

IEEE 1703

Το IEEE 1703, με την ονομασία IEEE Standard for Local Area Network/Wide Area Network(LAN/WAN) Node Communication Protocol to Complement the Utility Industry End Device Data Tables, είναι το αντίστοιχο πρότυπο ANSI C12.22 του οργανισμού ANSI. Έχει σχεδιασθεί για την κάλυψη του ANSI C12.22 κάτω από έναν παγκόσμιο οργανισμό, ενώ σκοπός του είναι η ανταλλαγή δεδομένων του ANSI C12.19. Στο πρότυπο αυτό επίσης, έχουν σημειωθεί μικρές διορθώσεις σε σχέση με το ANSI C12.22 όπως και η δομή του προτύπου έχει αναπτυχθεί σύμφωνα με την δομή που ορίζει η IEEE. Κύρια εφαρμογή βρίσκει στους έξυπνους μετρητές ενέργειας. Από πλευράς μερών που αποτελείται το πρότυπο, ορίζονται οι ίδιοι ακριβώς τύποι κόμβων με το ANSI C12.22 όπως και τα υπόλοιπα χαρακτηριστικά του προτύπου. Παρακάτω αναφέρονται οι υπηρεσίες που παρέχονται από το πρότυπο αυτό και είναι κοινές και για τα δύο:

Πίνακας 3 "Υπηρεσίες που παρέχονται από το πρότυπο IEEE 1703"

Request	Response
Ident	Ident-r
Read	Read-r
Write	Write-r
Logon	Logon-r
Security	Security-r
Logoff	Logoff-r
Terminate	Terminate-r
Disconnect	Disconnect-r
Wait	Wait-r
Register	Register-r
Deregister	Deregister-r
Trace	Trace-r

Οι υπηρεσίες όπως Register, Deregister, Resolve, Trace, δηλαδή τα μηνύματα τους, δεν κρυπτογραφούνται αλλά μόνο αυθεντικοποιούνται.

1. Η υπηρεσία Ident, χρησιμοποιείται για την ανάκτηση πληροφοριών σχετικά με την συσκευή. Η συσκευή απαντάει με τον τύπο του προτύπου και την έκδοση που τρέχει.
2. Η υπηρεσία Read, χρησιμοποιείται για την μεταφορά ενός Table Data στην συσκευή που έχει αποστείλει το αίτημα.
3. Η υπηρεσία write, χρησιμοποιείται για την αποστολή ενός table Data, σε μια συγκεκριμένη συσκευή.
4. Η υπηρεσία Logon χρησιμοποιείται, για την δημιουργία ενός session, με συγκεκριμένα δικαιώματα.
5. Η υπηρεσία Security χρησιμοποιείται για την εκχώρηση δικαιωμάτων, η οποία γίνεται με βάση κωδικούς, ενώ η αντιστοίχιση των κωδικών στα δικαιώματα ορίζεται από το ANSI C12.19.
6. Η υπηρεσία Logon χρησιμοποιείται για τον τερματισμό ενός session που έχει δημιουργηθεί από την εντολή Logon.
7. Η υπηρεσία Terminate, χρησιμοποιείται όπως η Logoff, για τερματισμό ενός session, αλλά για λόγους έκτακτους, όπως είναι λόγους ασφαλείας.
8. Η υπηρεσία Disconnect χρησιμοποιείται για την απομάκρυνση ενός C12.22 Node από το C12.22 Network Segment όπου ανήκει.
9. Η υπηρεσία Wait χρησιμοποιείται, για την διατηρήσει ενός session ανοιχτό, ώστε να μην κλείσει αυτόματα, αυτό που κάνει είναι να επεκτείνει το χρόνο μέχρι το time-out.

10. Η υπηρεσία Registration χρησιμοποιείται για διατήρηση των πινάκων δρομολόγησης στους C12.22 Relays. Για να γίνει ένας C12.22 Node, δεκτός σε ένα C12.22 Network, πρέπει να αποστείλει ένα τέτοιο αίτημα στο C12.22 Master Relays
11. Η υπηρεσία Deregistration χρησιμοποιείται για την απομάκρυνση των εγγράφων από τους πίνακες δρομολόγησης των C12.22 Relays και Master Relays.
12. Η υπηρεσία Resolve χρησιμοποιείται για την ανάκτηση μιας διεύθυνσης ενός C12.22 Node από έναν C12.22 Relay για την επικοινωνία μεταξύ δύο Node. Ονομάζεται και direct messaging, αυτού του είδους η άμεση επικοινωνία.
13. Η υπηρεσία Trace χρησιμοποιείται για την ανάκτηση λίστας των C12.22 Relays, που έχουν προωθήσει ένα συγκεκριμένο μήνυμα προς έναν συγκεκριμένο Node.

Επίσης, από πλευράς μηχανισμών ασφαλείας υπάρχουν τρεις τύποι μεταφοράς δεδομένων:

1. Cleartext, όπου τα δεδομένα ενός μηνύματος δεν κρυπτογραφούνται, ούτε αυθεντικοποιούνται.
2. Authenticated Cleartext, όπου τα δεδομένα ενός μηνύματος μόνο αυθεντικοποιούνται.
3. Authenticated Ciphertext, όπου τα δεδομένα ενός μηνύματος κρυπτογραφούνται και αυθεντικοποιούνται.

Ο αλγόριθμός κρυπτογράφησης που χρησιμοποιείται είναι ο AES 128bit σε συνδυασμό με το EAX Mode, το οποίο είναι τύπος κρυπτογράφησης δύο περασμάτων, παρέχοντας αυθεντικοποίηση σε συνδυασμό με εμπιστευτικότητα. Υπάρχουν περιπτώσεις όπου μέρη ενός μηνύματος δεν κρυπτογραφούνται όπως είναι οι κεφαλίδες των μηνυμάτων και στέλνονται ως Cleartext. (Board, 1703-2012 - IEEE Standard for Local Area Network/Wide Area Network (LAN/WAN) Node Communication Protocol to Complement the Utility Industry End Device Data Tables, 2012)

IEEE 1377

Το πρότυπο IEEE 1377, με την ονομασία IEEE Standard for Utility Industry Metering Communication Protocol Application Layer(End Device Data Tables), είναι το αντίστοιχο πρότυπο με το ANSI C12.19 που ορίζει ο οργανισμός ANSI. Το IEEE 1377 συνδέεται άμεσα με το πρότυπο IEEE 1703. Το πρότυπο αυτό ορίζει την δομή των πινάκων που περιλαμβάνουν τα δεδομένα που διακινούνται μεταξύ των κόμβων που υλοποιούν το IEEE 1377 και το IEEE 1703. Οι πίνακες όπως και στο ANSI C12.19 ομαδοποιούνται σε “decades” σύμφωνα με το δεδομένα που σχετίζονται. (Board, 1377-2012 - IEEE Standard for Utility Industry Metering Communication Protocol Application Layer (End Device Data Tables), 2012)

IEEE 1686

Το πρότυπο IEEE 1686, με την ονομασία IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, είναι ένα πρότυπο της IEEE που σχετίζεται με την ασφάλεια των IEDs. Ειδικότερα, σχετίζεται με την πρόσβαση, την λειτουργία, την παραμετροποίηση, την ανταλλαγή δεδομένων, αλλά και την κρυπτογράφηση των επικοινωνία από και προς τις IEDs. Το πρότυπο παρέχει γενικές οδηγίες προστασίας και δεν καθορίζει ποιες συσκευές και με ποιες απαιτήσεις μπορούν να το υλοποιήσουν. Οι οδηγίες ταξινομούνται σε: (Society I. P., 2013)

1. Electronic access Control

Παρέχονται οδηγίες σχετικά με την πρόσβαση στις IED, τοπικά ή απομακρυσμένα. Χαρακτηριστικά αναφέρεται ότι κάθε συσκευή πρέπει να προστατεύεται από την μη-εξουδιοδοτημένη πρόσβαση με username/password, μοναδικά για κάθε χρήστη. Ακόμη, οι ρόλοι πρέπει να είναι καθορισμένοι με ανάλογα δικαιώματα πρόσβασης, ενώ ο μέγιστος αριθμός χρηστών που υποστηρίζονται δεν πρέπει να ξεπερνάει τους δέκα. Τέλος, καθορίζεται ένα σύνολο κανόνων για τους κωδικούς πρόσβασης αλλά και χαρακτηριστικό time-out, για την αποσύνδεση, μετά από ένα διάστημα απραξίας του συνδεμένου χρήστη.

2. Audit Trail

Είναι απαραίτητο να καταγράφονται όλες οι κινήσεις των χρηστών που συνδέονται, χωρίς την δυνατότητα της διαγραφής ή της παραποίησης των στοιχείων. Έμφαση δηλαδή να δίνεται στην ακεραιότητα των δεδομένων αυτών. Ακόμη, απαιτούνται δυνατότητες αποθήκευσης τουλάχιστον 2048 καταγραφών, πριν την διαγραφή των στοιχείων. Ειδικότερα απαιτείται να καταγράφεται, ένα μοναδικός κωδικός για κάθε event, ημερομηνία και ώρα, το αναγνωριστικό του χρήστη, και ο τύπος του event.

3. Supervisory monitoring and control

Εκτός από την καταγραφή των κινήσεων απαιτείται και η ζωντανή παρακολούθηση από το κέντρο διαχείρισης του ευφυούς δικτύου ενέργειας. Οι πληροφορίες που μεταδίδονται προς το κέντρο διαχείρισης διαχωρίζονται σε δύο κατηγορίες, events και alarms.

4. IED cyber security features

Στην κατηγορία αυτή συγκεντρώνονται ένα σύνολο γενικών οδηγιών με μέτρα προστασίας. Ειδικότερα, αναφέρεται ότι οι IED, πρέπει να χρησιμοποιούν πρωτόκολλα όπως είναι το Hypertext Transfer Protocol Secure(HTTPS), το Secure File-Transfer Protocol(SFTP), το Secure Shell(SSH), το Single Network Management Protocol(SMNPv3), το Network Time Protocol(NTP) και τέλος το Virtual Private Network(VPN).

5. IED configuration software

Στην κατηγορία αυτή, προτείνονται εφαρμογές όπως είναι αυθεντικοποίησης, ψηφιακής υπογραφής, διαχείρισης username/password που σχετίζονται με την ασφάλεια του λογισμικού που τρέχει στις IEDs.

6. Communication port access

Όλες οι θύρες μιας IED, λογικές(εικονικές) ή φυσικές, εκτός από τις θύρες που χρησιμοποιείται για διαγωνιστικούς ελέγχους, είναι απαραίτητο, να έχουν δυνατότητα ενεργοποίησης ή απενεργοποίησης. Σε περίπτωση απενεργοποίησης, το αποτέλεσμα είναι η αποκοπή της επικοινωνίας στην θύρα αυτή. Επίσης, κάθε θύρα που δεν χρησιμοποιείται και δέχεται πακέτα TCP ή UDP, πρέπει υποχρεωτικά να είναι απενεργοποιημένη.

7. Firmware quality assurance

Δεν παρέχονται οδηγίες από το πρότυπο αυτό, σχετικά με το firmware των IEDs, αλλά πρέπει να ακολουθούνται οδηγίες που παρέχει το πρότυπο IEEE C37.231.

IEEE 1901.2

Το πρότυπο IEEE 1901.2, είναι ένα πρότυπο που σχεδιάστηκε πρόσφατα για την εφαρμογή της PLC τεχνολογίας στα ευφυή δίκτυα ενέργειας. Η πλήρης ονομασία του προτύπου είναι, IEEE Standard for Low-Frequency(less than 500kHz) Narrowband Power Line Communication for Smart Grid Applications. Καθορίζει το φυσικό επίπεδο και το επίπεδο MAC του OSI, για επικοινωνία σε χαμηλή συχνότητα, για εσωτερική ή εξωτερική χρήση, σε γραμμές χαμηλής(κάτω από 1000 volt) και μεσαίας τάσης(1000 μέχρι 72kV) ακόμα και μέσα από μετασχηματιστές(transformers). Ο ρυθμός μετάδοσης των δεδομένων φτάνει μέχρι τα 500kb/s και η εφαρμογή του προτείνεται και για αστικές αλλά και για απομακρυσμένες περιοχές. Οι εφαρμογές του εστιάζουν στην επικοινωνία στο HAN και NAN, για την συλλογή δεδομένων από έξυπνους μετρητές, αλλά επικοινωνία ανάμεσα και διάφορα τμήματα ενός ευφυούς δικτύου ενέργειας, όπως είναι σταθμοί φόρτισης ηλεκτρικών οχημάτων. Να σημειωθεί ότι το IEEE 1901.2 αν και αποτελεί μέλος της οικογένειας του IEEE 1901-2010, τεχνικά δεν σχετίζεται με αυτό. (Society I. C., 1901.2-2013 - IEEE Standtard for Low-Frequency(less than 500kHz) Narrowband Power Line Communications for Smart Grid Applications, 2013)

IEEE C37.118

Το πρότυπο αυτό έχει πλήρη ονομασία, IEEE Standard for Synchrophasors for Power System. Οι Synchrophasors είναι συσκευές που χρησιμοποιούνται στα ευφυή δίκτυα ενέργειας, για να μετρούν στοιχεία όπως είναι το ηλεκτρικά σήματα στο δίκτυο ενέργειας, ενώ χρησιμοποιούν κάποια πηγή για συγχρονισμό. Ο συγχρονισμός στα ευφυή δίκτυα ενέργειας μπορεί να γίνει με την χρήση Global

Positioning System(GPS) ή με χρήση του IEEE 1588(PTP). Το πρότυπο αυτό επίσης ορίζει πως θα γίνεται η επικοινωνία για καταγραφή των δεδομένων που θα λαμβάνονται. Το C37.118, είναι από τα σημαντικότερα πρωτόκολλα στους αυτοματισμούς και στα συστήματα παρακολούθησης των ευφυών δικτύων ενέργειας. (K. E Martin, 2008)

IEEE 1909.1

Το πρότυπο αυτό, έχει πλήρη ονομασία IEEE Draft Recommended Practice for Smart Grid Communication Equipment-Test methods and installation requirements. Στόχος του είναι ο καθορισμός χαρακτηριστικών που πρέπει να έχει το υλικό (hardware) των τεχνολογιών επικοινωνίας και γενικώς οι συσκευές που χρησιμοποιούνται στα ευφυή δίκτυα ενέργειας. Επίσης, παρέχει οδηγίες σύμφωνα με οργανισμούς και πιστοποιήσεις για την σχεδίαση του υλικού μέρους. (Group P. W.)

7.2 IEC

IEC 61850

Ο οργανισμός International Electrotechnical Commission(IEC) έχει δημιουργήσει το Smart Grid Strategic Group, το οποίο ασχολείται με την προτυποποίηση στα ευφυή δίκτυα ενέργειας, με κύριο στόχο την εξασφάλιση της διαλειτουργικότητας σε συσκευές και συστήματα που σχετίζονται με τις επικοινωνίες. (Group S. G., 2010). Ένα από τα γνωστότερα πρότυπα που σχετίζονται με τις επικοινωνίες στα ευφυή δίκτυα ενέργειας, και ειδικότερα αυτό που σχετίζεται στην επικοινωνία ανάμεσα στις κεντρικές υποδομές(υποσταθμούς, κέντρο διαχείρισης) είναι το IEC 61850. Το IEC 61850 έχει αναφερθεί στο κεφάλαιο 2 που έχουν ορισθεί οι απαιτήσεις καθυστέρησης για τις κεντρικές υποδομές(υποσταθμούς, κέντρο διαχείρισης) των ευφυών δικτύων ενέργειας, η οποίες είναι η πιο απαιτητικές σε όλο το εύρος ενός ευφυούς δικτύου ενέργειας. Το πρότυπο αυτό, αρχικά σχεδιάστηκε για επικοινωνία σε αυτοματισμούς ελέγχου και διαχείρισης για κρίσιμες υποδομές και κυρίως ενέργειας. Μαζί με το DNP3 είναι τα σημαντικότερα πρότυπα που χρησιμοποιούνται στο WAN των ευφυών δικτύων ενέργειας. Στα ευφυή δίκτυα ενέργειας βρίσκει συχνή εφαρμογή στο κέντρο διαχείρισης αλλά και στους υποσταθμούς του δικτύου ενέργειας, καλύπτοντας τις ανάγκες επικοινωνίας ανάμεσα στις IED συσκευές.

Η αρχική σχεδίαση του IEC 61850 είναι για χρήση σε TCP/IP δίκτυα και ειδικά σε Ethernet δίκτυα, ενώ για τον διαχωρισμό με βάση της εφαρμογές που καλύπτει καθορίζονται πέντε τύποι υπηρεσιών:

1. Abstract Communication Service Interface(ACSI)
2. Generic Object Oriented Substation Event(GOOSE)
3. Sampled Measured Value Multicast(SMV)

4. Time synchronization(TS)

Οι υπηρεσίες ACSI, περιλαμβάνουν μηνύματα ερωτημάτων και καταγραφής που σχετίζονται με την κατάσταση λειτουργίας των IED. Η ανταλλαγή δεδομένων εδώ μοιάζει με την επικοινωνία βασισμένη στο File Transfer Protocol(FTP), όπου δημιουργείται ένα session, και γίνεται ανταλλαγή δεδομένων, αφού έχει προηγηθεί το handshaking. Στην δεύτερη κατηγορία, όπου αναφέρονται και ως Generic Substation Events(GSE), τα μηνύματα αυτά χρησιμοποιούνται για την γρήγορη και αξιόπιστη ανταλλαγή δεδομένων ανάμεσα σε δύο ή περισσότερες IED. Χρησιμοποιούνται κυρίως σε δίκτυο Ethernet σε συνδυασμό με Virtual Lans(VLANS) και multicast επικοινωνία για την παράδοση του ίδιου μηνύματος ταυτόχρονα σε ένα σύνολο IED. Το IEC 61850, επίσης εισάγει και ένα σχήμα επανάποστολής για την αξιόπιστη παράδοση των μηνυμάτων. Επίσης, τα μηνύματα TS, χρησιμοποιούνται για το συγχρονισμό των IED για μεγαλύτερη ακρίβεια στην συλλογή δεδομένων, ενώ γίνονται broadcast σε όλες τις IED. Το IEC 61850, αποτελείται στους αναφέρθηκε στο κεφάλαιο 2, από έξι διαφορετικούς τύπους μηνυμάτων με βάση τα όρια καθυστέρησης παράδοσης των μηνυμάτων για την επικοινωνία στους υποσταθμούς του δικτύου ηλεκτρικής ενέργειας. (Reduan H. Khan, A comprehensive review of the application characteristics and traffic, 2013)

Πίνακας 4 "Τύποι μηνυμάτων, όρια καθυστέρησης και συσχέτιση με τύπους υπηρεσιών"

Τύπος μηνύματος	Όριο καθυστέρησης(ms)	Services	Εφαρμογή
1A	3-100	GOOSE	Fast Message(trip)
1B	20-100	GOOSE	Fast Message(other)
2	100	ACSI	Medium Speed
3	500	ACSI	Low Speed
4	3-10	SMV	Raw data
5	>1000	ACSI	File Transfer
6	No requirement	TS	Time Synchronization

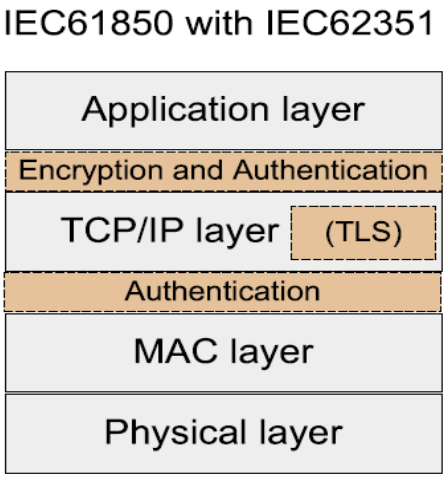
Ένα ιδιαίτερο χαρακτηριστικό του IEC 61850, είναι ότι εισάγει την χρήση της Substation Configuration Language(SCL), η οποία βασίζεται στην eXtensible Markup Language(XLM), για την περιγραφή των παραμέτρων στο IEC 61850. Η SCL ορίζει μια ιεραρχία από αρχεία ρυθμίσεων που χρησιμοποιείται στα επιμέρους τμήματα του IEC 61850 όπως είναι στις IED συσκευές. Επίσης, η SCL ορίζει ένα μοντέλο UML, για την περιγραφή ενός δικτύου επικοινωνιών και των

διεπαφών του. Με αυτό τον τρόπο μπορούμε από ένα αρχείο ρυθμίσεων που βασίζεται στην SCL, να ανακτούμε πληροφορίες σχετικά με την τοπολογία του δικτύου, τα πρωτοκόλλα που χρησιμοποιούνται και όλες τις διεπαφές ανάμεσα στα επιμέρους τμήματα.

IEC 62351

Μέχρι στιγμής έχουμε αναλύσει το IEC 61850, το οποίο είναι πρότυπο που σχετίζεται με την επικοινωνία, για την προστασία του προτύπου αυτού, έχει σχεδιασθεί το IEC 62351, το οποίο καλείται να καλύψει ευπάθειες του IEC 61850. Το IEC 62351 υλοποιεί μηχανισμούς αυθεντικοποίησης και κρυπτογράφησης. Ειδικότερα, εισάγει δύο επίπεδα:

1. Ένα επίπεδο αυθεντικοποίησης και κρυπτογράφησης πάνω από το TCP/IP επίπεδο και κάτω από το επίπεδο εφαρμογών. Στο επίπεδο αυτό, χρησιμοποίει το Transport Layer Security(TLS), όπου με συμμετρική κρυπτογράφηση και Media Key Block(MKB) παρέχει ιδιωτικότητα και αυθεντικοποίηση.
2. Ένα επίπεδο αυθεντικοποίησης εισάγεται μεταξύ του MAC και IP επιπέδου. Το επίπεδο αυτό χρησιμοποιείται αποκλειστικά για την αυθεντικοποίηση σε κρίσιμες ως προς την καθυστέρηση εφαρμογές και συγκεκριμένα με τα μηνύματα GOOSE και SMV, τα οποία δεν περνούν σε ανώτερο επίπεδο στην στοίβα. Για να μην ξεπερνιούνται τα όρια καθυστέρησης τα δεδομένα δεν κρυπτογραφούνται και από πλευράς ασφαλείας υπάρχει μόνο η αυθεντικοποίηση.



Εικόνα 45 "Επίπεδα που εισάγονται από το IEC 62351 για προστασία του IEC 61850" (Wenye Wang Z. L., 2013)

IEC 62056

Είναι ένα σύνολο προτύπων για την ανταλλαγή μετρικών δεδομένων ανάμεσα σε συσκευές των ευφυών δικτύων ενέργειας. Το IEC 62056 είναι οι διεθνείς εκδόσεις των Device Language Message Specification(DLMS)/Companion Specification for Energy Metering(COSEM). Το DLMS έχει αναπτυχθεί από το οργανισμό DLMS User Association και έχει υιοθετηθεί από το IRC TC13 WG14 στο σύνολο του IEC 62056. Το COSEM περιλαμβάνει ένα σύνολο χαρακτηριστικών, που ορίζουν το επίπεδο Transport και Application του DLMS πρωτοκόλλου. Χαρακτηριστικά το DLMS/COSEM έχει την δυνατότητα να υλοποιηθεί σε δίκτυα TCP/IP και UDP/IP ενώ βασίζεται στην αρχιτεκτονική Client-Server. Η πλευρά του Server, θεωρείται ο έξυπνος μετρητής ενώ του Client το κέντρο διαχείρισης, ή ο Server ο έξυπνος μετρητής και ο Client είναι ο συλλέκτης δεδομένων.

Ακόμη, παρέχεται συγχρονισμός αλλά μέχρι στιγμής δεν υποστηρίζονται λειτουργίες όπως απομακρυσμένη εγκατάσταση firmware, και χρήση ψηφιακών υπογραφών. Για την ασφάλεια, εφαρμόζεται αυθεντικοποίηση και ιδιωτικότητα μέσω συμμετρικής κρυπτογράφησης, ενώ δεν υποστηρίζεται το TLS/SSL όπως άλλα πρωτόκολλα. Η χρήση ασύμμετρης κρυπτογράφησης αναπτύσσεται από τον οργανισμό CENELEC στο WG 02 TC13. Από πλευράς δομής, κάθε παράμετρος, αναπαρίσταται ως COSEM αντικείμενο, δηλαδή οι λειτουργικότητα των έξυπνων μετρητών μοντελοποιείται ως αντικείμενα COSEM συγκεκριμένων κλάσεων. Τέτοιες κλάσεις είναι οι Real Time Clock, Date and time, Voltage, Billing Counter, Timestamp και άλλες. Κάθε κλάση έχει μεταβλητές και μεθόδους που εφαρμόζονται πάνω στα αντικείμενα. Για την ανάκτηση των δεδομένων των μεταβλητών παρέχεται συνάρτηση GetRequest, ώστε να απαντήσει ο Server, με τα δεδομένα που ζητούνται. Το DLMS/COSEM επίσης κατά κύριο λόγο υλοποιείται στην Ευρώπη ανάμεσα σε διαφορετικούς έξυπνους μετρητές. (Stefan Feuerhahn, 2011) (Gordan Štruklec, 2011)

7.3 ANSI

ANSI C12.22

Ο οργανισμός American National Standards Institute(ANSI) συμμετέχει στην προσπάθεια προτυποποίησης των ευφυών δικτύων ενέργειας με κύριο πρότυπο το ANSI C12.22. Το ANSI C12.22 είναι ένα ανοιχτό πρότυπο επιπέδου εφαρμογών(application layer), ανεξάρτητο από τα κατώτερα επίπεδα του OSI, για την μεταφορά δεδομένων που βασίζονται στο ANSI C.12.19 μεταξύ έξυπνων μετρητών αλλά και άλλων συσκευών που το υποστηρίζουν στα πλαίσια των ευφυών δικτύων ενέργειας. Παρέχει αξιοπιστία, αλλά και ασφάλεια μέσω κρυπτογράφησης AES για την μεταφορά δεδομένων ακόμη και μέσω ετερογενών δικτύων. Το κύριο πλεονέκτημα του προτύπου αυτού είναι εισάγει την διαλειτουργικότητα ανάμεσα σε διαφορετικούς έξυπνους μετρητές που μπορούν

να χρησιμοποιηθούν. Το ANSI C12.22 όπως αναφέρθηκε είναι ανεξάρτητο από πρωτόκολλα δικτύου και μεταφοράς. Δεν θα μπορούσε όμως να μην συνδυαστεί με το γνωστότερο πρωτόκολλο δικτύου το IP, αλλά και με το TCP και UDP που ανήκουν στο επίπεδο μεταφορών. Στο (Moise A, 2011) μελετάται η μεταφορά τον μηνυμάτων του ANSI C12.22 μέσω IP(IPv4 ή IPv6) και των TCP και UDP. Ειδικότερα το ANSI C12.22 over IP, καθορίζει πως οι κόμβοι(έξυπνοι μετρητές, IEDs) επικοινωνούν μεταξύ τους, το οποίο προσθέτει, διαλειτουργικότητα αλλά και ευελιξία στο “last-mile”. Τα κυριότερα σημεία του συστήματος αυτού είναι: (Moise A, 2011) (Institute, 2008)

1. C12.22 IP Node

Αποτελείται από C12.22 Module και Device. Ανήκει, σε ένα IP Network Segment και σε κάθε κόμβο, τρέχουν μία ή περισσότερες c12.22 εφαρμογές. Μπορεί να επικοινωνεί και με άλλες κόμβους με την χρήση του κατάλληλου Module που υποστηρίζει το ανάλογο PHY/MAC επίπεδο. Κύριο χαρακτηριστικό του είναι η δυνατότητα εγκατάστασης “plug-n-play”.

2. C12.22 IP Network Segment

Είναι ένα σύνολο κόμβων, που χρησιμοποιούν το IP πρωτόκολλο, και μπορούν να επικοινωνούν μεταξύ τους χωρίς την προώθηση μηνυμάτων σε κάποιο Relay. Κάθε IP Segment, μπορεί να χαρακτηριστεί ως ένα private lan, ή ένα subnet ενός δικτύου.

3. C12.22 IP Network

Είναι ένα σύνολο από IP Segments, που συνδέονται μεταξύ τους μέσω IP Relays. Κάθε δίκτυο, περιλαμβάνει τουλάχιστον ένα c12.22 Master Relay.

4. C12.22 IP Relay

Είναι ένα είδος κόμβου το οποίο πραγματοποιεί λειτουργίες όπως είναι μετάφραση διευθύνσεων, προώθηση μηνυμάτων σε κόμβους. Λειτουργεί, ως γέφυρα ανάμεσα σε δύο Segments. Τοποθετείται στο σημείο που διαχωρίζονται τα δύο δίκτυα, Backhaul και “last-mile”, υποστηρίζοντας μέσω του ανάλογου Module διαφορετικά interface για την Backhaul πλευρά. Για παράδειγμα, ένα Backhaul δίκτυο θα μπορούσε να είχε υλοποιηθεί με το WiMAX, ενώ το “last-mile” με PLC, ή mesh τεχνολογία.

5. C12.22 IP Master Relay

Βρίσκεται στην κορυφή της ιεραρχίας από το σύνολο των IP Relay και στεγάζεται στο κέντρο διαχείρισης(head end). Κάθε IP Device, καταγράφεται από το Master Relay και περιλαμβάνει πληροφορίες δρομολόγησης για κάθε IP Relay. Ενώ, κάθε IP Relay διατηρεί πληροφορίες δρομολόγησης για κάθε IP Device που συνδέεται σε αυτόν.

6. C12.22 Communications Module

Είναι το hardware εκείνο που προσαρμόζεται σε μια C12.22 IP Device, για την σύνδεση στο Network Segment. Μπορεί να βρίσκεται και εξωτερικά της συσκευής.

7. C12.22 The C12.22 Device

Θεωρείται η συσκευή που τρέχει μια C12.22 εφαρμογή και έχει τουλάχιστον ένα interface για σύνδεση με Communication Module.

8. C12.22 IP Host

Είναι ένας C12.22 κόμβος που τρέχει μια εφαρμογή C12.22.

Δύο ειδικές κατηγορίες είναι οι:

- C12.22 Authentication Host

Παρέχει εγγραφή και διαγραφή των κόμβων που ανήκουν σε ένα δίκτυο ενός συγκεκριμένου Relay. Μπορεί να είναι ενσωματωμένος στο Relay ή ως ξεχωριστός κόμβος.

- C12.22 Notification Host

Καταγράφει στοιχεία σχετικά με την εγγραφή και την διαγραφή κόμβων από τον Authentication Host σε ένα δίκτυο.

9. C12.22 Gateway

Η πύλη αυτή χρειάζεται όταν ένας κόμβος του δικτύου ANSI C12.22 πρέπει να επικοινωνεί με έναν κόμβο που δεν είναι συμβατός με το πρότυπο C12.22. Όποτε η πύλη αναλαμβάνει να μεταφράζει τα μηνύματα C12.22 σε κάποια άλλη μορφή. Χαρακτηριστικό παράδειγμα είναι η σύνδεση με IED που δεν υποστηρίζουν το C12.22.

10. C12.22 Server

Ένα κόμβος όπου εκτελεί χρέη εξυπηρετητή για το δίκτυο. Χρησιμοποιείται για επικοινωνία με sessions με άλλους κόμβους.

Άλλα σημαντικά χαρακτηριστικά είναι:

1. Το TCP είναι το προεπιλεγμένο πρωτόκολλο για το C12.22 over IP.
2. Για την διασφάλιση της διαλειτουργικότητας μεταξύ των κόμβων χρησιμοποιείται το TCP και UDP port 1153 ως προεπιλογή για την ανταλλαγή των μηνυμάτων. Συνεπώς, οι IP Relays και Master Relays, πρέπει να δέχονται να αποστέλλουν πακέτα σε αυτό την θύρα.
3. Τουλάχιστον μία Unicast TCP ή UDP λειτουργία πρέπει να υποστηρίζεται από κάθε κόμβο.
4. Υποστήριξη QoS, μέσω tags που παρέχονται από το C12.22 για την επισήμανση των κρίσιμων μηνυμάτων από και προς του έξυπνους μετρητές. Για παράδειγμα, το QoS μπορεί να εφαρμοσθεί σε ένα σημείο στο “last-mile” όπως για παράδειγμα σε ένα Access Point για το διαχωρισμό και την προτεραιότητα των μηνυμάτων που αφορούν λειτουργίες DR.

5. Όλοι οι συσκευές που λειτουργούν ως IP Relays, είναι απαραίτητο να υποστηρίζουν IP Multicast για παράδοση μηνυμάτων σε συγκεκριμένους κόμβους ή σε ένα ολόκληρο δίκτυο.
6. Το ANSI C12.22 χρησιμοποιεί για μηχανισμό ασφαλείας το AES 128bit. (Technology, NIST PAP 01-The Role of IP in the Smart Grid, 2009)

ANSI C12.19

Η δομή των δεδομένων που ανταλλάσσονται καθορίζεται όπως αναφέρθηκε από το ANSI C12.19, ενώ το C12.22 αναλαμβάνει την διακίνηση των δεδομένων ανεξάρτητα από την αρχιτεκτονική ή την τεχνολογία του δικτύου. Το ANSI C12.19 καθορίζει την δομή των δεδομένων με την μορφή “table data” και δύο ειδών συσκευές, η μία που χαρακτηρίζεται ως “end device”, αναφερόμενη στους έξυπνους μετρητές και μια ως “computer” η οποία αναφέρεται στο σύστημα συλλογής των δεδομένων(head end). Οι πίνακες των δεδομένων, ομαδοποιούνται σε “decades” Κάθε “decade” έχει ένα συγκεκριμένο σκοπό του σχετίζεται με τα δεδομένα. Τα κυριότερα είναι: (Instute, 2008)

1. General Configuration Tables
2. Data Source Tables
3. Register Tables
4. Local Display Tables
5. Security Tables
6. Time-of-Use Tables
7. Load Profile Tables
8. History & Event Logs Tables
9. User- Defined Tables
10. Telephone Control Tables
11. Load Control and Pricing Tables
12. Node Network Control Tables
13. Network Relay Control Tables
14. Extended User- Defined Tables
15. Quality of Service Tables
16. One-way Devices Tables

Επίσης, χρησιμοποιείται η Extensible Markup Language(XML), στο περιεχόμενο των πινάκων. Στο (Snyder A.F, 2007), εκτός από τα “decades” παρουσιάζονται και οι κωδικοποιημένες λειτουργίες που υποστηρίζονται από το πρότυπο.

7.4 ITU

ITU G.hnem

Ο οργανισμός International Telecommunication Union(ITU) συμμετέχει στην ανάπτυξη των ευφυών δικτύων ενέργειας, με το πρότυπο G.hnem. Το πρότυπο ITU G.hnem αποτελείται στην πραγματικότητα από δύο άλλα πρότυπα που καθορίζουν τα χαρακτηριστικά του. Αυτά είναι, τα ITU-T G.9955 και ITU-T G.9956. Το πρώτο σχετίζεται με τα χαρακτηριστικά στο φυσικό επίπεδο(PHY), ενώ το δεύτερο σχετίζεται με το δεύτερο επίπεδο(MAC). Παραπάνω αναφέρθηκε ότι το NIST με το PAP15 καθορίζει τις απαιτήσεις για φυσικό και MAC επίπεδο, το G.hnem έχει λάβει υπόψη τις προτάσεις αυτές και τις έχει συμπεριλάβει στην σχεδίαση του προτύπου. Το G.hnem, λειτουργεί σε συχνότητες από 35 μέχρι 143KHz για την Ευρώπη, οι οποίες καθορίζονται από τον CENELEC και από 34-475KHZ για συχνότητες που καθορίζονται από τον FCC. Ο ρυθμός μετάδοσης δεδομένων φτάνει το 1Mbps, ενώ υποστηρίζει πρωτόκολλα δικτύου όπως είναι το IPv4 και IPv6. (Jin Zhang, 2011)

ITU G.hn

Εκτός από το ITU G.hnem που χρησιμοποιείται κυρίως σε εφαρμογές AMI, υπάρχει ένα ακόμη πρότυπο ότι οποίο έγινε αποδεκτό και έχει αναγνωριστεί ως πρότυπο για χρήση στα ευφυή δίκτυα ενέργειας. Αυτό είναι το ITU G.hn, τα αρχικά του οποίου σημαίνουν Gigabit home networking. Το πρότυπο αυτό φτάνει σε ρυθμούς μετάδοσης το 1Gb/s ενώ χρησιμοποιεί την τεχνική OFDM. Επιτρέπει την λειτουργία μέχρι 250 συσκευών, ενώ η αρχιτεκτονική του βασίζεται στο ότι μια συσκευή στο ίδιο domain, λειτουργεί ως Master Domain(SM). Ο Master Domain είναι υπεύθυνος, για την διαχείριση όλων των συσκευών στο domain, όπως εγγραφή στο domain, καταμερισμός εύρους ζώνης κτλ. Σε περίπτωση που ο DM έχει κάποιο λειτουργικό πρόβλημα, την θέση του λαμβάνει κάποια άλλη συσκευή στο δίκτυο. Για την προστασία από τις παρεμβολές κατά την μετάδοση, ο DM αναλαμβάνει τον καθορισμό του χρόνου μετάδοσης κάθε συσκευής στο δίκτυο. Για την επικοινωνία μιας συσκευής ενός domain με μια άλλη που ανήκει σε άλλο domain, απαιτείται η χρήση γεφύρας, δηλαδή μιας συσκευή που αναλαμβάνει να διασύνδεει δύο διαφορετικά δίκτυα. (Stefano Galli, 2009) Τέλος, το πρότυπο αυτό έχει καθαρά εφαρμογή σε μικρά δίκτυα και προορίζεται για εφαρμογή μελλοντικά στα HAN των ευφυών δικτύων ενέργειας.

7.5 NIST

NISTIR 7628

Το πρότυπο NISTIR 7628 είναι μέρος του προγράμματος του NIST για την προτυποποίηση στα ευφυή δίκτυα ενέργειας. Εστιάζει στην ασφάλεια των ευφυών δικτύων ενέργειας και βασίζεται σε αναλύσεις ασφαλείας που προκύπτουν από σενάρια και υποθέσεις. Ο στόχος του είναι ο καθορισμός των απαιτήσεων ασφαλείας. Κάθε σενάριο που σχεδιάζεται στα πλαίσια του NISTIR 7628, μελετάται από ένα υψηλό επίπεδο αντίληψης που περιλαμβάνει αναγνώριση απειλών, ευπαθειών και πιθανών στόχων σε ένα ευφυές δίκτυο ενέργειας. Το αποτελέσματα από τα σενάρια χρησιμοποιούνται ως βάση για την ανάλυση και

των καθορισμό των απαιτήσεων ασφαλείας, ενώ έμφαση δίνεται στην κάλυψη κενών που υπάρχουν από άλλα πρότυπα και πρωτόκολλα που σχετίζονται με την ασφάλεια. Επίσης, αποτελείται από, ένα σύνολο λογικών διεπαφών και κάθε διεπαφή ανήκει σε μία από τις 22 κατηγορίες με βάσης τα χαρακτηριστικά που έχει. Κάθε κατηγορία, έχει μια μοναδική προτεραιότητα για κάθε στόχο(εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα), που είναι, χαμηλή, μέση, υψηλή. Σημαντικό είναι να αναφερθεί ότι το NIST αναγνωρίζει ότι ένα κύριο πρόβλημα είναι η φυσική ασφάλεια των υποδομών ενός ευφυούς δικτύου ενέργειας, λόγω του μεγέθους του, και ότι στο NISTIR 7628 είναι απαραίτητο να ληφθεί υπόψη η φυσική ασφάλεια όλων των υποδομών. Ένα δεύτερο αναγνωρισμένο πρόβλημα προκύπτει από την υπόθεση ότι ο πάροχος ηλεκτρικής ενέργειας ή ο διαχειριστής του ευφυούς δικτύου ενέργειας είναι έμπιστος. Το παραπάνω δεν μπορεί να θεωρείται δεδομένο, μιας και αφορά την ιδιωτικότητα μαζικά πολλών καταναλωτών. Τέλος, αυτά τα δύο προβλήματα είναι που έχει σκοπό να εστιάσει στο μέλλον το NIST στο NISTIR 7628. (Aldar C-F. Chan, 2013)

NIST Framework and Roadmap for Smart Grid Interoperability Standards

Το NIST συμμετέχει στην προσπάθεια προτυποποίησης των ευφυών δικτύων ενέργειας, με μια από της σημαντικότερες κινήσεις τα τελευταία χρόνια, την δημιουργία και εξέλιξη ενός πλαισίου για τον καθορισμό πρωτοκόλλων και προτύπων για την επίτευξη της διαλειτουργικότητας στα ευφυή δίκτυα ενέργειας. Το πλαίσιο αυτό είναι το NIST Framework and Roadmap for Smart Grid Interoperability Standards. Η ανάγκη που οδήγησε στην σχεδίαση του πλαισίου αυτή βασίζεται στο μέγεθος των ευφυών δικτύων ενέργειας, και η πληθώρα πρωτοκόλλων προτύπων αλλά και διαφορετικών συσκευών, είναι συνεπώς κατανοητό πως μόνο μέσα από την συνεργασία για την επίτευξη της διαλειτουργικότητας θα υπάρξει εξέλιξη στα ευφυή δίκτυα ενέργειας. Σημείο αναφοράς για το πλαίσιο αυτό είναι η ανάπτυξη ενός εννοιολογικού μοντέλου το οποίο έχει ως στόχο τον καθορισμό των αλληλεπιδράσεων μεταξύ τμημάτων απαρτίζεται ένα ευφυές δίκτυο ενέργειας, τον καθορισμό των καναλιών επικοινωνίας και τον ενδιαφερόμενων τμημάτων.

Το μοντέλο αυτό δεν είναι μια αρχιτεκτονική σχεδίασης αλλά ένα αφαιρετικό μοντέλο για το καθορισμό αρχιτεκτονικών. Στην τελευταία έκδοση του το πλαίσιο αυτό, ενθαρρύνει επίσης και την χρήση δικτύων που βασίζονται στο IP, και ειδικότερα στο IPv6, αναφέροντας ότι ο αριθμός των ipv4 διευθύνσεων εξαντλείται. Η επίτευξη της διαλειτουργικότητας επιτυγχάνεται μέσα από τον καθορισμό των πρωτόκολλων που μπορούν να χρησιμοποιηθούν στα ευφυή δίκτυα ενέργειας. Μέχρι στιγμής τα πρότυπα και πρωτόκολλα που έχουμε μελετήσει έχουν αναγνωρισθεί στο πλαίσιο αυτό. Μια άλλη σημαντική διεργασία είναι η ανάπτυξη των Priority Action Plans(PAPs), τα οποία καταγράφουν τις δύο παρακάτω καταστάσεις:

1. Όταν ανακαλύπτεται ένα κενό στις απαιτήσεις, και απαιτείται η σχεδίαση ενός προτύπου ή η επέκταση ενός προτύπου για την κάλυψη του κενού.
2. Όταν δύο πρότυπα έχουν την ίδια εφαρμογή και καλύπτουν τις ίδιες απαιτήσεις.

Η καταγραφή των PAP βοηθάει στην μελέτη πια πρότυπα θα αναγνωριστούν και θα μπουν στην λίστα των αναγνωρισμένων για εφαρμογή. (NIST, 2012)

7.6 ΠΡΟΤΥΠΑ-ΠΡΩΤΟΚΟΛΛΑ ΑΛΛΩΝ ΟΡΓΑΝΙΣΜΩΝ

Smart Energy Profile

Το Smart Energy Profile(SEP) 2.0 έχει αναπτυχθεί από τον οργανισμό ZigBee Alliance σε συνδυασμό με τον οργανισμό HomePlug Alliance για εφαρμογή στα ευφυή δίκτυα ενέργειας. Το πρωτόκολλο αυτό η IEEE το παρέχει με την ονομασία IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard, IEEE 2030.5-2013. Στόχος του είναι, η σχεδίαση ενός πρωτοκόλλου, με έμφαση στην διαλειτουργικότητα που θα συνδέει τις έξυπνες συσκευές με τους έξυπνους μετρητές σε ένα HAN, δηλαδή η εφαρμογή του εστιάζει αποκλειστικά στο HAN. Έχει σχεδιασθεί για να τρέχει πάνω στο TCP/IP και καλύπτει τα επίπεδα εφαρμογών, μεταφοράς και διαδικτύου του TCP/IP. Συνεπώς παραμένει ανεξάρτητο από τα κατώτερα επίπεδα και δεν εστιάζει σε αυτά. Προτείνεται ωστόσο για εφαρμογή σε συνδυασμό με το 802.15.4, 802.11 και το 1901. Εστιάζει όμως στην ανταλλαγή μηνυμάτων στα επίπεδα που ασχολείται, περιλαμβανομένων και ων μηχανισμών ασφαλείας για την προστασία των μηνυμάτων. Το SEP παρέχει ένα σύνολο λειτουργιών που ταξινομούνται σε sets και παρέχει το καθένα διαφορετικές λειτουργίες. Υπάρχουν μια πληθώρα από set, που σχετίζονται με την χρέωση ενέργειας, την καταγραφή της ενέργειας που έχει καταναλωθεί, την διαδικασία demand response, αλλά και την ανταλλαγή μηνυμάτων ανάμεσα στις συσκευές που υλοποιούν το πρωτόκολλο αυτό. Τα sets, αυτά επιτρέπουν εκτός από την ενημέρωση του χρήστη σχετικά με την καταναλωμένη ενέργεια, την συμμετοχή του στην διαχείριση της ενέργειας, μιας και το πρότυπο έχει δυνατότητες να υλοποιηθεί σε εφαρμογές κινητών τηλεφώνων-Smartphone, όπως και σε άλλες συσκευές ενημέρωσης, In-Home-Display, για την ζωντανή παρακολούθηση και διαχείριση της ενέργειας στο HAN. Οι πληροφορίες αυτές μπορούν να μεταδίδονται από τους έξυπνους μετρητές ή από κάποια υπηρεσία από το κέντρο διαχείρισης του ευφυούς δικτύου ενέργειας πρόσβαση από το διαδίκτυο. Να σημειωθεί ότι για την διαδικασία αυτή, στο μέλλον ενδέχεται να εμφανιστούν και χρήσεις υπολογιστικής νέφους(Cloud Computing). Από πλευράς ασφάλειας το πρωτόκολλο χρησιμοποιεί το HTTPS, λίστες πρόσβασης και ψηφιακά πιστοποιητικά. Τέλος, να σημειωθεί ότι το πρωτόκολλο είναι υπό εξέλιξη. Στο πίνακα παρακάτω παρουσιάζονται ταξινομημένα τα function sets που πρωτοκόλλου. (Society I. C., 2030.5-2013 - IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard, 2013)

Πίνακας 5 "Function Sets του SEP 2.0"

Common Resources	Smart Energy Resources
Time Function Set	Common Functionality
Device Information Function Set	Demand Response and Load Control
Power Status	Metering Function Set
Network Status	Pricing Function Set
LogEvent List	Messaging Function Set
Configuration Resource	Billing Function Set
File Download Function Set	Prepayment Function Set
	Energy Flow Reservation Function Set
	Distributed Energy Resources Function Set
	Metering Mirror

HomePlug Green PHY

Ο οργανισμός HomePlug Alliance εστιάζοντας στα ευφυή δίκτυα ενέργειας έχει αναπτύξει το HomePlug Green PHY(HomePlug GP) Specification, το οποίο έχει σχεδιασθεί για εφαρμογές στο HAN. Έμφαση έχει δοθεί στο χαμηλό κόστος υλοποίησης σε σχέση με το HomePlug AV. Επιτυγχάνει ρυθμό μετάδοσης μέχρι 10Mbps σε συχνότητα λειτουργίας από 2MHz μέχρι 30MHz ενώ χρησιμοποίει την τεχνική CSMA/CA. Υποστηρίζει ipv4 και ipv6. Στην τελευταία έκδοση 1.1 υποστηρίζει την σύνδεση Plug-in Electric Vehicle(PEV). Τέλος, για την μείωση της κατανάλωσης ενέργειας επίσης έχει σχεδιαστεί ένα Power Saving Mode. (Alliance H. P., HomePlug Green PHY 1.1, The Standard for In-Home Smart Grid Powerline Communications: An application and technology overview, 2012)

RFC 6272

Από το 2010 ο οργανισμός NIST έχει προτείνει την χρήση του IP πρωτοκόλλου στα ευφυή δίκτυα ενέργειας αφού έχει ήδη μπει στα Priority Action Plans(PAP). Με βάση το παραπάνω, ο οργανισμός Internet Engineering Task Force(IETF) έχει δημοσιεύσει από το 2011 το Request For Comments(RFC) 6272, με την ονομασία Internet Protocols for the Smart Grid. Το RFC 6272, παρέχει γενικές πληροφορίες σχετικά με τα μέρη που αποτελείται το IP με σκοπό την υλοποίηση δικτύων βασισμένα στο IP πρωτόκολλο. Συνεπώς οι οδηγίες που παρέχονται είναι πολύ γενικές και μέχρι στιγμής δεν έχουν υπάρξει λύσεις. (D. Meyer, 2011)

RFC 6142

Μια ακόμη μη επίσημη προσπάθεια από τον IETF, που σχετίζεται με την μεταφορά μηνυμάτων ANSI C12.22/IEEE 1703, βασισμένη στο IP, σε συνδυασμό

με TCP ή UDP. Να σημειωθεί ότι δεν προτείνονται λύσεις, αλλά μόνο οδηγίες για την ανάπτυξη ενός IP δικτύου. (A. Moise, 2011)

PRIME

Το Powerline Intelligent Metering Evolution (PRIME) είναι μια τεχνολογία PLC, που έχει σχεδιασθεί από το οργανισμό PRIME Alliance, για εφαρμογές στα ευφυή δίκτυα ενέργειας. Με το πρότυπο αυτό ορίζονται δύο επίπεδα, το φυσικό επίπεδο(PHY) και το επίπεδο MAC, ενώ το πρότυπο είναι ανοιχτό προς υλοποίηση. Έμφαση κατά την ανάπτυξή έχει δοθεί στο χαμηλό κόστος υλοποίησης του προτύπου. Από πλευράς χαρακτηριστικών χρησιμοποιεί την τεχνική OFDM και φτάνει σε ρυθμό μετάδοσης τα 130kbps. ΜΕ την υλοποίηση ενός ενδιάμεσου επιπέδου υπάρχει δυνατότητα χρήση του IPv4 πρωτοκόλλου για την δημιουργία IP δικτύων. Εφαρμογή έχει στο NAN και ειδικά στο “last-mile” του AMI, σε εφαρμογές παρακολούθησης του δικτύου ενέργειας, αλλά και εφαρμογές επικοινωνίας σε μονάδες ανανεώσιμων πηγών ενέργειας. Σημαντική κίνηση του PRIME Alliance, είναι η δημιουργία ενός πιστοποιητικού με την ονομασία PRIME Certification για την πιστοποίηση του hardware, έξυπνων μετρητών και συλλεκτών δεδομένων. Για την ασφάλεια των δεδομένων, παρέχονται αυθεντικοποίηση και ιδιωτικότητα μέσω μηχανισμών όπως είναι ο AES 128bit. (Project P. , 2008)

G3-PLC

Ένα πρότυπο που είναι ανταγωνιστικό του PRIME, είναι το G3-PLC που έχει αναπτυχθεί από το οργανισμό G3-PLC Alliance. Το G3-PLC, έχει σχεδιασθεί για επικοινωνία σε μεγάλες αποστάσεις και ανήκει στην κατηγορία των NB-PLC. Χρησιμοποιεί και αυτό την τεχνική OFDM, σημαντικό είναι ότι το MAC επίπεδο παρέχει υποστήριξη mesh αρχιτεκτονικής, ενώ για την πρόσβαση στο μέσο χρησιμοποιείται η τεχνική CSMA/CA. Ο ρυθμός μετάδοσης των δεδομένων είναι χαμηλότερος σε σχέση με το PRIME και φτάνει περίπου τα 33kbps όμως και το G3-PLC έχει δυνατότητα να μεταδίδει πληροφορίες ακόμα και μέσα από μετασχηματιστές του δικτύου ηλεκτρικής ενέργειας. Να σημειωθεί ότι το frame του G3-PLC, έχει σχεδιασθεί με μεταφέρει IPv6 πακέτα, το οποίο είναι μεγάλο πλεονέκτημα για μελλοντικές εφαρμογές. Για την ασφάλεια γίνεται χρήση του αλγόριθμού AES 128bit και στο επίπεδο εφαρμογών προτείνεται η χρήση του ANSI C12.19/ANSI C12.22. (Jean Vigneron, 2012)

7.7 ΣΥΓΚΕΝΤΡΩΤΙΚΟΣ ΠΙΝΑΚΑΣ ΠΡΩΤΥΠΩΝ ΚΑΙ ΠΡΩΤΟΚΟΛΛΩΝ

Πίνακας 6 "Πρότυπα και πρωτοκόλλα που σχετίζονται με τις επικοινωνίες και την ασφάλεια των ευφυών δικτύων ενέργειας"

ΤΥΠΟΣ/ΟΝΟΜΑ ΠΡΟΤΥΠΟΥ	ΚΑΤΗΓΟΡΙΑ	ΠΕΡΙΟΧΗ ΕΦΑΡΜΟΓΗΣ	ΠΕΡΙΓΡΑΦΗ
IEEE 2030	Δίκτυα	Wan, Nan, Han	Ανάπτυξη διαλειτουργικότητας, μοντέλο αναφοράς
IEEE 1815(DNP3)	Δίκτυα	Wan	Πρωτόκολλο επικοινωνίας IED
IEEE 1588(PTP)	Δίκτυα	Wan	Συγχρονισμός συσκευών δικτύου, υποσταθμών
IEEE 1686	Ασφάλεια	Wan	Οδηγίες για την προστασία των IED στους υποσταθμούς
IEEE 1901.2	Δίκτυα	Nan, Han	PLC χαμηλής συχνότητας, Κύρια εφαρμογή στο last-mile του NAN
IEEE 1901	Δίκτυα	Nan, Han	Broadband(500Mbps) PLC, Δικτύωση στο HAN, last-mile Του NAN, Μικρή απόσταση λειτουργίας
IEEE C37.118	Δίκτυα	Wan	Καθορίζει την επικοινωνία των Phasor Measurement Unit(PMU) και τα χαρακτηριστικά τους
IEEE 1909.1	Δίκτυα	Wan, Nan	Οδηγίες σχεδίασης hardware, καθορισμός χαρακτηριστικών
IEC 61850	Δίκτυα	Wan	Επικοινωνία ανάμεσα σε κεντρικές υποδομές, Υποσταθμούς, Καθορισμός απαιτήσεων καθυστέρησης, οδηγίες αυτοματισμών
IEC 62351	Ασφάλεια	Wan	Προστασία του 61850, κ δεδομένων, μηχανισμοί αυθεντικοποίησης και κρυπτογράφησης

ΤΥΠΟΣ/ΟΝΟΜΑ ΠΡΟΤΥΠΟΥ	ΚΑΤΗΓΟΡΙΑ	ΠΕΡΙΟΧΗ ΕΦΑΡΜΟΓΗΣ	ΠΕΡΙΓΡΑΦΗ
IEC 62056	Δίκτυα	Wan, Nan	DLMS/COSEM-πρωτόκολλο ανταλλαγής δεδομένων έξυπνων μετρητών, επικοινωνία AMI
ANSI C12.22	Δίκτυα	Wan, Nan	Πρωτόκολλο μεταφοράς μηνυμάτων c12.19, επικοινωνία AMI
ANSI C12.19	Δίκτυα	Wan, Nan	Πρωτόκολλο ανταλλαγής δεδομένων, επιπέδου εφαρμογών, εφαρμογή στο AMI
ITU G.hnem	Δίκτυα	Nan, Han	PLC επικοινωνία για AMI, EV, μονάδων παραγωγής ενέργειας, δυνατότητα εφαρμογής στο HAN
ITU G.hn	Δίκτυα	Han	Plc επικοινωνία ανάμεσα σε συσκευές και έξυπνους μετρητές, χαμηλό κόστος υλοποίησης, ρυθμός μετάδοσης μέχρι 1gbit/s, υποστήριξη ipv4, ipv6
Nistir 7628	Ασφάλεια	Wan, Nan, Han	Βασικές αρχές, ορισμοί, Γενικές οδηγίες προστασίας ευφυών δικτύων ενέργειας
NIST Framework and Roadmap for Smart Grid Interoperability Standards	Δίκτυα	Wan, Nan, Han	Επίτευξη διαλειτουργικότητας μεταξύ προτύπων και πρωτοκόλλων, Μελέτη κάλυψης κενών στις απαιτήσεις, καθορισμός των PAP
Smart Energy Profile(SEP)	Δίκτυα	Han	Πρωτόκολλο επιπέδου εφαρμογών για διαχείριση ενέργειας συσκευών, πιστοποίηση συσκευών που το χρησιμοποιούν

ΤΥΠΟΣ/ΟΝΟΜΑ ΠΡΟΤΥΠΟΥ	ΚΑΤΗΓΟΡΙΑ	ΠΕΡΙΟΧΗ ΕΦΑΡΜΟΓΗΣ	ΠΕΡΙΓΡΑΦΗ
HomePlug Green PHY	Δίκτυα	Han	Πρότυπο καθορισμού κατώτερων επιπέδου επικοινωνίας PLC, χαμηλό κόστος υλοποίησης, υποστήριξη IP, έμφαση στην μείωση κατανάλωσης ενέργειας
RFC 6272	Δίκτυα	Wan, Nan, Han	Πλαίσιο προσπάθειας εφαρμογής του IP στα ευφυή δίκτυα ενέργειας
RFC 6142	Δίκτυα	Wan, Nan, Han	Πλαίσιο σχεδίασης μεταφοράς μηνυμάτων ANSI C12.19 μέσω IP
Prime	Δίκτυα	Nan	PLC πρότυπο για το last-mile του AMI, συλλογή δεδομένων από έξυπνους μετρητές, μικρός ρυθμός μετάδοσης
G3-Plc	Δίκτυα	Wan, Nan	Εμβέλεια πάνω από 10 χλμ, υποστήριξη αρχιτεκτονικής mesh και ipv6, ικανότητα επικοινωνίας μέσα από μετασχηματιστές, μερική εφαρμογή στο WAN παρακολούθηση δικτύου ενέργειας, περιορισμός ο μικρός ρυθμός μετάδοσης
ZigBee	Δίκτυα	Han	Ασύρματη επικοινωνία μεταξύ συσκευών και έξυπνων μετρητών, μικρό κόστος, μικρή κατανάλωση, μικρή απόσταση λειτουργίας
Wi-Fi	Δίκτυα	Wan, Nan, Han	Last-mile στο NAN, σε point to point ή mesh. Εφαρμογή σε υποσταθμούς για παρακολούθηση δικτύου, επικοινωνίας συσκευών με έξυπνων μετρητή στο HAN

ΤΥΠΟΣ/ΟΝΟΜΑ ΠΡΟΤΥΠΟΥ	ΚΑΤΗΓΟΡΙΑ	ΠΕΡΙΟΧΗ ΕΦΑΡΜΟΓΗΣ	ΠΕΡΙΓΡΑΦΗ
WiMAX	Δίκτυα	Wan, Nan	Δίκτυο κορμού WAN, επικοινωνία μεταξύ υποσταθμών, point to point επικοινωνία με έξυπνους μετρητές, μεγάλη απόσταση λειτουργίας
Pftth	Δίκτυα	Wan, Nan	End to-end επικοινωνία έξυπνων μετρητών, επικοινωνία μεταξύ υποσταθμών, παρακολούθηση δικτύου ενέργειας, βρίσκεται υπό ανάπτυξη
Lte	Δίκτυα	Wan, Nan	End to-end επικοινωνία έξυπνων μετρητών, κάλυψη σε όλο το εύρος το WAN, NAN, επικοινωνία υποσταθμών, κινητών μονάδων, χρήση ιδιωτικού ή δημοσίου δικτύου
3g/Gprs	Δίκτυα	Wan, Nan	End to-end επικοινωνία έξυπνων μετρητών, χρήση ήδη λειτουργικών δικτύων, μεγάλη γεωγραφική κάλυψη

ΕΠΙΛΟΓΟΣ

Στα ευφυή δίκτυα ενέργειας βρίσκουν εφαρμογή μεγάλο πλήθος προτύπων και πρωτοκόλλων ασύρματων και ενσύρματων τεχνολογιών. Οι ιδιαιτερότητες όμως των ευφυών δικτύων ενέργειας, έχουν οδηγήσει στην σχεδίαση νέων προτύπων και πρωτοκόλλων που βρίσκουν αποκλειστική εφαρμογή στα ευφυή δίκτυα ενέργειας τα οποία δίνουν έμφαση στην χαμηλή κατανάλωση ενέργειας και στην χρήση ήδη διαθέσιμων μέσων βασιζόμενα σε γνωστές τεχνολογίες όπως είναι η PLC. Σημαντική εξέλιξη έχει γίνει και σε επίπεδο εφαρμογών με την ανάπτυξη πρωτοκόλλων ανταλλαγής δεδομένων μεταξύ των έξυπνων μετρητών ενέργειας και τους ευφυούς δικτύου ενέργειας για την συλλογή δεδομένων παρέχοντας επιπλέον και προστασία των δεδομένων. Για την ανάπτυξη όμως προτύπων και πρωτοκόλλων απαιτούνται οδηγίες και συμβουλές, στο πλαίσιο αυτό οργανισμοί όπως ο NIST και η IEEE έχουν εκδώσει οδηγίες για τις επικοινωνίες και την ασφάλεια με την μορφή προτύπων.

ΚΕΦΑΛΑΙΟ 8

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα ευφυή δίκτυα ενέργειας κερδίζουν συνεχώς το ενδιαφέρον και αναμφίβολα θα αποτελέσουν θέμα πολλών μελλοντικών μελετών. Στην παρούσα πτυχιακή εργασία ασχοληθήκαμε με τις τεχνολογίες επικοινωνιών που μπορούν να χρησιμοποιηθούν σε αυτά για την κάλυψη των απαιτήσεων επικοινωνίας των WAN, NAN και HAN. Το δίκτυο επικοινωνιών αποτελεί άρρηκτο κομμάτι του ευφυούς δικτύου ενέργειας για την λειτουργία του, ενώ η διαθεσιμότητα είναι καθοριστικός παράγοντας. Υποστηρίζεται ένα πλήθος λειτουργιών όπως είναι η συλλογή δεδομένων από τους έξυπνους μετρητές ενέργειας, η παρακολούθηση του δικτύου μεταφοράς και διανομής ενέργειας, η απαιτητική από πλευράς καθυστέρηση επικοινωνίας ανάμεσα στις κεντρικές υποδομές όπως είναι οι υποσταθμοί και άλλες μελλοντικές λειτουργίες όπως είναι η επικοινωνία οχημάτων.

Η επιλογή της κατάλληλης τεχνολογίας για το δίκτυο επικοινωνιών δεν είναι εύκολη υπόθεση καθώς παράγοντες όπως η αρχιτεκτονική, το εύρος λειτουργίας, το κόστος υλοποίησης αλλά και η ασφάλεια που υποστηρίζεται από την εκάστοτε τεχνολογία ασύρματης ή ενσύρματης δικτύωσης είναι καθοριστικοί. Από την άλλη μεριά όμως, μέσα από την μελέτη της κάθε τεχνολογίας και των απαιτήσεων κάθε περιοχής, όπως είναι το WAN, NAN και το HAN, το αποτέλεσμα που προκύπτει είναι ότι, τεχνολογίες τετάρτης γενιάς όπως είναι το LTE και το WiMAX, θεωρούνται το φαβορί, ενώ για το HAN, το ZigBee και οι τεχνολογίες PLC ξεχωρίζουν και αυτές. Το NAN που ενώνει αυτές τις δύο περιοχές, επίσης αποτελεί πρόκληση για την αρχιτεκτονική του σχεδίαση, ενώ οι τεχνολογίες τετάρτης γενιάς μπορούν να καλύψουν και αυτό, το Wi-Fi σε αρχιτεκτονική mesh, για το last-mile, αποτελεί μια καλή λύση. Οι επιλογές είναι πολλές, όμως ας μην ξεχνάνε ότι και κάθε ευφυές δίκτυο ενέργειας, που υλοποιείται περιλαμβάνει διαφορετικές περιοχές και ενδέχεται να εμφανιστούν ιδιαιτερότητες. Επιπλέον, είδαμε πρότυπα και πρωτόκολλα όλων των επιπέδων τα οποία έχουν αναπτυχθεί για εφαρμογή στα ευφυή δίκτυα ενέργειας. Στα κατώτερα επίπεδα για επικοινωνία PLC, στο HAN και στο NAN, αλλά και πρωτόκολλα επιπέδου εφαρμογών όπως είναι το SEP 2.0 και το ANSI C12.22 για την επικοινωνία συσκευών στο HAN και επικοινωνία των έξυπνων μετρητών αντίστοιχα.

Η σχεδίαση και η ανάπτυξη προτύπων απαιτεί αρχικά καθορισμό των στόχων και των απαιτήσεων κάθε προτύπου ή πρωτοκόλλου, διεθνείς οργανισμοί όπως η IEEE και ο NIST, έχουν κάνει σημαντικά βήματα προς αυτή την κατεύθυνση. Τα πρότυπα και τα πρωτόκολλα είναι απαραίτητα για την επίτευξη της διαλειτουργικότητας μεταξύ διαφορετικών συσκευών στο HAN, μέχρι και την επικοινωνία μέσω ετερογενών δικτύων διαφορετικής τεχνολογίας. Συνεπώς, στο μέλλον αναμένεται μεγάλη εξέλιξη στο κομμάτι αυτό.

Στο δεύτερο μέρος της παρούσας πτυχιακής εργασίας μελετήθηκε η ασφάλεια στα ευφυή δίκτυα ενέργειας, όπου εστιάζει στην προστασία του δικτύου επικοινωνιών και των δεδομένων που διακινούνται από ευπάθειες και απειλές. Η

μελέτη της ασφάλειας στα ευφυή δίκτυα ενέργειας επικεντρώνεται σε τρεις βασικές αρχές, την διαθεσιμότητα του δικτύου επικοινωνιών, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, ενώ βαρύτητα έχει δοθεί και στην αυθεντικοποίηση συσκευών και χρηστών. Η διαθεσιμότητα είναι ο βασικότερος στόχος και ειδικά στο WAN, ενώ για την συλλογή δεδομένων αντίστοιχα είναι η εμπιστευτικότητα των δεδομένων κάθε έξυπνου μετρητή ενέργειας. Η χρήση διαφορετικών τεχνολογιών, προτύπων και πρωτοκόλλων αυξάνει τον αριθμό των ευπαθειών και συνεπώς το επιθέσεων. Οι επιθέσεις έχουν ως πρώτο στόχο την διαθεσιμότητα του δικτύου και συνήθως ανήκουν στην κατηγορία των DoS, ενώ υπάρχουν και νέες επιθέσεις που εμφανίζονται στα ευφυή δίκτυα ενέργειας όπως είναι η false data injection και η remote disconnect.

Για την αντιμετώπιση των επιθέσεων έχουν σχεδιασθεί συστήματα ανίχνευσης απειλών, που είναι απαραίτητο να εφαρμοσθούν σε όλο το εύρος ενός ευφυούς δικτύου ενέργειας. Τα συστήματα αυτά χρειάζεται να είναι ανεξάρτητα από πρότυπα και πρωτόκολλα που χρησιμοποιούνται ενώ θα πρέπει να μελετηθεί περαιτέρω ο φόρτος που εισάγουν στο δίκτυο. Όπως αναφέραμε η αυθεντικοποίηση και η κρυπτογράφηση των δεδομένων, είναι κρίσιμα στοιχεία για την προστασία έναντι σε επιθέσεις παραποίησης ή προσποίησης. Όλες οι συσκευές, και ειδικά αυτές που δεν προστατεύονται από την περίμετρο του ευφυούς δικτύου ενέργειας, όπως είναι ένας υποσταθμός, που εξασφαλίζεται κατά έναν βαθμό η φυσική ασφάλεια απαιτούν αυθεντικοποίηση. Η αυθεντικοποίηση εστιάζει στους έξυπνους μετρητές, στους συλλέκτες δεδομένων και οποία άλλη δικτυακή συσκευή συμπεριλαμβάνεται στο δίκτυο επικοινωνιών. Ενώ έχουν υπάρξει αρκετά σχήματα αυθεντικοποίησης, κυρίως βασιζόμενα στην υποδομή δημοσίου κλειδιού, η πρόκληση είναι πως θα γίνεται η διαχείριση των κλειδιών μιας και εάν αναλογιστούμε το πλήθος των συσκευών σε ένα ευφυές δίκτυο καταλαβαίνουμε το διαχειριστικό κόστος που προκύπτει.

Μεγάλη εξέλιξη το τελευταίο καιρό γνωρίζουν τα σχήματα που βασίζονται στην δημιουργία των κλειδιών με βάση ένα μοναδικό αναγνωριστικό για κάθε συσκευή ή χρήστη. Επίσης, το τελευταίο καιρό έχει γίνει μελέτη των στόχων που πρέπει να έχουν τα σχήματα αυθεντικοποίησης, οι οποίοι είναι η αποδοτικότητα, το μικρότερο δυνατό διαχειριστικό κόστος και τέλος το μικρότερο δυνατό overhead. Εκτός από την αυθεντικοποίηση η ιδιωτικότητα των δεδομένων που ανταλλάσσονται στο AMI, είναι πολύ σημαντική, γιατί θέλουμε τα δεδομένα κάθε HAN να παραμένουν κρυφά, από κάθε κακόβουλο χρήστη.

Η εξασφάλιση της ιδιωτικότητας είναι απαραίτητη για να αντιμετωπιστούν επιθέσεις υποκλοπών αλλά και παραβιάσεις της ιδιωτικότητας τύπου Load Signature που εμφανίζεται πλέον στα ευφυή δίκτυα ενέργειας. Όπως και στην αυθεντικοποίηση και εδώ το overhead που προσθέτουν οι τεχνικές που απαιτούνται να εφαρμοσθούν είναι σημαντική παράμετρος στην σχεδίαση. Γνωστές τεχνικές βασίζονται στην ανωνυμία των δεδομένων(data anonymization), όπου τα δεδομένα χωρίζονται σε high-frequency και low-frequency, για την προστασία έναντι σε παραβιάσεις τύπου Load Signature. Ο στόχος των σχημάτων

αυτών είναι να περιέλθουν τα δεδομένα σε μια μορφή μη κατανοητή προς τρίτους, εκτός του ευφυούς δικτύου ενέργειας που τα συλλέγει. Το πρόβλημα όμως που δημιουργείται είναι ότι απαιτείται η χρήση μιας τρίτης πιστοποιημένης αρχή, που θα συλλέγει τα high-frequency δεδομένα, το οποίο δημιουργεί νέα προβλήματα, εμπιστευτικότητας αλλά και προσβασιμότητας των δεδομένων αυτών. Μια διαφορετική ιδέα όπου δεν περιορίζεται από την εισαγωγή της τρίτης αυτής αρχής, βασίζεται στο data aggregation, δηλαδή στην συλλογή των δεδομένων από τους έξυπνους μετρητές σε αρχιτεκτονική mesh, ή στους συλλέκτες δεδομένων, για την μετατροπή του σε μια μορφή σύνοψης.

Το παραπάνω όμως δεν προστατεύει από παραβιάσεις της ιδιωτικότητας σε μεγάλο βαθμό, όποτε σε συνδυασμό με μια άλλη γνωστή τεχνική κρυπτογράφησης την ομομορφική κρυπτογράφηση, η οποία είναι ένα είδος κρυπτογράφησης όπου επιτρέπεται η διενέργεια, αλγεβρικών πράξεων, επάνω στα δεδομένα και μεταφέρονται στο Ciphertext. Το κρυπτογραφημένο αυτό αποτέλεσμα, όταν αποκρυπτογραφείται έχει τα ίδια αποτελέσματα με την εφαρμογή των ίδιων πράξεων πάνω στα δεδομένα. Η χρήση αυτού του είδους την κρυπτογράφησης σε συνδυασμό με το data aggregation έχει γνωρίζει σημαντική μελέτη για την εφαρμογή της, όμως απαιτεί περεταίρω εξέλιξη για την επίτευξη του μικρότερου δυνατού overhead και υπολογιστικού κόστους, μιας και οι έξυπνοι μετρητές απαιτείται να έχουν υπολογιστικές ικανότητες. Επίθεση που αποτελεί πρόκληση, και που μπορεί να πλήξει το παραπάνω σχήμα είναι η false data injection. Για την αντιμετώπιση απαιτείται η εξασφάλιση της φυσικής ασφάλειας, ώστε κάποιος κακόβολος να μην έχει πρόσβαση σε έξυπνο μετρητή, με σκοπό την παραβίαση της ακεραιότητας των δεδομένων. Συνεπώς η ακεραιότητα των δεδομένων στα παραπάνω σχήματα χρειάζεται να ληφθεί υπόψη κατά την σχεδίαση.

Παρατηρούμε, ότι ενώ έχουν γίνει σημαντικά βήματα για την προστασία των ευφυών δικτύων ενέργειας, υπάρχουν ακόμα σοβαρές κενά, μιας και οι υπάρχουσες τεχνικές ακόμη, δεν μπορούν να καλύψουν όλο το εύρος των ευπαθειών και των απειλών, ενώ ταυτόχρονα να διατηρούν της μεγάλες απαιτήσεις που έχουν τα ευφυή δίκτυα ενέργειας. Στο μέλλον, προκύπτει ότι η σχεδίαση τεχνικών αυθεντικοποίησης και ιδιωτικότητας θα γνωρίζει μεγάλη βελτίωση μέσα από δοκιμές και βελτιώσεις ήδη υπαρχόντων σχημάτων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

3gpp. (n.d.). *3gpp*. Ανάκτηση από 3rd Generation Partnership Project: http://www.3gpp.org/LTE

A. Moise, J. B. (2011). *ANSI C12.22, IEEE 1703, and MC12.22 Transport Over IP.* Internet Engineering Task Force.

Ahmad Usman, S. H. (2013). Evolution of Communication Technologies for Smart Grid applications. *Renewable and Sustainable Energy Reviews* , 191-199.

Ahmed ElShafee, K. A. (2012). *Design and Implementation of a WiFi based Home Automation System.* World Academy of Science, Engineering and Technology 68 2012.

Alcides Ortega, A. A. (2013). Performance analysis of smart grid communication protocol DNP3 over TCP/IP in a heterogeneous traffic environment. *Communications and Computing* (σσ. 1 - 6). Medellin: IEEE.

Aldar C-F. Chan, J. Z. (2013). On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628. *Communications Magazine* , 58 - 65.

Alliance, H. P. (2012). *HomePlug Green PHY 1.1.* HomePlug Powerline Alliance.

Alliance, H. P. (2012). *HomePlug Green PHY 1.1, The Standard for In-Home Smart Grid Powerline Communications: An application and technology overview.* HomePlug Powerline Alliance.

Alliance, W.-F. (2010). *Wi-Fi for the Smart Grid: Mature, Interoperable, Secure Technology for Advanced Smart Energy Management Communications.* Wi-Fi Alliance.

Alliance, Z. (2010). *ZigBee specification, document 053474r17.*

Alvaro A. Cárdenas, R. B. (2014). A Framework for Evaluating Intrusion Detection Architectures in Advanced Metering Infrastructures. *IEEE Transactions on Smart Grid (TSG)* , 906 - 915.

Arabyat, E. A. (2013). Candidate solutions to improve Wireless Mesh Networks WMNs performance to meet the needs of Smart Grid applications - Survey paper. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.3, No.4* , 1-9.

Arjun Athreya, P. T. (2012). Survivable Smart Grid Communication: Smart-Meters Meshes to the Rescue. *1st International Workshop on Communication Technologies Support for the Smart Grid (SGCom).* Cape Town, South Africa: IEEE.

B.E. Bilgin, V. G. (2012). Performance evaluations of ZigBee in different smart grid environments. *Elsevier Computer Networks 56* , 2196-2205.

Bacchillone, S. S. (2012). Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid. *Computer Networks and Communications* , 1-20.

Beigi-Mohammadi, H. K. (2012). On intrusion detection in a neighbourhood area network in the smart grid. *Information Technology & Applications vol. 2 Issue 1* , 7-13.

Bernhard Baumgartner, C. R. (2013). *IEEE 1588/PTP: The Future of Time Synchronization in the Electric Power Industry.* OMICRON electronics GmbH.

Board, I.-S. S. (2012). *1377-2012 - IEEE Standard for Utility Industry Metering Communication Protocol Application Layer (End Device Data Tables).* IEEE.

Board, I.-S. S. (2012). *1703-2012 - IEEE Standard for Local Area Network/Wide Area Network (LAN/WAN) Node Communication Protocol to Complement the Utility Industry End Device Data Tables.* IEEE.

Byrne, D. (2013). *WiGRID – A Wireless Broadband Solution for Utilities.* WiMAX forum.

Carl H. Hauser, D. E. (2012). Evaluating Multicast Message Authentication Protocols for Use in Wide Area Power Grid Data Delivery Services. *45th Hawaii International Conference on System Science (HICSS)* (σσ. 2151 - 2158). Maui, HI: IEEE.

Christian Muller, M. P. (2012). Traffic Engineering Analysis of Smart Grid Services in Cellular Networks. *IEEE International Conference on Smart Grid Communication (SmartGridComm)* (σσ. 1-6). Tainan City, Taiwan: IEEE.

Christian Müller, S. S. (2010). RF Mesh Systems for Smart Metering: System Architecture and Performance. *Smart Grid Communications (SmartGridComm),* (σσ. 379 - 384). Gaithersburg, MD : IEEE.

Commission, I. E. (n.d.). *International Electrotechnical Commission*. Ανάκτηση April 15, 2014, από http://www.iec.ch/smartgrid/background/explained.htm

Costas Efthymiou, G. K. (2010). Smart Grid Privacy via Anonymization of Smart Metering Data. *Smart Grid Communications* (σσ. 238 - 243). Gaithersburg, MD : IEEE.

Craig Valli, A. W. (2013). Eavesdropping on the Smart Grid. *10th Austalian Digital Forensics Conference* (σσ. 54-59). 10th Austalian Digital Forensics Conference.

D. Meyer, F. B. (2011). *RFC 6272 - Internet Protocols for the Smart Grid.* Internet Engineering Task Force.

Daojing He, C. C. (2012, August). Secure Service Provision in Smart Grid Communications. *IEEE Communications Magazine* , σσ. 53-61.

David Famolari, Y. O. (2012). A key management framework for AMI networks in smart grid. *Communications Magazine* , 30 - 37.

David Grochocki, J. H. (2012). AMI threats, intrusion detection requirements and deployment recommendations . *Smart Grid Communications (SmartGridComm)* (σσ. 395 - 400). IEEE.

Dong Wei, Y. L. (2010). An integrated security system of protecting Smart Grid against cyber attacks. *Innovative Smart Grid Technologies (ISGT)* (σσ. 1 - 7). Gaithersburg, MD: IEEE.

Dong Wei, Y. L. (2011). Protecting Smart Grid Automation Systems Against Cyberattacks. *IEEE TRANSACTIONS ON SMART GRID* , 782 - 795.

Donghyun Choi, S. L. (2010). Efficient Secure Group Communications for SCADA. *IEEE Transactions on Power Delivery (Volume:25 , Issue: 2)* , 714 - 722.

Emiliano Pallotti, F. M. (2011). Smart grid cyber security requirements . *Environment and Electrical Engineering (EEEIC)* (σσ. 1-4). Rome : IEEE.

Emilio Ancillotti, R. B. (2013). The Role of Communication Systems in Smart Grids: Architectures, Technical. *Computer Communications* , 1-40.

Ericsson. (n.d.). *Ericsson*. Ανάκτηση από Ausgrid, Australia: Smart grid network to use LTE: http://www.ericsson.com/article/ausgrid_1595655399_c

Erman Ayday, S. R. (2011). Secure, intuitive and low-cost device authentication for Smart Grid networks. *Consumer Communications and Networking Conference* (σσ. 1161 - 1165). Las Vegas, NV: IEEE.

Eugene Crozier, A. K. *WiMAX's technology for LOS and NLOS environments.* WiMAX Forum.

Eun-Kyu Lee, M. G. (2012, August). Physical Layer Security in Wireless Smart Grid. *IEEE Communications Magazine* , σσ. 46-52.

Eun-Kyu Lee, M. G. (2012, August). Physical Layer Security in Wireless Smart Grid. *IEEE Communications Magazine* , σσ. 46-52.

Fahad Khan, S. B. (2012). An Overview of OFDM Based Narrowband and Power Line Communication Standards for Smart Grid Applications. *World Applied Sciences Journal 20* , 1236-1242.

Fangming Zhao, Y. H. (2012). Secure authenticated key exchange with revocation for smart grid. *Innovative Smart Grid Technologies (ISGT)* (σσ. 1 - 8). Washington, DC: IEEE.

Felipe Gómez-Cuba, R. A.-C.-C. (2012). WiMAX for smart grid last-mile communications: TOS traffic mapping and performance assessment. *Innovative Smart Grid Technologies* (σσ. 1-8). Berlin: IEEE.

Fengjun Li, B. L. (2012). Preserving data integrity for smart grid data aggregation. *Smart Grid Communications* (σσ. 366 - 371). Tainan: IEEE.

Fengjun Li, B. L. (2010). Secure Information Aggregation for Smart Grids Using Homomorphic Encryption. *Smart Grid Communications* (σσ. 327 - 332). Gaithersburg, MD: IEEE.

Feuerhahn S, Z. M. (2011). Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications. *International Conference on Smart Grid Communications(SmartGridComm)* (σσ. 410 - 415). Brussels : IEEE.

Forum, W. (2013). *WiMAX FORUM System Profile Requirements for Smart Grid Applications, Requirements for WiGRID.* WiMAX Forum.

Forum, W. (2006). *WiMAX Part I: A technical over view and performance evaluation.*

Galli S, S. A. (2011). For the Grid and Through the Grid: The Role of Power Line Communications in the Smart Grid . *Proceedings of the IEEE (Volume:99 , Issue: 6)* (σσ. 998 - 1027). IEEE.

Gharbaoui M, V. L. (2012). Effective management of a public charging infrastructure through a smart management system for electric vehicles. *Energy Conference and Exhibition (ENERGYCON), 2012 IEEE International* (σσ. 1095 - 1100). Florence : IEEE.

(2011). Smart Meter Security Management. Στο M. C. Gilbert N. Sorebo, *Smart Grid Security: An End-to-End View of Security in the New Electrical Grid.* CRC Press.

Gordan Štruklec, J. M. (2011). Implementing DLMS/COSEM in smart meters. *Energy Market* (σσ. 747 - 752). Zagreb: IEEE.

Grids, E. C. (2010). *Functionalities of smart grids and smart meters.* EU Commission.

Group, h. S.–C. (2010). *Guidelines for smart grid cyber security, NISTIR 7628.* NIST.

Group, P. A. (2012). *Draft Specification for PowerLine Intelligent Metering Evolution.* Prime Alliance.

Group, P. W. (n.d.). *IEEE Standards Assosation*. Ανάκτηση 4 18, 2014, από http://standards.ieee.org/develop/project/1909.1.html

Group, S. G. (2010). *IEC Smart Grid Standardization Roadmap.* IEC.

Hamid Gharavi, B. H. (2011). Multigate Communication Network for Smart Grid . *Proceedings of the IEEE volume 99, number 6* (σσ. 1028 - 1045). IEEE.

Hamid Gharavi, B. H. (2011). Multigate Mesh Routing for Smart Grid Last Mile. *IEEE Wireless Communications & Networking Conference* (σσ. 275-280). Cancun, Mexico: IEEE.

Hasen Nicanfar, P. J. (2012). Efficient authentication and key management for the Home Area Network. *Communication and Information Systems Security Symposium* (σσ. 878 - 882). Ottawa, ON: IEEE.

Hasen Nicanfar, P. J. (2011). Smart grid authentication and key management for unicast and multicast communications. *Innovative Smart Grid Technologies Asia* (σσ. 1 - 8). Perth, WA: IEEE.

Hayden K.-H. So, S. H.-S. (2010). Zero-Configuration Identity-Based Signcryption Scheme for Smart Grid. *Smart Grid Communications* (σσ. 321 - 326). Gaithersburg, MD: IEEE.

Himanshu Khurana, R. B. (2010). Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols. *System Sciences* (σσ. 1 - 10). Honolulu, HI: IEEE.

Hoi Yan Tung, K. F. (2012). A WiFi-ZigBee Building Area Network Design of High Traffics AMI for Smart Grid. *Smart Grid and Renewable Energy* , 324-333.

Home, G. 2. (n.d.). *Grid2Home*. Ανάκτηση April 15, 2014, από Grid2Home: http://www.grid2home.com/Smartgrid.html

Hrasnica Halid, H. A. (2004). *Broadband Powerline Communications: Network Design.* Wiley.

IEEE. (2011). *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads.* IEEE Std 2030-2011.

IEEE. (n.d.). *IEEE Smart Grid* . Ανάκτηση April 15, 2014, από IEEE & Smart Grid : http://smartgrid.ieee.org/ieee-smart-grid

Institute, A. N. (2008). *ANSI C12.22 Draft.* American National Standards Institute.

Instute, A. N. (2008). *ANCI C12.19 Draft.* American National Stantards Instute.

Integrated, M. *PLC G3 PROFILE SPECIFICATION.* Maxim Integrated.

ITU, T. S. (2011). *Unified high-speed wireline-based home networking transceivers – System architecture and physical layer specification, Recommendation ITU-T G.9960.* ITU.

ITU, T. S. (2011). *Unified high-speed wireline-based home networking transceivers – System architecture and physical layer specification, Recommendation ITU-T G.9960.* ITU.

James Weimer, Y. X. (2012). A Virtual Laboratory for Micro-Grid information and communication infrastructures. *Innovative Smart Grid Technologies (ISGT Europe)* (σσ. 1 - 6). Berlin : IEEE.

Jason Brown, J. Y. (2012). Key performance aspects of an LTE FDD based Smart Grid communications network. *Computer Communications* , 551-561.

Jason Brown, J. Y. (2012). Performance analysis of an LTE TDD based smart grid communications network for uplink biased traffic. *Globecom Workshops* (σσ. 1502 - 1507). Anaheim, CA: IEEE.

Jason Brown, J. Y. (2012). Performance comparison of LTE FDD and TDD based Smart Grid communications networks for uplink biased traffic. *Smart Grid Communications* (σσ. 276 - 281). Tainan: IEEE.

Jean Vigneron, K. R. (2012). *G3-PLC Powerline Communication Standard for Today's Smart Grid.* G3-PLC Alliance.

Jeff Drake, D. N. (2010). *Energy Efficiency Comparisons of Wireless Communication Technology Options for Smart Grid Enabled Devices.* General Electric Company.

Jennic. (2009). *An Introduction to Smart Energy.* United Kingdom: Jennic.

Jie Lin, W. Y. (2012). On False Data Injection Attacks against Distributed Energy Routing in Smart Grid . *Cyber-Physical Systems (ICCPS)* (σσ. 183 - 192). Beijing : IEEE.

Jim LeClare, A. N. (2012). *How a standard is born: IEEE P1901.2 for narrowband OFDM PLC.* Maxim Integrated.

Jin Zhang, V. O. (2011). G.HNEM: the new ITU-T standard on narrowband PLC technology. *Communications Magazine* , 36 - 44.

Joseph Kamto, L. Q. (2012). Key Distribution and management for power aggregation and accountability in Advance Metering Infrastructure. *Smart Grid Communications* (σσ. 360 - 365). Tainan: IEEE.

K. E Martin, D. H. (2008). Exploring the IEEE Standard C37.118–2005 Synchrophasors for Power Systems. *Power Delivery* , 1805-1811.

Kalkunte, V. (2010). *Role of WiFi / IEEE 802.11n & Related Protocols in Smart Grid .* IEEE ComSoc.

Laboratories, N. (2013). *ZigBee PRO Smart Energy API.* UK.

Lars Torsten Berger, A. S.-G. (2013). Power Line Communications for Smart Grid Applications. *Hindawi Journal of Electrical and Computer Engineering* , 1-17.

Leccese, F. (2012). An overwiev on IEEE Std 2030. *Environment and Electrical Engineering* (σσ. 340 - 345). Venice: IEEE.

Lee P, L. L. (2007). A practical approach to wireless GPRS on-line power quality. *Power engineering society general meeting* , 1-7.

Leon, G. (2011). *Smart Planning for Smart Grid AMI Mesh Networks.* Eugene, Oregon, USA: EDX Wireless.

Liu Jianming, W. J. (2011). Application of PFTTH in smart grid. *Advanced Communication Technology* (σσ. 389 - 392). Seoul: IEEE.

Liu Jianming, Z. B. (2011). The smart grid multi-utility services platform based on power fiber to the home. *Cloud Computing and Intelligence Systems* (σσ. 17 - 22). Beijing: IEEE.

Luan S, T. J. (2010). Development of an Automatic Reliability Calculation System for Advanced Metering Infrastructure. *Eighth IEEE international conference on Industrial informatics (INDIN)* (σσ. 342-347). IEEE.

Management, I. S. (2012). *IEEE Standard for Local Area Network/Wide Area Network (LAN/WAN) Node Communication Protocol to Complement the Utility Industry End Device Data Tables, IEEE 1703-2012.* IEEE.

Management, I. S. (2012). *IEEE Standard for Utility Industry Metering Communication Protocol Application Layer (End Device Data Tables), IEEE 1377-2012.* IEEE.

Manisa Pipattanasomporn, M. K. (2014). Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks* , 1-15.

McCain, D. (n.d.). *www.ecnmag.com*. Ανάκτηση 2013, από www.ecnmag.com: http://www.ecnmag.com/articles/2011/05/enabling-zigbee%E2%80%99s-smart-energy-20-advanced-wireless-modules

Mohamad Badra, S. Z. (2013). Key management solutions in the smart grid environment. *Wireless and Mobile Networking Conference* (σσ. 1-7). Dubai: IEEE.

Moise A, B. J. (2011). *ANSI C12.22, IEEE 1703, and MC12.22 Transport Over IP (RFC 6142).* Internet Engineering Task Force (IETF).

Nico Saputro, K. A. (2012). A survey of routing protocols for smart grid communications. *Elsevier Computer Networks* , 2742-2771.

NIST. (2012). *Framework and Roadmap for Smart Grid Interoperability Standards 2.0.* National Institute of Standards and Technology.

Palak P. Parikh, M. G. (2010). Opportunities and Challenges of Wireless Communication Technologies for Smart Grid Applications. *Power and Energy Society General Meeting* (σσ. 1-7). Minneapolis, MN: IEEE.

Pan Deng, L. Y. (2012). A secure and privacy-preserving communication scheme for Advanced Metering Infrastructure. *Innovative Smart Grid Technologies* (σσ. 1 - 5). Washington, DC: IEEE.

Paolin, M. (2010). *Empowering the smart grid with WiMAX.* Senza Fili, WiMAX Forum.

paper, E. W. (September 2013). *Lte for Utilities.* Ericsson.

Paria Jokar, H. N. (2011). Specification-based Intrusion Detection for Home Area Networks in Smart Grids. *Smart Grid Communications* (σσ. 208 - 213). Brussels: IEEE.

Philip Huu Huynh, C. E. (2013). Design and Analysis of Hybrid Wireless Mesh Networks for Smart Grids. *Advances in Intelligent Systems and Applications - Volume 1* , 713-721.

Piyush Ghune, R. N. (2013). Application of Wireless Sensor Networks in Smart Grid Opportunities, Challenges & Technologies Available (A Survey). *International Journal on Advanced Computer Theory and Engineering* , 11-18.

Project, P. (2008). *Draft Specification for Powerline Intelligent Metering Evolution.* PRIME.

Project, P. (2008). *Prime PHY, MAC and Convergence layers.* Prime.

Punith K. Neelam, A. P. *Best Anti Jamming Solution for Home Area networks.* Wichita, Kansas: Department of Electrical Engineering and Computer Science, Wichita State University.

Qing Wang, Y. L. (2012). A hybrid wireless system for power line monitoring. *Innovative Smart Grid Technologies - Asia* (σσ. 1 - 6). Tianjin: IEEE.

Qinghua Li, G. C. (2011). Multicast Authentication in the Smart Grid With One-Time Signature. *IEEE Transactions on Smart Grid VOL. 2, NO. 4* , 686 - 696.

Qiyan Wang, H. K. (2009). Time Valid One-Time Signature for Time-Critical Multicast Data Authentication. *INFOCOM* (σσ. 1233 - 1241). Rio de Janeiro: IEEE.

Qualcomm. (2012). *3G Cellular Technology for Smart Grid Communications.* Qualcomm.

Rahman M.M, C. S. (2011, June 6). Medium Access Control for Power Line Communications: An Overview of the IEEE 1901 and ITU-T G.hn Standards. *Communications Magazine, IEEE (Volume:49 , Issue: 6)* , σσ. 183 - 191.

Reduan H. Khan, J. Y. (2013). A comprehensive review of the application characteristics and traffic. *Computer Networks 57* , 825-845.

Reduan H. Khan, J. Y. (2012). Wide area PMU communication over a WiMAX network in the smart grid. *Smart Grid Communications* (σσ. 187-192). Tainan: IEEE.

Robin Berthier, W. H. (2011). Specification-Based Intrusion Detection for Advanced Metering Infrastructures. *Pacific Rim International Symposium on Dependable Computing* (σσ. 184 - 193). Pasadena, CA : IEEE.

Robin Berthier, W. S. (2010). Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions. *Smart Grid Communications (SmartGridComm)* (σσ. 350 - 355). Gaithersburg, MD: IEEE.

Ronald Mao, V. J. (2012). WiMAX for advanced metering infrastructure. *Green and Ubiquitous Technology* (σσ. 15 - 19). Jakarta: IEEE.

Rossello-Busquet, A. (2012). G.hnem for AMI and DR . *Computing, Networking and Communications (ICNC)* (σσ. 111-115). Maui, HI : IEEE.

Rossi, M. *Communication Technologies and Architectures for Smart Grids.*

Sangji Lee, J. B. (2014). A security mechanism of Smart Grid AMI network through smart device mutual authentication. *Information Networking* (σσ. 592 - 595). Phuket: IEEE.

Sanz, A. (2010). *Analysis of standards for Low frequency narrow band power line communication for smart grid applications, For P1901.2.* Nanterre, France: IEEE.

Serbulent Tozlu, M. S. (2012, June). Wi-Fi Enabled Sensors for Internet of Things: A Practical Approach. *IEEE Communications Magazine* , σσ. 134-143.

Seung-Hyun Seo, X. D. (2013). Encryption key management for secure communication in smart advanced metering infrastructures. *Smart Grid Communications* (σσ. 498 - 503). Vancouver, BC: IEEE.

Shehla Rana, H. Z. (2012). The Not-So-Smart Grid: Preliminary work on identifying vulnerabilities in ANSI C12.22. *Globecom Workshops (GC Wkshps)* (σσ. 1514 - 1519). Anaheim, CA: IEEE.

Snyder A.F, S. M. (2007). The ANSI C12 protocol suite - updated and now with network capabilities. *Power Systems Conference: Advanced Metering, Protection, Control, Communication and Distributed Resources* (σσ. 117 - 122). Clemson, SC : IEEE.

Society, I. C. (2013). *1901.2-2013 - IEEE Standtard for Low-Frequency(less than 500kHz) Narrowband Power Line Communications for Smart Grid Applications.* IEEE.

Society, I. C. (2013). *2030.5-2013 - IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard.* IEEE.

Society, I. P. (2010). *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3), IEEE 1815.* IEEE.

Society, I. P. (2013). *1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities.* IEEE.

Soohyun Oh, J. K. (2012). Mutual Authentication and Key establishment mechanism. *Applied Mathematics & Information Sciences* , 257-564.

Sophia Kaplantzis, Y. A. (2012). Security and smart metering . *European Wireless* (σσ. 1-8). Poznan, Poland : IEEE.

Sörries, B. (2013). *Communication technology and networks for Smart Grid and Smart Metering.* CDG 450 Connectivity Special Interest Group(450 SIG).

Stefan Feuerhahn, M. Z. (2011). Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications. *Smart Grid Communications* (σσ. 410 - 415). Brussels: IEEE.

Stefano Galli, V. O. (2009). G.hn: The new ITU-T home networking standard. *Communications Magazine* , 138 - 145.

Su, D. (2013). *Guideline for the Implementation of Coexistence for Low Frequency Narrowband Power Line Communication Standards.* NIST.

Tadashige Iwao, K. Y. (2010). Dynamic Data Forwarding in Wireless Mesh. *Smart Grid Communications (SmartGridComm)* (σσ. 385-390). Gaithersburg, Meryland: IEEE.

Tadashige Iwao, K. Y. (2010). Dynamic Data Forwarding in Wireless Mesh Networks. *Smart Grid Communications (SmartGridComm)* (σσ. 385 - 390). Gaithersburg, MD : IEEE.

Technology, N. I. (2009). *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0.*

Technology, N. I. (2009). *NIST PAP 01-The Role of IP in the Smart Grid.* NIST.

tutorialspoint.com. (n.d.). *tutorialspoint.com*. Ανάκτηση από http://www.tutorialspoint.com/WiMAX/WiMAX_technology.htm

Upeka Kanchana Premaratne, J. S.-C. (2010). An Intrusion Detection System for IEC61850 Automated Substations. *IEEE TRANSACTIONS ON POWER DELIVERY* , 2376-2383.

V. Cagri Gungor, D. S. (2012). A Survey on Smart Grid Potential Applications and Communication Requirements. *IEEE Transactions on Industrial Informatics vol. 9, no. 1* , 28-42.

V.C. Gungor, F. L. (2006). A survey on communication networks for electric system automation. *Computer Networks* , 877-897.

V.K. Sood, D. F. (2009). Developing a Communication Infrastructure for the Smart Grid. *Electrical Power & Energy Conference (EPEC), 2009 IEEE* , 1-7.

Vinod Namboodiri, V. A. (2013). Towards a Secure, Wireless-Based, Home Area Network for Metering in Smart Grids. *Systems Journal, IEEE (Volume:PP , Issue: 99)* , 1 - 12.

Visvakumar Aravinthan, V. N. (2011). Wireless AMI application and security for controlled home area networks. *Power and Energy Society General Meeting* (σσ. 1 - 8). San Diego, CA: IEEE.

Wasi-ur-Rahman, M. T. (2009). Design of an Intelligent SMS based Remote Metering System. *International Conference on Information and Automation* (σσ. 1040-1043). Zhuhai/Macau, China: IEEE.

WEI Yong, X. W.-g.-l.-h. (2012). Application Analysis on EPON Technology Applied in Communication System of Smart Substation. *Information Engineering and Applications* , 163-169.

Weixiao Meng, R. M.-H. (2014). Smart grid neighborhood area networks: a survey. *IEEE Network* , 24 - 32.

Wenye Wang, Y. X. (2011). A survey on the communication architectures in smart grid. *Computer Networks 55* , 3604–3629.

Wenye Wang, Z. L. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks 57* , 1344–1371.

Xi Fang, D. Y. (2011). *Wireless Communication and Networking Technologies for Smart Grid: Paradigms and Challenges.* eprint arXiv:1112.1158.

Xie Shu-Hong, Z. J.-M.-J.-S. (2011). Study of the Power Fiber to the Home Technologies Based on the OPLC Cable. *Proceedings of the 60th IWCS Conference* (σσ. 315-319). Nantong, Jiangsu Province, PR China: International Wire & Cable Symposium.

Xu Li, I. L. (2012). Securing smart grid: cyber attacks, countermeasures, and challenges. *Communications Magazine* , 38 - 45.

Y. Yang, S. S. (2014). Multiattribute SCADA-Specific Intrusion Detection System for Power Networks . *IEEE TRANSACTIONS ON POWER DELIVERY* , 1-11.

Yacine Challal, H. B. (2004). A taxonomy of multicast data origin authentication: Issues and solutions. *Communications Surveys & Tutorials* , 34 - 57 .

Ye Yan, Y. Q. (2012). A Survey on Cyber Security for Smart Grid Communications. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS* , 1-13.

Ye Yan, Y. Q. (FIRST QUARTER 2013). A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS ,VOL. 15, NO. 1* , 5-20.

Yee Wei Law, M. P. (2013). WAKE: Key management scheme for wide-area measurement systems in smart grid. *IEEE Communications Magazine (Volume:51 , Issue: 1)* , 34 - 41.

Yilin Mo, T. H.-J. (2012). Cyber–Physical Security of a Smart Grid Infrastructure . *Proceedings of the IEEE Volume 100* (σσ. 195-209). IEEE.

Zach Yordy, H. Z. *Using SANs to Model DDoS Attacks in Simple AMI Networks.* Illinois: University of Illinois.

Zahedi, A. (2011). Developing a system model for future smart grid. *Innovative Smart Grid Technologies Asia* (σσ. 1 - 5). Perth, WA: IEEE.

Zhong Fan, P. K. (2013). Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities. *IEEE Communications Surveys & Tutorials* , 21 - 38.

Zhuo Lu, X. L. (2010). Review and evaluation of security threats on the communication networks in the smart grid . *MILITARY COMMUNICATIONS CONFERENCE* (σσ. 1830 - 1835). San Jose, CA : IEEE.

Zyren, J. (2011). he HomePlug Green PHY specification & the in-home Smart Grid. *Consumer Electronics (ICCE)* (σσ. 241 - 242). Las Vegas, NV: IEEE.