ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΜΣ στην Επιστήμη και την Τεχνολογία Υπολογιστών

Smart grid security

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ηλίας Φάκλαρης

Επιβλέπων : Νικόλαος Κολοκοτρώνης

Μάρτιος 2016

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον κύριο Νικόλαο Κολοκοτρώνη, για την ανάθεση αυτής της διπλωματικής εργασίας, για το χρόνο του που διέθεσε για μένα, το ενδιαφέρον, την πολύτιμη βοήθεια και την καθοδήγησή του κατά τη διάρκεια εκπόνησης της διπλωματικής εργασίας. Τέλος, θα ήθελα να ευχαριστήσω ιδιαίτερα την οικογένειά μου και τους φίλους μου για την ενθάρρυνση, τη συμπαράσταση και τη στήριξή τους κατά τη διάρκεια όλων αυτών των χρόνων.

ΗΛΙΑΣ ΦΑΚΛΑΡΗΣ

ΜΑΡΤΙΟΣ 2016

ΠΕΡΙΛΗΨΗ

Το έξυπνο δίκτυο επιχειρεί να εκσυγχρονίσει το υπάρχον απαρχαιωμένο σύστημα δικτύου ηλεκτρικής ενέργειας. Τα ευεργετικά χαρακτηριστικά του έξυπνου δικτύου, κύριος εκφραστής των οποίων αποτελεί ο έξυπνος μετρητής, συμβάλλουν στη βέλτιστη αξιοποίηση ηλεκτρικής ενέργειας τόσο στην πλευρά της παραγωγής όσο και στην πλευρά της κατανάλωσης. Εισάγοντας τις νέες τεχνολογίες επικοινωνιών και πληροφορικής σε καίρια σημεία του δικτύου, επιτυγχάνεται η ενσωμάτωση ανανεώσιμων πηγών ενέργειας καθώς και η ενεργητικότητα των καταναλωτών στο σενάριο λειτουργίας του έξυπνου πλέγματος.
Ωστόσο, η ενσωμάτωση των νέων τεχνολογιών, ειδικά αυτών που σχετίζονται με το Διαδίκτυο, ίσως εισάγουν νέες απειλές για την ασφάλεια του έξυπνου πλέγματος. Ορισμένοι κακοπροαίρετοι επιτιθέμενοι μπορούν να εκμεταλλευτούν τα ευάλωτα σημεία του δικτύου επικοινωνιών και να καταλάβουν ηλεκτρονικές συσκευές, να υποκλέψουν απόρρητες ή προσωπικές πληροφορίες, να απαγορεύσουν τη διαθεσιμότητα απαραίτητων υπηρεσιών και να προκαλέσουν μια εκτεταμένη διακοπή ρεύματος, με συνέπεια ένα δυσμενές οικονομικό κόστος.
Για αυτό το λόγο, η αντιμετώπιση των ζητημάτων ασφάλειας στο έξυπνο δίκτυο παίζει πρωταρχικό ρόλο. Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των διακινούμενων πληροφοριών είναι ανάγκη να προστατευθούν, έτσι ώστε να αυξηθεί η αξιοπιστία του συστήματος.

Επιπλέον, οι συνεργατικές ασύρματες επικοινωνίες στο έξυπνο δίκτυο έχουν τη δυνατότητα να συνεισφέρουν στην αποδοτικότερη αξιοποίηση της διαθέσιμης ενέργειας των συνεργαζόμενων κόμβων, αυξάνοντας με αυτό τον τρόπο την ποιότητα μετάδοσης υπηρεσιών. Εκμεταλλευόμενο τα πλεονεκτήματα συνεργασίας, το έξυπνο δίκτυο μέτρησης, αποτελούμενο από χωρικά διασκορπισμένους έξυπνους μετρητές, κρυπτογραφεί τα προσωπικά δεδομένα μέτρησης και τα μεταφέρει αποτελεσματικά στο κέντρο ελέγχου αποφεύγοντας συγκρούσεις και προβλήματα δρομολόγησης.

Λέξεις κλειδία: Έξυπνο δίκτυο, Έξυπνοι μετρητές, Διαδικτυακές επιθέσεις, ασφάλεια, προστασία προσωπικών δεδομένων, κρυπτογραφία

ABSTRACT

The smart grid is attempting to modernize the existing antiquated electricity grid system. The beneficial features of the smart grid, whose main representative is the smart meter, contribute to the optimal use of electricity in both the production side and consumption side. Introducing the new communications and information technologies at key points in the network achieved the integration of renewable energy and the energy consumer in the scenario of operation of the smart grid.
However, integration of new technologies, especially those related to the Internet, may introduce new security threats to the smart grid. Some malicious attackers can exploit the vulnerabilities of network communications and seize electronic devices, steal confidential personal information or to prohibit the availability of essential services, causing a widespread power outage, resulting in adverse economic costs.
For this reason, addressing safety issues in smart grid plays a key role. The confidentiality, integrity and availability of mobile information need to be protected so as to increase system reliability.

In addition, cooperative wireless communications in smart grid has the potential to contribute to more efficient utilization of the available energy of cooperating nodes, increasing thereby the quality of transmission services. By leveraging the advantages of cooperation, the smart metering network, which consists of spatially dispersed smart meters, encrypts personal data measurement and effectively transmit them to the control center to avoid conflicts and routing problems.

Keywords: Smart grid, Smart meters, Cyber Attacks, security, privacy, cryptography

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

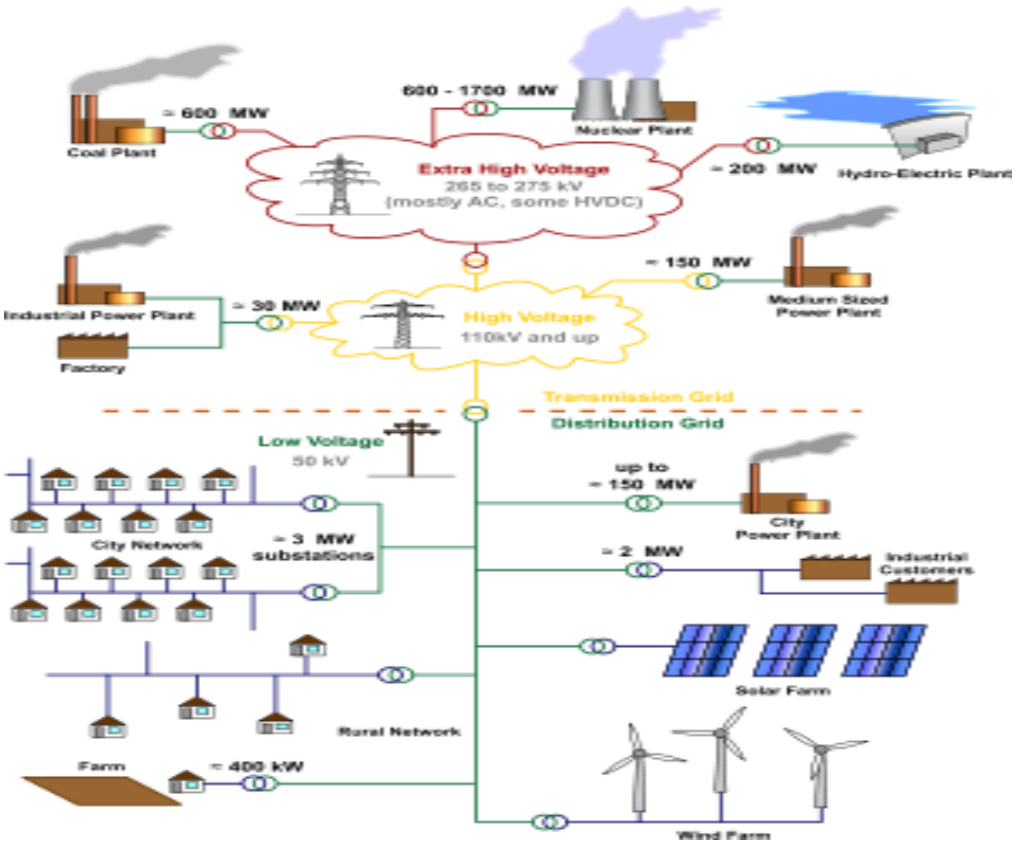
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
DES	Data Encryption Standard
DNP	Distributed Network Protocol
DOE	Department of Energy
DoS	Denial of Service
FAN	Field Area Network
HAN	Home Area Network
HMAC	Keyed Hash Message Authentication Code
HMI	Human Machine Interface
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
LAN	Local Area Network
MDMS	Meter Data Management System
NARC	Non –Aggressive Challenge Response
NIST	National Institute of Standards and Technology
PKG	Private Key Generator
PKI	Public Key Infrastructure
PLC	Power Line Communication
RA	Registration Authority
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition System

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΠΑΡΑΔΟΣΙΑΚΟ ΔΙΚΤΥΟ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ

Στα σημερινά δίκτυα ηλεκτρικής ενέργειας η ενέργεια παράγεται από κεντρικούς σταθμούς ηλεκτρικής ενέργειας χρησιμοποιώντας ορυκτά καύσιμα (άνθρακα , φυσικό αέριο, βιομάζα) τον αέρα το νερό τα πυρηνικά καύσιμα και τον ήλιο και μεταφέρεται στους καταναλωτές μέσω τον δικτύων μεταφοράς και διανομής. Το σύστημα μεταφοράς διασυνδέει όλους τους μεγάλους σταθμούς παραγωγής καθώς και διαφορετικά συστήματα μεταξύ τους και μεταφέρει μεγάλα μεγέθη ισχύος σε μεγάλες αποστάσεις στους υποσταθμούς που βρίσκονται κοντά σε κατοικημένες περιοχές και αποτελεί την σπονδυλική στήλη του δικτύου. Το σύστημα διανομής διανέμει το ηλεκτρικό ρεύμα από τους υποσταθμούς προς τους τελικούς καταναλωτές όπως, βιομηχανικούς και αστικούς καταναλωτές λειτουργώντας σε μεσαία και χαμηλά επίπεδα τάσης (λιγότερο από 100KV).



Εικόνα 1.1 Παραδοσιακό δίκτυο ηλεκτρικής ενέργειας

1.1ΠΡΟΒΛΗΜΑΤΑ ΣΗΜΕΡΙΝΟΥ ΔΙΚΤΥΟΥ

Το σημερινό απαρχαιωμένο δίκτυο ηλεκτρικής ενέργειας χαρακτηρίζεται από λειτουργικές δυσκαμψίες οι οποίες σε ορισμένες περιπτώσεις φέρνουν σε κίνδυνο την προμήθεια ηλεκτρικής ενέργειας. Με το πέρασμα των χρόνων η βαθμιαία αύξηση της κατανάλωσης οδήγησε σε αύξηση της ζήτησης και σαν αποτέλεσμα και της παραγωγής. Έτσι το σύστημα αναγκάστηκε να λειτουργεί πιο κοντά στα όρια του λόγω οικονομικών και περιβαντολογικών περιορισμών και οι γραμμές μεταφοράς στη μέγιστη χωρητικότητα τους. Όταν ο εξοπλισμός τροφοδοσίας αναγκάζεται να μεταφέρει ρεύμα υπερβαίνοντας τις τιμές θερμικής αξιολόγησης γίνεται υπερθέρμανση και η μόνωση επιδεινώνεται ραγδαία. Αυτό οδηγεί σε μείωση της ζωής του εξοπλισμού και αυξάνεται η συχνότητα εμφάνισης βλαβών (blackout). Επίσης όταν σε μια εναέρια γραμμή περνά πάρα πολύ ρεύμα, ο αγωγός μικραίνει και η χαλάρωση της γραμμής αυξάνεται, με συνέπεια να μειώνεται η απόσταση από το έδαφος. Η μείωση της απόστασης της εναέριας γραμμής από το έδαφος έχει σημαντικές συνέπειες τόσο για την αύξηση του αριθμού των βλαβών όσο και για την αύξηση του κινδύνου για την δημόσια ασφάλεια.

Η δομή των επικοινωνιών που υπάρχει αυτή την στιγμή στο δίκτυο ηλεκτρικής ενέργειας σχεδιάστηκε για να ανταποκριθεί στις ανάγκες της βιομηχανίας που υπήρχαν πριν αρκετές δεκαετίες. Τα δίκτυα επικοινωνιών στα σημερινά δίκτυα ηλεκτρικής ενέργειας σχεδιάστηκαν για να υποστηρίζουν λειτουργίες ελέγχου και επικοινωνίες δεδομένων μεταξύ των κέντρων ελέγχου και των υποσταθμών. Τα συστήματα SCADA που χρησιμοποιούν έχουν την δυνατότητα να μετρούν τάση, θερμοκρασία καλωδίων, κατάσταση ασφαλειών και να εκτελούν εντολές να ανοίξουν η να κλείσουν ασφάλειες.

Η ραγδαία εξέλιξη της τεχνολογίας έρχεται σε αντιδιαστολή με το απαρχαιωμένο ηλεκτρικό δίκτυο που δεν μπορεί να υποστηρίξει τις τεράστιες δυνατότητες που μπορούν να μας δώσουν τεχνολογίες όπως οι προσωπικοί υπολογιστές, τα Microsoft Windows, τα πρωτόκολλα επικοινωνίας TCP/IP/Ethernet, οι οπτικές ίνες, η ασύρματη τεχνολογία, τα πρότυπα ZigBee, WIMAX, η ψηφιακή τεχνολογία και πολλές άλλες τεχνολογίες. Έτσι δημιούργησαν σκέψεις για αποτελεσματική εκμετάλλευση τους στον τομέα της ηλεκτρικής ισχύος.

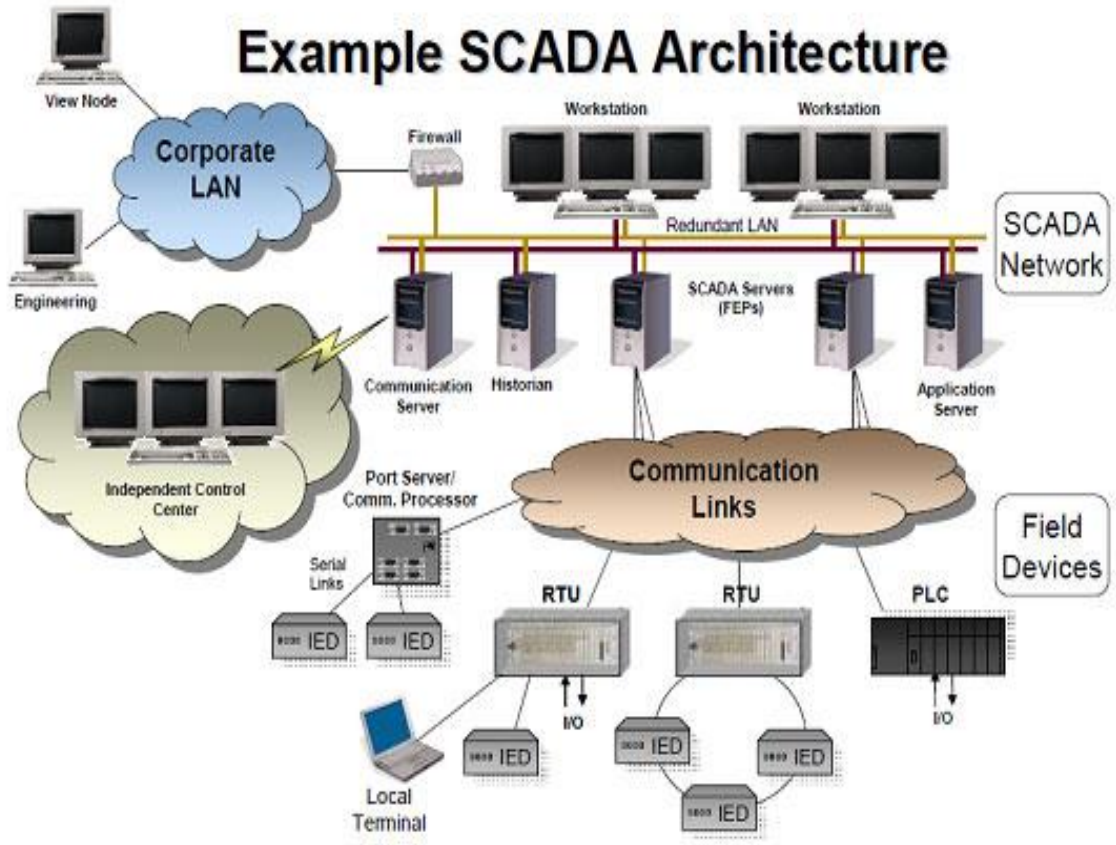
Ως εκ τούτου, το δίκτυο ηλεκτρικής ισχύος άρχισε να αντιμετωπίζει την τάση ενσωμάτωσης της υποδομής ηλεκτρικού ρεύματος με την υποδομή της πληροφορικής και των τηλεπικοινωνιών. Αυτή η αλλαγή θα μετέφερε το σύστημα ηλεκτρικής ισχύος από τις ξεπερασμένες και αποκλειστικές τεχνολογίες στη χρησιμοποίηση των κοινών σύγχρονων τηλεπικοινωνιών για ζεύξεις επικοινωνιών μεταξύ τους και στην αλλαγή του τρόπου παραγωγής, διαχείρισης και κατανάλωσης ηλεκτρικού ρεύματος.

1.2 ΣΥΣΤΗΜΑΤΑ SCADA

Τα συστήματα ελέγχου και συλλογής δεδομένων SCADA (supervisory control and data acquisition) είναι συστήματα που χρησιμοποιούνται για τον έλεγχο την παρακολούθηση και

τη μεταφορά δεδομένων από απόσταση. Είναι συνεπώς συστήματα τηλεμετρίας και τηλεχειρισμού τα οποία συλλέγουν πληροφορίες από διάφορες διεργασίες και χρησιμοποιούνται για τον εποπτικό έλεγχο.

Τα συστήματα SCADA βρίσκουν τεράστιες εφαρμογές τόσο σε βιομηχανικές μονάδες όσο και σε συστήματα μεταφοράς και διανομής ηλεκτρικής ενέργειας. Στο σημερινό δίκτυο ηλεκτρικής ενέργειας το δίκτυο επικοινωνίας υποστηρίζει μόνο ενέργειες και αλληλεπιδράσεις μεταξύ των κέντρων ελέγχου και των υποσταθμών. Τα μηνύματα που αποστέλλονται μεταξύ του κέντρου ελέγχου και των υποσταθμών είναι πληροφορίες σχετικά με την κατάσταση του ηλεκτρικού (τάσεις, ρεύματα, κατάσταση διακοπτών, θερμοκρασίες) είτε από εντολές οι οποίες αλλάζουν την διαμόρφωση του δικτύου όπως εντολές για να ανοίξει η για να κλείσει ένας διακόπτης.



Εικόνα 1.2 Αρχιτεκτονική συστήματος SCADA

Οι ενέργειες ενός συστήματος SCADA σε ένα δίκτυο ηλεκτρικής ενέργειας μπορούν να κατηγοριοποιηθούν ως εξής[9]:

- *Συλλογή δεδομένων* : Είναι πληροφορίες που περιγράφουν την κατάσταση του λειτουργικού συστήματος που συλλέγονται αυτόματα από

απομακρυσμένες τερματικές μονάδες (RTUs). Αυτό περιλαμβάνει την κατάσταση των συσκευών καθώς και συναγερμούς και τιμές μέτρησης

- *Παρακολούθηση, επεξεργασία συμβάντων και συναγερμών:*
  Μια σημαντική λειτουργία του SCADA είναι να συγκρίνει τα μετρούμενα δεδομένα με κανονικές τιμές και όρια, για παράδειγμα, να παρακολουθεί την υπερφόρτωση του εξοπλισμού (μετασχηματιστές και κυκλώματα τροφοδοσίας), καθώς και παραβιάσεις των ορίων τάσης. Επίσης ανιχνεύει την αλλαγή της κατάστασης του διακόπτη και της λειτουργίας των ρελέ προστασίας. Ένα συμβάν δημιουργείται εάν υπάρχει αλλαγή στην κατάσταση της διακοπής ή παραβίαση των ορίων του κυκλώματος. Όλα τα συμβάντα που δημιουργούνται από τη λειτουργία παρακολούθησης υποβάλλονται σε επεξεργασία από τη λειτουργία επεξεργασίας, η οποία κατατάσσει και χωρίζει σε ομάδες τα συμβάντα και παρέχει τις κατάλληλες πληροφορίες στους διαχειριστές του συστήματος μέσω της διεπαφής Ανθρώπου-Μηχανής (HMI). Πιο κρίσιμα συμβάντα θα αποσταλούν στους φορείς ως συναγερμοί, για παράδειγμα, με ηχητικά σήματα ή αναβοσβήνοντας χρώματα.

- *3. Έλεγχος:* Ο έλεγχος μέσω ενός συστήματος SCADA μπορεί να ξεκινήσει χειροκίνητα ή αυτόματα. Ο έλεγχος που ξεκινάει χειροκίνητα μπορεί να είναι ο άμεσος έλεγχος μιας συγκεκριμένης συσκευής (για παράδειγμα, ενός διακόπτη). Ορισμένες λειτουργίες ξεκινάνε χειροκίνητα από τον χειριστή θαλάμου ελέγχου, αλλά στη συνέχεια, ακολουθούν τη λογική τοπικού ελέγχου για να εξασφαλιστεί ότι ο εξοπλισμός λειτουργεί μετά από μια συγκεκριμένη ακολουθία ή εντός συγκεκριμένων ορίων. Ο έλεγχος που ξεκινάει αυτόματα ενεργοποιείται από ένα συμβάν ή σε μία συγκεκριμένη χρονική στιγμή.

- ***4***. Αποθ*ήκευση δεδομένων, αρχείο καταγραφής συμβάντων, ανάλυση και υποβολή εκθέσεων:*
  Οι μετρήσεις σε πραγματικό χρόνο αποθηκεύονται στη βάση δεδομένων σε πραγματικό χρόνο του συστήματος SCADA κατά το χρόνο που λήφθησαν. Επειδή η ενημέρωση των δεδομένων αντικαθιστά παλιές τιμές με νέες, τα σημασμένα ως προς τον χρόνο δεδομένα αποθηκεύονται στο ιστορικό της βάσης δεδομένων σε περιοδικά διαστήματα, για παράδειγμα, κάθε 5 λεπτά ή κάθε ώρα, για μελλοντική χρήση. Προκειμένου να αναλυθούν οι διαταραχές του συστήματος σωστά, είναι απαραίτητη μια ακριβής καταγραφή χρόνο-σημασμένων συμβάντων. Ορισμένα είδη εξοπλισμού (για παράδειγμα, RTUs) έχουν τη δυνατότητα εγγραφής γεγονότων με ακρίβεια χιλιοστού του δευτερολέπτου και, στη συνέχεια, την παράδοση χρονο-σημασμένων πληροφοριών στο σύστημα SCADA. Η αλληλουχία των συμβάντων που σχηματίζεται από τις χρονο-σημασμένες πληροφορίες, είναι χρήσιμη για το διαχειριστή του συστήματος για να αναλύσει ένα συμβάν για να καθοριστεί η αιτία για την εμφάνιση του.

ΚΕΦΑΛΑΙΟ 2

ΕΞΥΠΝΟ ΠΛΕΓΜΑ

Το έξυπνο ηλεκτρικό δίκτυο θεωρείται ως εκσυγχρονισμός του τωρινού ηλικιωμένου συστήματος ηλεκτρικής ισχύος που έχει σκοπό να δημιουργήσει ένα δίκτυο πιο στιβαρό πιο αποτελεσματικό και ευέλικτο καθώς επιτρέπει την πολλαπλών κατευθύνσεων (multi-directional) ροή ισχύος και ανταλλαγή πληροφοριών.

Ο όρος έξυπνο πλέγμα δεν έχει ένα ενιαίο σαφή ορισμό. Η χροιά που μπορεί να αποδοθεί από διαφορετικές οπτικές γωνιές και η ερμηνεία από τους ειδικούς των διάφορων πεδίων διαφέρει. Διαφορετικοί ορισμοί του Έξυπνου δικτύου περιλαμβάνουν[16]:

- Η Ευρωπαϊκή Πλατφόρμα Τεχνολογίας (European Technology Platform) το ορίζει ως:

Ένα Έξυπνο Πλέγμα είναι ένα ηλεκτρικό δίκτυο που μπορεί έξυπνα να ενοποιήσει τις δράσεις όλων των συνδεδεμένων σε αυτό χρηστών –παραγωγούς, καταναλωτές και αυτούς που κάνουν και τα δυο– με σκοπό την αποδοτική διανομή βιώσιμων, οικονομικών και ασφαλών ηλεκτρικών προμηθειών.

- Σύμφωνα με το Τμήμα Ενέργειας των ΗΠΑ:

Ένα Έξυπνο Πλέγμα χρησιμοποιεί την ψηφιακή τεχνολογία για να βελτιώσει την αξιοπιστία, την ασφάλεια και την αποδοτικότητα (τόσο την οικονομική όσο και την ενεργειακή) του συστήματος ηλεκτρικής ενέργειας –από τη μεγάλη παραγωγή, μέσω των συστημάτων μεταφοράς, έως τους καταναλωτές– και έναν αυξανόμενο αριθμό μέσων αποθήκευσης και κατανεμημένης παραγωγής.

- Σε άλλη αναφορά το Έξυπνο Πλέγμα ορίζεται:

Ένα Έξυπνο Πλέγμα χρησιμοποιεί αισθητήρες, ενσωματωμένη επεξεργασία και ψηφιακές επικοινωνίες για να καταστήσει το ηλεκτρικό δίκτυο παρατηρήσιμο (ικανό να υπολογιστεί και να απεικονιστεί), ελέγξιμο (διαχειρίσιμο και ικανό να βελτιστοποιηθεί), αυτοματοποιημένο (ικανό να προσαρμοστεί και να αυτό-θεραπευτεί), πλήρως διασυνδεδεμένο (πλήρως διαλειτουργικό με τα υπάρχοντα συστήματα και με την ικανότητα να ενσωματώσει ένα διαφορετικό σύνολο πηγών ενέργειας)[16].

2.1 Οφελη του εξυπνου πλεγματος

Το έξυπνο πλέγμα (Smart Grid) παρέχει πολλές χρήσιμες δυνατότητες τόσο στους καταναλωτές όσο και στις εταιρίες ηλεκτρικής ενέργειας. Το υπουργείο ενέργειας των ΗΠΑ (DOE Department of energy) περιγράφει σε άρθρο του ποια είναι τα βασικά οφέλη του έξυπνου δικτύου[17].

- *Η ενεργοποίηση της ενεργού συμμετοχής των καταναλωτών.*

Ένα πιο έξυπνο πλέγμα δημιουργείται με αυτόν τον τρόπο, δίνοντας στους καταναλωτές τη δυνατότητα να συμμετάσχουν και να επιλέξουν. Η αμφίδρομη επικοινωνία θα δημιουργήσει έναν διάλογο μεταξύ των επιχειρήσεων κοινής ωφέλειας και των καταναλωτών επιτρέποντας στους καταναλωτές να δουν τι ηλεκτρική ενέργεια χρησιμοποιούν, πότε τη χρησιμοποιούν, και πόσο κοστίζει. Για πρώτη φορά, πολλοί θα είναι σε θέση να διαχειριστούν τα ενεργειακά τους κόστη εκ των προτέρων, είτε αυτό σημαίνει ότι θα επενδύσουν σε ευφυείς συσκευές εξοικονόμησης ενέργειας ή στην πώληση ενέργειας πίσω στην επιχείρηση κοινής ωφέλειας για έσοδα ή ως μέσο άσκησης περιβαλλοντικής διαχείρισης. Από τη σκοπιά της επιχείρησης κοινής ωφέλειας, «η συμμετοχή των πελατών», θα επιτρέψει στις επιχειρήσεις να στρατολογήσουν τη ζήτηση των καταναλωτών ως μια άλλη πηγή, αντισταθμίζοντας την ανάγκη για πρόσθετη παραγωγή ηλεκτρικής ενέργειας. Με τη βοήθεια από τους πελάτες, οι επιχειρήσεις κοινής ωφέλειας θα είναι σε θέση να βοηθήσουν στην ισορροπία προσφοράς και ζήτησης και τη διασφάλιση της αξιοπιστίας, τροποποιώντας τον τρόπο που χρησιμοποιούν και αγοράζουν ηλεκτρική ενέργεια. Για πρώτη φορά, οι ιδιώτες πελάτες θα έχουν τα ίδια είδη των επιλογών ζήτησης-απόκρισης, όπως απολαμβάνουν σήμερα πολλοί εμπορικοί και βιομηχανικοί πελάτες.

- *Βελτιστοποίηση της χρήσης των πόρων και αποδοτική λειτουργία.*

Το έξυπνο πλέγμα θα είναι σε θέση να εκμεταλλευτεί αποδεδειγμένες τεχνολογίες για να βελτιστοποιήσει τη χρήση των πόρων του - σταθμούς παραγωγής ηλεκτρικής ενέργειας, υποσταθμούς διανομής και άλλων κρίσιμων υποδομών. Τέτοιες βελτιώσεις θα οδηγήσουν σε περισσότερη ισχύ των πόρων καθώς και θα δώσουν στις επιχειρήσεις κοινής ωφέλειας μια πιο ακριβή εικόνα για την ανάγκη νέων σταθμών ηλεκτροπαραγωγής. Οι λειτουργικές βελτιώσεις θα κυμαίνονται από τη βελτίωση παραγόντων πληρότητας σε μειώσεις των απωλειών του συστήματος. Το αποτέλεσμα: Μια καθαρή μείωση των λειτουργικών εξόδων, καθώς και μεγιστοποίηση της αποδοτικότητας σε όλο το σύστημα.

- *Πρόβλεψη και ανταπόκριση στις διαταραχές του συστήματος.*

Με την εκτέλεση συνεχούς αυτο-αξιολόγησης, το έξυπνο πλέγμα θα είναι σε θέση να αποφεύγει διακοπές και όχι απλώς να αντιδρά σε αυτές και θα δρα ταχύτερα από ότι

θα μπορούσαν ποτέ οι χειριστές να επιλύσουν προβλήματα που δημιουργούνται πολύ γρήγορα.

- *Ικανοποιώντας όλες τις επιλογές παραγωγής και αποθήκευσης.*

Βασικό στοιχείο για την επιτυχία του έξυπνου πλέγματος είναι η δυνατότητα για την ασφαλή και απρόσκοπτη ικανοποίηση ενός ευρέως φάσματος της παραγωγής, από τεράστιες κεντρικές μονάδες μέχρι μικρά ηλιακά πάνελ και όλα τα ενδιάμεσα. «Όλα τα ενδιάμεσα», αναφέρεται στον αυξανόμενο κατάλογο των κατανεμημένων ενεργειακών πόρων (DER) που περιλαμβάνουν:

- Κατανεμημένη παραγωγή (DG)
- Μικρά, σε μεγάλη διασπορά εργοστάσια, γενικά πολύ κοντά στο φορτίο.
- Ανανεώσιμες πηγές ενέργειας - αιολική, ηλιακή, βιομάζα, κλπ.
- Αποθήκευση ενέργειας - στην ουσία, γιγάντιες «μπαταρίες» και «πυκνωτές».
- Ανταπόκριση στη ζήτηση (DR) - μείωση της ζήτησης αντί αύξησης της προσφοράς για την αντιμετώπιση φορτίων αιχμής.

Οι ευκαιρίες για διασυνδεδεμένη κατανεμημένη παραγωγή είναι σημαντικές. Με την εξέλιξη της υιοθέτησης του Smart Grid, το DER προβλέπεται να αυξηθεί γρήγορα σε όλο το μήκος της αλυσίδας αξιών, από τους προμηθευτές προς τους εμπόρους προς τους πελάτες. Η κατάληξη: Ένα πλέγμα που είναι λιγότερο ακριβό, πιο αξιόπιστο και φιλικό προς το περιβάλλον.

- *Παροχή ποιότητας ισχύος για την ψηφιακή οικονομία.*

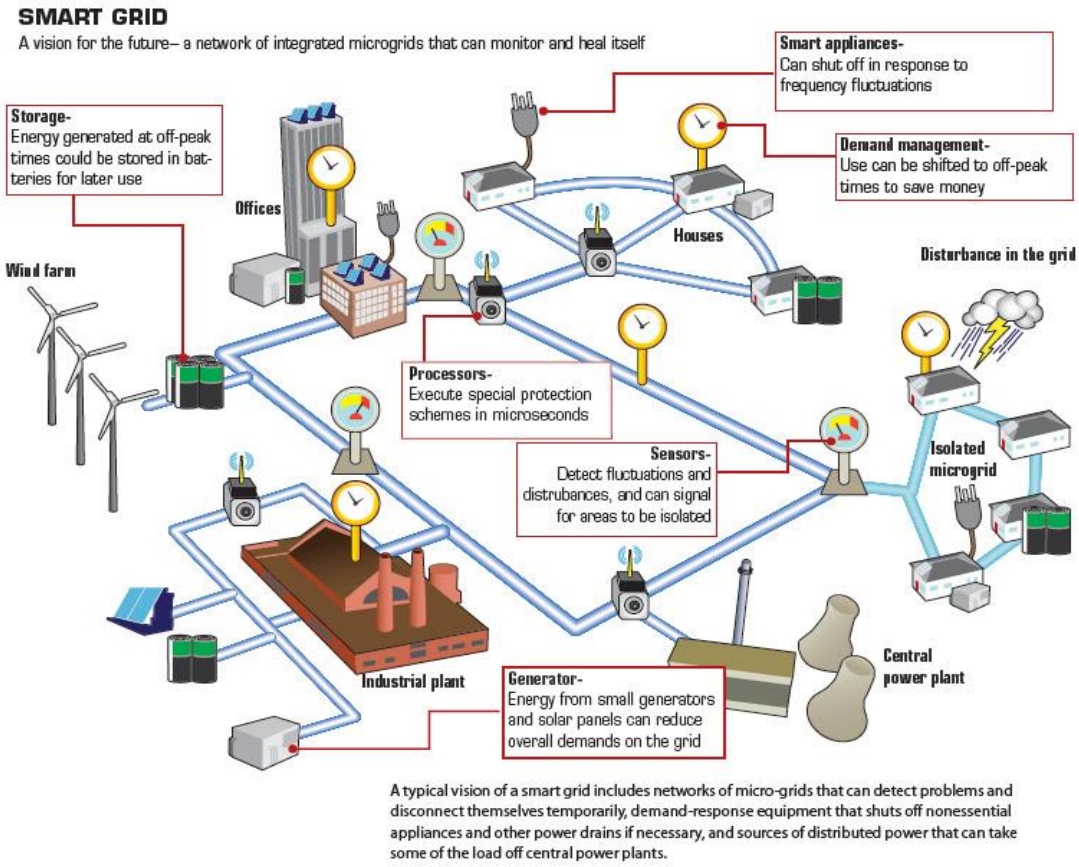
Είναι ένα γεγονός της σύγχρονης ζωής ότι η οικονομία μας γίνεται ασταμάτητα όλο και περισσότερο ψηφιακή λεπτό προς λεπτό. Δείτε για παράδειγμα τη πλησιέστερη φάρμα διακομιστών, τη λειτουργία μεσιτείας ή την υψηλής ευκρίνειας τηλεόραση σας. Σύμφωνα με το Electric Power Research Institute (EPRI), από το 2011, το 16% του ηλεκτρικού φορτίου του έθνους μας θα απαιτήσει ισχύ ψηφιακής ποιότητας. Και δεν υπάρχει γυρισμός. Το Smart Grid θα είναι σε θέση να παρέχει διάφορους βαθμούς ποιότητας της ενέργειας με μια ποικιλία από επιλογές τιμολόγησης. Θα μπορεί επίσης να εντοπίσει και να διορθώσει την κακή ποιότητα ρεύματος πριν τα αποτελέσματά της να δημιουργήσουν πρόβλημα, μειώνοντας δραματικά τις απώλειες των πελατών λόγω ζητημάτων ποιότητας ισχύος - που σήμερα εκτιμώνται σε 25 δισεκατομμύρια δολάρια ετησίως - και αυξάνοντας το συνολικό ποιοτικό ελέγχου του πλέγματος.

- *Ενεργοποίηση νέων προϊόντων, υπηρεσιών και αγορών.*

Με την επικάλυψη νοημοσύνης σε ολόκληρο το εθνικό δίκτυο, οι αρχές και οι τεχνολογίες του Smart Grid υποστηρίζουν τη δημιουργία καλά ολοκληρωμένων αγορών ηλεκτρικής ενέργειας σε σύγκριση με τις κάπως Βαλκανοποιημένες αγορές του σήμερα. Η βεβαιότητα και η ζωντάνια που ενέχουν αυτές οι αγορές θα προσελκύσει νέους συμμετέχοντες στην αγορά - μεσίτες, συγκεντρωτές και λοιπούς - και θα ανοίξει την πόρτα σε νέες ιδέες, προϊόντα και υπηρεσίες.

- *Λειτουργώντας με ανθεκτικότητα έναντι σε επιθέσεις και φυσικές καταστροφές.*

Το σημερινό πλέγμα είναι πολύ ευαίσθητο σε διασπάσει, τόσο μέσω φυσικών καταστροφών όσο και ανθρώπινων ενεργειών ή επιθέσεων. Το Smart Grid θα αντιμετωπίσει κρίσιμα ζητήματα ασφάλειας από την αρχή, κάνοντας την ασφάλεια απαίτηση για όλα του τα στοιχεία.



Εικόνα 2.1 Έξυπνο πλέγμα

2.2 ΔΙΑΦΟΡΕΣ ΤΟΥ ΕΞΥΠΝΟΥ ΠΛΕΓΜΑΤΟΣ ΜΕ ΤΟ ΣΥΜΒΑΤΙΚΟ ΔΙΚΤΥΟ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ

Το έξυπνο δίκτυο απέχει σε μεγάλο βαθμό από το συμβατό δίκτυο ηλεκτρικής ενέργειας. Παρακάτω περιγράφονται μερικές από τις σημαντικές διαφορές που προκύπτουν συγκρίνοντας τα δίκτυα[3].

- Η ροή της ηλεκτρικής ενέργειας στο συμβατό δίκτυο γίνεται μόνο σε μια διεύθυνση από την παραγωγή προς την κατανάλωση. Ενώ στο έξυπνο δίκτυο η επικοινωνία είναι αμφίδρομη και επιτρέπει στον καταναλωτή να ελέγχει την κατανάλωση του προσφέροντας περισσότερες επιλογές.

- Το έξυπνο δίκτυο είναι προσαρμοστικό και έχει την δυνατότητα αυτοϊασης. Εστιάζει στην πρόληψη, ανιχνεύει πιθανά προβλήματα και αποκρίνεται

άμεσα χωρίς να επιδρά στον καταναλωτή. Αντιθέτως, στο συμβατικό δίκτυο υπάρχουν δυσλειτουργίες που συχνά καταλήγουν σε εκτεταμένες διακοπές ρεύματος (blackout) ώστε να αποτραπούν περαιτέρω ζημιές.

- Το υπάρχον δίκτυο είναι ευάλωτο σε καταπονήσεις και φυσικές καταστροφές ενώ το έξυπνο δίκτυο είναι ανθεκτικό σε τέτοιους κινδύνους με ικανότητα ταχείας αποκατάστασης της βλάβης.

- Στο συμβατικό δίκτυο ο βασικός στόχος είναι προσφορά αδιάλειπτης ηλεκτρικής ενέργειας χωρίς να εστιάζει σε θέματα ποιότητας της παρεχόμενης ενέργειας. Σε αντίθεση με το έξυπνο δίκτυο το οποίο έχει στόχο να ικανοποιήσει τις απαιτήσεις των καταναλωτών προσφέροντας υψηλής ποιότητας ηλεκτρική ενέργεια ή διαφορετικές ποιότητες σε διαφορετικές τιμές.

- Τα έξυπνα δίκτυα επιτρέπουν την επιλογή χρησιμοποίησης όλων των πηγών ενέργειας σε μεγάλη κλίμακα μέσα στο ηλεκτρικό δίκτυο αλλά και της αποθήκευσης της ενέργειας. Κάτι τέτοιο δεν μπορεί να συμβεί στο σημερινό δίκτυο κεντρικής παραγωγής όπου με δυσκολία ενσωματώνονται τα παραπάνω.

- Το σημερινό δίκτυο διαθέτει ελάχιστους αισθητήρες, δεν υπάρχει παρακολούθηση και αμφίδρομη ροή πληροφοριών σε αντίθεση με το έξυπνο δίκτυο που χρησιμοποιεί αισθητήρες παρακολούθησης, επικοινωνίες αυτοματισμού και υπολογιστικά συστήματα για να βελτιώσει την ευελιξία την ασφάλεια την αξιοπιστία και την αποδοτικότητα του ηλεκτρικού συστήματος.

Υπάρχον Δίκτυο	**Έξυπνο δίκτυο**
Ηλεκτρομηχανολογικό	Ψηφιακό
Μονόδρομη επικοινωνία	Αμφίδρομη επικοινωνία
Κεντρική παραγωγή	Κατανεμημένη παραγωγή
Λίγοι αισθητήρες	Αισθητήρες παντού
Χειροκίνητη παρακολούθηση	Αυτό-παρακολούθηση
Χειροκίνητη αποκατάσταση/επαναφορά	Αυτό-θεραπεία
Βλάβες και διακοπές ρεύματος	Προσαρμοστικότητα και νησιδοποίηση
Περιορισμένος έλεγχος	Έλεγχος
Λίγες επιλογές των πελατών	Πολλές επιλογές πελατών

Πίνακας 2.2 Σύντομη σύγκριση μεταξύ του υπάρχοντος και του έξυπνου δικτύου

2.3 ΤΕΧΝΟΛΟΓΙΕΣ ΕΞΥΠΝΟΥ ΠΛΕΓΜΑΤΟΣ

Για τον εκσυγχρονισμό του συμβατικού δικτύου και την εξέλιξή του, ώστε να αποκτήσει ευφυΐα, απαιτείται η υιοθέτηση κάποιων τεχνολογιών. Άλλες από αυτές βρίσκονται σε στάδιο ανάπτυξης ενώ άλλες έχουν ήδη εφαρμοστεί. Παρακάτω παρουσιάζονται οι τεχνολογίες του έξυπνου δικτύου[4]:

- Γενική παρακολούθηση και έλεγχος

Πρόκειται για γενική παρακολούθηση όλου του συστήματος ηλεκτρικής ενέργειας. Η παρακολούθηση γίνεται σε πραγματικό χρόνο και αφορά τις λειτουργίες παραγωγής, μεταφοράς, διανομής και τις διασυνδέσεις μεταξύ των διάφορων περιοχών. Έτσι μειώνεται η πιθανότητα εμφάνισης σφαλμάτων στο δίκτυο και παρέχεται εποπτεία σε ειδικού τύπου τεχνολογίες παραγωγής όπως οι ανανεώσιμες πηγές ενέργειας. Επίσης, τα δεδομένα που συγκεντρώνονται αποτελούν τη βάση για τις στρατηγικές λήψης αποφάσεων.

- Information Communication (ICT)

Αποτελεί την υποδομή της μεταφοράς της πληροφορίας. Το έξυπνο δίκτυο προϋποθέτει τη μεταφορά πληροφορίας διπλής ροής και μέσα για την επίτευξη αυτής της λειτουργίας είναι το διαδίκτυο, τα τηλεφωνικά δίκτυα, τα ραδιοφωνικά δίκτυα κτλ.

- ΑΠΕ και διανεμημένη παραγωγή

Η αποκέντρωση της παραγωγής έχει απασχολήσει τους φορείς λήψης αποφάσεων στην αγορά ενέργειας. Η διανεμημένη παραγωγή προσφέρει λύσεις για την κάλυψη απομονωμένων φορτίων. Εμπορικά κτίρια και κατοικίες θα μπορούσαν να καλύπτουν μέρος των αναγκών τους από μονάδες διανεμημένης παραγωγής. Το ευφυές δίκτυο περιλαμβάνει μονάδες ελέγχου και αποθηκευτικά μέσα για τη βέλτιστη λειτουργία τους.

- Διαχείριση του δικτύου διανομής

Το έξυπνο δίκτυο χρησιμοποιεί αισθητήρες σε καλώδια τροφοδοσίας, σε μετασχηματιστές και αυτόματους διακόπτες και εισάγει αυτοματισμούς στους υποσταθμούς που συμβάλλουν στη σταθεροποίηση της τάσης, στην ανίχνευση των σφαλμάτων και στη μείωση του χρόνου αποκατάστασης τους.

- Εξελιγμένη υποδομή μέτρησης (Advanced Metering Infrastructure, AMI)

Η εξελιγμένη υποδομή μέτρησης είναι από τις βασικότερες τεχνολογίες ευφυούς δικτύου και παρέχει αμφίδρομη επικοινωνία, καταγραφή του φορτίου σε πραγματικό χρόνο, αποστολή δεδομένων που αφορούν τις τιμές της ηλεκτρικής ενέργειας κ.α. Χρησιμοποιεί έξυπνους μετρητές και αισθητήρες για την καταγραφή των δεδομένων των φορτίων, τα οποία χρησιμοποιούνται για την εξαγωγή συμπερασμάτων για τα πρότυπα κατανάλωσης.

- Συστήματα στην πλευρά των καταναλωτών

Είναι οι διατάξεις και οι εφαρμογές που αποσκοπούν στον έλεγχο της κατανάλωσης και στην εγκατάσταση έξυπνων συσκευών. Νέες προσεγγίσεις προτείνουν την ανάπτυξη εφαρμογών για συσκευές κινητής τηλεφωνίας αλλά και τη χρήση των μέσων κοινωνικής δικτύωσης για τη δημιουργία τάσεων ευρείας αποδοχής της ενεργειακής αποδοτικότητας.

2.4 ΕΞΥΠΝΟΣ ΜΕΤΡΗΤΗΣ

Ο έξυπνος μετρητής είναι μια συσκευή η οποία έρχεται να αντικαταστήσει το μέχρι σήμερα βασικό εργαλείο για τη μέτρηση της ηλεκτρικής ισχύος και ενέργειας το οποίο είναι ο ηλεκτρομηχανικός ή επαγωγικός μετρητής. Η συσκευή αυτή μετράει την ενέργεια που χρησιμοποιείται και στέλνει τις πληροφορίες στο σύστημα και από κει καταλήγει στον πελάτη ενημερώνοντάς τον για την εκάστοτε κατανάλωση του και το αντίστοιχο κόστος αυτής. Οι έξυπνοι μετρητές έχουν τη δυνατότητα αμφίδρομης επικοινωνίας, δυνατότητα δηλαδή εκτός από την αποστολή δεδομένων, και τη λήψη εντολών. Αποτελούν έναν οικονομικό τρόπο για μέτρηση και παρακολούθηση της κατανάλωσης, που επιτρέπει την καλύτερη ρύθμιση της παραγωγής βασιζόμενη σε ημερήσια δεδομένα πραγματικού χρόνου (εξοικονόμηση ενέργειας και χρημάτων – μικρότερες επενδύσεις σε δίκτυα διανομής). Στόχος είναι με τους έξυπνους μετρητές οι χρεώσεις στους καταναλωτές να γίνονται βάσει του ακριβούς ποσού ενέργειας που έχει καταναλωθεί.

Εικόνα 2.3 Επαγωγικός μετρητής

Εικόνα 2.4 Έξυπνος μετρητής

Οι έξυπνοι μετρητές θα έχουν την δυνατότητα να μετρούν άμεσα την κατανάλωση ηλεκτρικής ισχύος και να μεταδίδουν τις μετρήσεις στις βάσεις δεδομένων στο κέντρο διαχείρισης. Ο καταναλωτής μπορεί οποιαδήποτε στιγμή να έχει γνώση της πραγματικής κατανάλωσης ηλεκτρικής ενέργειας. Η ενημέρωση του καταναλωτή μπορεί να γίνεται με ευκολία στην οθόνη του ηλεκτρονικού του υπολογιστή, εφόσον υπάρχει ασύρματη σύνδεση μεταξύ υπολογιστή και μετρητή. Η συνεχής ενημέρωση του καταναλωτή αποσκοπεί στη μείωση χρήσης κάποιων ηλεκτρονικών συσκευών, οι οποίες καταναλώνουνε μεγάλες ποσότητες ενέργειας.

2.4.1 Τα οφελη του εξυπνου μετρητη για τον καταναλωτη

Τα οφέλη του Smart Metering για τους καταναλωτές θα είναι πολύπλευρα καθώς με την χρήση έξυπνων μετρητών οι καταναλωτές μέσω της καλύτερης πληροφόρησης του θα μπορούν να λαμβάνουν καλύτερα αποφάσεις όσον αφορά την ορθολογική χρήση του ηλεκτρικού ρεύματος. Τα πλεονεκτήματα αυτά μπορούν να αυξηθούν σημαντικά εάν προστεθούν κάποια ακόμα στοιχεία στους μετρητές (π.χ. έλεγχος συσκευών). Παρακάτω θα αναλύσουμε τα πλεονεκτήματα που εξασφαλίζει ο καταναλωτής με την χρήση έξυπνου μετρητή.

- *Εξοικονόμηση ενέργειας.* Η αφύπνιση του καταναλωτικού κοινού είναι ένα μείζων σημασίας ζήτημα. Οι έξυπνοι μετρητές είναι συσκευές που καταγραφούν την κατανάλωση ενέργειας και προσφέρουν πληροφορίες στους καταναλωτές σχετικά με τη χρέωση τους για διαφορετικές ώρες της ημέρας. Με αυτό τον τρόπο δίνεται στον καταναλωτή η δυνατότητα να προσαρμόσει την ενεργειακή του κατανάλωση και να εξορθολογήσει τους λογαριασμούς του. Όσο πιο ακριβείς και άμεση είναι η πληροφορία της κατανάλωσης στον χρήστη τόσο αυξάνονται οι πιθανότητες να μειώσει την σπατάλη της ηλεκτρικής ενέργειας. Αυτός ο τρόπος κρίνεται πιο αποτελεσματικός καθώς με το τωρινό σύστημα ο καταναλωτής μαθαίνει την ώρα που του έρχεται ο λογαριασμός. Υπάρχει επίσης δυνατότητα μέσω κατάλληλου λογισμικού να γίνει η τροποποίηση σε kWh ή ακόμα και σε CO2, έτσι μπορεί να επιτευχθεί ακόμα μεγαλύτερη μείωση καθώς ο καταναλωτής θα βρεθεί αντιμέτωπος με την περιβαλλοντική του συνείδηση.
- *Αξιόπιστη μέτρηση και τιμολόγηση***.** Με τους έξυπνους μετρητές η τιμολόγηση βασίζεται σε πραγματική παρά σε εκτιμώμενη μέτρηση. Αυτό συντελεί στην βελτίωση του επιπέδου υπηρεσιών και κατ' επέκταση σε αυξημένο επίπεδο ικανοποίησης του πελάτη. Επιπροσθέτως οι έξυπνοι μετρητές μας παρέχουν την δυνατότητα απομακρυσμένης ενεργοποίησης/απενεργοποίησης και έτσι είναι ευκολότερη η αλλαγή εταιρίας παροχής.
- *Βελτιωμένη ποιότητα υπηρεσιών.* Η δυνατότητα που έχουν πλέον οι καταναλωτές να παίρνουν και οι ίδιοι μετρήσεις, αναγκάζει τους διαχειριστές του δικτύου να δείξουν μεγαλύτερη μέριμνα στη βελτίωση του δικτύου διανομής. Αποτέλεσμα αυτού η καλύτερη ποιότητα υπηρεσιών στον πελάτη.
- *Ευελιξία επιλογής τιμοκαταλόγου***.** Όπως γνωρίζουμε οι εταιρίες παροχής προσφέρουν μια σειρά τιμολογίων με βάση τα οποία χρεωνόμαστε. Η έλλειψη ακριβών στοιχείων καθιστούσαν την αλλαγή τιμολογίου απαγορευτική λόγω του ότι δεν ήταν σαφές αν αυτό ήταν συμφέρον. Πλέον με τις δυνατότητες που μας παρέχονται θα μπορεί ο κάθε καταναλωτής να παίρνει σωστές αποφάσεις οι οποίες θα εξυπηρετούν καλύτερα τις ανάγκες του και θα είναι πολύ πιο συμφέρουσες για αυτόν.
- *Καλύτερη αντιμετώπιση ευπαθών ομάδων***.** Δυστυχώς ακόμα και στην εποχή μας φαινόμενα φτώχειας είναι συνήθη. Παλαιότερα η αντιμετώπιση αυτών των ομάδων που δεν είχαν την ικανότητα να εκπληρώσουν άμεσα τις υποχρεώσεις τους ήταν η διακοπή της ηλεκτροδότησης. Πλέον είναι πιο εύκολο στις εταιρίες να αποστέλλουν προειδοποιητικά σημειώματα και να αποφεύγουν την έσχατη λύση της διακοπής.

- *Ευκολότερη σύγκριση της αγοράς και αλλαγή παρόχου***.** Με τη χρήση των δυνατοτήτων των έξυπνων μετρητών και λαμβάνοντας υπόψη τα στοιχεία που μας δίνουν, θα μπορούμε να κάνουμε μια αξιολόγηση για το ποια προσφορά θα μας συμφέρει καλύτερα. Κατ' επέκταση μας δίνεται η δυνατότητα γρήγορης μετάβασης μεταξύ δυο παρόχων καθώς η ανάγνωση των στοιχείων μπορεί να γίνει ανά πάσα στιγμή άρα και η μεταβίβαση.
- *Δυνατότητα προσθήκης συσκευών στο δίκτυο του έξυπνου σπιτιού***.** Αυτό μπορεί να περιλαμβάνει από ξεχωριστούς μετρητές αερίου, νερού κ.λπ. μέχρι οποιαδήποτε άλλη συσκευή π.χ. Smart T.V.
- Διαχείριση φωτοβολταϊκών**.** Δεν είναι πλέον απαραίτητο να συνδέσουμε ξεχωριστό μετρητή για να παρακολουθήσουμε την παραγωγή ηλεκτρικής ενέργειας στα φωτοβολταϊκά της οικίας μας, καθώς πλέον συνδέονται κατευθείαν με τον μετρητή και μας δίνουν πληροφορίες π.χ. παραγωγή ανά ημέρα που δεν ήταν δυνατές μέχρι στιγμής[5].

2.4.2 Οφελη για τους προμηθευτες ενεργειας

Στις ελεύθερες αγορές τις οποίες ο προμηθευτής έχει τη δυνατότητα να προσφέρει μεγάλο εύρος προσφορών μέτρησης, υπάρχει μεγαλύτερη δυνατότητα διαφοροποίησης. Εάν οι μετρητές ανήκουν στους διανομείς τότε η δυνατότητα διαφοροποίησης έχει να κάνει με την ευελιξία που παρέχει το εκάστοτε σύστημα μέτρησης.

- *Επιλογές τιμολόγησης***.** Η ικανότητα των προμηθευτών να γνωρίζουν τα κριτήρια αγοράς των καταναλωτών δίνουν την δυνατότητα για μεγαλύτερη προσαρμογή των πακέτων τιμολόγησης στις ανάγκες του καταναλωτή. Οι διαφοροποιήσεις που μπορούν να γίνουν ποικίλουν καθώς μπορεί να ξεκινούν από την τιμή του ρεύματος γενικά μέχρι και την διαφοροποίηση της τιμής ανά ώρα λειτουργίας.
- *Υπηρεσίες after-sale.* Η γνώση του προμηθευτή για τις ενεργειακές συνήθειες του καταναλωτή μπορεί να ωθήσει στην ανάπτυξη υπηρεσιών ώστε ο καταναλωτής να γίνει πιο ενεργειακά αποδοτικός.
- *Γρήγορη αλλαγή προμηθευτή* Η αυτοματοποίηση της διαδικασίας αλλαγής διευκολύνει μια προηγουμένως χρονοβόρα γραφειοκρατική διαδικασία.
- *Μικρότερο ποσοστό παραπόνων τιμολόγησης***.** Με την ακρίβεια μέτρησης που μας παρέχουν οι έξυπνοι μετρητές θα υπάρχει μικρότερο ποσοστό παραπόνων άρα και μικρότερο λειτουργικό κόστος της εταιρίας στον τομέα της εξυπηρέτησης πελατών.
- *Καλύτερη διοίκηση χαρτοφυλακίου***.** Οι προμηθευτές αποκτούν ένα ακριβές προφίλ της ενεργειακής κατανάλωσης των καταναλωτών τους και μπορούν να διαχειριστούν καλύτερα την αγορά ενέργειας[5].

2.4.3 Οφελη για τους διαχειριστες δικτυου διανομης (DSO)

Το smart metering όταν αναπτυχθεί πλήρως θα επιτρέπει ακριβή πληροφόρηση για τους καταναλωτές χαμηλής τάσης προσφέροντας αρκετές διευκολύνσεις στους διαχειριστές του δικτύου. Το πλεονεκτήματα αυτά αρχικά θα είναι εμφανή από την εξομάλυνση των λειτουργιών του δικτύου, την αξιοπιστία του δικτύου καθώς και την γρηγορότερη απόκριση

σε τυχόν βλάβες που προκαλούνται στο δίκτυο, βελτιώνοντας έτσι την ποιότητα υπηρεσιών τους. Η καλύτερη πληροφόρηση έχει επίσης ως συνέπεια μικρότερες απώλειες δικτύου και καλύτερο προγραμματισμό επενδύσεων.

- *Εντοπισμός σφάλματος δικτύου.* Με τους συμβατικούς μετρητές όταν υπήρχε κάποιο πρόβλημα στην ηλεκτροδότηση ο καταναλωτής θα έπρεπε να ενημερώσει τον διαχειριστή. Πλέον ο έξυπνος μετρητής αναλαμβάνει τη δουλειά αυτή στέλνοντας απευθείας σήμα στον κεντρικό υπολογιστή μειώνοντας έτσι το χρόνο εντοπισμού της βλάβης. Επιπλέον ο διαχειριστής μπορεί να ενημερώσει τους καταναλωτές σε τυχόν περίπτωση βλάβης ή προγραμματισμένης διακοπής ηλεκτροδότησης συντελώντας έτσι σε καλύτερη παροχή υπηρεσιών.
- *Γρηγορότερη αποκατάσταση βλαβών.* Όπως είναι προφανές ο χρόνος αποκατάστασης μιας βλάβης μειώνεται σημαντικά, μειώνοντας ταυτόχρονα το κόστος λειτουργίας των ομάδων αποκατάστασης βλαβών μέσω εγκυρότερης πληροφόρησης.
- *Βελτιωμένη παροχή υπηρεσιών.* Τα κέρδη απ' αυτό μπορεί να είναι πολλά εφόσον ο διαχειριστής συμμετέχει σε πρόγραμμα επιβολής ποινής σε περίπτωση αργοπορημένης αποκατάστασης βλάβης.
- *Ακριβέστερος εντοπισμός απωλειών δικτύου***.** Οι έξυπνοι μετρητές παρέχουν ακριβείς πληροφορίες σχετικά με τις απώλειες δικτύου αναλογικά με την περιοχή.
- *Τάση δικτύου και παρακολούθηση φάσεων.* Από εδώ θα μπορούμε να βελτιώσουμε τη σταθερότητα του δικτύου και την αξιοπιστία του συστήματος.
- *Βελτίωση της υποδομής του δικτύου και της διαχείρισης των κεφαλαίων***.** Η ικανότητα για στιγμιαία περιγραφική πληροφόρηση για τομή του δικτύου όπως η τάση, η σταθερότητα, ο φόρτος και οι απώλειες όλου του δικτύου χαμηλής τάσης, επιτρέπει την εξομάλυνση της λειτουργίας του δικτύου διανομής. Οι ακριβείς πληροφορίες μπορούν να βελτιώσουν συνολικά το επενδυτικό πλάνο. Τέτοιου τύπου πληροφόρηση μπορεί να βοηθήσει στη χρηματοδότηση για επέκταση του δικτύου όπως και τη βελτίωση του[5].

2.5 Τεχνολογιες AMR και AMI

Το AMR (Automatic Meter Reading) είναι μια τεχνολογία που καταγράφει και συγκεντρώνει τις μετρήσεις του ηλεκτρικού ρεύματος, του γκαζιού και του νερού που καταναλώνουμε. Μέσω αυτού του συστήματος μπορούμε να παρακολουθήσουμε σε πραγματικό χρόνο τη χρέωση, να διαγνώσουμε ένα σφάλμα ανάμεσα στο χρήστη και στον πάροχο μεταξύ άλλων. Αυτή η τεχνολογία μας βοήθα στον καλύτερο υπολογισμό της προβλεπόμενης κατανάλωσης καθώς βασίζεται όπως αναφέραμε σε κατανάλωση πραγματικού χρόνου. Η χρήση της τεχνολογίας προϋποθέτει την ύπαρξη ενσύρματου η ασύρματου δικτύου για τη μεταφορά των μετρήσεων. Τα πλεονεκτήματα που προσφέρει η τεχνολογία AMR είναι πολλά τόσο για τις επιχειρήσεις ηλεκτρισμού, όσο και για τους πελάτες καταναλωτές. Παρακάτω αναφέρονται μερικά από αυτά[11]:

- Ακριβής τιμολόγηση χωρίς την έκδοση έναντι λογαριασμών.

- Δυνατότητα παροχής εναλλακτικών τιμολογίων μειωμένου κόστους, ανάλογα με τα χαρακτηριστικά που εμφανίζει η κατανάλωση των μεγάλων ομάδων καταναλωτών.
- Άμεση πληροφόρηση των πελατών με στοιχεία της κατανάλωσής τους.
- Μειωμένο κόστος καταμέτρησης για την επιχείρηση.
- Εξαγωγή συμπερασμάτων χρήσιμων τόσο για την επιχείρηση όσο και για την ρυθμιστική αρχή ενέργειας, τα οποία είναι απαραίτητα για την χάραξη και υλοποίηση των πολιτικών στο απελευθερωμένο περιβάλλον της αγοράς ηλεκτρικής ενέργειας.
- Μείωση του λειτουργικού κόστους.
- Έλεγχος της ποιότητας της παρεχόμενης ενέργειας.

Η τεχνολογία AMI (Advanced Metering Infrastructure) είναι μια από τις πιο σημαντικές τεχνολογίες του έξυπνου δικτύου και αποτελεί την εξέλιξη του AMR. Το AMI παρέχει στους καταναλωτές τις πληροφορίες που χρειάζονται για να πάρουν έξυπνες αποφάσεις αφού τους δίνει την δυνατότητα σε μια ποικιλία από επιλογές που τους οδηγούν σε σημαντικά οφέλη. Για παράδειγμα τους δίνει την δυνατότητα σε ώρες αιχμής να κάνουν μετατόπιση του φορτίου ώστε να έχουν καλύτερη τιμολόγηση. Έτσι επιτυγχάνεται αποσυμφόρηση του δικτύου, αποφεύγοντας ένα πιθανό blackout αλλά και ο καταναλωτής μεταφέροντας την κατανάλωση του σε ώρες που δεν υπάρχει συμφόρηση στο δίκτυο έχει οικονομικά οφέλη.

ΚΕΦΑΛΑΙΟ 3

ΤΕΧΝΟΛΟΓΙΕΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΠΟΥ ΒΡΙΣΚΟΥΝ ΕΦΑΡΜΟΓΗ ΣΤΑ ΕΞΥΠΝΑ ΠΛΕΓΜΑΤΑ

3.1 Αρχιτεκτονικη του δικτυου επικοινωνιων

Η υποδομή επικοινωνίας στο έξυπνο πλέγμα πρέπει να υποστηρίζει τις αναμενόμενες λειτουργικές δυνατότητες και να ικανοποιεί τις απαιτήσεις επίδοσης. Καθώς η υποδομή αυτή συνδέει ένα τεράστιο αριθμό ηλεκτρικών συσκευών και διαχειρίζεται την περίπλοκη επικοινωνία τους, είναι οργανωμένη σε μια ιεραρχική υποδομή με διασυνδεδεμένα επιμέρους υποδίκτυα, το καθένα από τα οποία είναι υπεύθυνο για ξεχωριστή γεωγραφική περιοχή. Γενικά, τα δίκτυα επικοινωνιών μπορούν να ταξινομηθούν σε τρεις κατηγορίες: δίκτυα WAN (Wide Area Networks), δίκτυα FAN (Field Area Networks) και δίκτυα HAN (Home Area Networks).

Τα δίκτυα WAN σχηματίζουν τη ραχοκοκαλιά που συνδέει τα κατανεμημένα, μικρότερα δίκτυα που εξυπηρετούν τα συστήματα ηλεκτρικής ενέργειας σε διάφορες θέσεις. Όταν τα κέντρα ελέγχου βρίσκονται μακριά από τους υποσταθμούς ή τους τελικούς καταναλωτές, οι μετρήσεις πραγματικού χρόνου που λαμβάνονται από τις ηλεκτρικές συσκευές μεταφέρονται στα κέντρα ελέγχου μέσω των δικτύων WAN και, κατά την αντίστροφη κατεύθυνση, τα WAN αναλαμβάνουν τη μεταφορά εντολών από τα κέντρα ελέγχου προς τις συσκευές.

Τα δίκτυα FAN συνιστούν τη μονάδα επικοινωνίας για τα συστήματα διανομής ηλεκτρικής ενέργειας. Οι ηλεκτρικοί αισθητήρες στα τροφοδοτικά και τους μετασχηματιστές της διανομής, οι έξυπνες ηλεκτρικές συσκευές (IEDs) ικανές να εκτελούν εντολές ελέγχου από τα συστήματα DMS (Distribution Management System), οι κατανεμημένοι ενεργειακοί πόροι (Distributed Energy Resources – DER) στα συστήματα διανομής, οι σταθμοί φόρτισης plug-in ηλεκτρικών οχημάτων (PEVs) και οι έξυπνοι μετρητές στις εγκαταστάσεις των πελατών αποτελούν τις κύριες πηγές πληροφοριών προς παρακολούθηση και έλεγχο από τα συστήματα DMS στα κέντρα ελέγχου. Οι εφαρμογές του συστήματος ενέργειας στον τομέα της διανομής χρησιμοποιούν δίκτυα FAN για να μοιράζονται και να ανταλλάσουν πληροφορίες.

Τα οικιακά δίκτυα απαιτούνται στον τομέα του καταναλωτή, για την παρακολούθηση και τον έλεγχο των έξυπνων συσκευών στο χώρο των πελατών και για την εφαρμογή νέων λειτουργιών όπως DR και AMI

Ένα επικοινωνιακό σύστημα είναι το βασικό στοιχείο για μια υποδομή έξυπνου πλέγματος. Την επικοινωνιακή δομή ενός έξυπνου ηλεκτρικού δικτύου συνθέτουν στην ουσία τέσσερις τομείς δικτύωσης: ο *πυρήνας* (core) ή αλλιώς κορμός (backbone), ο *τομέας μεσαίων μιλίων*

(middle-mile) ή backhaul, ο *τομέας τελευταίων μιλίων* (last-mile) ή πρόσβαση/διανομή (access/distribution) καθώς και τα *σπίτια* και τα *κτήρια* (Premises Area Network). Οι τέσσερις τομείς, που διασυνδέονται ο ένας με τον άλλον, υποστηρίζονται από διάφορες τεχνολογίες και συγκεντρώνουν ουσιαστικά την επικοινωνιακή υποδομή του έξυπνου πλέγματος.

Το δίκτυο πυρήνας στηρίζει τη σύνδεση μεταξύ των πολυάριθμων υποσταθμών και των εδρών των επιχειρήσεων κοινής ωφέλειας. Το δίκτυο WAN απαιτεί υψηλή χωρητικότητα και διαθεσιμότητα εύρους ζώνης για να διαχειριστεί τα δεδομένα μεγάλου όγκου που μεταφέρονται από άλλους τομείς, καθώς και από τους πολλαπλούς διανομείς. Το δίκτυο κορμού είναι συνήθως χτισμένο σε οπτικές ίνες.

Ο τομέας μεσαίων μιλίων συνδέει τους συγκεντρωτές δεδομένων στο AMI (Advanced Metering Infrastructure) με τον αυτοματισμό υποσταθμών/διανομής και τα κέντρα ελέγχου που σχετίζονται με τη λειτουργία των επιχειρήσεων κοινής ωφέλειας. Αυτός ο τομέας όχι μόνο χρειάζεται να παρέχει ευρυζωνικά μέσα, αλλά απαιτεί η εγκατάσταση του δικτύου του να είναι όσο το δυνατόν πιο εύκολη και αποδοτική οικονομικά. Επιπλέον, οι διαδρομές και οι συνδέσεις μέσω των οποίων θα ρέουν τα δεδομένα πρέπει να είναι ευέλικτες και αδιάλειπτες. Το πιο σημαντικό είναι η συνολική απόδοση να είναι προβλέψιμη για την αξιόπιστη μεταφορά δεδομένων πριν την είσοδο στον κορμό.

Ο τομέας τελευταίων μιλίων καλύπτει τις περιοχές των FAN/HAN και AMI και είναι υπεύθυνος τόσο για τη συλλογή δεδομένων από τους έξυπνους μετρητές όσο και για τη μεταφορά τους στους συγκεντρωτές. Υπάρχει ποικιλία ασύρματων και ενσύρματων τεχνολογιών που είναι διαθέσιμες για να εφαρμοστούν στον τομέα αυτό, οι οποίες θα πρέπει όμως να παρέχουν ευρυζωνική ταχύτητα και ασφάλεια.

Το δίκτυο των κτηρίων κερδίζει μεγαλύτερη προσοχή όντας ο τελευταίος τομέας του έξυπνου δικτύου. Οι τεχνολογίες επικοινωνιών που υποστηρίζουν Home Area Networks (HAN) καθώς και τον σχετιζόμενο αυτοματισμό κτηρίων θα βασιστούν κατά κύριο λόγο στα πρότυπα IEEE 802.15.4, IEEE 802.11 και PLC. Η διαχείριση της ενέργειας του σπιτιού που θα συμβαίνει στα HAN θα ρυθμίζει αρκετά στοιχεία, όπως θερμοστάτες, HVAC (θέρμανση, εξαερισμό και κλιματισμό), έξυπνες συσκευές, έλεγχο φωτισμού, οικιακό αυτοματισμό, PHEV/EV (Plug-in Hybrid Electric Vehicle/ Electric Vehicle) και DG. Η συλλογή και μεταφορά δεδομένων από αυτόν τον τομέα πρέπει να χαρακτηρίζονται από σταθερότητα, ακρίβεια και ασφάλεια[6].

3.2 WIMAX

Το WiMax είναι μια τεχνολογία ασύρματων δικτύων η οποία λειτουργεί με παρεμφερή τρόπο με το WiFi με πολύ μεγαλύτερη εμβέλεια όμως. Το WiMax παρέχει ρυθμούς δεδομένων μέχρι 70Mbps και εξασφαλίζει εμβέλεια επικοινωνίας κοντά στα 48 χιλιόμετρα. Ωστόσο, η κάλυψη και η ταχύτητα του δικτύου είναι μεγέθη αντιστρόφως ανάλογα το ένα προς το άλλο. Τα αδειοδοτημένα φάσματα επιτρέπουν μετάδοση υψηλότερης ισχύος και σε μεγαλύτερες αποστάσεις, κάτι που τα καθιστά πιο κατάλληλα για επικοινωνίες μεγάλων αποστάσεων.

Μερικές από τις εφαρμογές των έξυπνων δικτύων όπου θα μπορούσε να χρησιμοποιηθεί το WiMAX είναι: 1) Ασύρματα Αυτόματα Συστήματα Ανάγνωσης Μετρητών (WAMRS), 2) Τιμολόγηση σε πραγματικό χρόνο (Real-time Pricing), 3) Ανίχνευση και αποκατάσταση διακοπής λειτουργίας.

Στα πλεονεκτήματα της σημερινής τεχνολογίας WiMAX συμπεριλαμβάνονται το μικρότερο κόστος ανάπτυξης και λειτουργίας, η ομαλή επικοινωνία, οι υψηλοί ρυθμοί μετάδοσης (ως τα 75Mbps), το επαρκές εύρος ζώνης και η επεκτασιμότητα.

Ένα από τα αρνητικά του WiMAX είναι ότι το εύρος ζώνης διαμοιράζεται με τους χρήστες. Αυτό εξηγείται από το γεγονός ότι οι συχνότητες πάνω από 10GHz δεν μπορούν να διαδοθούν μέσω εμποδίων. Έτσι, ειδικά για αστικές περιοχές, οι χαμηλότερες συχνότητες είναι πιο χρήσιμες, όμως έχουν ήδη αδειοδοτηθεί. Άρα, ο πιο πιθανός τρόπος να χρησιμοποιήσουν οι πάροχοι των έξυπνων δικτύων αυτή την τεχνολογία είναι να τη μισθώσουν από άλλον. Επίσης, το WiMAX παρουσιάζει ασυμμετρία των ταχυτήτων στις ζεύξεις ανόδου και καθόδου, ενώ το trade off μεταξύ απόστασης και ρυθμού μετάδοσης αποτελεί μια ακόμη αδυναμία.

3.3 Κυψελωτες επικοινωνιες

Το υπάρχον δίκτυο κυψελωτών επικοινωνιών είναι μια καλή επιλογή τόσο για την επικοινωνία μεταξύ των έξυπνων μετρητών και των επιχειρήσεων κοινής ωφέλειας, όσο και μεταξύ απομακρυσμένων κόμβων. Χρησιμοποιώντας την υπάρχουσα υποδομή επικοινωνιών, οι επιχειρήσεις αποφεύγουν σημαντικό κόστος και χρόνο που θα απαιτούνταν για τη δημιουργία μιας νέας και αποκλειστικής υποδομής.
Οι 3G (3rd Generation) / 4G (4rd Generation) τεχνολογίες λειτουργούν στο φάσμα 824-894MHz/1900MHz, που είναι οι αδειοδοτημένες ζώνες συχνοτήτων. Οι ρυθμοί μεταφοράς δεδομένων αυτής της τεχνολογίας έχουν βελτιωθεί τελευταία, αλλά η απόσταση κάλυψης εξαρτάται από τη διαθεσιμότητα της κυψελωτής υπηρεσίας. Η τοπολογία του δικτύου αποτελείται από κυψέλες, οι οποίες καλύπτουν μια ευρεία περιοχή και εξυπηρετούνται η καθεμία από τουλάχιστον έναν ασύρματο πομπό χαμηλής ισχύος, γνωστό ως σταθμό βάσης. Κάθε κυψέλη χρησιμοποιεί διαφορετικό σύνολο συχνοτήτων από τις γειτονικές της, ώστε να αποφεύγεται η παρεμβολή και να παρέχεται εγγυημένο εύρος ζώνης εντός των ορίων της.
Όσον αφορά τα πλεονεκτήματα, το σημαντικότερο είναι ότι τα κυψελωτά δίκτυα υπάρχουν ήδη. Έτσι, όπως έχει αναφερθεί, οι πάροχοι δε θα επιβαρυνθούν με κόστος κατασκευής. Επίσης, παρέχεται επαρκές εύρος ζώνης για αρκετές από τις εφαρμογές, ενώ με την πρόσφατη ανάπτυξη στις 3G / 4G τεχνολογίες, ο ρυθμός δεδομένων και η ποιότητα υπηρεσίας (QoS) βελτιώνονται πολύ γρήγορα.
Από την άλλη, μερικές κρίσιμες εφαρμογές των έξυπνων δικτύων χρειάζονται αδιάλειπτη διαθεσιμότητα επικοινωνιών. Ωστόσο, το κυψελωτό δίκτυο θα χρησιμοποιείται παράλληλα και από την αγορά των καταναλωτών, γεγονός που μπορεί να οδηγήσει σε συμφόρηση του δικτύου ή μείωση της επίδοσης σε καταστάσεις έκτακτης ανάγκης. Ακόμη, οι κυψελωτές επικοινωνίες είναι πιθανόν ακατάλληλες για εφαρμογές που σχετίζονται με πολλά δεδομένα και απαιτούν πολύ μεγάλο εύρος ζώνης.

3.4 ZIGBEE

Το ZigBee είναι μια τεχνολογία ασύρματης επικοινωνίας η οποία έχει σχετικά χαμηλή κατανάλωση ενέργειας, ρυθμό μετάδοσης δεδομένων, πολυπλοκότητα και κόστος εγκατάστασης. Είναι μια ιδανική τεχνολογία για την επίβλεψη της ενέργειας (energy monitoring), τον οικιακό αυτοματισμό (home automation), και την αυτόματη ανάγνωση των μετρητών (automatic meter reading). Το ZigBee και το ZigBee Smart Energy Profile (SEP), έχουν χαρακτηριστεί ως τα πλέον κατάλληλα πρότυπα επικοινωνίας για το έξυπνο δίκτυο στον τομέα του οικιακού δικτύου. Η επικοινωνία μεταξύ των έξυπνων μετρητών και μεταξύ των έξυπνων συσκευών σε ένα σπίτι, είναι πολύ σημαντικός παράγοντας. Οι ενσωματωμένοι έξυπνοι μετρητές με τεχνολογία ZigBee μπορούν να επικοινωνούν με τις αντίστοιχες συσκευές και να τις ελέγξουν. Το ZigBee SEP παρέχει βοηθητικά προγράμματα για να στείλει μηνύματα προς τους ιδιοκτήτες σπιτιού, τα οποία σε πραγματικό χρόνο τους ενημερώνουν για την κατανάλωση της ενέργειας.

Πλεονεκτήματα: Το ZigBee έχει 16 κανάλια στη ζώνη των 2.4GHz, το καθένα με 5 MHz εύρους ζώνης. Η μέγιστη ισχύς εξόδου είναι 0 dBm (1 mW) με εύρος μετάδοσης μεταξύ 1 και 100 μέτρα, 250 Kb/s ρυθμό μετάδοσης δεδομένων και 00PSK διαμόρφωση. Θεωρείται ως μία καλή επιλογή για τη μέτρηση και την διαχείριση ενέργειας και είναι ιδανικό για εφαρμογές έξυπνων δικτύων, καθώς επιδεικνύει απλότητα, ελαστικότητα, αντοχή, χαμηλές απαιτήσεις εύρους ζώνης, χαμηλό κόστος εγκατάστασης, λειτουργεία μέσα ένα μη αδειοδοτημένο φάσμα και εύκολη υλοποίηση του δικτύου. Ακόμα διαθέτει ένα τυποποιημένο πρωτόκολλο που βασίζεται στο πρότυπο IEEE 802.15.4. Το ZigBee SEP παρουσιάζει ορισμένα πλεονεκτήματα για το φυσικό αέριο, το νερό και την παροχή ηλεκτρικής ενέργειας, όπως ο εύκολος έλεγχος του φορτίου, η μείωση της απόκρισης στη ζήτηση τα προγράμματα τιμολόγησης σε πραγματικό χρόνο, η παρακολούθηση του συστήματος σε πραγματικό χρόνο και η προηγμένη υποστήριξη μέτρησης.

Μειονεκτήματα: υπάρχουν ορισμένοι περιορισμοί σχετικά με το ZigBee για πρακτικές εφαρμογές, όπως η χαμηλή δυνατότητα επεξεργασίας , το μικρό μέγεθος μνήμης, οι μικρές απαιτήσεις καθυστέρησης και οι παρεμβολές από άλλες συσκευές, οι οποίες μοιράζονται τις ίδιες ζώνες με τα IEEE 802.11 ασύρματα τοπικά δίκτυα (WLAN) ΤΟ WIFI, το Bluetooth και τα μικροκύματα. Έτσι οι ανησυχίες για την ευρωστία του ZigBee υπό συνθήκες θορύβου αυξάνουν την πιθανότητα να ‘διεφθαρεί’ όλο το κανάλι επικοινωνίας λόγω της παρεμβολής του 802.11/b/g στην περιοχή του ZigBee. Θα πρέπει να εφαρμοστούν συστήματα ανίχνευσης παρεμβολών, συστήματα αποφυγής παρεμβολών και ενεργειακά αποδοτικά πρωτόκολλα δρομολόγησης, που θα παρατείνουν τον χρόνο ζωής του δικτύου και θα παρέχουν μια αξιόπιστη και ενεργειακά αποδοτική επίδοση του δικτύου[6].

3.5 WIRELESS MESH

Ένα ασύρματο δίκτυο mesh, είναι ένα ευέλικτο δίκτυο που αποτελείται από μια ομάδα κόμβων, με δυνατότητα ένταξης νέων. Κάθε κόμβος μπορεί να λειτουργήσει ως ανεξάρτητος δρομολογητής (rooter). Η ικανότητα ‘αυτοίασης’ είναι χαρακτηριστικό του δικτύου, όπου επιτρέπει στα σήματα επικοινωνίας να βρουν μια άλλη διαδρομή για τον προορισμό τους

μέσω των ενεργών κόμβων, σε περίπτωση κατειλημμένης διαδρομής. Ειδικά στην Βόρεια Αμερική, τα συστήματα που βασίζονται σε RF mesh είναι ιδιαίτερα διαδεδομένα. Σε αυτά τα συστήματα κάθε έξυπνη συσκευή (smart devise) είναι εξοπλισμένη με μια ασύρματη μονάδα, δρομολογώντας τα συλλεγόμενα δεδομένα μέσω των κοντινών μετρητικών συσκευών. Κάθε μετρητής λειτουργεί ως επαναλλήπτης του σήματος μέχρι τα συλλεγόμενα δεδομένα να φτάσουν στο σημείο πρόσβασης του ηλεκτρικού δικτύου. Στη συνέχεια, τα συλλεγόμενα δεδομένα μεταφέρονται στον πάροχο μέσω ενός άλλου συνήθως δικτύου τηλεπικοινωνιών.

Πλεονεκτήματα: η δικτύωση mesh είναι μια οικονομικά αποδοτική λύση με δυναμική αυτοργάνωση και αυτοίαση. Είναι αυτορρυθμιζόμενη, με υψηλής επεκτασιμότητας υπηρεσίες, οι οποίες παρέχουν πολλά πλεονεκτήματα, όπως η βελτίωση της απόδοσης του δικτύου, η εξισορρόπηση του φορτίου στο δίκτυο και η επέκταση της ικανότητας κάλυψης του δικτύου. Η δυνατότητα πολλαπλών βημάτων δρομολόγησης μπορεί να παρέχει ικανοποιητική κάλυψη σε αστικές και ημιαστικές περιοχές. Επίσης, η φύση του mesh δικτύου επιτρέπει στους μετρητές να λειτουργούν ως αναμεταδότες σήματος, κάτι που μπορεί να επεκτείνει την κάλυψη και την χωρητικότητα του δικτύου. Προηγμένες υποδομές μέτρησης (advanced metering infrastructures) και διαχείρισης οικιακής ενέργειας (home energy management), είναι μερικές από τις εφαρμογές όπου η ασύρματη τεχνολογία mesh μπορεί να χρησιμοποιηθεί.

Μειονεκτήματα: η χωρητικότητα του δικτύου, η διακύμανση του πλάτους του σήματος (fading) και οι παρεμβολές, θεωρούνται οι μεγάλες προκλήσεις των ασυρμάτων mesh συστημάτων. Στις αστικές περιοχές τα δίκτυα αυτά έχουν να αντιμετωπίσουν το ότι οι μετρητές δεν μπορούν να παράσχουν πλήρη κάλυψη επικοινωνίας. Από οικονομικής πλευράς η τοποθέτηση μετρητών σε όλους τους κόμβους που απαιτούνται για την ισορρόπηση της αξιοπιστίας και της ευέλικτης δρομολόγησης είναι ένα σημαντικό μειονέκτημα. Επιπλέον ένας τρίτος φορέας απαιτείται για τη διαχείριση του δικτύου, και εφόσον οι πληροφορίες μέτρησης περνούν από κάθε σημείο πρόσβασης, είναι αναγκαία η εφαρμογή τεχνικών κρυπτογράφησης στα δεδομένα για λόγους ασφαλείας. Ακόμα αφού τα πακέτα δεδομένων ταξιδεύουν γύρω από πολλούς κόμβους, μπορεί να υπάρξουν προβλήματα στο βρόχο, κάτι που θα οδηγήσει σε μείωση του διαθέσιμου εύρους ζώνης[6].

3.6 ΔΟΡΥΦΟΡΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ

Οι δορυφορικές επικοινωνίες μας παρέχουν την δυνατότητα του απομακρυσμένου ελέγχου και παρακολούθησης. Οι δορυφόροι έχουν την μοναδική ικανότητα να παρέχουν κάλυψη μεγάλων γεωγραφικών περιοχών, να διασυνδέουν μακρινούς τηλεπικοινωνιακούς κόμβους και αποτελούν σήμερα αναπόσπαστο τμήμα των περισσότερων τηλεπικοινωνιακών συστημάτων.

Σε ορισμένα σενάρια όπου δεν υπάρχει υποδομή επικοινωνίας, ιδιαίτερα σε απομακρυσμένους υποσταθμούς και παραγωγή, οι δορυφορικές επικοινωνίες είναι μια οικονομικά αποδοτική λύση. Τέτοιου είδους επικοινωνία μπορεί εύκολα να εγκατασταθεί και απαιτεί μόνο την απόκτηση του απαραίτητου εξοπλισμού δορυφορικής επικοινωνίας. Εδώ ας σημειωθεί ότι ορισμένες επιχειρήσεις κοινής ωφέλειας έχουν ήδη εγκαταστήσει τέτοιον εξοπλισμό για την παρακολούθηση των αγροτικών υποσταθμών.

Επιπλέον, μια αποκλειστικά επίγεια αρχιτεκτονική είναι ευάλωτη σε καταστροφές ή βλάβες του συστήματος επικοινωνίας. Κατά συνέπεια, προκειμένου να εξασφαλιστεί η ασφαλής

λειτουργία και η παράδοση της κρίσιμης κίνησης δεδομένων σε περιπτώσεις καταστροφών ή βλαβών του επίγειου συστήματος επικοινωνιών, οι δορυφόροι μπορούν να χρησιμοποιηθούν ως εφεδρικό σύστημα για τα υπάρχοντα δίκτυα επικοινωνιών.
Ωστόσο, θα πρέπει να σημειωθούν και τα μειονεκτήματα των δορυφορικών επικοινωνιών, καθώς υπάρχουν δυο σημαντικές αδυναμίες. Πρώτον, ένα δορυφορικό σύστημα επικοινωνίας έχει σημαντικά υψηλότερη καθυστέρηση από αυτή ενός επίγειου συστήματος. Δεύτερον, τα χαρακτηριστικά ενός δορυφορικού καναλιού ποικίλλουν ανάλογα με την επίδραση της εξασθένησης και τις καιρικές συνθήκες. Αυτή η ιδιότητα μπορεί να μειώσει σε μεγάλο βαθμό την επίδοση ολόκληρου του συστήματος επικοινωνίας

3.7 BLUETOOTH

Το Bluetooth είναι πρότυπο για ασύρματα προσωπικά δίκτυα υπολογιστών (Wireless Personal Area Networks, WPAN). Πρόκειται για μια ασύρματη τηλεπικοινωνιακή τεχνολογία μικρών αποστάσεων, η οποία μπορεί να μεταδώσει σήματα μέσω μικροκυμάτων σε ψηφιακές συσκευές και να προσφέρει κάλυψη από 1-100 m. Το Bluetooth λειτουργεί στο «αδέσμευτο» φάσμα συχνοτήτων των 2.4 GHz, ώστε οι συσκευές που το ενσωματώνουν να μπορούν να λειτουργήσουν απροβλημάτιστα σε οποιοδήποτε σημείο του πλανήτη. Για να περιοριστούν στο ελάχιστο οι παρεμβολές από παρεμφερείς συσκευές, το Bluetooth εκμεταλλεύεται την αμφίδρομη επικοινωνία και τη μέθοδο μετάδοσης με διασπορά φάσματος Frequency Hopping (έως και 1600 εναλλαγές συχνότητας ανά δευτερόλεπτο). Από φυσική άποψη επίσης το Bluetooth λειτουργεί περίπου στα 2.4 GHz, προδιαγράφει τρία επίπεδα ισχύος της εκπομπής από τα οποία εξαρτάται και η εμβέλεια επικοινωνίας, ενώ η τακτική αλλαγή της συχνότητας εκπομπής λόγω της αξιοποίησης του FHSS καθορίζεται ψευδοτυχαία από έναν κεντρικό κόμβο, τον Master.

Το Bluetooth επιτρέπει τις απευθείας συνδέσεις από συσκευή προς συσκευή (point to point) όσο και από μία συσκευή σε πολλές. Μπορεί να χρησιμοποιηθεί για τοπικές, online εφαρμογές απεικόνισης ως μέρος των συστημάτων αυτοματισμού.

Οι συσκευές αυτές επηρεάζονται πολύ από τριγύρω επικοινωνιακές ζεύξεις και μπορεί να παρεμβάλουν με τα, βασισμένα στο IEEE 802.11, ασύρματα LAN δίκτυα. Γενικά, το Bluetooth προσφέρει ασθενή ασφάλεια συγκριτικά με άλλα πρότυπα.

3.8 ΕΠΙΚΟΙΝΩΝΙΑ ΓΡΑΜΜΗΣ ΡΕΥΜΑΤΟΣ (PLC)

Η τεχνολογία PLC είναι μια παλιά ιδέα και χρονολογείται από τις αρχές του 1900. Το PLC είναι μια τεχνολογία που χρησιμοποιεί τις ηλεκτρικές γραμμές μεταφοράς ως επικοινωνιακό μέσο ώστε να παρέχει ένα δίκτυο επικοινωνιών όπως στο διαδίκτυο αλλά ταυτόχρονα υποστηρίζει τις υπηρεσίες που σχετίζονται με την διανομή ενέργειας π.χ έλεγχο φορτίου και απομακρυσμένη ανάγνωση μετρητών. Το πρότυπο στενής ζώνης PLC χρησιμοποιεί τη φασματική ζώνη 1-500 KHz παρέχοντας ρυθμούς δεδομένων μέχρι 1 Mbps με μέγιστο μήκος μετάδοσης 1.5 km. Η τεχνολογία PLC είναι από τις επικρατέστερες για τη σύνδεση μετρητών και συγκεντρωτών στο δίκτυο ΧΤ, ενώ είναι δυνατή και η δικτύωση μεταξύ οικιακών ευφυών συσκευών.

Πλεονεκτήματα: Μεγάλο πλεονέκτημα είναι η ύπαρξη των καλωδίων ισχύος (φυσικό στρώμα), που εξοικονομούν για τις εταιρίες ηλεκτρισμού το κόστος εγκατάστασης τηλεπικοινωνιακής υποδομής. Επίσης, παρέχεται μεγάλη γεωγραφική κάλυψη. Η διαμόρφωση ενός δικτύου PLC στο δίκτυο πρόσβασης απαλλάσσει τις εταιρίες ηλεκτρισμού από το κόστος ενοικίασης και χρήσης δικτυακού εξοπλισμού και της εξάρτησης από διαχειριστές δικτύων επικοινωνιών.

Μειονεκτήματα: Το καλώδιο ισχύος είναι έντονα θορυβώδες μέσο, που εισάγει μεγάλη εξασθένηση και παραμόρφωση. Παράλληλα, η παρεμβολή είναι ανάλογη του αριθμού των μετρητών που είναι συνδεδεμένοι σε ένα τοπικό δίκτυο. Για τους ανωτέρω λόγους, είναι αναγκαία η χρήση επαναληπτών για την επικοινωνία σε αποστάσεις μεγαλύτερες του ενός χιλιομέτρου, γεγονός που αυξάνει το κόστος υλοποίησης του δικτύου πρόσβασης. Επιπλέον, λόγω της τοπολογίας διαύλου που χαρακτηρίζει το δίκτυο ΧΤ και του θορυβώδους καλωδίου ισχύος, η αποστολή δεδομένων είναι ευαίσθητη σε πτώση τάσης, δεν προσφέρεται εναλλακτική δρομολόγηση δεδομένων, ενώ με δυσκολία μπορούν να επιτευχθούν υψηλοί ρυθμοί δεδομένων[6].

3.9 ΨΗΦΙΑΚΗ ΣΥΝΔΡΟΜΗΤΙΚΗ ΓΡΑΜΜΗ (DSL)

Digital subscriber lines (DSLs) είναι μια ψηφιακή τεχνολογία μετάδοσης δεδομένων υψηλής ταχύτητας που χρησιμοποιεί τα καλώδια του τηλεφωνικό δικτύου. Η ήδη υπάρχουσα υποδομή των γραμμών DSL μειώνει το κόστος εγκατάστασης. Συνεπώς πολλές εταιρίες επέλεξαν την τεχνολογία DSL για την ανάπτυξη των έξυπνων δικτύων τους. Ο όμιλος Smart Grid Solution Company, συνεργάστηκε με την εταιρία Qwest για να υλοποιήσει ένα σχέδιο για smart grid. Το υπάρχον χαμηλού λανθάνον χρόνου, ασφαλές και υψηλής χωρητικότητας δίκτυο DSL της Qwest θα χρησιμοποιηθεί για την μετάδοση δεδομένων. Η απόδοση της σύνδεσης εξαρτάται από το πόσο μακριά είναι ο συνδρομητής από το τηλεφωνικό κέντρο που τον εξυπηρετεί, κάτι που καθιστά δύσκολο να χαρακτηρίσει κανείς την απόδοση της τεχνολογίας.

Πλεονεκτήματα: η μεγάλη διαθεσιμότητα, το χαμηλό κόστος και το υψηλό εύρος ζώνης μετάδοσης δεδομένων είναι οι πιο σημαντικοί λόγοι για να καταστεί η τεχνολογία DSL υποψήφια από τις εταιρίες παροχής ενέργειας για την ανάπτυξη του smart grid και τις εφαρμογές λήψης και αποστολής δεδομένων.

Μειονεκτήματα: η αξιοπιστία και ο πιθανός κορεσμός της τεχνολογίας μπορεί να μην είναι αποδεκτά για ορισμένες κρίσιμες εφαρμογές. Η εξάρτηση από την απόσταση και η έλλειψη τυποποίησης μπορεί να προκαλέσουν πρόσθετα προβλήματα. Τα ενσύρματα συστήματα επικοινωνιών με βάση το DSL απαιτούν την εγκατάσταση και τη συντήρηση καλωδίων, που σημαίνει ότι δεν μπορούν να υλοποιηθούν σε αγροτικές περιοχές λόγω του υψηλού κόστους για την εγκατάσταση υποδομών σε αραιοκατοικημένες περιοχές[6].

ΚΕΦΑΛΑΙΟ 4

ΠΡΩΤΟΚΟΛΛΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

4.1 Πρωτοκολλα επικοινωνιας του διαδικτυου

Τα πρωτόκολλα επικοινωνίας του διαδικτύου χωρίζονται σε πέντε επίπεδα, καθένα από τα οποία είναι υπεύθυνο για την υλοποίηση μιας συγκεκριμένης λειτουργίας και την απόκρυψη των λεπτομερειών υλοποίησης από τα πρωτόκολλα των ανώτερων πεδίων. Στη συνέχεια για κάθε επίπεδο αναφέρονται τα πλέον διαδεδομένα πρωτόκολλα.

4.1.1 Πρωτοκολλα φυσικου στρωματος

Τα πρωτόκολλα φυσικού στρώματος είναι υπεύθυνα για την τηλεπικοινωνιακή σύνδεση δύο κόμβων προκειμένου να γίνει ανταλλαγή δεδομένων. Στα πρωτόκολλα αυτά καθορίζονται τα εξής:

1. Το φυσικό μέσο επικοινωνίας.
2. Το φάσμα συχνοτήτων που χρησιμοποιείται.
3. Τα σχήματα διαμόρφωσης και κωδικοποίησης FEC (Forward Error Correction) που χρησιμοποιούνται.
4. Οι μέθοδοι πολλαπλής πρόσβασης και ελέγχου συγκρούσεων.

Το κατάλληλο πρωτόκολλο φυσικού στρώματος επιλέγεται με κριτήριο τις προδιαγραφές των διατάξεων που επικοινωνούν και τα φυσικά μέσα επικοινωνίας που είναι διαθέσιμα. Τα πλέον διαδεδομένα πρωτόκολλα είναι τα εξής[39]:

- **IEEE 802.3**: Είναι το παραδοσιακό πρωτόκολλο σύνδεσης μέσω καλωδίων συνεστραμμένων ζευγών που υιοθετείται στην περίπτωση των ενσύρματων τοπικών δικτύων. Το πρωτόκολλο εξελίσσεται συνεχώς και σήμερα υποστηρίζει ταχύτητες μετάδοσης μέχρι 10 Gbps σε αποστάσεις μέχρι 100m από το πρότυπο 10GBASE-T. Στην ίδια οικογένεια προτύπων ανήκουν και τα πρωτόκολλα επικοινωνίας μέσω καλωδίων οπτικών ινών. Με τη χρήση του πρωτοκόλλου οπτικών ινών 10GBASE- PR αυξάνεται η μέγιστη απόσταση επικοινωνίας στα 20km, επιτρέποντας τη σύνδεση κόμβων σε μεγάλες αποστάσεις με πολύ υψηλούς ρυθμούς μετάδοσης.
  Το πρωτόκολλο αυτό συναντάται πολύ συχνά στα εταιρικά πληροφοριακά δίκτυα του διαχειριστή του δικτύου ΗΕ και των προμηθευτών ΗΕ. Ακόμη, εμφανίζεται και σε βιομηχανικά πληροφοριακά δίκτυα.
- **IEEE 802.11:** Η οικογένεια πρωτοκόλλων 802.11 αφορά το ευρύτατα γνωστό και χρησιμοποιούμενο Wi-Fi που επιτρέπει τη λειτουργία ασφαλών ασύρματων τοπικών δικτύων. Αυτή τη στιγμή το πρωτόκολλο λειτουργεί με ρυθμούς μετάδοσης μέχρι 1 Gbps, αναμένεται, ωστόσο, να φθάσει σύντομα τα 7 Gbps

- **IEEE1901:** Αφορά τη χρήση των γραμμών μεταφοράς ηλεκτρικής ενέργειας για τη μετάδοση τηλεπικοινωνιακών σημάτων. Αξιοποιεί τμήματα του φάσματος στη ζώνη συχνοτήτων 1-100 MHz και επιτυγχάνει ταχύτητες μετάδοσης μέχρι 500 Mbps.
- **IEEE 802.15.4:** Το συγκεκριμένο πρότυπο αφορά ασύρματη επικοινωνία χαμηλού ρυθμού μετάδοσης. Χαρακτηρίζεται από τις μικρές ενεργειακές του ανάγκες και επιτρέπει τη μετάδοση πληροφορίας με ρυθμό μέχρι 250 Kbps σε μέγιστη απόσταση 10m.

4.1.2 Πρωτοκολλα ζευξησ δεδομενων

Τα πρωτόκολλα του στρώματος μεταφοράς είναι αρμόδια για τη λογική σύνδεση μεταξύ γειτονικών κόμβων ενός τοπικού δικτύου. Το καθολικά χρησιμοποιούμενο πρωτόκολλο στρώματος μεταφοράς είναι το Ethernet ή IEEE 802.3. Η διευθυνσιοδότηση των κόμβων γίνεται μέσω των διευθύνσεων MAC που διαθέτει κάθε συσκευή δικτύου.

4.1.3 Πρωτοκολλα στρωματοσ δικτυου

Τα πρωτόκολλα του στρώματος αυτού είναι υπεύθυνα για την υποστήριξη της επικοινωνίας μεταξύ διαφορετικών δικτύων. Στο στρώμα αυτό χρησιμοποιούνται διάφορα πρωτόκολλα για να επιτελούν αντίστοιχες λειτουργίες, τα σημαντικότερα των οποίων είναι τα εξής:

- **Internet Protocol** (**IP**): Το πρωτόκολλο IP αποτελεί το κύριο πρωτόκολλο επικοινωνίας για τη μετάδοση πακέτων δεδομένων. Το Πρωτόκολλο IP είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων ανάμεσα στα διάφορα δίκτυα, ανεξάρτητα από την υποδομή τους, και αποτελεί το κύριο πρωτόκολλο πάνω στο οποίο είναι βασισμένο το διαδίκτυο. Καθορίζει τη μορφή των πακέτων που στέλνονται μέσω ενός διαδικτύου, καθώς και τους μηχανισμούς που χρησιμοποιούνται για την προώθηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό μέσω ενός ή περισσότερων δρομολογητών. Γι' αυτούς τους σκοπούς, το πρωτόκολλο IP, χρησιμοποιεί συγκεκριμένες μεθόδους διευθυνσιοδότησης και δομές για την ενθυλάκωση των πακέτων δεδομένων. Η πρώτη μεγάλης κλίμακας έκδοση του Πρωτοκόλλου IP, ήταν η έκδοση 4 (IPv4) η οποία επικρατεί μέχρι και σήμερα σε όλο το Διαδίκτυο. Ωστόσο, λόγω του ότι δεν επαρκούν πλέον οι διευθύνσεις, τα τελευταία χρόνια, έχει αναπτυχθεί η διάδοχη έκδοση του πρωτοκόλλου, η έκδοση 6 (IPv6), η οποία είναι εν ενεργεία και χρησιμοποιείται εξαπλωνόμενη σε όλο τον κόσμο.
- **Internet Control Message Protocol (ICMP)**: Το πρωτόκολλο ICMP λειτουργεί σε όλα τα ενδιάμεσα κι όλα τα συστήματα-προορισμούς που χρησιμοποιούν το πρωτόκολλο IP. Το ICMP χρησιμοποιείται για την αναφορά προβλημάτων κατά την παράδοση IP datagrams μέσα σε ένα δίκτυο IP. Χρησιμοποιείται ώστε να δείχνει πότε ένα σύστημα-προορισμός δεν αποκρίνεται, πότε δεν υπάρχει πρόσβαση σε ένα IP δίκτυο, πότε ένας κόμβος παρουσιάζει συμφόρηση, κ.λ.π. Αποσκοπεί επίσης, για να διαπιστωθεί η σωστή λειτουργία των συστημάτων- προορισμών και για να ελεγχθεί κατά πόσο οι δρομολογητές κατευθύνουν σωστά τα πακέτα προς την διεύθυνση προορισμού.

- **Address Resolution Protocol (ARP)**: Το πρωτόκολλο ARP χρησιμοποιείται για να βρεθεί μια διεύθυνση του επιπέδου ζεύξης δεδομένων ενός host με βάση μια διεύθυνση του επιπέδου δικτύου. Αυτό που κάνει στην πραγματικότητα είναι να αντιστοιχίζει μια MAC διεύθυνση σε μια IP διεύθυνση. Η επίλυση διευθύνσεων που πραγματοποιεί το πρωτόκολλο ARP, λαμβάνει χώρα μέσα στα όρια ενός τοπικού δικτύου. Μεταξύ των τοπικών δικτύων εφαρμόζονται αλγόριθμοι δρομολόγησης. Δηλαδή, το πακέτο δρομολογείται προς τον κόμβο που υποδεικνύουν οι πίνακες δρομολόγησης.

4.1.4 Πρωτοκολλο στρωματος μεταφορας

Τα πρωτόκολλα του στρώματος μεταφοράς είναι υπεύθυνα για τη διαχείριση της από άκρο σε άκρο σύνδεσης δύο συσκευών, παρακάμπτοντας τις ανομοιογένειες των δικτύων μέσω των οποίων γίνεται η μεταφορά πακέτων. Τα πρωτόκολλα που χρησιμοποιούνται για το σκοπό αυτό είναι τα εξής:

- **Πρωτόκολλο TCP:** Το πρωτόκολλο TCP είναι ένα αξιόπιστο πρωτόκολλο σύνδεσης το οποίο οργανώνει το εισερχόμενο μήνυμα σε διακριτικά μηνύματα και το περνά στο επίπεδο του διαδικτύου. Κατά τη λήψη γίνεται συναρμολόγηση του μηνύματος για να παραδοθεί στο επόμενο επίπεδο. Ταυτόχρονα το πρωτόκολλο TCP αποστέλλει επιβεβαίωση στον αποστολέα.
- **Πρωτόκολλο UDP:** Το πρωτόκολλο UDP είναι ένα πρωτόκολλο χωρίς επιβεβαίωση προς τον αποστολέα. Έτσι το πρωτόκολλο UDP χρησιμοποιείται όταν επιζητούμε πολύ ταχύτερη αποστολή δεδομένων, έστω και χωρίς αυστηρή επιβεβαίωση και χρησιμοποιείται κυρίως σε περιπτώσεις μετάδοσης πακέτων φωνής και video.

4.1.5 Πρωτοκολλο στρωματος εφαρμογης

Στο υψηλότερο επίπεδο της στοίβας πρωτοκόλλων του Διαδικτύου συγκαταλέγονται τα συγκεκριμένα πρωτόκολλα που ορίζονται από κάθε εφαρμογή που χρησιμοποιείται στο Διαδίκτυο. Οι συχνότερα χρησιμοποιούμενες εφαρμογές είναι οι εξής:

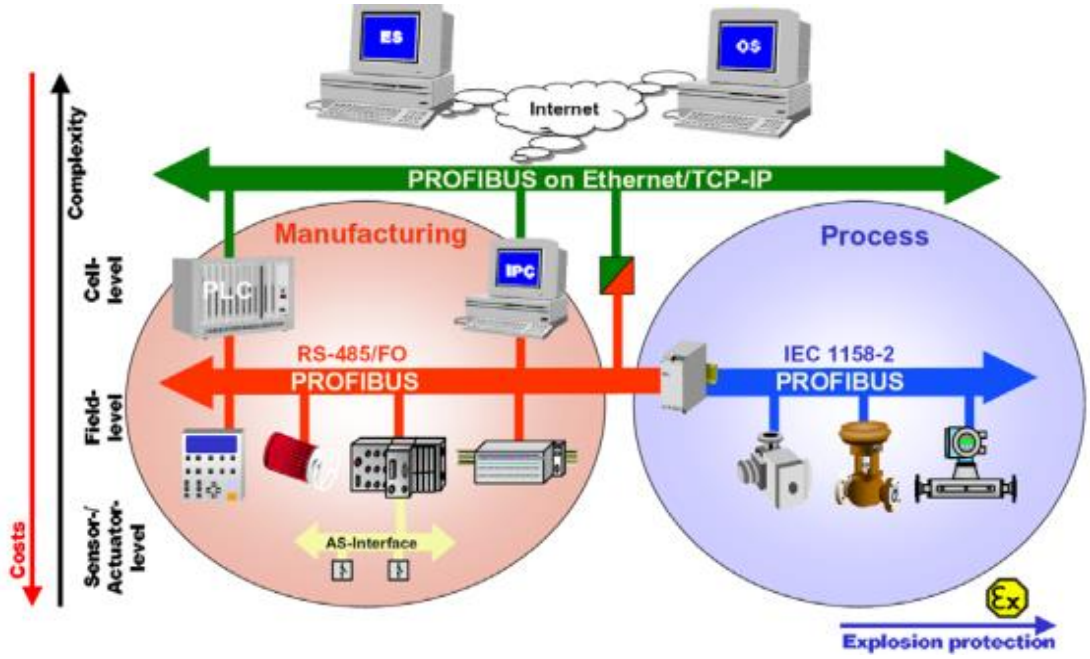
- **Telnet:** Με το πρωτόκολλο δίνεται η δυνατότητα σε κάποιον χρήστη να συνδεθεί με μία απομακρυσμένη μηχανή.
- **FTP:** το πρωτόκολλο μεταφοράς αρχείων παρέχει την δυνατότητα εύκολης μεταφοράς αρχείων από μία μηχανή σε μία άλλη.
- **HTTP**: Είναι πρωτόκολλο το οποίο χρησιμοποιεί το World Wide Wed.
- **DHCP**: Είναι υπεύθυνο για τη δυναμική απόδοση IP διευθύνσεων σε συσκευές που συνδέονται στο τοπικό δίκτυο για το οποίο είναι υπεύθυνη η συσκευή που υλοποιεί τη συγκεκριμένη υπηρεσία.
- **DNS:** Το πρωτόκολλο DNS είναι υπεύθυνο για την αντιστοίχιση των ονομάτων των ιστοσελίδων με τις διευθύνσεις IP των διακομιστών τους.

4.2 ΠΡΩΤΟΚΟΛΛΑ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΚΤΥΩΝ

Παραδοσιακά, τα βιομηχανικά πληροφοριακά δίκτυα επικοινωνούν μέσω σειριακών διαύλων επικοινωνίας. Τα τελευταία χρόνια, ωστόσο, έχουν αναπτυχθεί παραλλαγές των πρωτοκόλλων βιομηχανικών πληροφοριακών δικτύων ώστε να είναι δυνατή η επικοινωνία των διατάξεων χρησιμοποιώντας τα πρωτόκολλα TCP/IP και το Ethernet. Τα βιομηχανικά πρωτόκολλα επικοινωνίας τα οποία, χρησιμοποιούνται συχνότερα στα βιομηχανικά πληροφοριακά δίκτυα είναι τα πρωτόκολλα Modbus, DNP3, OPC και Profibus.

4.2.1 Πρωτοκολλο PROFIBUS

Το πρωτόκολλο PROFIBUS(Process Field Bus) είναι ένα πρότυπο για την επικοινωνία συστημάτων διαύλου πεδίου, σε εφαρμογές αυτοματισμού. Το 1986 στη Γερμανία, 21 εταιρείες και ινστιτούτα συνεργάστηκαν με σκοπό να υλοποιήσουν και να διαδώσουν τη χρήση του σειριακού διαύλου πεδίου, το οποίο θα ήταν βασισμένο στις απαιτήσεις των διεπαφών των συσκευών πεδίου. Η προώθησή του ξεκίνησε το 1989 από το Γερμανικό οργανισμό BMBF και έπειτα χρησιμοποιήθηκε από τη Siemens. Σήμερα παγκοσμίως φθάνει να χρησιμοποιείται σε 43.8 εκατομμύρια συσκευές, εκ των οποίων πάνω από 7.5 εκατομμύρια είναι στη βιομηχανία[65].



Εικόνα 4.1 : Αρχιτεκτονική δικτύου Profibus

Χαρακτηριστικά πρωτοκόλλου[65]:

- Μέσω ενός διαύλου, το PROFIBUS συνδέει συστήματα ελέγχου με αποκεντρωμένες συσκευές πεδίου (αισθητήρες, ενεργοποιητές κ.α.) και επίσης επιτρέπει τη συνεχή ανταλλαγή δεδομένων με συστήματα επικοινωνίας που βρίσκονται υψηλότερα στη διαβάθμιση.

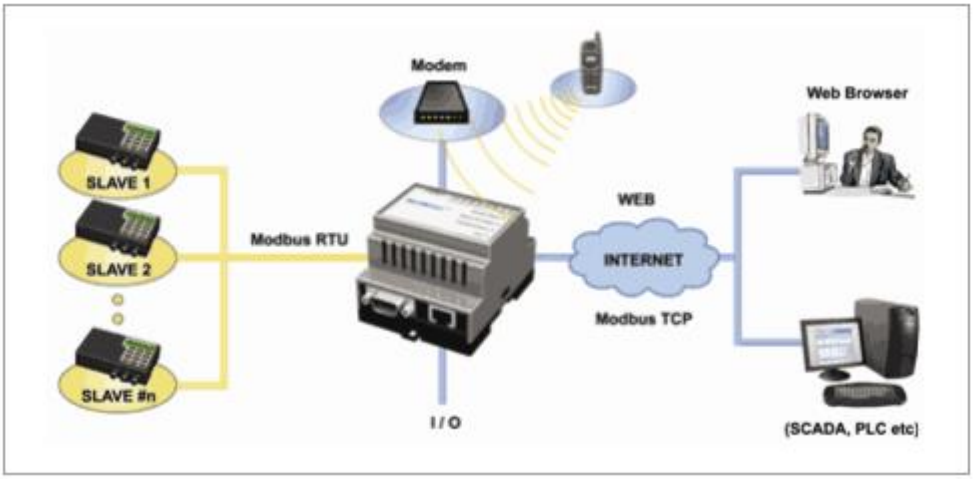
- Είναι βελτιστοποιημένο για κατανεμημένες εφαρμογές εισόδου-εξόδου. Μέχρι 126 τέτοιες συσκευές μπορούν να συνδεθούν σε ένα δίκτυο. Από τη στιγμή που κάθε τέτοια συσκευή μπορεί να ελέγχει εκατοντάδες συνδέσεις σημείων, το PROFIBUS παρέχει ένα πολύ μεγάλο αριθμό πιθανών συνδέσεων για κάθε ελεγκτή.

- Χωρίζεται σε δυο μοντέλα το PROFIBUS DP(Decentralized Periphery) και το PROFIBUS PA(Process Automation). Το μεν πρώτο χρησιμοποιείται κυρίως για συσκευές εισόδου/εξόδου υψηλών ταχυτήτων. Μπορεί να χρησιμοποιεί διαφορετικά φυσικά στρώματα όπως RS485, ασύρματη επικοινωνία ή οπτική ίνα. Το δε δεύτερο αναφέρεται σε λειτουργίες όπως: δίαυλο που χρησιμοποιεί το φυσικό στρώμα MBP(Manchester encoded Bus Powered) σύμφωνα με το πρότυπο IEC 61158-2, ρύθμιση κάποια συσκευής μέσω διαύλου και ασφαλή σχεδιασμό

- Επίσης η αρχιτεκτονική που χρησιμοποιείται για την επικοινωνία μεταξύ των συσκευών είναι τύπου master/slave. Οι master συσκευές καλούνται ενεργοί σταθμοί και χαρακτηριστικές τέτοιες συσκευές είναι τα PLC (Programmable Logic Controler), CNC (Compare Numerical Controler) και ελεγκτές κυττάρων. Οι slave συσκευές καλούνται παθητικοί σταθμοί στο πρωτόκολλο PROFIBUS και χαρακτηριστικές συσκευές είναι οι αισθητήρες, ενεργοποιητές και συσκευές αποστολής μηνυμάτων.

4.2.2 Πρωτοκολλο Modbus

Το πρωτόκολλο Modbus είναι ένα σειριακό πρωτόκολλο επικοινωνίας που εκδόθηκε από την εταιρεία Modicon(σημερινή Schneider Electric) το 1979, βασισμένο στην αρχιτεκτονική master/slave, για να χρησιμοποιηθεί σε προγραμματιζόμενους λογικούς ελεγκτές (PLCprogrammable logic controllers). Λόγω της απλότητας και της αξιοπιστίας που το διακρίνει, έχει γίνει ένα πρότυπο επικοινωνίας που χρησιμοποιείται αρκετά συχνά για να συνδέσει βιομηχανικές ηλεκτρονικές συσκευές. Η επικοινωνία μεταξύ των κόμβων γίνεται μέσω μηνυμάτων, όπου υπάρχει ανοιχτό πρότυπο που περιγράφει τη δομή τους. Αρχικά, η διεπαφή του πρωτοκόλλου έτρεχε σε καλώδιο RS-232, αλλά αργότερα χρησιμοποιήθηκε RS-485 γιατί επιτρέπει την επικοινωνία σε μεγαλύτερες αποστάσεις και μπορεί να υποστηρίξει υψηλότερες ταχύτητες. Επίσης, το Modbus είναι ένα ευέλικτο πρότυπο που επιτρέπει την επικοινωνία μεταξύ πολλών συσκευών που είναι συνδεδεμένες στο ίδιο δίκτυο, για παράδειγμα ένας μετεωρολογικός σταθμός που μετράει θερμοκρασία, ταχύτητα αέρα, υγρασία κτλ. και δίνει τα αποτελέσματα σε έναν Η/Υ. Ανάλογα με το ποιο πρωτόκολλο Modbus χρησιμοποιείται, η επικοινωνία μπορεί να είναι είτε απλή είτε από άκρη σε άκρη(peer to peer). Οι διαφορές μεταξύ των εκδόσεων του πρωτοκόλλου είναι στην κωδικοποίηση των μηνυμάτων, στο μήκος του καλωδίου που τρέχει πάνω το εκάστοτε πρωτόκολλο και στον αριθμό των συσκευών που μπορούν να συνδεθούν στο ίδιο δίκτυο [65].

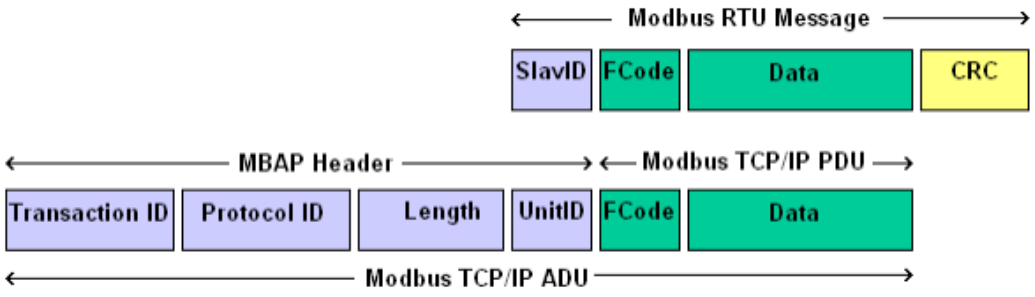


Εικόνα 4.2: Αρχιτεκτονική πρωτοκόλλου Modbus

4.2.2.1 Πρωτοκολλο Modbus TCP/IP

Το Modbus TCP/IP(Transmission Control Protocol and Internet Protocol) είναι το πρωτόκολλο Modbus RTU συνοδευόμενο από μια TCP διεπαφή, η οποία τρέχει πάνω σε Ethernet. Όταν στέλνονται πληροφορίες, χρησιμοποιώντας αυτά τα δυο πρωτόκολλα, τα δεδομένα περνάνε στο TCP όπου προσαρτώνται επιπλέον πληροφορίες και έπειτα δίνονται στο IP. Εκεί, τα δεδομένα τοποθετούνται σε πακέτα και εκπέμπονται. Η δομή του μηνύματος του Modbus είναι η εφαρμογή του πρωτοκόλλου που καθορίζει τους κανόνες για οργάνωση και ερμηνεία των δεδομένων, ανεξάρτητα από τα δεδομένα του μέσου μετάδοσης. Το TCP/IP αναφέρεται στο πρωτόκολλο ελέγχου μεταδόσεων και διαδικτύου, που παρέχει το μέσο μετάδοσης για το μήνυμα του Modbus TCP/IP. Επιτρέπει δηλαδή, την ανταλλαγή πακέτων δυαδικών δεδομένων μεταξύ υπολογιστών, χωρίς να καθορίζει τι σημαίνουν αυτά τα δεδομένα ή πώς ερμηνεύονται (στη συγκεκριμένη περίπτωση, αυτό αποτελεί δουλειά του Modbus). Η πρωταρχική λειτουργία του TCP είναι να διασφαλίσει ότι όλα τα πακέτα δεδομένων λαμβάνονται σωστά, και παράλληλα το IP διασφαλίζει ότι τα μηνύματα διευθυνσιοδοτούνται και δρομολογούνται κατάλληλα[65].

Το Modbus TCP ενσωματώνει ένα παράθυρο δεδομένων του προτύπου RTU σε ένα παράθυρο TCP, όπως φαίνεται στο παρακάτω σχήμα:



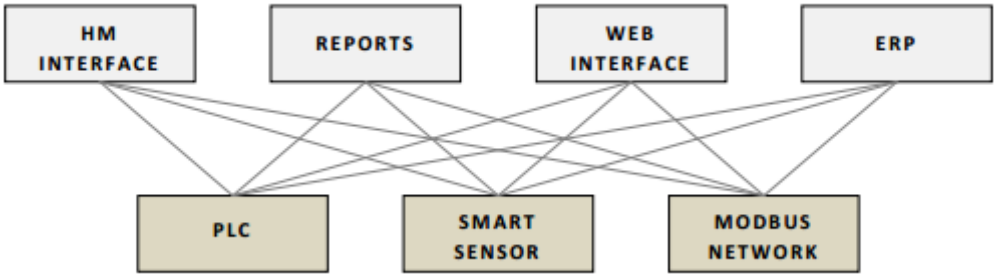
Σχήμα 4.3 : Απεικόνιση μηνύματος Modbus RTU μέσα σε TCP/IP

Οι Modbus εντολές και τα δεδομένα του χρήστη, ενσωματώνονται στο πακέτο του TCP/IP χωρίς να τροποποιούνται. Όπως φαίνεται και από το παραπάνω σχήμα, το πεδίο για τον έλεγχο σφαλμάτων(CRC), στο πρότυπο RTU, δε χρησιμοποιείται, καθώς στο πρότυπο Ethernet TCP/IP υπάρχουν άλλες μέθοδοι για τον έλεγχο σφαλμάτων που εγγυόνται την ακεραιότητα των δεδομένων. Επιπλέον, το πεδίο διευθύνσεων του παραθύρου Modbus (SlavID) αντικαταστάθηκε από το αναγνωριστικό μονάδας (UnitID) και έγινε μέρος της επικεφαλίδας MBAP (Modbus Application Protocol header). Η επικεφαλίδα MBAP αποτελείται από 7 bytes και τοποθετείται στην αρχή του μηνύματος. Περιλαμβάνει τα 4 πρώτα πεδία από τον παρακάτω πίνακα:

Όνομα	**Μήκος(bytes)**	**Λειτουργία**
Αναγνωριστικό συναλλαγής	2	Για τον συγχρονισμό μεταξύ μηνυμάτων πελάτη/εξυπηρετητή
Αναγνωριστικό πρωτοκόλλου	2	Μηδέν για το Modbus TCP/IP πρωτόκολλο
Μήκος πεδίου	2	Αριθμός bytes που απομένουν στο πλαίσιο
Αναγνωριστικό συσκευής	1	Διεύθυνση slave συσκευής
Συνάρτηση	1	Δείχνει τον κωδικό της συνάρτησης όπως διάβασμα εισόδου, καταχωρητών κτλ.
Δεδομένα	n	Δεδομένα είτε ως απάντηση σε μια ερώτηση, είτε ως εντολή

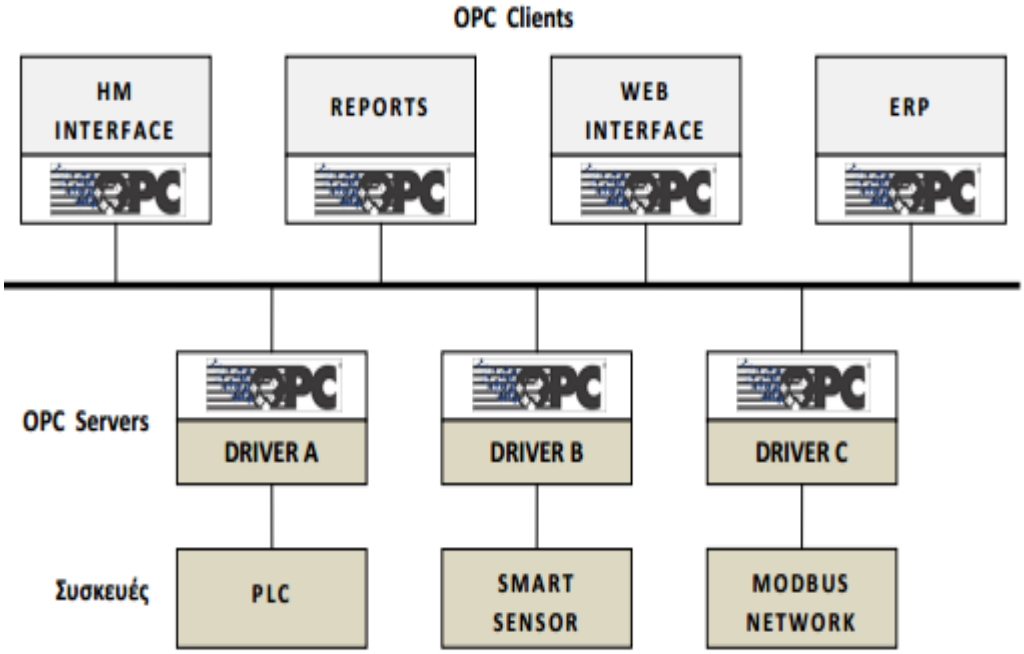
4.2.3 Πρωτοκολλο OPC

Τα συστήματα SCADA δε θα γνώριζαν την ανάπτυξη που υπάρχει σήμερα, αν πρώτα δεν είχε αναπτυχθεί η δυνατότητα δικτύωσης και επικοινωνίας μεγάλης κλίμακας συσκευών (PLC, RTU, DCS). Η εγκατάσταση διαφορετικών λογισμικών προκειμένου ελεγχθούν διαφορετικά είδη συσκευών απαιτούσε περισσότερο κόπο, κόστος και χρόνο. Αυτό σήμαινε ότι οποιαδήποτε software εφαρμογή (όπως και οι εφαρμογές SCADA) ήταν άμεσα εξαρτημένες από τον κατασκευαστή και τον τύπο του υλικού. Κάτι τέτοιο έθετε περιορισμούς και έβαζε εμπόδια στις δυνατότητες σχεδίασης και λειτουργίας του συνολικού συστήματος. Λύση σε



Εικόνα 4.4 : Πρωτόκολλο OPC

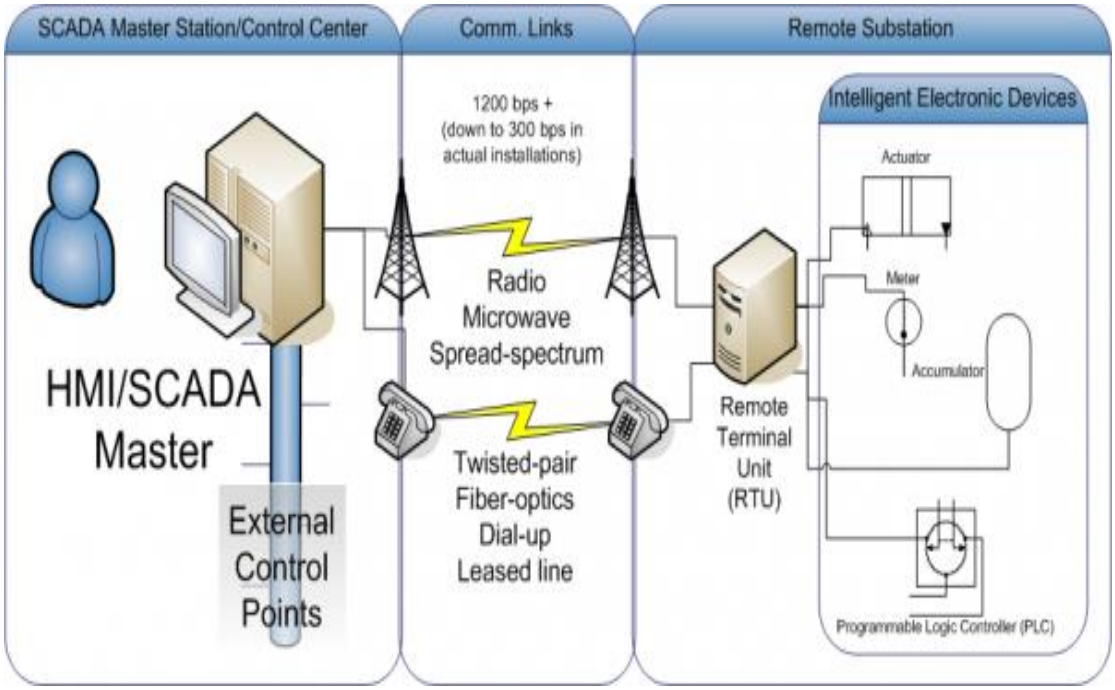
αυτό το πρόβλημα δίνει η τεχνολογία OPC, OLE for Process Control ή Open Process Control. Το OPC είναι ουσιαστικά ένα πρότυπο που επιτρέπει ανταλλαγές δεδομένων υλικού/λογισμικού ανεξάρτητα από τον τύπο του κατασκευαστή. Το πρότυπο OPC υπήρξε για τα βιομηχανικά δίκτυα, ότι και τα drivers ενός εκτυπωτή για το περιβάλλον των Windows. Αμέσως γίνεται κατανοητή η χρησιμότητα της συγκεκριμένης τεχνολογίας στο Βιομηχανικό Περιβάλλον και στον Αυτοματισμό. Διαφορετικού τύπου PLC μπορούν να συνδεθούν σε έναν κεντρικό υπολογιστή, ο οποίος λειτουργώντας ως server παρέχει δεδομένα σε συστήματα εποπτείας και συλλογής δεδομένων (HMI, HISTORIAN, SCADA κλπ). Το μόνο που απαιτείται από τα διάφορα αυτά software που υλοποιούν τον Εποπτικό Έλεγχο, είναι να έχουν ενσωματωμένη την εφαρμογή OPC client ώστε να ανακτούν τα δεδομένα από τον OPC server[66].



Εικόνα 4.5: Παράδειγμα υλοποίησης με την τεχνολογία OPC

4.2.4 Πρωτοκολλο επικοινωνιας DNP3

Το κατανεμημένο πρωτόκολλο δικτύου 3 (Distributed Network Protocol Version 3 - DNP3) είναι το πλέον σύγχρονο βιομηχανικό πρωτόκολλο επικοινωνίας. Το πρωτόκολλο DNP3 έχει σχεδιαστεί για να διευκολύνει την επικοινωνία των κεντρικών σταθμών ηλεκτρικής ενέργειας με τους υποσταθμούς μέσω πρωτοκόλλων σειριακής γραμμής ή μέσω πρωτοκόλλων TCP/IP. Είναι από τα πλέον αξιόπιστα βιομηχανικά πρωτόκολλα αφού διαθέτει μηχανισμό ασφάλειας ώστε η μετάδοση πληροφοριών να γίνεται με ασφάλεια. Ο μηχανισμός αυτός βασίζεται στη χρήση μιας συνάρτησης hash σε συνδυασμό με ένα μυστικό κλειδί και ονομάζεται HMAC και του πρωτοκόλλου πρόκλησης-απάντησης (Challenge Response)[63].



Εικόνα 4.6: Το πρωτόκολλο DNP3 είναι ένα από τα βασικά πρωτόκολλα για την επικοινωνία των συστημάτων του έξυπνου δικτύου.

Ένα κομμάτι αίτησης ή απόκρισης του πρωτοκόλλου DNP3 αποτελείται από έναν τομέα ελέγχου της εφαρμογής, έναν κώδικα λειτουργίας και ένα πεδίο κεφαλίδας αντικειμένου. Επιπλέον με την απόκριση, εισάγεται επίσης και ένα επιπλέον πεδίο που ονομάζεται «εσωτερική ένδειξη». Τα πεδία αυτά περιγράφονται παρακάτω[63]:

1. Έλεγχος εφαρμογής: Περιέχει διάφορα υπο-πεδία που παρέχουν τις απαραίτητες πληροφορίες για την κατασκευή και επανασυναρμολόγηση πολλαπλών τμημάτων μηνυμάτων DNP3.

2. Κώδικας λειτουργίας: Ορίζει τον σκοπό που αποστέλλεται το μήνυμα. Δηλαδή, αν ένας απομακρυσμένος σταθμός δεχτεί μία αίτηση από έναν κύριο σταθμό, τότε ο κώδικας λειτουργίας λέει στον εξωτερικό σταθμό τι να κάνει.

3. Κεφαλίδα αντικειμένου: Πρόκειται για επιπλέον συμπληρωματικές πληροφορίες που μπορεί να χρειαστούν για την δημιουργία ενός πλήρους μηνύματος DNP3. Συνδέεται με αντικείμενα DNP3 (δηλ. διάφορα μέρη που κρατούν δυαδικά δεδομένα εισόδου/εξόδου, αναλογικά δεδομένα και μετρητές). Αποτελείται από διάφορα επιμέρους πεδία και σκοπός του είναι να διασφαλίσει ότι, όταν ένας κύριος σταθμός για παράδειγμα στέλνει μια εντολή ανάγνωσης σε έναν απομακρυσμένο σταθμό, η κεφαλίδα αντικειμένου που την συνοδεύει στο κομμάτι της αίτησης προσδιορίζει στον απομακρυσμένο σταθμό τη μορφή, το είδος ή την ομάδα στοιχείων που θα πρέπει να διαβάσει και να επιστρέψει ως απόκριση.

4. Εσωτερική ένδειξη: Αυτό είναι ένα πεδίο που εμφανίζεται μόνο σε κομμάτια απόκρισης από απομακρυσμένους σταθμούς. Περιέχει δύο υποπεδία για να υποδείξει ορισμένες καταστάσεις και συνθήκες σφάλματος μέσα στους απομακρυσμένους σταθμούς.

ΚΕΦΑΛΑΙΟ 5

ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΑ ΕΞΥΠΝΑ ΠΛΕΓΜΑΤΑ

5.1 Προκλησεις και κινδυνοι

Το έξυπνο δίκτυο προσφέρει τόσο στους καταναλωτές όσο και στους προμηθευτές πολλά πλεονεκτήματα τα οποία οφείλει κυρίως στην προσθήκη των νέων τεχνολογιών. Τα ευεργετικά χαρακτηριστικά του έξυπνου δικτύου, συμβάλουν στη βέλτιστη αξιοποίηση ηλεκτρικής ενέργειας τόσο στην πλευρά της παραγωγής όσο και στην πλευρά της κατανάλωσης. Εισάγοντας τις νέες τεχνολογίες τηλεπικοινωνιών και πληροφορικής σε καίρια σημεία του δικτύου, επιτυγχάνεται η ενσωμάτωση ανανεώσιμων πηγών ενέργειας καθώς και η ενεργητικότητα των καταναλωτών στο σενάριο λειτουργίας του έξυπνου δικτύου.

Ωστόσο, η ενσωμάτωση των νέων τεχνολογιών, ειδικά αυτών που σχετίζονται με το διαδίκτυο, εισάγουν νέες απειλές για την ασφάλεια του έξυπνου δικτύου. Με τα εκατομμύρια των πελατών που γίνονται μέρος του έξυπνου δικτύου, οι πληροφορίες και η υποδομή επικοινωνίας θα χρησιμοποιήσουν τις διαφορετικές τεχνολογίες επικοινωνιών και τις δικτυακές αρχιτεκτονικές που μπορούν να γίνουν τρωτές στην κλοπή των στοιχείων ή των κακόβουλων διαδικτυακών επιθέσεων.

Κακοπροαίρετοι επιτιθέμενοι θα μπορούσαν να εκμεταλλευτούν τα ευάλωτα σημεία του δικτύου και να υποκλέψουν απόρρητες πληροφορίες πελατών, να καταλάβουν ηλεκτρονικές συσκευές, να απαγορεύσουν τη διαθεσιμότητα απαραίτητων υπηρεσιών και να προκαλέσουν μια εκτεταμένη διακοπή ρεύματος, με συνέπεια ένα δυσμενές οικονομικό κόστος.

Για το λόγο αυτό η αντιμετώπιση των ζητημάτων ασφαλείας παίζει πρωταρχικό ρόλο και έχει αναγνωριστεί παγκόσμια ως ένα μείζον θέμα με πιθανώς καταστροφικές συνέπειες.

Ένα έξυπνο δίκτυο για να πληροί της προυποθέσεις ασφαλείας και να έχουμε εύρυθμη λειτουργεία θα πρέπει να εξασφαλίζει τα εξής[18]:

- Διαθεσιμότητα (Availability): Ο λόγος που θέλουμε να έχουμε ένα Smart Grid είναι η διαθεσιμότητα. Ο βασικός στόχος του έξυπνου δικτύου είναι να παρέχει αδιάλειπτη παροχή ρεύματος στους χρήστες.
- Εμπιστευτικότητα(Confidentiality):
  Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Το έξυπνο δίκτυο θα πρέπει να παρέχει προστασία των πληροφοριών του χρήστη. Εάν τα δεδομένα δεν είναι κατάλληλα προστατευμένα μπορεί ένας επιτιθέμενος να αποκαλύψει πληροφορίες για τον χρήστη και να χρησιμοποιήσει αυτές τις πληροφορίες δημιουργώντας τεράστια προβλήματα.
- Ακεραιότητα (Integrity): Ως ακεραιότητα ορίζουμε τη διαβεβαίωση πως τα δεδομένα που ανταλλάσσονται μεταξύ εξουσιοδοτημένων οντοτήτων είναι

ορθά συνεπή και χρονικά έγκυρα. Δηλαδή δεν έχουν επιδεχθεί οποιαδήποτε αλλοίωση και δεν έχουν υποστεί καταστροφή η απώλεια κατά τη διάδοση τους.

5.2 ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΠΡΟΣΩΠΙΚΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΣΤΟ ΕΞΥΠΝΟ ΠΛΕΓΜΑ

Το έξυπνο πλέγμα έχει την ικανότητα να συλλέγει και να αποθηκεύει πλήθος δεδομένων και πληροφοριών σχετικά με την κατανάλωση ενέργειας. Οι έξυπνοι μετρητές στα σπίτια μεταφέρουν τα δεδομένα που έχουν καταγράψει στις εταιρίες ηλεκτρισμού, στους καταναλωτές και σε άλλους τρίτους προμηθευτές υπηρεσιών. Αυτές οι πληροφορίες περιλαμβάνουν προσωπικά δεδομένα των καταναλωτών που εκθέτουν την ιδιωτικοτητά τους .

Εάν αυτές οι πληροφορίες γίνουν διαθέσιμες σε άλλες ομάδες ατόμων (εκτός των υπεύθυνων πάροχων εταιριών) όπως διαφημιστικές εταιρείες, δικαστικές αρχές και κακόβουλα άτομα, αυτό θα μπορούσε να αποτελέσει κίνδυνο για την προσωπική ζωή και την ασφάλεια των καταναλωτών. Για παράδειγμα μέσα από μια λεπτομερή αναφορά της ενεργειακής κατανάλωσης ενός σπιτιού θα μπορούν άτομα αλλά και εταιρίες να αποφανθούν για τις συνήθειες των ανθρώπων που μένουν στο σπίτι όπως για παράδειγμα πότε οι ένοικοι ξυπνάνε, τι ώρα φεύγουν κάθε πρωί για τη δουλειά τους, τι ώρα επιστρέφουν, σε ποια δωμάτια βρίσκονται ανά πάσα στιγμή, τι κάνουν σε αυτά, πότε απουσιάζουν για μεγάλα χρονικά διαστήματα, που πάνε (πληροφορίες φόρτισης του PEV) κτλ. Τέτοιες πληροφορίες θα μπορούσαν κάλλιστα να αξιοποιηθούν για την οργάνωση σοβαρότερων επιθέσεων με στόχο τους ίδιους τους καταναλωτές ή την περιουσία τους.

Επίσης ένα άλλο από τα κίνητρα που θα μπορούσαν να ωθήσουν μια εταιρεία να χρησιμοποιήσει προσωπικά δεδομένα είναι για λόγους διαφήμισης. Όπως για παράδειγμα μια εταιρεία να πουλήσει τις πληροφορίες αυτές μιας ολόκληρης περιοχής σε μια διαφημιστική εταιρεία, όπου η διαφημιστική εταιρεία αναλύοντας τη χρήση ηλεκτρικής ενέργειας του κάθε σπιτιού να δημιουργήσει ένα προφίλ για τον κάθε καταναλωτή και να κάνει στοχευμένη διαφήμιση.

Η ανάγκη για την προστασία των προσωπικών δεδομένων στο έξυπνο δίκτυο αναγνωρίζεται ως μείζον θέμα από πολλά σωματεία προτυποποίησης όπως το Εθνικό Ινστιτούτο Προτύπων και τεχνολογιών των ΗΠΑ και αναζητούνται ρωμαλέες πολιτικές για την προστασία των προσωπικών δεδομένων που θα καθορίσουν τη χρησιμοποίηση των δεδομένων μεταφοράς στο έξυπνο δίκτυο.

5.3 ΑΠΕΙΛΕΣ ΚΑΙ ΣΥΝΕΠΕΙΕΣ ΓΙΑ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΚΑΙ ΤΙΣ ΚΥΒΕΡΝΗΣΕΙΣ

Στην προηγούμενη ενότητα αναφερθήκαμε στις απειλές και τις επιπτώσεις που μπορεί να έχει ένας καταναλωτής από τα κενά ασφάλειας που μπορεί να εκμεταλλεύονται κάποια κακόβουλα άτομα θέτοντας σε κίνδυνο την προσωπική ζωή του καταναλωτή. Όταν όμως ο κίνδυνος αφορά δεδομένα πολλών καταναλωτών που τα διαχειρίζεται κάποια εταιρεία κοινής ωφελείας τότε το πρόβλημα είναι πιο σοβαρό.

Σε ένα αρνητικό σενάριο θα μπορούσε ένας εισβολέας να εισέλθει στις βάσεις δεδομένων μιας εταιρείας, με αποτέλεσμα να μπορεί να αποσπάσει από αυτήν πληροφορίες όπως ονόματα, διευθύνσεις πελατών κ.α. Για τους πελάτες που χρησιμοποιούν τις online δυνατότητες της εταιρείας για την αποπληρωμή οφειλών, ο εισβολέας μπορεί να αποσπάσει και λογαριασμούς τραπέζης όπως και αριθμούς πιστωτικών καρτών. Αυτός στην συνέχεια πουλάει το πλήθος αυτό των πληροφοριών στην μαύρη αγορά και όταν αυτό γίνει αντιληπτό από τους πελάτες ή από κυβερνητικούς οργανισμούς, επιβάλλεται πρόστιμο στην εταιρεία.

Η καταπάτηση της εμπιστευτικότητας των δεδομένων μπορεί όμως να γίνει και από κρατικές αρχές, όπως η αστυνομία, για την δίωξη των εγκληματιών. Τα δεδομένα αυτά χρησιμοποιούνται για να δείξουν την πιθανότητα κάποιος να βρίσκεται στην κατοικία του κατά την διάρκεια μιας εγκληματικής πράξης. Οι αντιδράσεις των καταναλωτών στην εικαζόμενη κατάχρηση των πληροφοριών κατανάλωσης, αναγκάζει τις εταιρείες να τροποποιήσουν το δίκτυο των έξυπνων μετρητών και να επιβαρυνθούν οικονομικά.

Τέλος σημαντικός κίνδυνος προκύπτει όταν οι πληροφορίες που αποσπώνται από εισβολείς αφορούν την ίδια την εταιρεία. Τέτοιες πληροφορίες μπορεί να είναι κάποια εμπορικά μυστικά της εταιρείας. Για παράδειγμα, μία ξένη κυβέρνηση, απογοητευμένη από τις κυρώσεις που δέχεται από τις ΗΠΑ, διορίζει τους δικούς της εισβολείς να αποσπάσουν εμπορικά μυστικά της εταιρείας. Αυτό το γεγονός επιτρέπει στην ξένη κυβέρνηση να αυξήσει σημαντικά τις δυνατότητές της για παραγωγή ΗΕ, παρά τις επιβαλλόμενες κυρώσεις. Παράλληλα η εταιρεία βλέπει τα κέρδη της να μειώνονται, καθώς τα εμπορικά της μυστικά είναι πλέον γνωστά[19].

Το μεγαλύτερο κίνητρο ενός εισβολέα όμως είναι το οικονομικό κέρδος. Οι περισσότεροι αν όχι όλοι από τους επαγγελματίες εισβολείς χρηματοδοτούνται γι αυτό που κάνουν. Αυτοί συνεργάζονται με εκείνους που κατανοούν τις χρηματοπιστωτικές αγορές ή συνεργάζονται με τρομοκρατικές οργανώσεις και αξιοποιώντας την υιοθέτηση του έξυπνου δικτύου μπορούν να επωφεληθούν οικονομικά σε σύντομο χρονικό διάστημα. Για παράδειγμα ένας επαγγελματίας εισβολέας προσλαμβάνεται από την Αλ Κάιντα για να επιτεθεί στο δίκτυο ΗΕ των ΗΠΑ. Διενεργώντας μία επίθεση που αξιοποιεί κακόβουλα συνημμένα email, ο εισβολέας είναι σε θέση να δημιουργήσει ένα σκουλήκι (worm) και να μολύνει την πλειονότητα των μεγάλων εταιριών κοινής ωφέλειας των ΗΠΑ, σταματώντας την παραγωγή ΗΕ σε πολλές εταιρίες ταυτόχρονα. Το blackout μπορεί να διαρκέσει αρκετές ημέρες, μέχρι το σκουλήκι να εντοπιστεί. Η οικονομική αλλά και ψυχολογική ζημιά για τις Ηνωμένες Πολιτείες είναι καταστροφική. Τέτοιες τεχνικές εφαρμόζονται και σε περιόδους πολέμου, με σκοπό το blackout να προκαλέσει χάος στην χώρα. Το αποτέλεσμα είναι πολλές ζωές να χάνονται και ο τελικός απολογισμός να είναι ανυπολόγιστος[19].

5.4 ΠΡΟΣΠΑΘΕΙΕΣ ΤΩΝ ΜΕΓΑΛΩΝ ΚΡΑΤΩΝ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΕΞΥΠΝΟΥ ΠΛΕΓΜΑΤΟΣ

Η δημιουργία του έξυπνου δικτύου μπορεί να έχει πολλά πλεονεκτήματα αλλά τα προβλήματα που μπορεί να προκύψουν από μία πιθανή επίθεση από τον κυβερνοχώρο είναι ένα θέμα που έχει προβληματίσει έντονα τις περισσότερες κυβερνήσεις οι οποίες είναι υπεύθυνες για θέματα εθνικής ασφάλειας.

Σε ορισμένες περιπτώσεις οι κυβερνοεπιθέσεις εναντίον του δικτύου μπορεί να ερμηνεύονται ως μία πράξη πολέμου. Σε αυτές τις περιπτώσεις θα πρέπει να υπάρχει η κατάλληλη νομοθετική πρόβλεψη που να προστατεύει την εθνική ακεραιότητα και να ορίζει τον υπεύθυνο για την αντιμετώπιση τους.

Επίσης οι εταιρείες παροχής ηλεκτρικής ενέργειας θα πρέπει να ακολουθούν τις προδιαγραφές των ρυθμιστικών αρχών σχετικά με το πώς θα πρέπει να προστατεύουν αποτελεσματικά τις τεχνολογίες έξυπνου δικτύου. Ενθαρρυντικό είναι ότι μέχρι σήμερα έχουν δημιουργηθεί αρκετές ρυθμιστικές αρχές οι οποίες έχουν σκοπό τη μεγαλύτερη ασφάλεια του δικτύου.

Παρακάτω παρουσιάζονται οι ενέργειες Ευρωπαϊκής Ένωσης και των ΗΠΑ για την προστασία των έξυπνων δικτύων:

Οι δραστηριότητες της Ευρωπαϊκής Επιτροπής που σχετίζονται με το έξυπνο δίκτυο περιλαμβάνουν την ίδρυση των εξής κυβερνητικών οργανισμών: [20]

- Directorate General for Energy (DG Ener): ιδρύθηκε το 2010 και επιβλέπει θέματα που αφορούν την ενεργειακή απόδοση (energy efficiency), την ασφάλεια σε θέματα προμήθειας ενέργειας, τις εσωτερικές αγορές ενέργειας και την ενέργεια που προκύπτει από ανανεώσιμες πηγές και πυρηνικούς σταθμούς.
- Agency for the Cooperation of Energy Regulators (ACER): ιδρύθηκε το 2009 και είναι υπεύθυνη για την δημιουργία και διατήρηση των κανόνων που διέπουν το ευρωπαϊκό δίκτυο ΗΕ. Αυτοί οι κανόνες αφορούν την αποτροπή πρόσβασης από τρίτους και τη λειτουργική ασφάλεια των διασυνοριακών υποδομών του ηλεκτρικού δικτύου.
- Executive Agency for Competitiveness and Innovation (EACI): ιδρύθηκε το 2009 και είναι υπεύθυνη για την εκλογή των κατάλληλων εμπειρογνωμόνων και χειριστών με σκοπό την ανάπτυξη και προώθηση ευφυών ενεργειακών συστημάτων.

Επιπλέον το 2009 κυβερνητικοί αξιωματούχοι και στελέχη εταιριών σε ενεργειακά θέματα από ομάδες όπως οι Smart Grids Technology System Platform (Smart Grid ETP), European Network of Transmission System Operators for Electricity (ENTSOE) και την CEER&ERGEG, ίδρυσαν το 2009 την ομάδα “Smart Grid Taskforce”, η οποία ανέλαβε δράσεις όπως:

- Ρυθμιστικές δράσεις σε ευρωπαϊκό επίπεδο.
- Εφαρμογή ευφυών δικτύων.
- Εφαρμογή ευφυών συστημάτων μέτρησης.
- Κεντρική και διανεμημένη παραγωγή.
- Ενσωμάτωση καταναλωτών που συμμετέχουν στην παραγωγή ενέργειας.
- Εξισορρόπηση παραγωγής ΗΕ με ζήτηση.
- Συγκρότηση συντονιστικής επιτροπής και ομάδων εμπειρογνωμόνων για να καθοδηγήσουν τις προσπάθειες.

Η πολιτική των ΗΠΑ που εφαρμόζεται σε θέματα που αφορούν το έξυπνο δίκτυο, [21] κατευθύνεται από την κεντρική ομοσπονδιακή κυβέρνηση των Ηνωμένων Πολιτειών με την καθοδήγηση βέβαια της Federal Smart Grid Task Force[22].

Μέλη αυτής της οργάνωσης είναι:

- Department Of Energy (DOE)
- U.S Department of Commerce (DOC)
- International Trade Administration (ITA)
- National Institute of Standards and Technology (NIST)
- Federal Energy Regulatory Commission (FERC)
- U.S Department of Homeland Security (DHS)
- U.S Department of State
- U.S Environmental Protection Agency (EPA)
- U.S Department of Agriculture (USDA)
- Department of Defence (DOD)
- Federal Oceanic and Atmosphenic Administration (NOAA)
- U.S Trade and Development Agency (USTDA)

Νομοθεσία ΗΠΑ: Energy Policy Act (EPAct)

Η βιομηχανία ΗΕ συνεργαζόμενη με το Κογκρέσο, θέσπισε υποχρεωτικά πρότυπα αξιοπιστίας με την ψήφιση του EPAct το 2005 και έτσι βοήθησε στην δημιουργία ενός πιο ασφαλούς συστήματος ΗΕ ενάντια επιθέσεων στον κυβερνοχώρο. Σύμφωνα με τον EPAct, ορίστηκε η NERC αρμόδια για την θέσπιση προτύπων ενεργειακής αξιοπιστίας, ιδιαίτερα την θέσπιση προτύπων που αφορούν την ασφάλεια έναντι επιθέσεων στον κυβερνοχώρο.

Όταν η NERC αποδεχτεί αυτά τα πρότυπα, τότε αυτά στέλνονται στην FERC για επανεξέταση και έγκριση και στη συνέχεια γίνονται δεσμευτικά.

Παρά το γεγονός ότι αυτά τα πρότυπα αξιοπιστίας παρέχουν ένα σημαντικό θεμέλιο για την ενίσχυση της ασφάλειας του δικτύου από επιθέσεις, δεν τον προστατεύουν σε καταστάσεις έκτακτης ανάγκης, οι οποίες απειλούν την εθνική ασφάλεια και την δημόσια ευημερία. Λύση σε αυτά τα ζητήματα πρέπει να δοθεί μέσω της συνεργασίας της βιομηχανίας και της κυβέρνησης. Επομένως αναπτύχθηκαν οι εξής αρχές (principles):

- Θα πρέπει να υπάρχει ανταλλαγή πληροφοριών μεταξύ του δημόσιου και ιδιωτικού τομέα.
- Είναι απαραίτητη η δημιουργία ενός ρυθμιστικού πλαισίου που να εστιάσει την προσοχή του στην προστασία κρίσιμων περιουσιακών στοιχείων από επικείμενες απειλές. Αυτό επίσης θα διασφαλίσει ότι επείγουσες εντολές θα έρχονται μόνο από κυβερνητικούς φορείς.

ΚΕΦΑΛΑΙΟ 6

ΑΠΕΙΛΕΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

6.1 HACKERS

Η ιστορία των Hackers ξεκινάει από 1960 από σπουδαστές του πανεπιστημίου MIT. Αυτοί οι σπουδαστές δημιούργησαν τα πρώτα Hacks προγράμματα που βοηθούσαν στη γρηγορότερη εκτέλεση υπολογισμών. Το Hacking πριν την έλευση των υπολογιστών σήμαινε την εύρεση έξυπνων λύσεων σε δύσκολα τεχνικά προβλήματα. Σήμερα με τον όρο Hacker χαρακτηρίζεται ένα άτομο που έχει πολλές τεχνικές γνώσεις για τους υπολογιστές αλλά και προχωρημένες γνώσεις προγραμματισμού και έχει την ικανότητα να διαχειρίζεται σε μεγάλο βαθμό υπολογιστικά συστήματα, εντοπίζοντας τις αδυναμίες του, να λύνει τεχνικά προβλήματα, να βελτιώνει εφαρμογές, αλλά και να συνεργάζεται με άλλους όμοιους για την επίλυση των προβλημάτων των υπολογιστών, χωρίς όμως να προξενεί κάποια ζημιά.

Οι Hackers αυτοί όμως που χρησιμοποιούν τις ικανότητες τους για μη ευγενικούς σκοπούς και έχουν ως στόχο την πρόκληση ζημιάς σε δίκτυα υπολογιστών, την εισβολή σε υπολογιστές χρηστών χωρίς εξουσιοδότηση, θεωρούνται ως οι κακόβουλοι Hackers και τους ονομάζουμε crackers[23].

6.1.1 ΤΑ ΚΙΝΗΤΡΑ ΤΩΝ ΕΠΙΤΙΘΕΜΕΝΩΝ ΣΤΟ ΕΞΥΠΝΟ ΠΛΕΓΜΑ

Τα κίνητρα των επιτιθέμενων Hackers μπορεί να κατηγοριοποιηθούν σε πέντε περιοχές:

1. Περιέργεια για πληροφορία
2. Υποκινούμενες επιθέσεις
3. Ανήθικη κλοπή ενέργειας
4. Κλοπή πληροφοριών κατανάλωσης ισχύος
5. Οικονομικά οφέλη

6.1.2 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΕΠΙΘΕΣΕΩΝ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΑΡΙΘΜΟ ΤΩΝ ΕΠΙΤΙΘΕΜΕΝΩΝ

Οι επιθέσεις μπορούν επίσης να αναλυθούν σε:

- *ατομικές επιθέσεις (single or individual attacks).* Απομονωμένες επιθέσεις εκτελούμενες από ένα και μοναδικό άτομο. Αποτελεί πρόκληση η συλλογή όλων των

απαραίτητων πληροφοριών και εργαλείων για να διαπράξει ένα μικρής κλίμακας blackout.

- *Οργανωμένες επιθέσεις (coordinated attacks)*. Ομάδες επιτιθέμενων συνεργάζονται για να χτυπήσουν ομαδικά ένα κοινό στόχο, μια κρίσιμη υποδομή. Συνήθως στοχεύουν ένα σύνθετο αποτέλεσμα με επίδραση μεγαλύτερης κλίμακας από αυτή των ατομικών επιθέσεων. Χρησιμοποιούν μέσα όπως το Διαδίκτυο και άλλες σύγχρονες τηλεπικοινωνίες για να συντονίσουν ταυτόχρονες επιθέσεις από γεωγραφικά απομακρυσμένες περιοχές. Για παράδειγμα, ένας επιτιθέμενος μπορεί να κατεβάσει το γενικό διακόπτη ηλεκτρικής ισχύος σε ένα κτίριο, δίνοντας την ευκαιρία για έναν άλλο επιτιθέμενο να εισβάλει στο κτίριο χωρίς να ενεργοποιηθεί ο συναγερμός[24].

6.1.3 ΚΑΤΗΓΟΡΙΟΠΟΊΗΣΗ ΗΛΕΚΤΡΟΝΙΚΏΝ ΕΠΙΘΈΣΕΩΝ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΣΤΟΧΟ

Μια προσπάθεια ηλεκτρονικής εισβολής μπορεί να στοχεύει οποιοδήποτε τομέα στο δίκτυο ηλεκτρικής ισχύος:

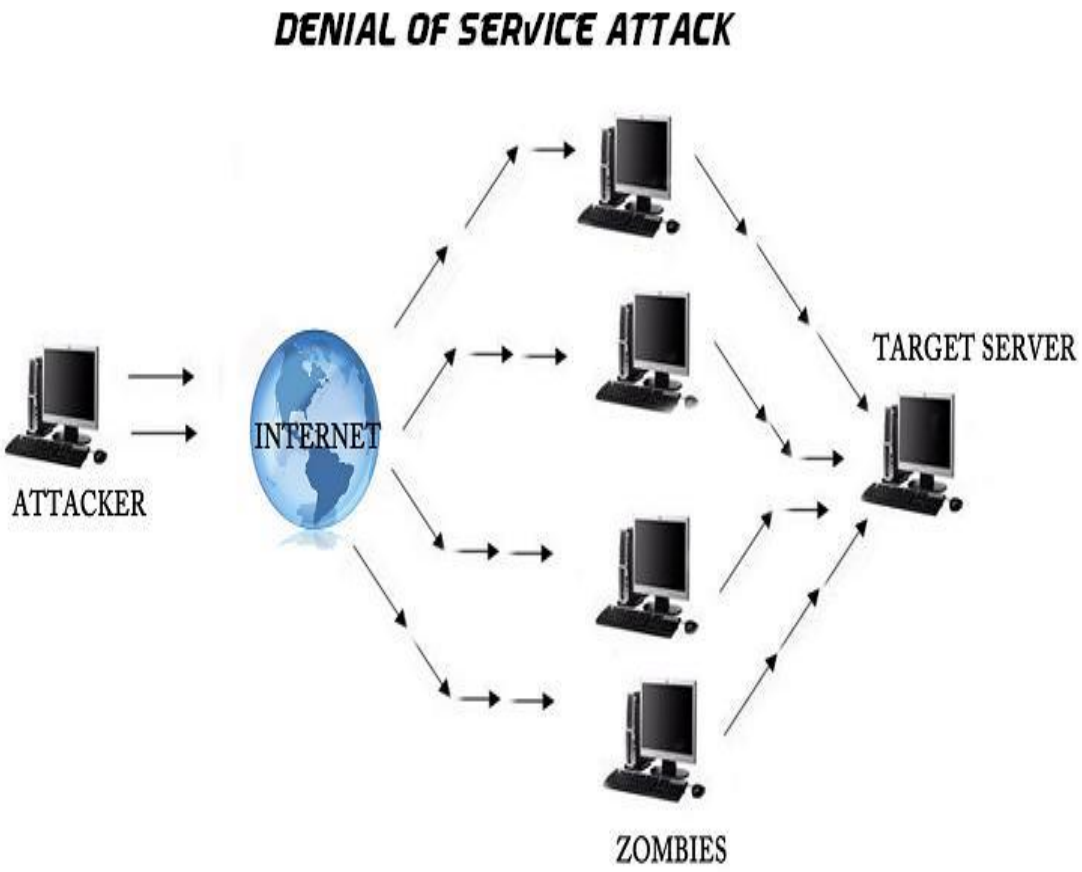
- *Παραγωγή (generation)*. Τα εργοστάσια παραγωγής ισχύος αποτελούν στόχο και σκοπός των επιθέσεων είναι να διακόψουν ή να καταλάβουν τη λειτουργία των γεννητριών.
- *Διανομή και Έλεγχος (distribution and control)*. Περιλαμβάνει εισβολές και προσπάθειες αλλαγής φάσης και άλλων πληροφοριών κατάστασης του δικτύου. Για παράδειγμα, οι επιτιθέμενοι επιθυμούν να καταλάβουν τους αισθητήρες μέτρησης ή να εισέλθουν στα routers που μεταφέρουν τις μετρήσεις προς το κέντρο ελέγχου με σκοπό να εισάγουν λάθη σε συγκεκριμένες μεταβλητές καταστάσεις.
- *Κατανάλωση (consumption)*. Περιλαμβάνει απότομη αλλαγή φορτίου μέσω Διαδικτύου σε συγκεκριμένες κρίσιμες τοποθεσίες του ηλεκτρικού δικτύου και πρόκληση υπερφόρτωσης των γραμμών μεταφοράς ηλεκτρικού ρεύματος[24].

6.2 ΒΑΣΙΚΟΙ ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ

6.2.1 Επιθεσεισ αρνησησ υπηρεσιων DOS

Η ανάπτυξη των υπολογιστικών και τεχνολογικών επικοινωνιών καθημερινά πλήττεται από ένα πλήθος απειλών που εμποδίζουν την ομαλή λειτουργία τους προκειμένου τα υπολογιστικά συστήματα του δικτύου να μη λειτουργούν κανονικά και να έχουμε απώλεια πόρων για τους νόμιμους χρήστες. Ένα από τα πιο προκλητικά θέματα όσον αφορά στη διαθεσιμότητα είναι οι επιθέσεις άρνησης εξυπηρέτησης DOS.

Οι επιθέσεις DOS αποτελούν μια από τις κύριες απειλές και μεταξύ των δυσκολότερων προβλημάτων ασφαλείας στα έξυπνα δίκτυα. Ο κύριος στόχος των επιθέσεων DOS είναι η διακοπή υπηρεσιών προσπαθώντας να περιορίσουν την πρόσβαση σε μια μηχανή η σε μια υπηρεσία αντί να υπομονεύσουν την ίδια την υπηρεσία. Αυτό το είδος επίθεσης έχει ως στόχο να καταστήσει το έξυπνο δίκτυο ανίκανο να παρέχει κανονική υπηρεσία[25].



Εικόνα 6.1:Τρόπος διεξαγωγής DoS επίθεσης.

Για παράδειγμα ένας επιτιθέμενος βρίσκοντας μια αδυναμία στο λειτουργικό σύστημα και το λογισμικό που χρησιμοποιείται από τους υπολογιστές του έξυπνου δικτύου θα μπορούσε να συλλέξει πολύτιμες πληροφορίες και αξιοποιώντας τα τρωτά σημεία ή bugs που τρέχει στους servers να πραγματοποιήσει μια επίθεση DOS(Εικόνα 6.1). Με αυτό τον τρόπο θα καθιστούσε τους servers που δέχτηκαν την επίθεση ανίκανους να εξυπηρετήσουν τους κανονικούς χρήστες λόγω υπερφόρτωσης η οποία προκαλείται από τον κακόβουλο χρήστη ο οποίος βομβαρδίζει με αιτήσεις το σύστημα. Τέτοιες αιτήσεις μπορούν να είναι :

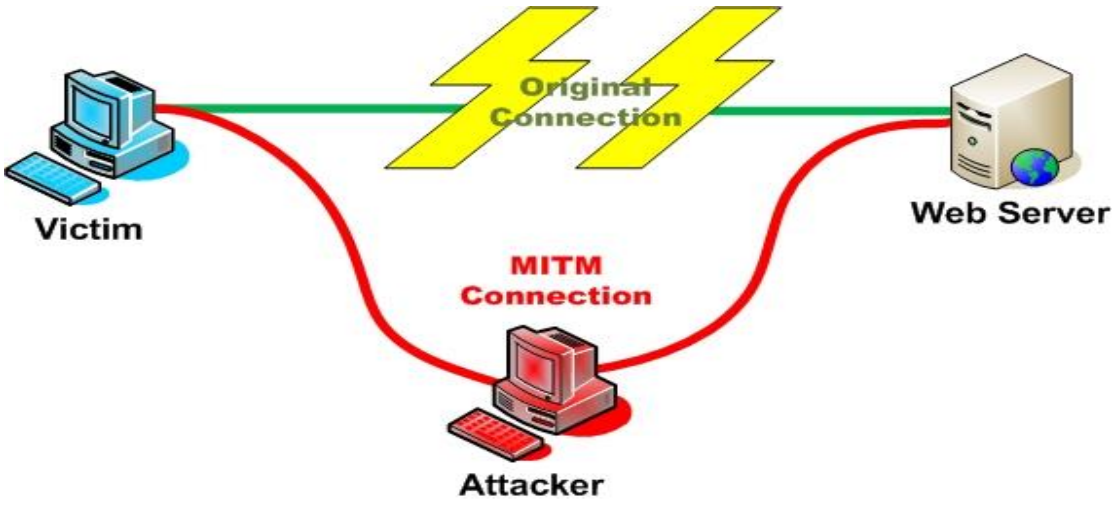
- Ψεύτικα πακέτα με τυχαίες τιμές
- Ημιτελείς αιτήσεις TCP, όπου αφήνουν το διακομιστή με χιλιάδες ημιτελείς συνδέσεις. Οι αιτήσεις ανανεώνονται με ρυθμό μεγαλύτερο από αυτόν με τον οποίο ο διακομιστής τις απορρίπτει, ώστε να μην μπορεί να ανταποκριθεί σε νέες πραγματικές αιτήσεις.
- Αιτήματα HTTP για πόρους και ιστοσελίδες που διαθέτει ο διακομιστής με πολύ μικρή ταχύτητα.[26]

Ο ρυθμός με το οποίο αποστέλλονται οι αιτήσεις των ανωτέρω τύπων είναι τέτοιος ώστε μετά από λίγο ο διακομιστής να μην είναι σε θέση να ανταποκριθεί σε νέες αιτήσεις, καθώς οι πόροι του, είτε υπολογιστικοί (CPU/RAM) είτε δικτυακοί (bandwidth) φθάνουν σε σημείο κορεσμού και δεν μπορούν να δεχθούν τις πραγματικές αιτήσεις.

Τέτοιες επιθέσεις μπορεί να έχουν ως αποτέλεσμα ολόκληρες περιοχές η μια μετά την άλλη να βυθίζονται στο απόλυτο σκοτάδι με τις συνέπειες να είναι καταστροφικές τόσο για την οικονομία όσο και για την κοινωνία μιας χώρας[27].

6.2.2 MAN IN THE MIDDLE ATTACK

Η επίθεση man in the middle είναι μία κοινή παράβαση ασφαλείας στις επικοινωνίες. Κατά την επικοινωνία δύο έμπιστων μεταξύ τους μερών ο επιτιθέμενος παρεμβάλλεται στη μέση με αποτέλεσμα όλη η επικοινωνία να διέρχεται από αυτόν. Τα μηνύματα αυτά μπορεί απλά να παρακολουθούνται, είτε να τροποποιούνται, είτε να απορρίπτονται ή να δημιουργούνται νέα. Για να πετύχει αυτή η επίθεση ο επιτιθέμενος πρέπει να πείσει τα δυο μέρη της επικοινωνίας ότι μιλούν απευθείας μεταξύ τους σε ασφαλές κανάλι (Εικόνα 6.2).



Εικόνα 6.2: Τρόπος λειτουργίας επίθεσης Man in the Middle

Για παράδειγμα στο έξυπνο δίκτυο ένας πελάτης επιθυμεί να εξουσιοδοτήσει κάποιον παροχέα υπηρεσιών που εμπιστεύεται να λαμβάνει ότι, πληροφορία χρειάζεται σχετικά με την κατανάλωση του, από το κεντρικό σύστημα του παροχέα. Σε ένα τέτοιο σενάριο όπου έχουμε μια επίθεση Man in the Middle στην οποία ο επιτιθέμενος προσποιείται το ένα άκρο επικοινωνίας στο άλλο αποσπά την πληροφορία που μεταφέρεται και την αλλοιώνει.

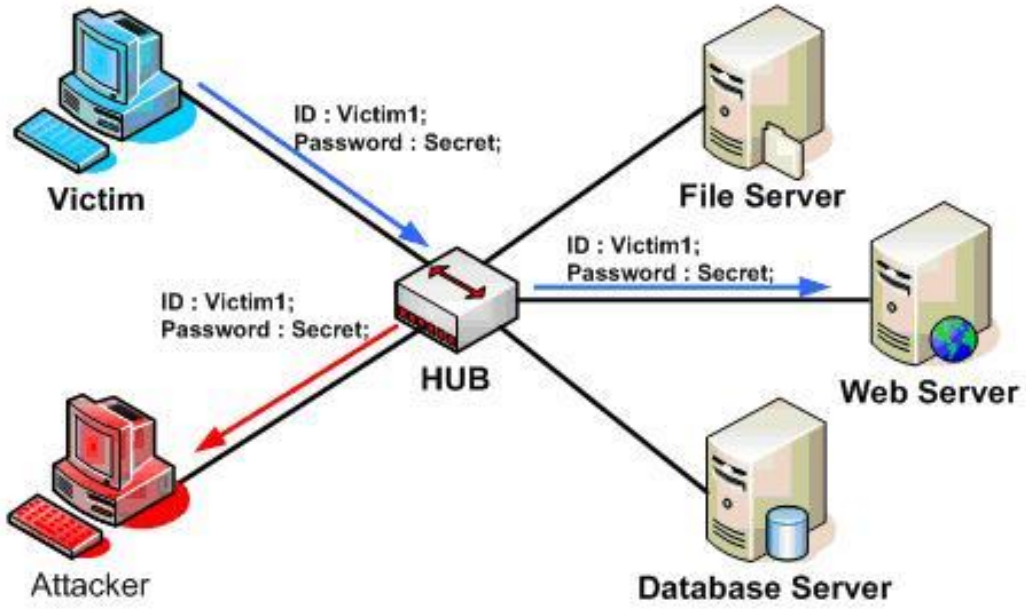
Σε αυτή την περίπτωση ο πελάτης θα μπορούσε να οδηγηθεί στη λήψη λανθασμένων αποφάσεων, θέτοντας τις συσκευές του σε λειτουργεία σε ώρες αιχμής όπου η ενέργεια κοστίζει πολύ περισσότερο (θεωρώντας ότι η περίοδος αυτή, είναι περίοδος χαμηλής χρέωσης) ή απενεργοποιώντας τις συσκευές του σε ώρες χαμηλής χρέωσης, θεωρώντας ότι είναι ώρες αιχμής. Κάτι τέτοιο θα μπορούσε προφανώς να έχει σημαντικό αντίκτυπο τόσο στον πελάτη (ο οποίος επιβαρύνεται το οικονομικό κόστος των αποφάσεών του) όσο και στο Smart Grid του οποίου ο φόρτος αυξάνεται επικίνδυνα (ιδιαίτερα αν μια τέτοια επίθεση γίνει

μαζικά) με ρίσκο να προκύψουν αστάθειες λόγω της απρόσμενα αυξημένης ζήτησης ,γεγονός που θα μπορούσε να οδηγήσει σε τοπικής κλίμακας διακοπές ρεύματος.

6.2.3 ΩΤΑΚΟΥΣΤΗΣ

Αυτή η επίθεση αποτελεί μία επίθεση στο στρώμα του δικτύου. Αποτελείται από την λήψη πακέτων από το δίκτυο, τα οποία διαβιβάζονται μέσω υπολογιστών και στην συνέχεια την ανάγνωση του περιεχομένου τους σε αναζήτηση ευαίσθητων πληροφοριών(Εικόνα 6.3). Η επίθεση μπορεί να γίνει με την χρήση εργαλείων, τα οποία ονομάζονται «sniffers». Αυτά τα εργαλεία συλλέγουν πακέτα που διακινούνται σε κάποιο δίκτυο και ανάλογα με την ποιότητά τους, αναλύουν τα δεδομένα που έχουν συλλεχθεί.

Η διαφορά της τεχνικής Eavesdropping με την τεχνική Man in the middle είναι ότι διαβάζει την συνομιλία χωρίς να παραποιεί το περιεχόμενο τους, δηλαδή απλά υποκλέπτει τη συνομιλία μεταξύ των δυο χωρίς αυτοί να το γνωρίζουν ενώ στην τεχνική Man in the middle ο εισβολέας προσποιείται ότι είναι ο παραλήπτης, λαμβάνει όλα τα μηνύματα που στέλνονται από τον αποστολέα και τα παραποιεί.



Εικόνα 6.3: Επίθεση Eavesdropping

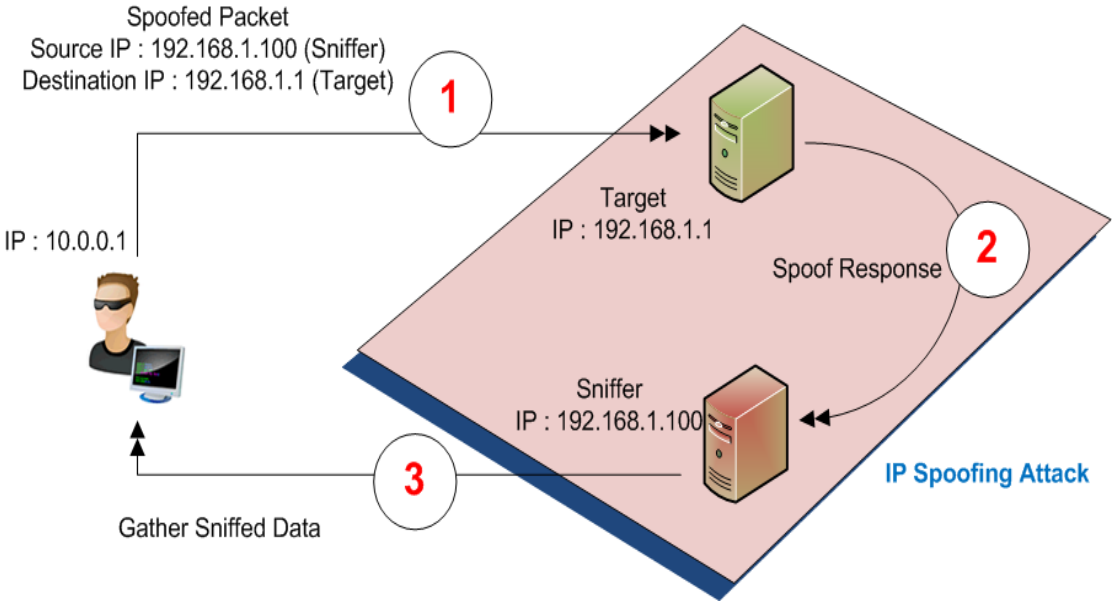
Μια τέτοια επίθεση Eavesdropping στο έξυπνο δίκτυο μπορεί να γίνει κατά την αποστολή των μηνυμάτων από τα Smart Meters προς τα NAN aggregators που αναλαμβάνουν τη συλλογή, την επεξεργασία και την προώθησή των μετρήσεων που συλλέγουν στα κεντρικά συστήματα της εταιρείας παροχής. Τέτοιες επιθέσεις, θα μπορούσαν να έχουν ως αποτέλεσμα, τόσο την αποκάλυψη ιδιωτικής πληροφορίας των κατοίκων, όσο και την αποκάλυψη στοιχείων που αφορούν στα πρωτόκολλα επικοινωνίας μεταξύ μετρητών και NAN aggregators (δομές μηνυμάτων κτλ.) και θα μπορούσαν να συμβάλουν ώστε ο

επιτιθέμενος να σχεδιάσει επιθέσεις προσωποποίησης μετρητών (ή απλώς τροποποίηση του δικού του), προκειμένου να εισάγει λανθασμένα στοιχεία τα οποία θα μπορούσαν να προκαλέσουν αστάθειες λόγω ανακρίβειας[28].

6.2.4 ΕΠΙΘΕΣΗ SPOOFING

Κατά τις επιθέσεις αυτές ο επιτιθέμενος προσποιείται κάποιον άλλον «μεταμφιέζεται» ώστε να αποκτήσει εξουσιοδοτημένη πρόσβαση στους πόρους του συστήματος με σκοπό να περιορίσει τους πόρους η να υποκλέψει χρήσιμες πληροφορίες. Οι χαρακτηριστικότερες επιθέσεις του είδους είναι το IP spoofing(Εικόνα 6.4), το DNs spoofing και το ARP spoofing.

Σε μια επίθεση spoofing ένας εισβολέας μπορεί να μιμηθεί την διεύθυνση IP ενός νόμιμου χρήστη, προκειμένου να μπει στον λογαριασμό του. Επίσης κάποιος μπορεί να στείλει παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου emails και να δημιουργεί ψεύτικες ιστοσελίδες προκειμένου να λάβει ονόματα χρήστη, κωδικούς πρόσβασης των χρηστών καθώς και άλλα στοιχεία του λογαριασμού κάποιου χρήστη. Μια άλλη μέθοδος spoofing περιλαμβάνει τη δημιουργία ενός ψεύτικου σημείου ασύρματης πρόσβασης και την εξαπάτηση θυμάτων σε παράνομη σύνδεση σε αυτό[29].



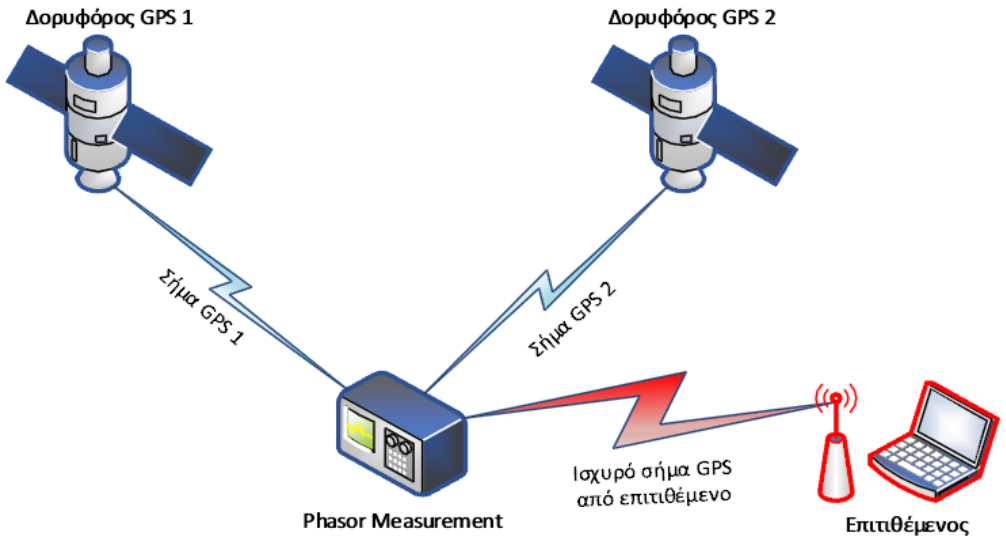
Εικόνα 6.4:Επίθεση IP spoofing

Στο επίπεδο του δικτύου ηλεκτρικής ενέργειας, τα δεδομένα από απομακρυσμένες τερματικές μονάδες (Remote Terminal Units), αισθητήρες (sensors) και έξυπνους μετρητές μεταδίδονται στο κέντρο ελέγχου για την περαιτέρω επεξεργασία τους. Αν κάποιος εισβολέας έκανε κάποια επίθεση σε μία συσκευή αλλά ταυτόχρονα τροποποιούσε τα συλλεγόμενα δεδομένα που προέρχονται από αυτήν, τότε ο χειριστής θα αντιλαμβανόταν μία ομαλή λειτουργία στο δίκτυο και έτσι η επίθεση θα ήταν απαρατήρητη. Δηλαδή κατά την διάρκεια μιας επίθεσης “spoofing” ο εισβολέας μπορεί να συνεχίσει να στέλνει εντολές σε κάποια συσκευή ή κάποιον ελεγκτή, με σκοπό να προκαλέσει μία κακόβουλη ενέργεια, ενώ ο χειριστής θα εξακολουθούσε να μη γνωρίζει την πραγματική κατάσταση του συστήματος[30].

6.2.4.1 GPS SPOOFING

Η επίθεση GPS spoofing πραγματοποιείται επηρεάζοντας το δέκτη του GPS στέλνοντας ισχυρότερο δορυφορικό σήμα με αποτέλεσμα να αποδιοργανώνει την τελική κατεύθυνση. Για να γίνει αυτό χρειάζεται το σήμα να είναι τόσο κατάλληλο ώστε να επηρεάσει σωστά τη σχέση χρόνου και χώρου.

Μια τέτοια επίθεση στο έξυπνο πλέγμα μπορεί να πραγματοποιηθεί στις μονάδες Phasor Measurement Units. Σε μια τέτοια επίθεση GPS spoofing (σχήμα 6.5) ο επιτιθέμενος έχει ως στόχο να εξαναγκάσει τις μονάδες Phasor Measurement Units να επιλέξουν το σταθμό του επιτιθέμενου ως πηγή συγχρονισμού, με τον επιτιθέμενο να αντικαθιστά τους δορυφόρους GPS. Ο επιτιθέμενος στην αρχή βρίσκει τα μηνύματα συγχρονισμού που αποστέλλουν οι δορυφόροι, κάτι το οποίο είναι πολύ εφικτό καθώς τα μηνύματα που αποστέλλουν οι δορυφόροι είναι προσδιορίσιμα, και εκπέμπει ακριβώς τα ίδια μηνύματα συγχρονισμού με τους πραγματικούς δορυφόρους. Στη συνέχεια ο επιτιθέμενος αυξάνει την ισχύ εκπομπής υπερκαλύπτοντας το σήμα των πραγματικών δορυφόρων με αποτέλεσμα ο δέκτης του στόχου να κλειδώνει το δικό του σήμα. Με το που κλειδώσει ο δέκτης το σήμα η διάταξη του επιτιθέμενου μετατοπίζει σε κάθε δευτερόλεπτο κατά μερικά ns τη χρονική στιγμή που αναφέρει στη διάταξη. Έτσι ο στόχος ολισθαίνει κατά μερικά ns για κάθε δευτερόλεπτο που περνάει. Με αυτόν τον τρόπο δεν ενεργοποιείται κάποιος συναγερμός καθώς ο επιτιθέμενος δεν γίνεται αντιληπτός οδηγώντας το σύστημα ελέγχου να ενεργοποιήσει μεθόδους για να αποτρέψει τις ακραίες τιμές που παρατηρούνται με συνέπεια να έχει αρνητικά αποτελέσματα[39].



Σχήμα 6.5: Επίθεσης GPS Spoofing

.

6.3 ΕΠΙΘΕΣΗ ΑΝΑΚΑΤΑΝΟΜΗΣ ΦΟΤΙΟΥ

Ο υπολογισμός κατάστασης αποτελεί στοιχείο κλειδί για τη λειτουργία και τον έλεγχο ενός αξιόπιστου συστήματος. Ο υπολογισμός κατάστασης συλλέγει πληροφορίες μετρήσεων από ένα μεγάλο αριθμό μετρητών και τις αναλύει συγκεντρωτικά στο κέντρο ελέγχου. Στη συνέχεια πραγματοποιείται υπολογισμός ελαχιστοποίησης του συνολικού λειτουργικού κόστους μέσω της ανακατανομής της ισχύος παραγωγής.
Ωστόσο, πρόσφατα αποδείχτηκε ότι ο υπολογισμός κατάστασης είναι ευάλωτος σε σκόπιμες επιθέσεις μόλυνσης με λανθασμένα δεδομένα. Συνεργατικά χειρίζονται τις μετρήσεις που λαμβάνουν οι διάφοροι μετρητές, διαστρεβλώνοντας έτσι το αποτέλεσμα του υπολογισμού κατάστασης. Σαν αποτέλεσμα, ένας λανθασμένος υπολογισμός ελαχιστοποίησης του συνολικού λειτουργικού κόστους θα οδηγήσει το σύστημα σε μη οικονομική λειτουργία, συνοδευόμενη ίσως από άμεση κατάρρευση φορτίου.

Μια ειδική κατηγορία επιθέσεων μόλυνσης με λανθασμένα δεδομένα είναι η επίθεση κακόβουλης ανακατανομής φορτίου. Σε αυτή την επίθεση, οι επιτιθέμενοι αυξάνουν το φορτίο σε κάποιους ζυγούς και ανάλογα μειώνουν το φορτίο σε άλλους ζυγούς, διατηρώντας αμετάβλητο το συνολικό φορτίο. Με αυτό τον τρόπο μπορούν να παραπλανήσουν τη διαδικασία υπολογισμού κατάστασης χωρίς να εντοπιστούν από μηχανισμούς που εντοπίζουν λανθασμένα δεδομένα. Σε πρώτο στάδιο, ίσως οδηγήσουν το σύστημα σε μια μη βέλτιστη κατανομή της παραγωγής ή τοπική κατάρρευση φορτίου, ενώ σε δεύτερο στάδιο, ίσως οδηγήσουν σε μη ασφαλή κατάσταση λειτουργίας(η ροή ισχύος σε κάποιες γραμμές μεταφοράς μπορεί να υπερβεί τη χωρητικότητά) [24].

ΚΕΦΑΛΑΙΟ 7

ΕΠΙΘΕΣΕΙΣ ΣΤΑ ΕΞΥΠΝΑ ΠΛΕΓΜΑΤΑ

7.1 Μεθοδοι επιθεσησ στο Hardware των εξυπνων μετρητων

Οι έξυπνοι μετρητές διαθέτουν αρκετές θύρες επικοινωνίας. Διαθέτουν θύρες για να επικοινωνούν με τις διάφορες οικιακές συσκευές και για να συνδέονται με το Default Gateway των οικιών ώστε να έχουν πρόσβαση στο διαδίκτυο και να συνδέονται με το κέντρο διαχείρισης δεδομένων του διαχειριστή του δικτύου ηλεκτρικής ενέργειας. Επίσης διαθέτουν θύρες για φυσική πρόσβαση στο υλικό των έξυπνων μετρητών για να μπορούν να έχουν πρόσβαση οι τεχνικοί σε περίπτωση βλάβης ή σε περιπτώσεις συντήρησης της συσκευής. Μέσω αυτών των θυρών οι τεχνικοί μπορούν να ελέγξουν, να ανιχνεύσουν και να διορθώσουν ενδεχόμενα σφάλματα που δεν μπορούν να διορθώσουν μέσω απομακρυσμένης σύνδεσης.

7.1.1 Επιθεσεισ στα πρωτοκολλα επικοινωνιασ φυσικων θυρων των εξυπνων μετρητων

Τα πρωτόκολλα επικοινωνίας που υλοποιούνται στις φυσικές θύρες των έξυπνων μετρητών διαφέρουν μεταξύ Ευρώπης και Αμερικής. Στην Αμερική χρησιμοποιούνται τα πρωτόκολλα C12.18, C12.19, C12.21 και C12.22 ενώ στην Ευρώπη το πρωτόκολλο IEC 62056. Τα πρωτόκολλα C12.21 και C12.18 έχουν εμφανίσει αρκετά κενά ασφάλειας τα οποία μπορούν πολύ εύκολα κάποιοι κακόβουλοι χρήστες να τα εκμεταλλευτούν και να πραγματοποιήσουν μια επίθεση. Το κενό ασφάλειας που έχει το πρωτόκολλο C12.18 είναι ότι δεν περιλαμβάνει μηχανισμούς ασφάλειας στη μετάδοση πληροφοριών. Ο μόνος μηχανισμός ασφάλειας που έχει το πρωτόκολλο C12.18 είναι ένας κωδικός πρόσβασης, ο οποίος έχει εισαχθεί για την ταυτοποίηση του τεχνικού προσωπικού, όταν είναι να επικοινωνήσει με τον έξυπνο μετρητή. Ο κωδικός πρόσβασης όμως δεν κρυπτογραφείται κατά την μετάδοση αλλά μεταδίδεται αυτούσιος, κάτι που σημαίνει ότι ένας επιτιθέμενος μπορεί να υποκλέψει με ένα δέκτη υπέρυθρων τη μετάδοση του κωδικού και να τον χρησιμοποιήσει για να αποκτήσει πρόσβαση στον έξυπνο μετρητή.

Σε αντίθεση με το πρωτόκολλο C12.18 στο πρωτόκολλο C12.21 ο κωδικός πρόσβασης που χρησιμοποιείται για την ταυτοποίηση του χρήστη που επικοινωνεί με τη συσκευή του μετρητή μεταδίδεται κρυπτογραφημένος, οπότε δεν μπορεί να υποκλαπεί κατά τη διαδρομή από τη συσκευή χρήστη στον έξυπνο μετρητή. Το πρόβλημα όμως που παρουσιάζει το πρωτόκολλο αυτό είναι ότι τα δεδομένα που ανταλλάσσονται στη συνέχεια δεν είναι

κρυπτογραφημένα και δεν περιλαμβάνουν μηχανισμούς για την προστασία από την αλλοίωση των δεδομένων. Σε μια τέτοια περίπτωση ένας επιτιθέμενος μπορεί να παρακολουθεί τη γραμμή, να υποκλέψει και να αλλοιώσει τα δεδομένα που ανταλλάσσονται.

Ωστόσο, το σημαντικότερο, ίσως, κενό ασφαλείας του πρωτοκόλλου C12.21 βρίσκεται στη διαδικασία ταυτοποίησης του μετρητή στο διαχειριστή του δικτύου HE. Αυτό το κενό ασφαλείας καθιστά τη διαδικασία ευάλωτη σε επίθεση επανάληψης. Η διαδικασία αυτή έχει χρησιμοποιηθεί για να ταυτοποιηθεί ξένη συσκευή στο δίκτυο της εταιρείας HE, προσποιούμενη το μετρητή, και να μεταδώσει ψευδή στοιχεία κατανάλωσης[31] [32].

7.1.2 Επιθεση υποκλοπης απο το διαυλο δεδομενων της μητρικης πλακετας

Η υποκλοπή πληροφοριών από το δίαυλο δεδομένων είναι μια δύσκολη μέθοδος και προϋποθέτει την πλήρη πρόσβαση στο εσωτερικό του έξυπνου μετρητή και τη χρήση εξειδικευμένων αισθητήρων για την ανίχνευση των σημάτων στο δίαυλο δεδομένων. Τα δεδομένα που εισάγονται μέσω των θυρών I/O της συσκευής μεταφέρονται στη μνήμη της συσκευής για περαιτέρω χρήση από το λειτουργικό σύστημα. Η μεταφορά αυτή γίνεται μέσω του διαύλου δεδομένων [31].

Το δυνατό σημείο της επίθεσης αυτού του τύπου είναι το γεγονός ότι μπορεί σε αρκετές περιπτώσεις να καταρρίψει τη χρήση κρυπτογράφησης κατά τη μεταφορά δεδομένων από τις θύρες I/O προς τη μνήμη. Για παράδειγμα, το πρωτόκολλο ANSI C12.22 χρησιμοποιεί κρυπτογράφηση AES 256-bit. Για την αποκρυπτογράφηση των δεδομένων αυτά οδηγούνται πρώτα στο εξειδικευμένο chip αποκρυπτογράφησης AES και στη συνέχεια μεταφέρονται αποκρυπτογραφημένα στη μνήμη του συστήματος. Η μεταφορά από το chip αποκρυπτογράφησης στους buffers της συσκευής γίνεται μέσω του διαύλου δεδομένων. Συνεπώς, ο επιτιθέμενος μπορεί να υποκλέψει τα δεδομένα παρά το ότι η μετάδοσή τους προς τη συσκευή έγινε με χρήση δυνατής κρυπτογράφησης [39].

7.1.3 Επιθεση μεσω της θυρας JTAG

Η θύρα JTAG δεν βρίσκεται στο εξωτερικό περίβλημα του έξυπνου μετρητή αλλά στο εσωτερικό του μετρητή και συγκεκριμένα πάνω στη μητρική πλακέτα. Αυτό καθιστά δύσκολη την πρόσβαση σε αυτή τη θύρα από έναν επιτιθέμενο. Η θύρα αυτή χρησιμοποιείται από τους κατασκευαστές των έξυπνων μετρητών για τον εντοπισμό σφαλμάτων των κυκλωμάτων που χρησιμοποιούνται στην πλακέτα και επίσης κατά τον ποιοτικό έλεγχο των ηλεκτρονικών συσκευών.

Ο λόγος που ένας επιτιθέμενος θα θελήσει να πραγματοποιήσει επίθεση μέσω της θύρας JTAG είναι οι πολλές δυνατότητες που του προσφέρει. Οι τρείς κυριότεροι είναι οι εξής :

- Πρόσβαση στις λειτουργίες τον επιμέρους κυκλωμάτων της μητρικής πλακέτας
- Επιτρέπει στον επιτιθέμενο να διαβάσει και να πραγματοποιήσει αλλαγές στα δεδομένα της μνήμης RAM
- Δίνει την δυνατότητα στον επιτιθέμενο να διαβάσει και να τροποποιήσει τα δεδομένα στη μη πτητική μνήμη του μετρητή

Ένας επιτιθέμενος έχοντας πρόσβαση στη μνήμη RAM μπορεί να υποκλέψει αποθηκευμένα δεδομένα από τις εφαρμογές που τρέχουν στον έξυπνο μετρητή, να αλλάξει τις τιμές σε επιλεγμένες θέσεις μνήμης και να διαπιστώσει πως επηρεάζεται η λειτουργία των εφαρμογών ώστε να ανακαλύψει τα αποτύπωμά τους στην μνήμη RAM. Για παράδειγμα πραγματοποιώντας κάποιες αλλαγές τον δεδομένων σε ορισμένες θέσεις μνήμης του μετρητή ενδέχεται να αλλάξουν τα δεδομένα κατανάλωσης που στέλνει ο μετρητής στο κέντρο διαχείρισης δεδομένων.

Στη μη-πτητική μνήμη φυλάσσονται δεδομένα όπως για το λειτουργικό σύστημα και το firmware του έξυπνου μετρητή, δεδομένα ταυτοποίησης της συσκευής με το διαχειριστή του δικτύου ηλεκτρικής ενέργειας αλλά και δεδομένα ταυτοποίησης των χρηστών στο σύστημα του μετρητή. Έχοντας πρόσβαση στη μη πτητική μνήμη ένας επιτιθέμενος ανιχνεύοντας τη λειτουργία του firmware θα μπορούσε να επιχειρήσει την αλλαγή τμημάτων του κώδικα προς όφελος του και να ανακαλύψει τις θέσεις στη μη πτητική μνήμη όπου βρίσκονται οι κωδικοί ασφαλείας και τα κλειδιά κρυπτογράφησης και να τα χρησιμοποιήσει ώστε να συνδέεται με το διαχειριστή του δικτύου ηλεκτρικής ενέργειας προσποιούμενος τον έξυπνο μετρητή.

7.1.4 Επιθεση ψυχρης εκκινησης

Η επίθεση ψυχρής εκκίνησης είναι μία μέθοδος που έχει στόχο να αποκτήσει τα δεδομένα που είναι αποθηκευμένα στη μνήμη RAM. Στην πληροφορική με τον όρο RAM αναφερόμαστε στην κύρια ή κεντρική μνήμη ενός υπολογιστικού συστήματος. Στη μνήμη αυτή αποθηκεύονται προγράμματα και δεδομένα προκειμένου είτε να εκτελεστούν είτε να υποστούν επεξεργασία αντίστοιχα. Βασικό χαρακτηριστικό σε αυτή τη μνήμη είναι ότι η μνήμη RAM διατηρεί τα περιεχόμενα της μόνο όσο της το επιτρέπει ο χρήστης ή το λογισμικό που εκτελείται και μόνο εφόσον το υπολογιστικό σύστημα τροφοδοτείται με ηλεκτρική ενέργεια. Σε αντίθετη περίπτωση με το που σταματάει η τροφοδοσία τα δεδομένα χάνονται ολοσχερώς.

Ο λόγος όμως που μπορεί να γίνει επίθεση ψυχρής εκκίνησης είναι ότι η απώλεια δεδομένων δε συμβαίνει ακαριαία. Ο χρόνος διατήρησης των δεδομένων που βρίσκονται στη μνήμη RAM αφού έχει γίνει η διακοπή τροφοδοσίας εξαρτάται από τις συνθήκες θερμοκρασίας που επικρατούν. Συγκεκριμένα πραγματοποιώντας μια βαθιά ψύξη των κυκλωμάτων της μνήμης είναι δυνατή η διατήρηση των δεδομένων για αρκετό χρονικό διάστημα. Το χρονικό αυτό διάστημα είναι αρκετό ώστε ένας επιτιθέμενος να υποκλέψει τα αποθηκευμένα δεδομένα, τα κλειδιά κρυπτογράφησης αλλά ακόμα και τμήματα κώδικα που είναι αποθηκευμένα στη μνήμη για λόγους instruction caching. Πάντως μια τέτοια μέθοδος είναι αρκετά δύσκολη να πραγματοποιηθεί καθώς ένας επιτιθέμενός θα πρέπει να έχει εξοπλισμό βαθιάς ψύξης και να έχει πρόσβαση στο ολοκληρωμένο κύκλωμα της μνήμης RAM για να μπορέσει να υποκλέψει τα δεδομένα της.

7.1.5 Επιθεσεις παραπλευρων καναλιων

Οι επιθέσεις παράπλευρων καναλιών έχουν ως στόχο τους αλγόριθμους κρυπτογράφησης που υλοποιούνται στον έξυπνο μετρητή. Αυτές οι επιθέσεις παρακάμπτουν την ασφάλεια αυτών των αλγόριθμων κρυπτογράφησης και βρίσκουν τις ευπάθειες των υλοποιήσεων αυτών των αλγόριθμων στο Hardware. Ο επιτιθέμενος για να πραγματοποιήσει μια τέτοια μελετάει τη μεταβολή πλευρικών σημάτων εισόδου και εξόδου από το ολοκληρωμένο κύκλωμα που πραγματοποιεί την κρυπτογράφηση. Πλευρικά σήματα ονομάζονται τα σήματα μεγεθών που επηρεάζονται από την ενέργεια που πραγματοποιείται στο ολοκληρωμένο κύκλωμα αλλά τα οποία δε χρησιμοποιούνται από αυτό για να μεταφέρουν κάποια πληροφορία. Τέτοια σήματα μπορούν να είναι η ισχύς που καταναλώνεται, οι εκπομπές ΗΜ κυμάτων, η χρονική καθυστέρηση στην απόκριση του ολοκληρωμένου κυκλώματος, ακόμα και ηχητικά κύματα που προέρχονται από αυτό[39].

Για να πραγματοποιηθούν οι παραπάνω επιθέσεις χρειάζεται ένας επιτιθέμενος τον κατάλληλο εξοπλισμό ανίχνευσης σημάτων των πλευρικών καναλιών ο οποίος όμως έχει υψηλό κόστος. Ωστόσο μέθοδοι όπως αυτή των ηχητικών κυμάτων μπορούν να πραγματοποιηθούν και από μια απλή συσκευή κινητού με την προϋπόθεσή ότι βρίσκεται σε απόσταση κάτω των τριάντα μέτρων από τον έξυπνο μετρητή. Τέτοιες επιθέσεις είναι αποτελεσματικές για την εξακρίβωση στοιχείων της εκτέλεσης του αλγορίθμου κρυπτογράφησης και σε αρκετές περιπτώσεις μπορούν να οδηγήσουν μέχρι και στην υποκλοπή του κλειδιού του αλγορίθμου RSA, που είναι θεμελιώδης για τους αλγόριθμους κρυπτογράφησης δημοσίου κλειδιού. Μία επιτυχημένη επίθεση τέτοιου είδους εναντίον των ευφυών μετρητών επιτρέπει στον επιτιθέμενο να παραβιάσει την κρυπτογράφηση που χρησιμοποιείται στην επικοινωνία με το κέντρο διαχείρισης δεδομένων, να «υφαρπάξει» την επικοινωνία, μέχρι και να εισάγει δικά του πακέτα στη σύνδεση χωρίς να γίνει αντιληπτός. Τέλος, είναι μια κατηγορία μεθόδων ιδιαίτερα διαδεδομένη λόγω του μικρού κόστους υλοποίησης, και στην οποία ανακαλύπτονται συνεχώς νέες επιθέσεις εναντίον συστημάτων που θεωρούνται ασφαλή[39][67].

7.2 Επιθεση DoS στα συστηματα SCADA μεσω του πρωτοκολλου DNP3

Τα περισσότερα βιομηχανικά πρωτόκολλα που χρησιμοποιούνται σήμερα δεν έχουν σχεδιαστεί με κριτήριο και την ασφάλεια, χαρακτηριστικό που επιτρέπει την εκμετάλλευση δομών του πρωτοκόλλου ώστε να τίθεται εκτός λειτουργίας το βιομηχανικό πληροφοριακό δίκτυο ΗΕ. Ενδεικτικά, για το πρωτόκολλο DNP3 που χρησιμοποιείται ευρέως στη βιομηχανία ΗΕ, υπάρχουν αρκετοί τρόποι ώστε μέσω του πρωτοκόλλου να γίνει επίθεση DoS εναντίον του δικτύου. Ορισμένοι από αυτούς είναι οι εξής[39]:

- Εισαγωγή μηνυμάτων broadcast τα οποία προκαλούν το φαινόμενο της πλημμύρας μηνυμάτων (flooding) στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ.
- Αλλοίωση των πακέτων χρονικού συγχρονισμού, με αποτέλεσμα διατάξεις να αποσυγχρονίζονται και τα πακέτα τους να καθίστανται άκυρα.
- Αλλοίωση ή απώλεια μηνυμάτων επιβεβαίωσης που θα οδηγούν σε καταστάσεις συνεχούς αναμετάδοσης δεδομένων, κάτι που διακόπτει τη λειτουργία του δικτύου.

Οι ανωτέρω μέθοδοι δεν εκμεταλλεύονται κάποια ευπάθεια του πρωτοκόλλου DNP3 για να προκαλέσουν απώλεια διαθεσιμότητας αλλά, αντίθετα, εκμεταλλεύονται υπάρχουσες λειτουργίες του πρωτοκόλλου σε συνδυασμό με έλλειψη ελέγχου των τιμών των πακέτων. Ωστόσο, μπορεί να προκληθεί απώλεια διαθεσιμότητας από εκμετάλλευση ευπαθειών του πρωτοκόλλου DNP3. Σε πολλές από αυτές τις επιθέσεις, η απώλεια διαθεσιμότητας επιτυγχάνεται με την αποστολή ειδικά διαμορφωμένων πακέτων στη διάταξη master, με στόχο να τεθεί ο εποπτικός σταθμός σε ατέρμονα βρόχο ώστε να μη λειτουργεί μέχρι να γίνει χειροκίνητη επανεκκίνηση. Έτσι, τίθεται ολοκληρωτικά εκτός λειτουργίας ο εποπτικός σταθμός SCADA.
Όλες οι ανωτέρω μέθοδοι μπορούν να υλοποιηθούν με μεγάλη ευκολία, έχοντας ταυτόχρονα καταστροφικές συνέπειες για τη λειτουργία του βιομηχανικού πληροφοριακού δικτύου ΗΕ για το χρονικό διάστημα κατά το οποίο πραγματοποιούνται. Συνεπώς, αν ένα τμήμα του βιομηχανικού πληροφοριακού δικτύου ΗΕ τεθεί εκτός λειτουργίας, οι υπηρεσίες και η λειτουργικότητα του Smart Grid εμφανίζουν σημαντικό πρόβλημα. Επομένως, πρέπει να λαμβάνεται ειδική μέριμνα για αυτού του είδους τις επιθέσεις.

7.3 Επιθεσεις στα πρωτοκολλα επικοινωνιας Modbus και IEC 60870-5- 104

Η εμπλοκή του πρωτοκόλλου Modbus μέσα στο σύστημα SCADA δεν έχει κατάλληλο μηχανισμό που να αντιμετωπίζει την ασφάλεια κατά την διάρκεια της επικοινωνίας μεταξύ συσκευών πεδίου με αποτέλεσμα, η επικοινωνία Modbus να είναι ευάλωτη από διάφορους τύπους επιθέσεων. Συνήθως κάθε σύστημα ή δίκτυο έχει διαφορετικές προδιαγραφές εφαρμογής και επικοινωνίας αλλά με κοινά θέματα ασφάλειας, ενώ συνδέεται με το διαδίκτυο. Η έλλειψη ασφάλειας μέσα στην επικοινωνία SCADA /Modbus έχει δημιουργήσει ένα σενάριο επιθέσεων. Χρησιμοποιώντας το εργαλείο επιθέσεων Snort σε πειράματα που έγιναν μας έδειξε πράγματι ότι το πρωτόκολλο Modbus είναι ευάλωτο και θα πρέπει να ενσωματώσει κάποιους μηχανισμούς ασφαλείας για να μπορεί να αποτρέπει τους επίδοξους εισβολείς [64].

Το πρωτόκολλο IEC 60870-5-104 έχει σχεδιαστεί χωρίς καμία πρόβλεψη ασφαλείας και επίσης στερείται μηχανισμού αυθεντικότητας ή κρυπτογράφησης. Αυτά τα χαρακτηριστικά το κάνουν ιδιαίτερα ευάλωτο σε επιθέσεις. Έχει διεξαχθεί μία ανάλυση για τις απειλές ασφάλειας και τις τρωτότητες του συστήματος και μία μέθοδο με την ονομασία “Fuzz” έχει προταθεί για τον έλεγχο του πρωτοκόλλου IEC60870-5-104 μεταξύ των κόμβων ή των συσκευών των πεδίων. Το “Fuzzing “ είναι ένα εργαλείο ή μέθοδος ελέγχου που χρησιμοποιείται για να ελέγχει το εισερχόμενο μήνυμα ή τα τυχαία bytes και να απεικονίζει τη συνέχεια στην διεπαφή του. Το εργαλείο “Fuzz” χρησιμοποιεί δύο τύπους ελέγχου όπως το έγκυρο Fuzz, στο οποίο bytes μοιάζουν ως προς το επιθυμητό αποτέλεσμα και το απλό fuzz στο οποίο τα εισερχόμενα bytes βασίζονται στη παραγωγή ψεύτικων τυχαίων αριθμών [64].

Multicasting communication security: Ο κεντρικός σταθμός εκκινεί την επικοινωνία πολλαπλής διανομής και αποστέλλει το μήνυμα σε απομακρυσμένους σταθμούς. Το μήνυμα έχει κρυπτογραφηθεί με ένα μυστικό κλειδί που έχει δημιουργηθεί από έναν αλγόριθμο AES

και έπειτα η κατακερματισμένη αξία υπολογίζεται χρησιμοποιώντας τον κατακερματισμένο αλγόριθμο SHA-2. Το μυστικό κλειδί έχει με ασφάλεια διανεμηθεί από τον κεντρικό σταθμό και τους απομακρυσμένους σταθμούς χρησιμοποιώντας ασφαλή κανάλια. (ο αλγόριθμος RSA δεν είναι αξιόπιστος για επικοινωνία πολλαπλής διανομής επειδή αποκτούνται πολλά κλειδιά κατά την διάρκεια της επικοινωνίας, που επηρεάζουν κατά πολύ την απόδοση σημαντικών συστημάτων.) Η κατάσταση M100/I20 (σχήμα 7. 1) αντιπροσωπεύει το αίτημα της διαδικασίας αρχικοποίησης του κεντρικού σταθμού και η κατάσταση M101/I22 αντιπροσωπεύει τη διαδικασία κρυπτογράφησης. Όταν η διαδικασία κρυπτογράφησης ολοκληρωθεί και ο κεντρικός σταθμός διανείμει πολλαπλώς το μήνυμα τότε οι απομακρυσμένοι σταθμοί αποκρυπτογραφούν το μήνυμα στην κατάσταση M102/I22. Εάν κάποιο μήνυμα απαντηθεί όπως η επιβεβαίωση ή οποιοδήποτε άλλο στον κεντρικό σταθμό, ο απομακρυσμένος σταθμός αλλάζει την απάντηση από τη κατάσταση M104/I24 σε κατάσταση M106/I26. Οι καταστάσεις M107/I27 και M108/I28 δείχνουν ότι ο κεντρικός σταθμός έχει λάβει απάντηση από τον απομακρυσμένο σταθμό. Οι καταστάσεις M310/I53 και M312 αντιπροσωπεύουν ότι οι επιθέσεις όπως η αυθεντικοποίηση, η ακεραιότητα και η εμπιστευτικότητα έχουν εντοπιστεί και η συμπεριφορά του συστήματος μετριέται στην κατάσταση M313/I56 [64].

Διαδικασία κρυπτογράφησης(απόδειξη)

- Μήνυμα πολλαπλής διανομής = $(\text{Encry}(\text{payload}_{(SCK,\ Hash\ ,Node)}))^{n}$, n =1,2,3……., n-1
- Κρυπτογραφημένο μήνυμα (ωφέλιμο φορτίο) πολλαπλή διανομή από το κόμβο –αποστολέα στους κόμβους –δέκτες

Όπου

- Total no ο συνολικός αριθμός κόμβων μέσα στην επικοινωνία εξαρτάται από την αξία “n”
- $SC_{K(Node)}$ (User bytes) το κρυπτογραφημένο φορτίο χρησιμοποιεί μυστικό κλειδί και είναι προγραμματισμένο ως payload[1]
- $Hash_{(node)}$ (User bytes) το φορτίο αφομοιώνεται χρησιμοποιώντας SHA-2 και προκαθορισμένο ως Hash_payload

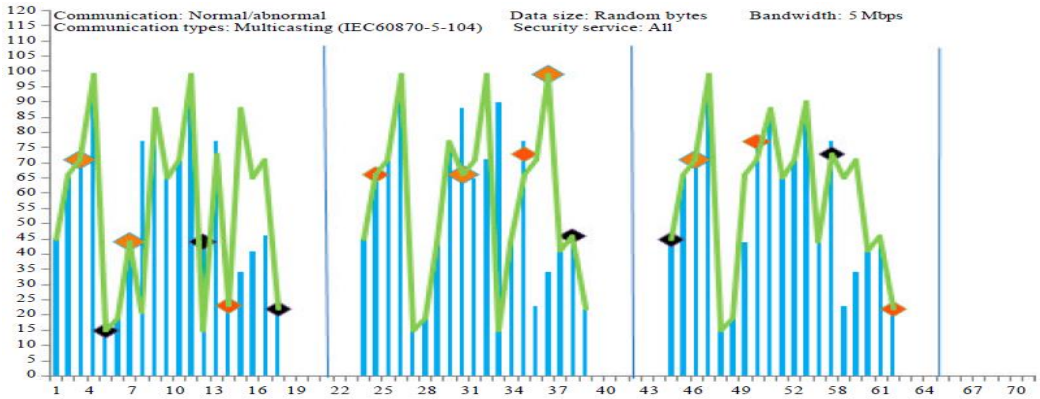
Διαδικασία αποκρυπτογράφησης(απόδειξη)

- Μήνυμα πολλαπλής διανομής =$\text{Decry}\ ((\text{payload}_{(SCK,\ Hash\ ,Node)}))^{1}$
- =$\text{Decry}\ ((\text{payload}_{(SCK,\ Hash\ ,Node)}))^{2}$,$(\text{Encry}(\text{payload}_{(SCK,\ Hash\ ,Node)}))^{2}$……$\text{decry}\ (\text{Encry}(\text{payload}_{(SCK,\ Hash\ ,Node)}))^{n-1}$
- Το μήνυμα πολλαπλής διανομής έχει ληφθεί από τον κεντρικό κόμβο στους απομακρυσμένους κόμβους
- $SC_{k(Sender,target\ node)}$ (User bytes)
- $Hash_{(target\ node)}$ (User bytes)=$Hash_{(sender)}$ (User bytes), έχει επιτυχώς επαληθεύσει τις υπηρεσίες ασφαλείας όπως αυθεντικοποίηση δεδομένων, δεδομένα ακεραιότητας και δεδομένα εμπιστευτικότητας κατά τη διάρκεια επικοινωνίας σε κάθε άκρο (κεντρικός προς κόμβους στόχευσης)

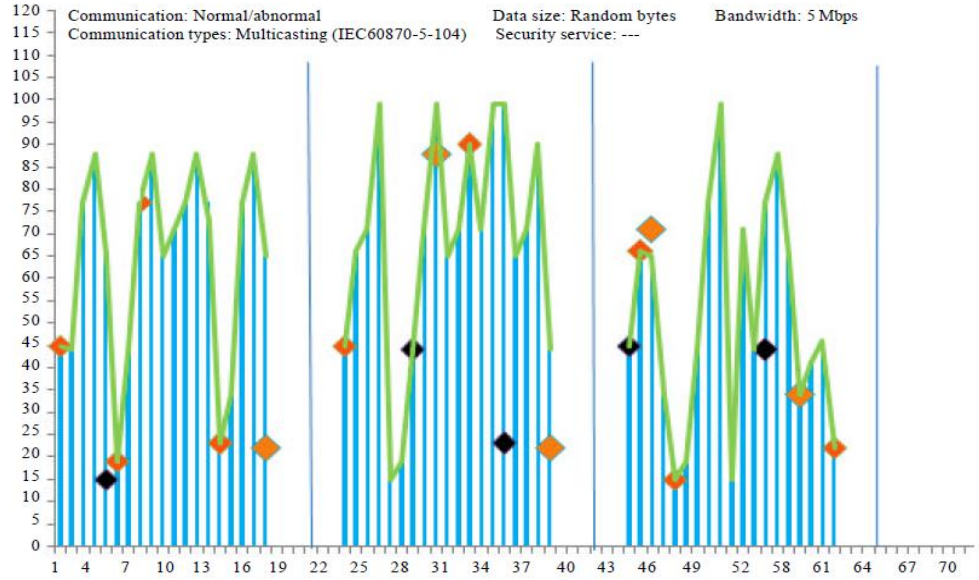
Οι πίνακες 7.1 και 7.2 δείχνουν τα αποτελέσματα συνολικής απόδοσης που έχουν μετρηθεί μέσα στο πεδίο δοκιμών SCADA κατά τη διάρκεια τόσο φυσιολογικής όσο και μη φυσιολογικής επικοινωνίας. Ο πίνακας 7.1 δείχνει τις μετρήσεις απόδοσης που έχουν αποθηκευτεί μέσα στο πεδίο δοκιμών SCADA/Modbus. Στους πίνακες 7.1 και 7.2 το κόκκινο αντιπροσωπεύει τις επιθέσεις αυθεντικότητας, το μαύρο τις επιθέσεις ακεραιότητας και το πορτοκαλί τις επιθέσεις εμπιστευτικότητας εν μέσω της επικοινωνίας. Ο πίνακας 7.3 αποτυπώνει την μέση αδράνεια που έχει μετρηθεί κατά την διάρκεια της επικοινωνίας. Η πράσινη γραμμή αντιπροσωπεύει την αδράνεια που υπολογίζεται από το πεδίο δοκιμών Modbus και η μπλε γραμμή δείχνει την αδράνεια από το πεδίο δοκιμών IEC60870-5 ως μέρος του συστήματος SCADA.

Polling communication security: Στο σύστημα SCADA, ο κεντρικός σταθμός ερευνά τον απομακρυσμένο σταθμό μέσα σε προκαθορισμένο διάλλειμα ή σε τυχαίο διάλλειμα ή συνεδρία. Το διάλλειμα χρόνου είναι μία σημαντική πτυχή με σημαντικές λειτουργίες του συστήματος SCADA. Σε μερικές περιπτώσεις, ο κεντρικός σταθμός καθορίζει το διάλλειμα έρευνας σε κάθε ένα μεμονωμένα και ο απομακρυσμένος σταθμός αποστέλλει την απάντηση μέσα στο προδιαγραμμένο διάλλειμα. Συνήθως οι λύσεις κρυπτογράφησης δεν είναι αξιόπιστες σε περίπτωση αιτήματος έρευνας μέσα στα συστήματα SCADA επειδή η κρυπτογράφηση καταναλώνει πολύ χρόνο για εφαρμογή. Εξαιτίας του περιορισμού ασφαλείας στο Modbus και του IEC 60870-5-104 ως μέρος του συστήματος SCADA, η λύση ασφάλειας που έχει προταθεί για να προστατεύσει τα πρωτόκολλα επικοινωνίας Modbus και του IEC 60870-5-104 είναι η εξής: Κάθε φορά ο κεντρικός σταθμός ερευνά τον απομακρυσμένο σταθμό και το αίτημα έρευνας κρυπτογραφείται με ένα κλειδί που έχει συγκεκριμένο χρόνο ζωής. Το αίτημα έρευνας είναι ρυθμισμένο ως προκαθορισμένο ή δυναμικό διάλλειμα και η διάρκεια ζωής του κλειδιού είναι ανάλογη με την συνεδρία έρευνας. Εάν η απάντηση δεν έχει ληφθεί μέσα στο προκαθορισμένο χρονικό διάστημα τότε το κλειδί περιόδου θα εκπνεύσει και ένα νέο κλειδί περιόδου θα αναπτυχθεί για ένα νέο αίτημα έρευνας [64].

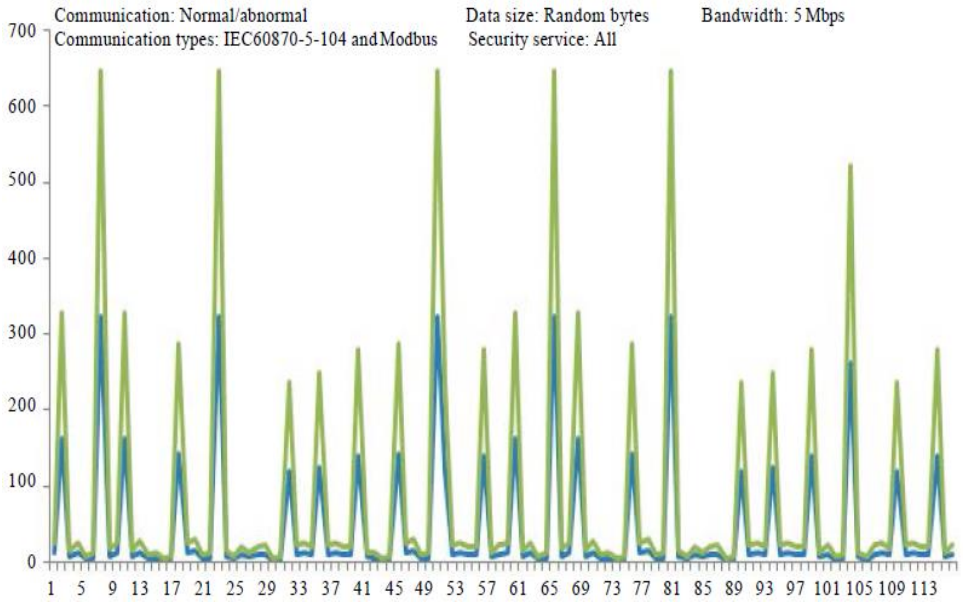
Οι καταστάσεις M500/I500, M502/I502, M507/I507 και M510/I510 στον πίνακα 7.4 αντιπροσωπεύουν τα αιτήματα συγκέντρωσης ενώ οι καταστάσεις M501/I501, M506/I506, M508/I508 και M511/I511 αντιπροσωπεύουν την απάντηση στην αίτηση έρευνας. Οι επιθέσεις όπως της αυθεντικοποίησης της ακεραιότητας και της εμπιστευτικότητας έχουν εντοπιστεί ως καταστάσεις M503/I503, M505/I504 και M505/I505 [64].



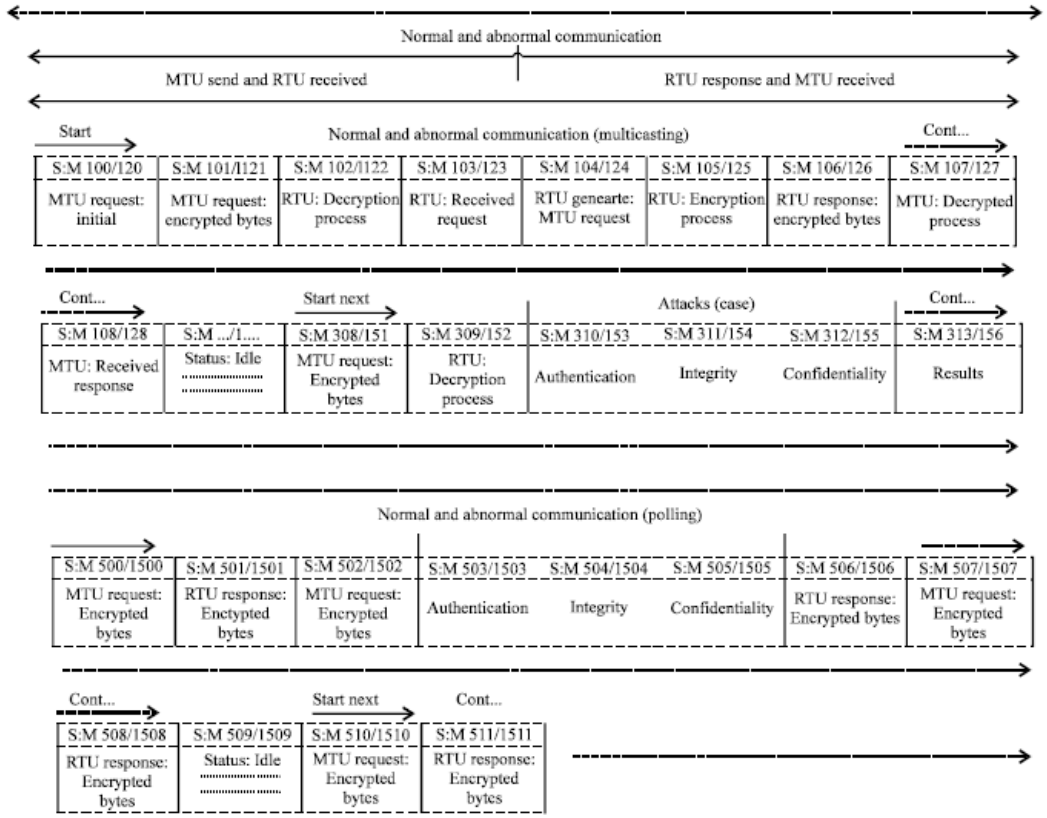
Εικόνα 7.1 Πολλαπλή διανομή κανονικής και μη κανονικής επικοινωνίας χρησιμοποιώντας το πρωτόκολλο IEC 60870-5-104



Εικόνα 7.2 Πολλαπλή διανομή κανονικής και μη κανονικής επικοινωνίας χρησιμοποιώντας το πρωτόκολλο Modbus



Εικόνα 7.3 Η μέση αδράνεια κατά την διάρκεια πολλαπλής διανομής χρησιμοποιώντας τα πρωτόκολλα Modbus και IEC60870-5-104



Εικόνα 7.4 SCADA πρωτόκολλα επικοινωνίας πολλαπλής διανομής και έλεγχος μετάδοσης

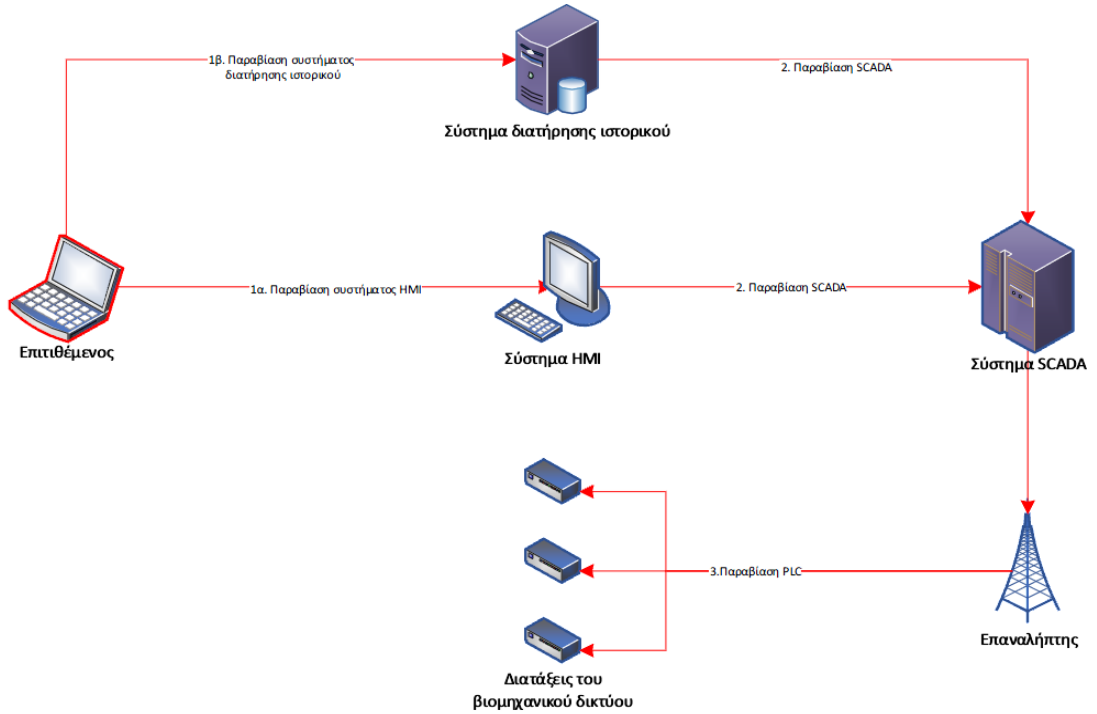
7.4 Μεθοδολογια μιας χαρακτηριστικης επιθεσης στα συστηματα SCADA

Η μεθοδολογία ενός επίδοξου εισβολέα για να πραγματοποιήσει μία επίθεση στα συστήματα SCADA με σκοπό να προκαλέσει τη διακοπή υπηρεσιών θα λέγαμε ότι αποτελείται από τα στάδια της ανίχνευσης, της πρόσβασης, της ανακάλυψης και του ελέγχου του συστήματος.

Στο στάδιο της ανίχνευσης ένας επίδοξος εισβολέας προσπαθεί να συγκεντρώσει όσες το δυνατόν περισσότερες πληροφορίες κυρίως από το διαδίκτυο. Οι πληροφορίες που ενδιαφέρουν έναν επιτιθέμενο μπορεί να είναι IP διευθύνσεις, διευθύνσεις email του εργατικού προσωπικού, πληροφορίες σχετικά με τα χαρακτηριστικά των πληροφοριακών συστημάτων που χρησιμοποιούνται και πολλές άλλες που θα του φανούν χρήσιμες για να πραγματοποιήσει μια επίθεση. Με την συγκέντρωση των απαραίτητων πληροφοριών ο επιτιθέμενος προχωράει σε ενέργειες που έχουν ως στόχο την είσοδο είτε στο σύστημα διατήρησης ιστορικού, είτε στο σύστημα HMI. Έχοντας αποκτήσει πρόσβαση στα συστήματα HMI ή στα συστήματα διατήρησης ιστορικού, επόμενος στόχος του εισβολέα είναι η πρόσβαση στα συστήματα SCADA.

Κακόβουλα λογισμικά τα οποία είναι κατάλληλα κατασκευασμένα έχουν τη δυνατότητα να εκμεταλλεύονται τις ευπάθειες στα λογισμικά SCADA και να είναι σε θέση να αποκτούν τον έλεγχο του συστήματος. Έτσι έχουν την δυνατότητα να επικοινωνούν με τις διατάξεις που

είναι υπό τον έλεγχο του συγκεκριμένου συστήματος και να αποκτούν τα ίδια δικαιώματα στο δίκτυο που έχει και το πραγματικό λογισμικό ελέγχου SCADA. Τα υπό έλεγχο του SCADA συστήματα διαθέτουν διατάξεις PLC στις οποίες προγραμματίζονται οι διαδικασίες αυτόματου ελέγχου που υλοποιούνται. Αυτές είναι προγραμματισμένες μέσω του βιομηχανικού πληροφοριακού δικτύου ηλεκτρικής ενέργειας από το σύστημα SCADA. Επομένως ένας επιτιθέμενος θα είναι σε θέση να διαβάσει τον κώδικα με τις διαδικασίες ελέγχου και να πραγματοποιήσει διάφορες τροποποιήσεις στον κώδικα εισάγοντας κακόβουλες εντολές με σκοπό να διακοπεί η σωστή λειτουργία της διάταξης του βιομηχανικού δικτύου ηλεκτρικής ενέργειας και να δημιουργήσει μεγάλα προβλήματα στην εύρυθμη λειτουργία του ηλεκτρικού δικτύου



Σχήμα 7.5: Σχηματική απεικόνιση επίθεσης προερχόμενης από το εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ

ΚΕΦΑΛΑΙΟ 8

ΤΕΧΝΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΑ SMART GRID

Η ασφάλεια είναι απαραίτητη σε όλα τα κατανεμημένα συστήματα προκειμένου να οικοδομηθούν αξιόπιστες και ασφαλείς υπολογιστικές πλατφόρμες. Στόχος της σχεδίασης ενός κατανεμημένου συστήματος, όπως έχει αναφερθεί, είναι η διατήρηση της εμπιστευτικότητας (confidentiality), ακεραιότητας (integrity) και διαθεσιμότητας (availability) των δεδομένων που μεταφέρονται σε αυτό.

Υπάρχουν διάφοροι τρόποι με τους οποίους ένα σύστημα μπορεί να τεθεί σε κίνδυνο. Όπως αναφέρει η Julie Greensmith (μέλος της ομάδας ASAP) [41]:

- *Υποκλοπή* μπορεί να συμβεί όταν ένας μη εξουσιοδοτημένος χρήστης αποκτά κάποια μορφή πρόσβασης σε μία υπηρεσία ή μία πηγή δεδομένων, όπως είναι η παράνομη αντιγραφή δεδομένων μετά την εισχώρηση σε κάποιο σύστημα αρχείων.
- *Διακοπή* μπορεί να συμβεί όταν καταστρέφονται ή διαγράφονται αρχεία ως αποτέλεσμα μιας DoS επίθεσης ή ενός ιού.
- *Τροποποίηση* μπορεί να συμβεί όταν ένας μη εξουσιοδοτημένος χρήστης ή πρόγραμμα αλλοιώνει τα δεδομένα ή κάνει αλλαγές στο σύστημα.
- *Παραγωγή* μπορεί να συμβεί όταν παράγονται δεδομένα που κανονικά δεν θα υπήρχαν. Ένα παράδειγμα είναι η προσθήκη δεδομένων σε κάποιον κωδικό με σκοπό να τεθεί ένα σύστημα σε κίνδυνο.

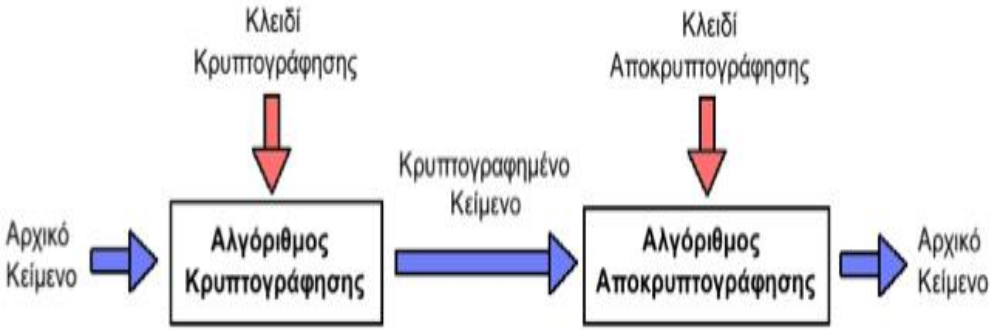
Το έξυπνο δίκτυο αποτελεί σήμερα μια πολλά υποσχόμενη λύση για τα παγκόσμια ενεργειακά θέματα, καθώς όχι μόνο προσφέρει σε υψηλό βαθμό αξιόπιστη και επαρκή ενέργεια αλλά επίσης εισάγει οικονομικότερους τρόπους διανομής και μεταφοράς της. Αυτές οι βελτιώσεις βασίζονται σε νέες τεχνολογίες που εισάγονται στο υφιστάμενο δίκτυο ηλεκτρικής ενέργειας καθώς επίσης και στη συνεργασία μεταξύ διαφορετικών οργανισμών με σκοπό την γρήγορη ταυτόχρονη μεταφορά και ανάλυση ενός μεγάλου ποσού δεδομένων.

Τελείως ασφαλή δίκτυα και εφαρμογές δεν μπορούν να υπάρξουν, και το έξυπνο δίκτυο δεν αποτελεί εξαίρεση σε αυτόν τον κανόνα. Αν και η γρήγορη εξάπλωση των νέων τεχνολογιών, ειδικά αυτών που σχετίζονται με το Διαδίκτυο, εισάγει πολλές λειτουργικές βελτιώσεις, εισάγει επίσης και πολλούς κινδύνους και έτσι αυξάνονται τα τρωτά σημεία του δικτύου. Αυτό ωθεί πολλούς εισβολείς να ανακαλύψουν τα νέα αυτά τρωτά σημεία και να αποκτήσουν πρόσβαση στο δίκτυο, έχοντας σαν κίνητρα την περιέργεια, το κέρδος, την αναγνώριση, το παραεμπόριο (warefare) και άλλα.

Επομένως η ανάπτυξη του έξυπνου δικτύου επιβάλλει και την ανάπτυξη νέων ή τη βελτίωση των υφιστάμενων μηχανισμών προστασίας του απαραβίαστου του προσωπικού και του επαγγελματικού απορρήτου των συναλλασσόμενων χρηστών. Παρακάτω παρουσιάζονται οι σημαντικότεροι μηχανισμοί προστασίας ενάντια στις απειλές μέσω του διαδικτύου[42].

8.1 ΚΡΥΠΤΟΓΡΑΦΙΑ

Βασικό μέλημα της κρυπτογραφίας είναι η ανταλλαγή μηνυμάτων μεταξύ δύο μερών κατά τρόπο τέτοιο που να καθιστά δυνατή την κατανόηση του περιεχομένου των μηνυμάτων αυτών αποκλειστικά και μόνο από τον αποστολέα και τον παραλήπτη. Το αρχικό μήνυμα ονομάζεται « καθαρό κείμενο » (plaintext ή cleartext), η διαδικασία παραμόρφωσης του αρχικού μηνύματος ώστε να μην είναι κατανοητό ονομάζεται κρυπτογράφηση (encryption), το κρυπτογραφημένο μήνυμα ονομάζεται κρυπτογράφημα (ciphertext), ενώ η διαδικασία ανάκτησης του αρχικού μηνύματος από το κρυπτογράφημα ονομάζεται αποκρυπτογράφηση (decryption). Η κρυπτογράφηση και αποκρυπτογράφηση συνήθως κάνουν χρήση κάποιου κλειδιού (key). Η κωδικοποίηση του μηνύματος είναι τέτοια ώστε η αποκρυπτογράφηση να μπορεί να υλοποιηθεί μόνο εάν είναι γνωστό το κατάλληλο κλειδί (Η διαδικασία απεικονίζεται διαγραμματικά στην εικόνα 8.1).



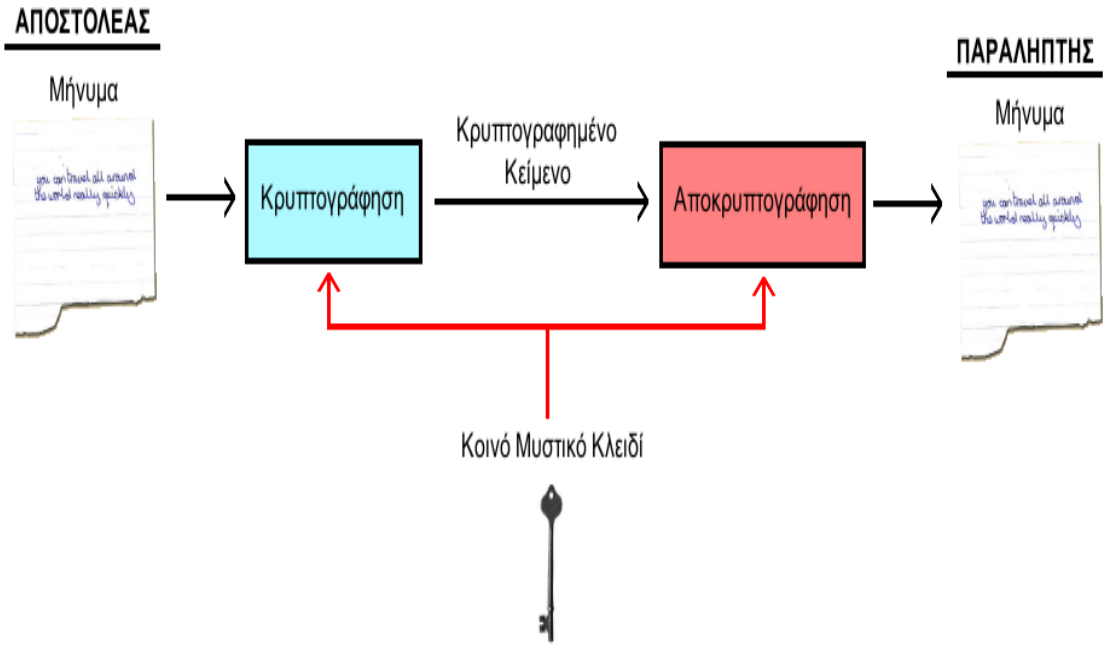
Εικόνα 8.1 Τυπικό σύστημα κρυπτογράφησης

. Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες (αντικειμενικοί σκοποί):

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

8.1.1 Συμμετρικη κρυπτογραφια

Η συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού(εικόνα 8.2) χρησιμοποιεί το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Κατά συνέπεια το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και άρα απαιτείται ασφαλές μέσο για την μετάδοση του. Η εξασφάλιση της ασφαλούς ανταλλαγής του κλειδιού μεταξύ των δύο μερών αποτελεί προϋπόθεση για ένα τέτοιο κρυπτοσύστημα. Σε διαφορετική περίπτωση η συμμετρική κρυπτογραφία καθίσταται αναποτελεσματική.



Εικόνα 8.2 Κρυπτογράφηση συμμετρικού κλειδιού

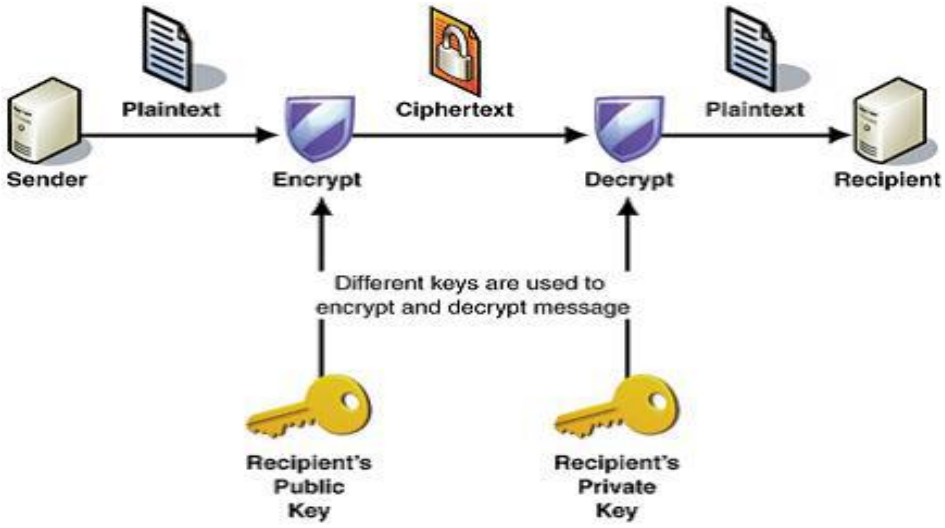
Σημαντικό πλεονέκτημα των συμμετρικών κρυπτογραφικών αλγόριθμων αποτελεί η ταχύτητα τους. Για το λόγο αυτό χρησιμοποιούνται όταν ο όγκος των δεδομένων προς κρυπτογράφηση είναι μεγάλος. Οι συμμετρικοί αλγόριθμοι διαχωρίζονται σε δύο κατηγορίες: stream ciphers και block ciphers.

Οι stream ciphers κρυπτογραφούν ένα bit καθαρού κειμένου κάθε φορά, ενώ οι block ciphers κρυπτογραφούν ένα σύνολο από bits ταυτόχρονα (8, 64, 128 bits κλπ.). Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με περισσότερο γνωστό το Data Encryption Standard (DES). Ο DES είναι ένα block ciphers με μέγεθος 56-bits, ενώ χρησιμοποιεί κλειδί μεγέθους 56-bits. Ο DES μπορεί να χρησιμοποιηθεί για να κρατήσει τα συστήματα ασφαλή από τους απλούς hackers αλλά σπάει εύκολα από ειδικό hardware που μπορούν να προμηθευτούν οι κυβερνήσεις ή οι οργανωμένοι εγκληματίες. Μία παραλλαγή του DES με μεγαλύτερη ασφάλεια είναι ο Triple –DES που βασίζεται στη χρήση του DES τρείς διαδοχικές φορές με δύο ή τρία διαφορετικά κλειδιά [43].

Ένας ακόμη συμμετρικός αλγόριθμος κρυπτογράφησης είναι ο Advanced Encryption Standard (AES) αλγόριθμος με μήκος κλειδιών 128, 192 ή 256 bits.

8.1.2 Ασυμμετρη Κρυπτογραφια

Η ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού (public key cryptography – PKI) είναι μια τεχνική, η οποία μπορεί να εξασφαλίσει την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, όταν αυτά διακινούνται σε κανάλια επικοινωνίας. Στην τεχνική αυτή, το κέντρο ελέγχου και ο μετρητής δημιουργούν από ένα ζεύγος κλειδιών κρυπτογράφησης, με το δημόσιο κλειδί να αποστέλλεται στην οντότητα με την οποία ανταλλάσσουν πληροφορίες και δεδομένα. Κατά την αποστολή ενός πακέτου σε έναν έξυπνο μετρητή, το κέντρο ελέγχου κρυπτογραφεί το περιεχόμενο του πακέτου με το ιδιωτικό του κλειδί και στη συνέχεια, εφόσον το λάβει ο μετρητής, μπορεί να το αποκρυπτογραφήσει μέσω του δημοσίου κλειδιού του κέντρου ελέγχου. Με αυτό τον τρόπο, μπορεί να γνωρίζει ο μετρητής ότι η πληροφορία προήλθε όντως από το κέντρο ελέγχου, ωστόσο δεν εξασφαλίζεται η ακεραιότητα των δεδομένων, μιας και οποιοσδήποτε έχει το δημόσιο κλειδί του κέντρου ελέγχου, μπορεί να διαβάσει και να τροποποιήσει το περιεχόμενο του πακέτου. Εναλλακτικά, εφόσον έχει ήδη κρυπτογραφηθεί η πληροφορία από το κέντρο ελέγχου, το κρυπτογραφημένο μήνυμα κρυπτογραφείται εκ νέου με το δημόσιο κλειδί του εκάστοτε έξυπνου μετρητή. Στην περίπτωση αυτή, μόνο ο συγκεκριμένος μετρητής μπορεί να αποκρυπτογραφήσει το μήνυμα με το ιδιωτικό κλειδί του, και στη συνέχεια με το δημόσιο κλειδί του κέντρου ελέγχου, εξασφαλίζοντας και την ακεραιότητα των δεδομένων που διακινούνται. Και στις δύο περιπτώσεις, η ανταλλαγή των κλειδιών μπορεί να γίνει διαμέσου ενός ασφαλούς καναλιού επικοινωνίας για να αποφευχθούν επιθέσεις eavesdropping ή man-in-the-middle, που διακινδυνεύουν την εμπιστευτικότητα των κλειδιών. Η κρυπτογράφηση δημοσίου κλειδιού, παρόλα τα πλεονεκτήματά της, προϋποθέτει οι μετρητές να έχουν επαρκή μνήμη και υπολογιστική ισχύ για την κρυπτογράφηση των δεδομένων. Αυτό όμως αυξάνει σημαντικά το κόστος τους, μιας και θα κληθούν να επιβαρυνθούν οι καταναλωτές με αυτό, οπότε μπορεί να λειτουργήσει ως τροχοπέδη στην υιοθέτηση του έξυπνου δικτύου, όπως αναφέρθηκε προηγουμένως. Αλλά και το κέντρο ελέγχου καλείται να διαχειριστεί έναν τεράστιο αριθμό από κλειδιά κρυπτογράφησης, όχι μόνο από τους μετρητές, αλλά και από τους υποσταθμούς, τα RTUs και τις άλλες υποδομές του δικτύου. Η διαχείριση όλων αυτών των κλειδιών, εισάγει σημαντικό λειτουργικό κόστος για το έξυπνο δίκτυο [44] [48] [50].

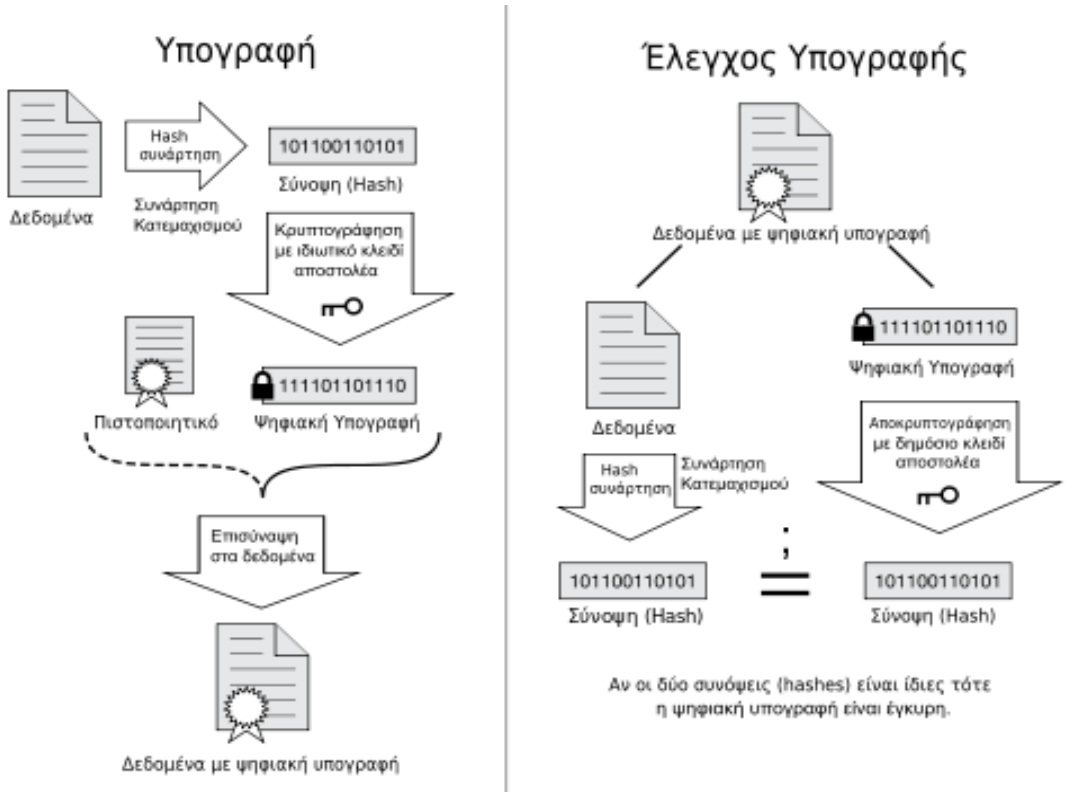


Είκονα 6.3: Διαδικασία Κρυπτογράφησης Δεδομένων με την τεχνική PKI

Τρία γνωστά συστήματα δημοσίου κλειδιού είναι τα RSA, EL-Gamal και το Elliptic Curve Cryptography (ECC). Τα τρία αυτά συστήματα έχουν αλγόριθμους με διαφορετικά χαρακτηριστικά, αλλά και οι τρείς χρησιμοποιούν ένα ιδιωτικό κλειδί για να κρυπτογραφούν τα μηνύματα και ένα δημόσιο για να τα αποκρυπτογραφούν.

8.1.3 Ψηφιακες υπογραφες

Η κρυπτογράφηση / αποκρυπτογράφηση αντιμετωπίζει το πρόβλημα της υποκλοπής (eavesdropping), αλλά όχι αυτά της παραποίησης και της προσποίησης. Για την αντιμετώπιση της παραποίησης χρησιμοποιείται μια μαθηματική συνάρτηση που ονομάζεται *μονόδρομος τεμαχισμός* (one-way hash) ή *σύνοψη μηνύματος* (message digest**).** Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.



Εικόνα 8.4 Ψηφιακή υπογραφή

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από τη σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης

(χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης. Η ηλεκτρονική υπογραφή, στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή, η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική για κάθε μήνυμα!!

Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή υπογραφή (εικόνα 6.4)είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος [45].

8.1.4 Ψηφιακα Πιστοποιητικα

Η αυθεντικοποίηση των επικοινωνούντων μερών είναι μια σημαντική παράμετρος της ασφάλειας, καθώς πρέπει να υπάρχουν μηχανισμοί που να επιβεβαιώνουν την ταυτότητα αυτών που στέλνουν ή λαμβάνουν τις πληροφορίες. Όταν μάλιστα χρησιμοποιούνται δημοσίως γνωστά κλειδιά, τότε χρειάζεται να υπάρχει ένας μηχανισμός που να μας εξασφαλίζει / πιστοποιεί ότι κάθε δημόσιο κλειδί ανήκει πράγματι σε αυτή την οντότητα που εμείς νομίζουμε ότι ανήκει.

Πιστοποίηση (certification) είναι η διαδικασία της αντιστοίχισης και δέσμευσης ενός δημοσίου κλειδιού σε ένα άτομο, οργανισμό ή μια άλλη οντότητα. Για το σκοπό αυτό χρησιμοποιούνται τα ψηφιακά πιστοποιητικά, τα οποία αποτελούν τελικά το μέσο με το οποίο μεταδίδονται με ασφαλή τρόπο οι τιμές των δημόσιων κλειδιών και οι πληροφορίες κατόχου που σχετίζονται με αυτά.
Τα ψηφιακά πιστοποιητικά είναι ηλεκτρονικά έγγραφα που χρησιμοποιούνται για την αναγνώριση ενός προσώπου / εξυπηρετητή / οργανισμού και τη συσχέτισή του με ένα δημόσιο κλειδί.
Η απόκτηση ενός ηλεκτρονικού πιστοποιητικού γίνεται μετά από αίτηση σε μια Αρχή Πιστοποίησης (Certificate Authority). Η Αρχή Πιστοποίησης επιβεβαιώνει την ταυτότητα του αιτούντος και εκδίδει το πιστοποιητικό, που περιλαμβάνει [49]:

- Το όνομα και πληροφορίες αναγνώρισης του χρήστη στον οποίο αναφέρεται το πιστοποιητικό,
- Το δημόσιο κλειδί του χρήστη,
- Την ημερομηνία λήξης του πιστοποιητικού,
- Το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε, κ.ά.

8.2 Συστημα ανιχνευσης εισβολης (Instruction Detection System IDS)

Το **Σύστημα Ανίχνευσης Εισβολής** (Intrusion Detection System, IDS) αποτελεί σύστημα παρακολούθησης και ανάλυσης των συμβάντων, τα οποία λαμβάνουν χώρα τόσο στους ίδιους τους ηλεκτρονικούς υπολογιστές αλλά και γενικότερα στα πληροφοριακά συστήματα. Στόχος είναι ο εντοπισμός ενδείξεων για πιθανές προσπάθειες εισβολής, κατά τις οποίες συχνά εντοπίζονται ίχνη παραβίασης της ακεραιότητας, της εμπιστευτικότητας και της

διαθεσιμότητας των πληροφοριακών πόρων. Οι προσπάθειες παράκαμψης των μηχανισμών ασφαλείας μπορεί να προέρχονται από εξωτερικούς χρήστες, προς το εσωτερικό εταιρικό δίκτυο, στους οποίους δεν επιτρέπεται η πρόσβαση στο υπάρχον πληροφοριακό σύστημα. Επίσης, οι προσπάθειες παράκαμψης πιθανόν να προέρχονται από εσωτερικούς χρήστες, με περιορισμένα δικαιώματα πρόσβασης.

Οι λόγοι εγκατάστασης ενός συστήματος ανίχνευσης εισβολής ποικίλουν. Οι πιο σημαντικοί από αυτούς τους λόγους είναι η πρόληψη προβλημάτων, η ανίχνευση παραβιάσεων, η τεκμηρίωση υπαρκτών απειλών, ο έλεγχος ποιότητας για το σχεδιασμό ασφαλείας, καθώς και η θωράκιση παλαιών συστημάτων σε περίπτωση που κρίνεται αναγκαία η διατήρησή τους

Το σύστημα εντοπισμού εισβολέων έχει την ικανότητα να ταξινομεί τα είδη των επιθέσεων με επάρκεια και αποτελεσματικότητα μέσω της χρήσης ενός σθεναρού αλγορίθμου ταξινόμησης. Σύμφωνα με την αρχιτεκτονική δικτύου που περιλαμβάνει HAN, NAN και WAN, κάθε κόμβος που ανήκει σε κάποιο από αυτά τα δίκτυα έχει και το ανάλογο σύστημα εντοπισμού εισβολέων του δικτύου. Το σύστημα εντοπισμού εισβολέων του WAN έχει τη μεγαλύτερη ικανότητα και ακρίβεια στην ταξινόμηση επιθέσεων. Έτσι σε περίπτωση που το σύστημα εντοπισμού εισβολέων του HAN δεν καταφέρει να ταξινομήσει μια δικτυακή κυκλοφορία δεδομένων, τότε τα δεδομένα μεταφέρονται στο σύστημα ανίχνευσης εισβολέων του δικτύου NAN. Σε περίπτωση που δεν τα καταφέρει ούτε το σύστημα ανίχνευσης εισβολέων NAN που είναι καλύτερο από αυτό του HAN τότε αναλαμβάνει το σύστημα εντοπισμού εισβολέων WAN. Εάν επιτευχθεί ταξινόμηση μιας επίθεσης, τότε η ταξινόμηση κατεβαίνει ιεραρχικά προς τον κόμβο-πηγή, εκπαιδεύοντας το σύστημα εντοπισμού και κάνοντάς το πιο σθεναρό [49].

Παρακάτω συνοψίζονται οι βασικές λειτουργίες ενός IDS [46]:

- Παρακολούθηση και ανάλυση των δραστηριοτήτων των χρηστών και του συστήματος,
- Έλεγχος της διαμόρφωσης του συστήματος και των τρωτών σημείων του δικτύου,
- Έλεγχος της ακεραιότητας των φακέλων που περιέχουν σημαντικά δεδομένα,
- Παρακολούθηση των δράσεων γνωστών επιθέσεων, με ανάλυση και υποβολή έκθεσης στον διαχειριστή,
- Έλεγχος του λειτουργικού συστήματος του δικτύου
- Ανάλυση όλων των παράνομων δραστηριοτήτων στο δίκτυο.

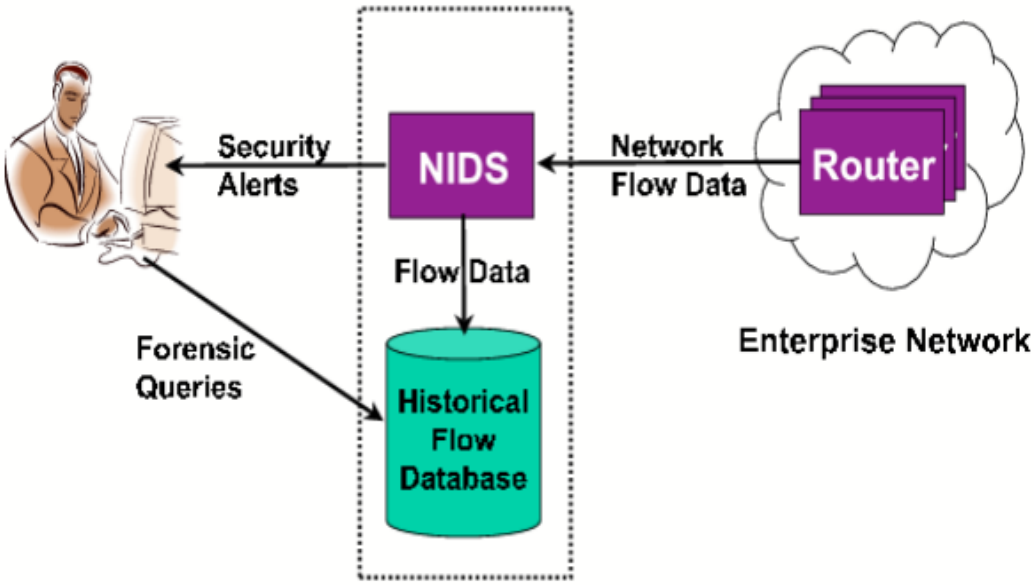
Βασικά υποσυστήματα του IDS είναι:

- Network Intrusion Detection System (NIDS)

Τα συστήματα ανίχνευσης εισβολών INDS (εικόνα 8.5) είναι τοποθετημένα σε κομβικά σημεία μέσα στο δίκτυο ώστε να επιβλέπουν την κίνηση από και προς όλες τις συσκευές του δικτύου. Τα NIDS παρακολουθούν και αναλύουν, σε πραγματικό χρόνο, κάθε πακέτο που κυκλοφορεί στο traffic ενός δικτύου και αποτελούνται από δύο λογικά τμήματα: το σταθμό παρακολούθησης δικτύου και το σταθμό διαχείρισης.

Τα συστήματα ανίχνευσης εισβολών έχουν αισθητήρες που παρακολουθούν την δικτυακή κίνηση και προσπαθούν να βρουν ύποπτα μοτίβα γνωστά και ως υπογραφές ή κανόνες. Εάν

για παράδειγμα παρατηρείται ένας μεγάλος αριθμός των TCP αιτήσεων σύνδεσης σε ένα πολύ μεγάλο αριθμό διαφορετικών πυλών, θα μπορούσε κανείς να υποθέσει ότι κάποιος διεξάγει σάρωση πυλών σε μέρος ή στο σύνολο των υπολογιστών στο δίκτυο. Ένα χαρακτηριστικό των αισθητήρων είναι ότι έχουν την δυνατότητα να κάνουν κρυφή την παρουσία τους χωρίς να μπορεί ο επιτιθέμενος να αντιληφθεί την ύπαρξη τους. Σε περίπτωση όπου το σύστημα ανίχνευσης εντοπίσει μία επίθεση ενημερώνει το σταθμό διαχείρισης. Ο σταθμός διαχειριστής έχει την δυνατότητα να εμφανίσει στην οθόνη του διαχειριστή τα σήματα κινδύνου που έλαβε από τους αισθητήρες με κάποιο συναγερμό ή να πραγματοποιήσει επιπλέον ανάλυση [47].



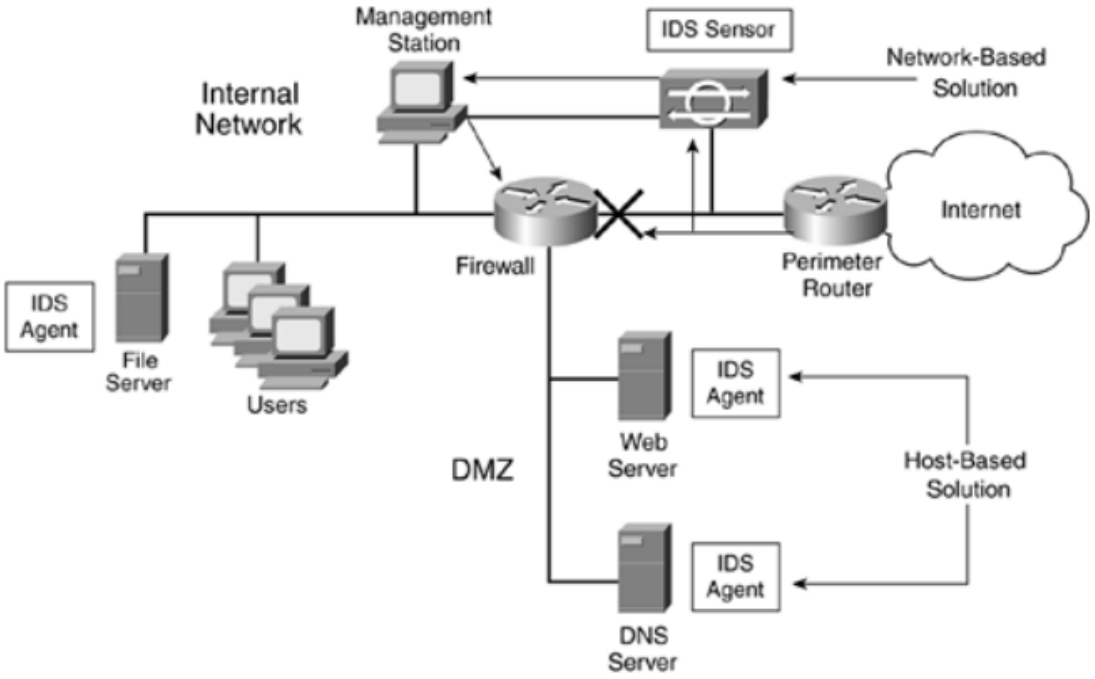
Εικόνα 8.5: Παρουσίαση λειτουργίας ενός συστήματος ανίχνευσης εισβολής βασισμένο στο δίκτυο(NIDS).

- Host-based Intrusion Detection System (HIDS):

Τα συστήματα ανίχνευσης εισβολών βασιζόμενα στον εξυπηρέτη λειτουργούν ως ατομικοί εξυπηρέτες ή ως συσκευές δικτύου. Τα HIDS (εικόνα 8.6) ψάχνουν για ίχνη εισβολής, ασυνήθιστες δραστηριότητες και παρακολουθούν τα εισερχόμενα και εξερχόμενα πακέτα από τη συσκευή και ενημερώνουν τον διαχειριστή εάν διαπιστώσουν ύποπτες ενέργειες. Ελέγχει τα κρίσιμα σημεία του λογισμικού (systems files) ερευνώντας για παράξενη πρόσβαση στα αρχεία και επίσης πραγματοποιεί ελέγχους στα γεγονότα συστήματος (systems events) και στα αρχεία ελέγχου και καταγραφής ασφάλειας (audit log files) ψάχνοντας για μη εγκεκριμένη αύξηση δικαιωμάτων ή μετατροπές δικαιωμάτων του συστήματος. Επομένως ένα HIDS μπορεί να θεωρηθεί ένας πράκτορας που παρακολουθεί οτιδήποτε ή οποιονδήποτε έχοντας καταστρατηγήσει την πολιτική ασφαλείας του συστήματος.

Η αρχή λειτουργίας ενός HIDS βασίζεται στο γεγονός ότι οι επιτυχημένοι εισβολείς θα αφήσουν ένα ίχνος των δραστηριοτήτων τους. Ένας επιτιθέμενος όταν πραγματοποιήσει με

επιτυχία μια εισβολή θέλει να καθιερώσει ως ιδιοκτησία του το σύστημα με την εγκατάσταση κακόβουλου λογισμικού με σκοπό να του εξασφαλίσει μελλοντική πρόσβαση σε οποιαδήποτε δραστηριότητα (keystroke logging, κλοπή ταυτότητας, spamming, botnet δραστηριότητα, spyware-usage, κλπ.). Επίσης οι περισσότεροι εισβολείς πολλές φορές όταν έχουν διεισδύσει πραγματοποιούν κάποιες αλλαγές στις τεχνικές ασφάλειας για να προστατέψουν το σύστημα που έχουν διεισδύσει αφήνοντας μόνο μία δική τους κερκόπορτα ανοιχτή, έτσι ώστε άλλοι εισβολείς να μην μπορούν να πάρουν τον έλεγχο του συστήματος [47].



Εικόνα 8.6: Ανίχνευση εισβολής βασιζόμενη στο δίκτυο

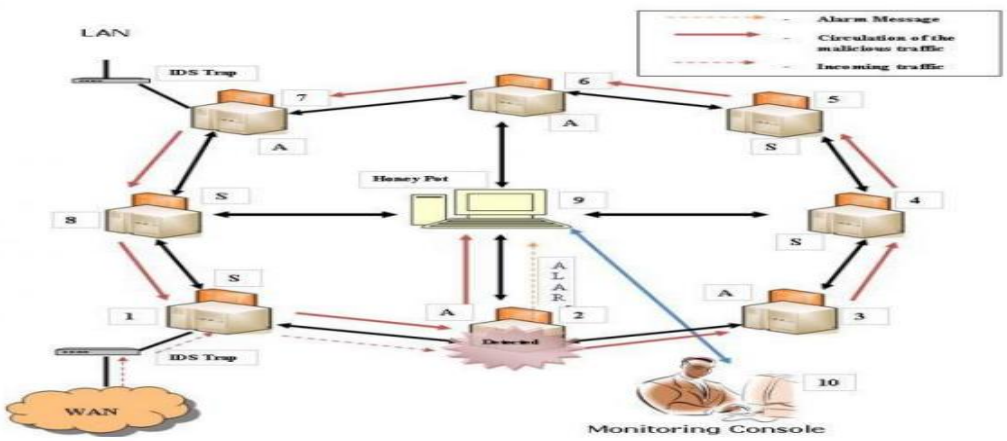
Μετά την ανάλυση των δύο σημαντικότερων κατηγοριοποιήσεων των IDSs, ακολουθεί η περιγραφή των τρόπων με τους οποίους επιτυγχάνεται η ανίχνευση εισβολέων. Υπάρχουν τέσσερις βασικές τεχνικές:

Α) η ανίχνευση ανωμαλίας,
Β) η ανίχνευση υπογραφής,
Γ) η παρακολούθηση στόχου και
Δ) η κρυφή ανίχνευση (stealth probe).

8.2.1 Ανιχνευση ανωμαλιων

Ένα σύστημα ανίχνευσης εισβολής που ανιχνεύει εισβολές με βάση την ανωμαλία (εικόνα 8.7) παρακολουθεί την κίνηση του δικτύου και την συγκρίνει με μια καθιερωμένη γραμμή βάσης(baseline). Η αρχική τιμή θα προσδιορίσει τι είναι "φυσιολογικό" για το δίκτυο, τι είδους εύρος ζώνης χρησιμοποιείται γενικά, ποια πρωτόκολλα χρησιμοποιούνται, ποιες

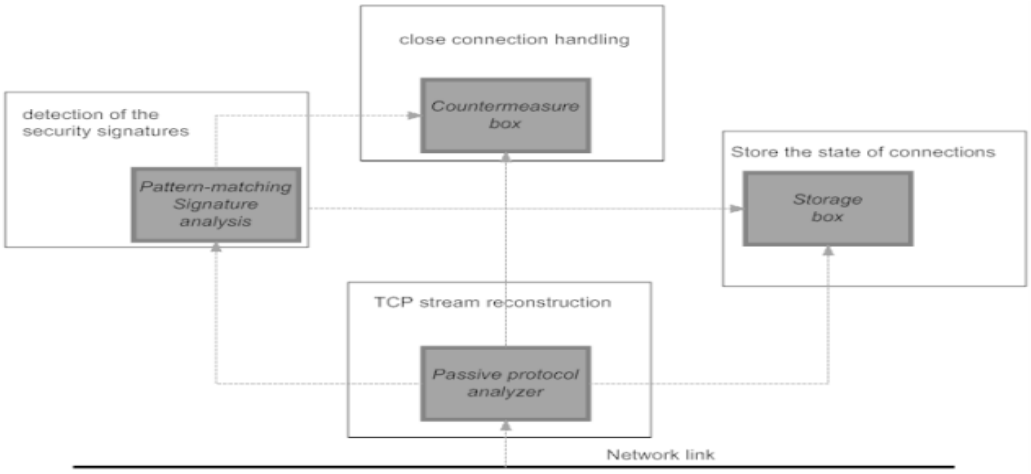
«πόρτες»(ports) και γενικά συσκευές συνδέονται μεταξύ τους, και να ειδοποιήσει το διαχειριστή ή το χρήστη όταν η κίνηση που ανιχνεύεται είναι ανώμαλη ή σημαντικά διαφορετική, από τη γραμμή βάσης.



Εικόνα 8.7: Σύστημα ανίχνευσης εισβολής με βάση την ανωμαλία

8.2.2 ΑΝΙΧΝΕΥΣΗ ΥΠΟΓΡΑΦΗΣ (SIGNATURE DETECTION)

Ένα σύστημα ανίχνευσης εισβολών που βασίζεται στην υπογραφή (εικόνα 8.8) παρακολουθεί τα πακέτα στο δίκτυο και τα συγκρίνει με μια βάση δεδομένων που αποτελείται από υπογραφές ή με ιδιότητες από γνωστές κακόβουλες απειλές. Είναι παρόμοιο με τον τρόπο που τα περισσότερα antivirus ανιχνεύουν κακόβουλο λογισμικό. Το θέμα είναι ότι θα υπάρξει ένα χρονικό κενό από όταν μια νέα απειλή ανακαλύπτεται και τη δημιουργία της υπογραφής για την ανίχνευση αυτής της απειλής που θα χρησιμοποιηθεί από το σύστημα ανίχνευσης εισβολής μετέπειτα. Κατά την περίοδο αυτή το σύστημα ανίχνευσης εισβολής δε θα είναι σε θέση να ανιχνεύσει τη νέα απειλή [47].



Εικόνα 8.8: : Σύστημα ανίχνευσης εισβολής με βάση την υπογραφή.

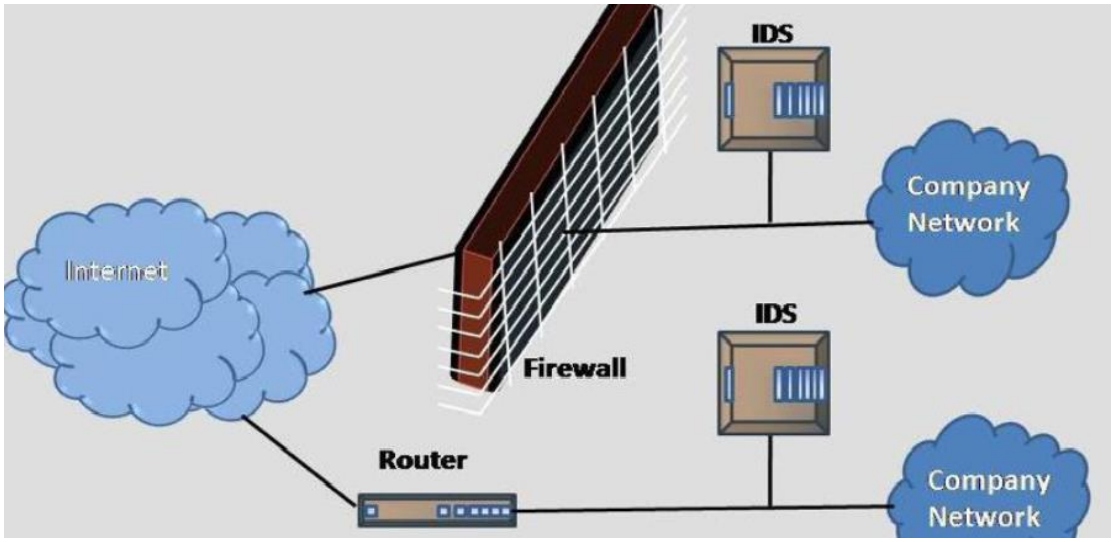
8.2.3 Παρακολουθηση στοχου (target monitoring)

Τα συστήματα αυτά παρακολουθούν αν γίνονται τροποποιήσεις σε συγκεκριμένα αρχεία. Με αυτόν τον τρόπο βρίσκουν μία μη εξουσιοδοτημένη τροποποίηση αφού αυτή συμβεί με σκοπό να την αναιρέσουν. Για να το κάνουν αυτό, δημιουργούν ένα κρυπτογράφημα του περιεχομένου του κάθε φακέλου ανά κάποιο χρονικό διάστημα. Στη συνέχεια συγκρίνουν το παλιό κρυπτογράφημα με το καινούργιο του ίδιου φακέλου και αν υπάρχουν τροποποιήσεις τις αναφέρουν στον διαχειριστή. Αυτή η τεχνική είναι εύκολη στην εφαρμογή γιατί δεν απαιτεί συνεχή παρακολούθηση από τον διαχειριστή [51].

8.2.4 Stealth Probes

Αυτή η τεχνική προσπαθεί να ανιχνεύσει τυχόν εισβολείς που επιλέγουν να πραγματοποιήσουν τις δράσεις τους για παρατεταμένες χρονικές περιόδους. Για παράδειγμα, ένας επιτιθέμενος θα ελέγχει το σύστημα για τυχόν ύπαρξη τρωτών σημείων, θα ανοίξει για παράδειγμα τις θύρες για μία περίοδο δύο μηνών και θα περιμένει άλλους δύο μήνες για να πραγματοποιήσει την επίθεση. Η τεχνική “Stealth Probes” συλλέγει δεδομένα του συστήματος που αναπαριστούν την συμπεριφορά του συστήματος για ένα μεγάλο χρονικό διάστημα και ελέγχει για επιθέσεις με κάποια μεθοδολογία. Προσπαθεί δηλαδή να ανακαλύψει τυχόν επιθέσεις με κοινούς συσχετισμούς [51].

Οι αισθητήρες IDS μπορούν αν τοποθετηθούν σε όλα τα πιθανά σημεία εισόδου σε κάποιο δίκτυο (όπως φαίνεται στην εικόνα 8.9) έτσι ώστε κάθε φορά που ανιχνεύεται ρήγμα ασφάλειας, να στέλνεται ειδοποίηση στην κεντρική κονσόλα διαχείρισης. Οι διαχειριστές έχουν πρόσβαση στους αισθητήρες οποιαδήποτε χρονική στιγμή με σκοπό να μπορούν να αλλάξουν τη διαμόρφωσή τους εάν αυτό απαιτηθεί. Οι όποιες αλλαγές στη λειτουργία τους θα πρέπει να γίνονται από ειδικευμένους τεχνικούς [46].



Εικόνα 8.9: Τοποθέτηση συστημάτων IDS σε ένα δίκτυο

8.3 Συστηματα αποτροπης εισβολης (IPS)

Ένα IDS (Intrusion Detection System) είναι ένα λογισμικό που αυτοματοποιεί την διαδικασία ανίχνευσης εισβολών. Ένα IPS (Intrusion Prevention System) είναι ένα λογισμικό που έχει όλες τις ιδιότητες ενός IDS αλλά μπορεί επιπλέον να συμβάλλει στην παρεμπόδιση πιθανών γεγονότων. Τα IPSs θεωρούνται δηλαδή επεκτάσεις των IDSs επειδή και τα δύο παρακολουθούν την κυκλοφορία σε ένα δίκτυο ή/και τις δραστηριότητες σε ένα σύστημα για να βρουν μία πιθανή κακόβουλη ενέργεια. Η διαφορά τους έγκειται μόνο στο γεγονός ότι τα IPSs ανταποκρίνονται σε μία απειλή που εντοπίστηκε προσπαθώντας να αποτρέψουν τη δημιουργία της [52].

Χρησιμοποιούνται διάφορες τεχνικές απόκρισης, οι οποίες μπορούν να ταξινομηθούν στις ακόλουθες ομάδες [53]:

- Το IPS σταματάει από μόνο του την επίθεση. Αυτό μπορεί να γίνει με τον τερματισμό της σύνδεσης δικτύου που χρησιμοποιείται από τον εισβολέα, με το μπλοκάρισμα της πρόσβασης του εισβολέα μέσω του συγκεκριμένου λογαριασμού χρήστη ή διεύθυνσης IP που χρησιμοποίησε και με το μπλοκάρισμα της πρόσβασης σε όλες τις υπηρεσίες και εφαρμογές, οι οποίες καταλήγουν στο ίδιο σημείο με αυτό στο οποίο ήθελε να καταλήξει ο εισβολέας.

- Το IPS μπορεί να αλλάξει το περιβάλλον ασφαλείας. Για παράδειγμα, το IPS θα μπορούσε να αλλάξει την διαμόρφωση μιας συσκευής του δικτύου (ενός firewall ή ενός router για παράδειγμα) με σκοπό να εμποδίσει κάποια εισερχόμενη επίθεση.
- Το IPS μπορεί να αλλάξει το περιεχόμενο της επίθεσης. Μερικές τεχνολογίες IPS μπορούν να αφαιρέσουν ή να αντικαταστήσουν τμήματα του κακόβουλου κώδικα μιας επίθεσης ώστε να μειωθούν οι κακόβουλες συνέπειές της. Για παράδειγμα, ένα IPS μπορεί να αφαιρέσει ένα μολυσμένο συνημμένο αρχείο από ένα μήνυμα ηλεκτρονικού ταχυδρομείου.

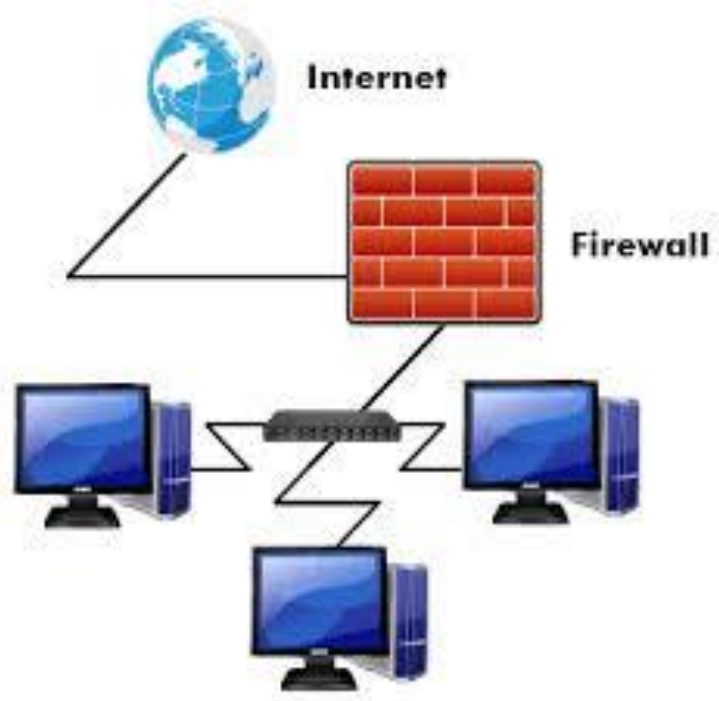
Τα IPSs μπορούν να κατηγοριοποιηθούν ως εξής:

- NIPS (Network-based IPS): παρακολουθεί όλη την κίνηση στο δίκτυο αναλύοντας τα αντίστοιχα πρωτόκολλα.
- WIPS (Wireless IPS): παρακολουθεί την κίνηση σε ένα ασύρματο δίκτυο αναλύοντας τα αντίστοιχα πρωτόκολλα.
- Network Behavior Analysis (NBA): εξετάζει την κυκλοφορία του δικτύου για τον εντοπισμό απειλών που δημιουργούν ασυνήθιστη ροή κυκλοφορίας, όπως οι επιθέσεις DDoS.
- HIPS (Host-based IPS): είναι ένα εγκατεστημένο πακέτο λογισμικού που παρακολουθεί έναν μεμονωμένο υπολογιστή για ύποπτη δραστηριότητα με την ανάλυση των γεγονότων που συμβαίνουν μέσα σε αυτόν τον υπολογιστή.

8.4 Τειχος προστασιας (Firewall)

Τα firewall αποτελούν ίσως την πιο συνηθισμένη τεχνική προστασίας στα επιμέρους δίκτυα του Smart Grid. Η βασική τους λειτουργία είναι να ελέγχουν τη δικτυακή κίνηση στη συσκευή

που προστατεύουν, ώστε να απορρίπτουν κάποια πακέτα, τα οποία φαίνονται ύποπτα ή δεν ικανοποιούν τις προϋποθέσεις προστασίας, που έχει θέσει ο χρήστης. Είναι αρκετά αποδοτική μέθοδος προστασίας, ειδικά για επιθέσεις πλημμύρας ICMP και UDP, μιας και η δικτυακή κίνηση που δημιουργείται, αποκλίνει σημαντικά από τη συνηθισμένη, είναι εύκολα ανιχνεύσιμη και μπορεί να απορριφθεί. Τα firewalls συνηθίζεται να τοποθετούνται και στους δρομολογητές των επιμέρους δικτύων, μιας και είναι το πλέον ευπαθές σημείο του έξυπνου δικτύου και αυτό που εκμεταλλεύονται συνήθως οι επιτιθέμενοι, για την πραγματοποίηση επιθέσεων.



Εικόνα 8.10 :Τοποθέτηση Firewall σε ένα δίκτυο

8.5 Εμπιστευτικοτητα κλειδιων κρυπτογραφησης

Τα περισσότερα υπολογιστικά συστήματα όπως είναι οι έξυπνοι μετρητές για να προστατεύσουν τα δεδομένα τους χρησιμοποιούν μηχανισμούς ασφάλειας που βασίζονται σε αλγόριθμους κρυπτογράφησης και κατακερματισμού. Οι αλγόριθμοι κρυπτογράφησης προϋποθέτουν την ύπαρξη ενός μυστικού κλειδιού που είναι γνωστό μόνο στο λογισμικό του έξυπνου μετρητή και στα εξουσιοδοτημένα συστήματα που επικοινωνούν με τους έξυπνους μετρητές. Αυτά τα κλειδιά φυλάσσονται στη μη-πτητική μνήμη του έξυπνου μετρητή. Σε προηγούμενο κεφάλαιο αναφέραμε σε επίθεση που είχε ως στόχο τη μη-πτητική μνήμη στην οποία φυλάσσονται τα μυστικά κλειδιά.

Μια καλή λύση που έχει προταθεί είναι η χρήση ειδικών κυκλωμάτων PUF (Physically Unclonable Function). Χαρακτηριστικό αυτών των κυκλωμάτων είναι πως παράγουν δεδομένα βάσει ενδογενούς τυχαιότητας ώστε να μην μπορεί η έξοδος τους να προβλεφθεί. Ακόμα, η τυχαιότητα προκύπτει από κατασκευαστικά χαρακτηριστικά ώστε σε περίπτωση απόπειρας παραβίασης του κυκλώματος να αλλοιώνουν τη διαδικασία παραγωγής δεδομένων με αποτέλεσμα να μην αποκτά πρόσβαση ο επιτιθέμενος. Έτσι με τα κυκλώματα

PUF είναι δυνατή η αποφυγή αποθήκευσης των κλειδιών κρυπτογράφησης στη μη-πτητική μνήμη η οποία αποτελούσε στόχο για πιθανές επιθέσεις. Επίσης ένα μεγάλο πλεονέκτημα των PUF κυκλωμάτων είναι ότι σε περίπτωση φυσικής παραβίασης αλλοιώνεται το χαρακτηριστικό που προδίδει την τυχαιότητα, καταστρέφοντας ουσιαστικά τα κλειδιά κρυπτογράφησης πριν αυτά υποκλαπούν από τον επιτιθέμενο. Τα παραπάνω πλεονεκτήματα τα καθιστούν μια από τις καλύτερες λύσεις για τη φύλαξη των κλειδιών κρυπτογράφησης στους έξυπνους μετρητές [54][55].

8.6 Μεθοδοι ασφαλειας επιθεσεων παραπλευρων καναλιων

Οι επιθέσεις των παράπλευρων καναλιών στηρίζεται στην ανάλυση σημάτων του συστήματος που επηρεάζονται εμμέσως από τους υπολογισμούς πάνω σε ευαίσθητα δεδομένα. Οι μέθοδοι ασφάλειας κινούνται πάνω σε δύο άξονες. Η μία μέθοδος είναι η όσο το δυνατόν μεγαλύτερη ανεξαρτητοποίηση του σήματος των παράπλευρων καναλιών από τα δεδομένα που διαχειρίζεται το κύκλωμα. Συγκεκριμένα, σε ό,τι αφορά τη μελέτη χρονικής καθυστέρησης, τα σύγχρονα σχέδια ολοκληρωμένων κυκλωμάτων, όπως ο μηχανισμός κρυπτογράφησης, υλοποιούνται με σχεδίαση που προβλέπει την ίδια χρονική καθυστέρηση ανεξάρτητα από τα δεδομένα εισόδου.

Ως προς το πλευρικό κανάλι της ισχύος που καταναλώνεται από το κύκλωμα, έχουν προταθεί συνδεσμολογίες πυλών που εισάγουν πρόσθετες φάσεις σε ένα κύκλο ρολογιού ώστε η κατανάλωση ισχύος να είναι ανεξάρτητη των δεδομένων υπολογισμού[68] [69]. Αυτό έχει ως συνέπεια να αυξάνεται ραγδαία το μέγεθος του δείγματος σημάτων που απαιτείται για να πραγματοποιηθεί μια επίθεση σε επίπεδα που την καθιστούν αδύνατη. Ωστόσο, πρέπει να σημειωθεί ότι το κόστος σε χώρο στην πλακέτα, σε απαιτήσεις ισχύος και σε καθυστέρηση είναι της τάξης του 3x, κάτι που καθιστά ιδιαίτερα ακριβή λύση τις συνδεσμολογίες αυτές. Για το λόγο αυτό, οι συνδεσμολογίες τέτοιου είδους χρησιμοποιούνται μόνο σε επιλεγμένα κυκλώματα τα οποία αποτελούν τους συχνότερους στόχους επίθεσης σε ένα σύστημα.

Η δεύτερη μέθοδος για την προστασία του έξυπνου μετρητή από τις επιθέσεις των παράπλευρων καναλιών είναι η απόκρυψη είτε του ίδιου του σήματος του πλευρικού καναλιού είτε των δεδομένων εισόδου ώστε ο επιτιθέμενος να μην μπορεί να το ανιχνεύσει. Μια απλή εφαρμογή για την παραπάνω μέθοδο είναι η χρησιμοποιήση κυκλωμάτων παραγωγής θορύβου ώστε να μειωθεί το SNR του σήματος του πλευρικού καναλιού σε επίπεδο οπού ο επιτιθέμενος να μην έχει την δυνατότητα να ανιχνεύσει το πραγματικό ηχητικό σήμα [39].

8.7 Μεθοδοι ασφαλειας στους εξυπνους μετρητες απο επιθεσεις υποκλοπης στο διαυλο δεδομενων της μητρικης πλακετας

Η υποκλοπή των δεδομένων από το δίαυλο δεδομένων είναι μια δύσκολη μέθοδος και προϋποθέτει την πλήρη πρόσβαση του επιτιθέμενου στο εσωτερικό του έξυπνου μετρητή. Εκτός από τη πρόσβαση στο εσωτερικό του έξυπνου μετρητή ο επιτιθέμενος θα πρέπει να χρησιμοποιήσει εξειδικευμένους αισθητήρες για την ανίχνευση των σημάτων στο δίαυλο δεδομένων. Οι βασικές μέθοδοι προστασίας από τέτοιου είδους επιθέσεις είναι δύο. Η

πρώτη μέθοδος είναι ο δίαυλος δεδομένων να μην είναι προσβάσιμος από τους αισθητήρες και η άλλη μέθοδος είναι τα δεδομένα που μεταφέρονται στο δίαυλο δεδομένων να κρυπτογραφούνται.

Για την πρώτη περίπτωση η αποτελεσματικότερη μέθοδος είναι να χρησιμοποιηθεί αρχιτεκτονική μικροελεγκτή. Με αυτή τη μέθοδο όλες οι διατάξεις του κυκλώματος, οι μνήμες, οι θύρες εισόδου/εξόδου και η μονάδα επεξεργασίας είναι όλες στο ίδιο chip. Αυτό έχει σαν αποτέλεσμα να υπάρχει απευθείας εσωτερική σύνδεση των κυκλωμάτων χωρίς την χρήση διαύλου δεδομένων και έτσι με αυτό τον τρόπο οι αισθητήρες που χρησιμοποιεί ο επιτιθέμενος δεν μπορούν να ανιχνεύσουν το σήμα.

Η δεύτερη μέθοδος βασίζεται στην κρυπτογράφηση των δεδομένων που μεταδίδονται στο δίαυλο. Οι περισσότερες προτάσεις για τέτοιου είδους μηχανισμούς προϋπέθεταν εξειδικευμένο κύκλωμα στο υλικό, με αυξητική επίπτωση στο κόστος κατασκευής των μετρητών [57].

8.8 Ασφαλεια πρωτοκολλου JTAG

Το πρωτόκολλο JTAG γίνεται συχνά στόχος επιτιθέμενων αλλά αυτό δεν οφείλεται σε κάποιο κενό ασφάλειας που έχει το πρωτόκολλο JTAG αλλά έχει να κάνει με τον τρόπο της κανονικής του λειτουργίας. Προκειμένου να γίνει με ασφαλή τρόπο η τοποθέτηση της θύρας JTAG στους ευφυείς μετρητές, είναι αναγκαίο να υπάρξουν ορισμένες προσθήκες στο υλικό και ενδεχομένως να αφαιρεθούν κάποιες από τις λειτουργίες του πρωτοκόλλου[39].

Αρχικά, πρέπει να γίνεται έλεγχος κάθε χρήστη που επιχειρεί να χρησιμοποιήσει το πρωτόκολλο JTAG στη συσκευή του μετρητή. Για να γίνει αυτό είναι απαραίτητος ένας μηχανισμός ταυτοποίησης χρηστών, δηλαδή ένας μηχανισμός κρυπτογράφησης των δεδομένων που μεταφέρονται μεταξύ χρήστη και ελεγκτή JTAG, μία συνάρτηση κατακερματισμού για την ακεραιότητα των δεδομένων, όπως επίσης και ένα μυστικό κλειδί το οποίο χρησιμοποιείται για την ταυτοποίηση του χρήστη με τη συσκευή. Εφόσον ο χρήστης διαθέτει το μυστικό κλειδί, μπορεί να συνδεθεί με τον ελεγκτή JTAG και να χρησιμοποιήσει το πρωτόκολλο. Το κεντρικό chip του μηχανισμού ασφάλειας για το JTAG είναι το κύκλωμα κρυπτογράφησης. Για λόγους εξοικονόμησης χώρου, και συμμόρφωσης με τις προδιαγραφές χρονισμού του JTAG, δεν μπορούν να χρησιμοποιηθούν block αλγόριθμοι κρυπτογράφησης. Αντ' αυτού προτιμώνται αλγόριθμοι κρυπτογράφησης ροής (stream ciphers) [58].

8.9 Μεθοδοι ασφαλειας στα συστηματα SCADA

Ένα σύστημα SCADA θα πρέπει να έχει όλους τους απαραίτητους μηχανισμούς ασφάλειας για να προστατεύεται από τους επίδοξους εισβολής. Μηχανισμοί όπως τα firewals και IDS/IPS είναι μηχανισμοί που παρέχουν μεγάλη προστασία στα συστήματα SCADA

Ο μηχανισμός firewall φιλτράρει τη δικτυακή κίνηση του συστήματος SCADA από και προς άλλα συστήματα. Στην ουσία το firewall απορρίπτει κάθε κίνηση που δεν εμπίπτει στο πλαίσιο κανονικής λειτουργίας που έχει τεθεί βάσει των κανόνων λειτουργίας του σταθμού

SCADA. Όταν παρατηρήσει μία κίνηση που δεν προέρχεται από εξουσιοδοτημένη πηγή την απορρίπτει. Σε περίπτωση όμως όπου η επίθεση γίνει από σύστημα που έχουν παραβιάσει οι εισβολείς και έχουν εξουσιοδότηση για να επικοινωνούν με τα συστήματα SCADA, το firewall θα επιτρέψει την επικοινωνία. Αυτό το κενό ασφάλειας έρχονται να καλύψουν οι μηχανισμοί ασφάλειας IDS/IPS.

Τα συστήματα ανίχνευσης εισβολής (IDS) ελέγχουν την κίνηση και χρησιμοποιούν μεθόδους αναγνώρισης ιχνών επίθεσης εναντίον σταθμών SCADA. Όταν γίνεται μια επίθεση εναντίον των συστημάτων SCADA ο επιτιθέμενος αφήνει αποτυπώματα. Τα αποτυπώματα αυτά μπορεί να είναι είτε αύξηση του όγκου πληροφοριών, είτε εμφάνιση πακέτων ασυνήθιστων πρωτοκόλλων. Εφόσον ο μηχανισμός IDS ανιχνεύσει κάποια τέτοια αλλαγή στο δίκτυο ενεργοποιείται ο μηχανισμός IPS. Ο μηχανισμός IPS θέτει αμέσως σε λειτουργία εξειδικευμένες μεθόδους αποτροπής επίθεσης. Σε περίπτωση όμως όπου τα συστήματα αποτροπής εισβολών IPS δεν αποδειχθούν επαρκείς ή η επίθεση κριθεί πολύ σοβαρή το σύστημα IDS αναλαμβάνει την άμεση ενημέρωση του υπεύθυνου ασφαλείας.

Οι μηχανισμοί firewall και IDS/IPS εμφανίζουν μεγάλα ποσοστά επιτυχίας στην αναγνώριση απειλών και σ' αυτό βοηθάει ένα χαρακτηριστικό των συστημάτων SCADA που αυξάνει σημαντικά την αποτελεσματικότητα των μηχανισμών ασφαλείας. Αυτό το χαρακτηριστικό είναι ότι η δικτυακή κίνηση που δημιουργούν οι σταθμοί SCADA όταν βρίσκονται σε κανονική λειτουργία έχει μικρή διακύμανση. Έτσι είναι εύκολο να ανιχνευθεί ο επιτιθέμενος καθώς θα παρατηρηθεί αλλαγή στις μετρήσεις κίνησης του δικτύου[39].

8.10 Επιπλεον λυσεις για την ασφαλεια του εξυπνου πλεγματος

Πέρα από τις προηγούμενες προτάσεις για την ασφάλεια στο έξυπνο δίκτυο, διακρίνονται και οι εξής ακόλουθες λύσεις [60]:

- Χρήση εικονικών ιδιωτικών δικτύων, για την εξασφάλιση ασφαλούς επικοινωνίας ανάμεσα στο κέντρο ελέγχου και τις υπόλοιπες υποδομές του δικτύου.
- Εκμάθηση χρηστών σε θέματα ασφάλειας στο έξυπνο δίκτυο, μιας και οι περισσότερες ευπάθειες είναι αποτέλεσμα ενεργειών του χρήστη.
- Σχεδίαση του έξυπνου δικτύου με γνώμονα την ασφάλεια, ώστε να αποφευχθούν φαινόμενα μη συμβατότητας με διάφορα λογισμικά προστασίας, όπως antivirus και firewalls.
- Δεδομένου του μεγαλύτερου χρόνου ζωής του έξυπνου δικτύου σε σχέση με τις τεχνολογίες που ενσωματώνονται σε αυτό, θα πρέπει να υπάρχει η δυνατότητα επεκτασιμότητας και αναβάθμισης των τεχνολογιών που θα χρησιμοποιούνται.
- Εκτίμηση της κατάστασης του δικτύου για τον πιθανό εντοπισμό ευπαθειών σε διάφορες συσκευές του, όπως τα IEDs και οι έξυπνοι μετρητές.

8.11 Το πειραμα GridEx

Ένα σημαντικό βήμα προς την υλοποίηση του cyber-physical security στο έξυπνο δίκτυο είναι το πείραμα GridEx II. Πρόκειται για μια άσκηση ασφαλείας, η οποία διεξήχθη από το

NERC (North America Electric Reliability Corporation) των Η.Π.Α και στην οποία συμμετείχαν εταιρείες ηλεκτρισμού, κυβερνήσεις, το FBI, το Υπουργείο Ενέργειας (DOE), το Υπουργείο Άμυνας (DHS) καθώς και πολλές βιομηχανίες, οι οποίες συσχετίζονται με το δίκτυο ηλεκτρικής ενέργειας. Η άσκηση, η οποία πρόκειται για μια συντονισμένη επίθεση μεγάλης κλίμακας στο σύστημα ενέργειας των Η.Π.Α, είχε σκοπό να εξετάσει κατά πόσο αυτό μπορεί να ανταποκριθεί σε μια τέτοια επίθεση άμεσα, διατηρώντας παράλληλα τη λειτουργικότητά του, αλλά και κατά πόσο έχει βελτιωθεί το σύστημα ασφαλείας, σε σχέση με προηγούμενα πειράματα, ώστε να είναι σε θέση να αντιμετωπίζει τέτοιου είδους απειλές ασφαλείας.

Κάθε ένας από τους συμμετέχοντες στην άσκηση αυτή, μπορούσε να επιλέξει το βαθμό εμπλοκής του ανάλογα με τους διαθέσιμους πόρους του και το χρόνο που μπορούσε να αφιερώσει. Οι «παίκτες» (“players”), που συμμετείχαν ενεργά στην άσκηση, ενημερώνονταν για τα σενάρια της επίθεσης μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, ενώ οι διάφορες ενέργειές τους για την αντιμετώπιση των δυσμενών συνθηκών της επίθεσης, καταγράφονταν. Επιπλέον, τα θύματα των επιθέσεων μπορούσαν να επικοινωνούν με τους συντονιστές της άσκησης προκειμένου, να γνωστοποιούν την κατάστασή τους και να συνεργαστούν, για την αντιμετώπιση της κατάστασης.

Ένα από τα βασικά συμπεράσματα του GridEx II είναι η ανάγκη περιοδικής εκτίμησης της κατάστασης του δικτύου, όσον αφορά τις ευπάθειες που υπάρχουν σε αυτό, ώστε να υιοθετηθούν τα κατάλληλα μέτρα ασφαλείας, για να αποφευχθούν όσο το δυνατόν γίνεται τέτοιου είδους επιθέσεις. Η χρήση μηχανισμών, οι οποίοι θα συλλέγουν δεδομένα σχετικά με την επίθεση που πραγματοποιείται, όπως συγκεκριμένα μοτίβα επίθεσης, ευπάθειες που έχει εκμεταλλευτεί ο επιτιθέμενος για την είσοδο στο σύστημα κ.α, θα βοηθήσουν σημαντικά στην ενίσχυση του συστήματος ασφαλείας για την αντιμετώπιση μελλοντικών επιθέσεων. Επιπλέον, το δίκτυο επικοινωνίας θα πρέπει να λαμβάνει μέριμνα, ώστε κατά τη διάρκεια μιας επίθεσης, να υπάρχουν ασφαλή κανάλια επικοινωνίας, ώστε να γνωστοποιεί την κατάστασή του και με τη συνδρομή άλλων οργανισμών, να οδηγείται στην ταχύτερη επίλυση της κρίσης[61].

8.12 Προτυπα

Υπάρχουν διάφορα πρότυπα που ισχύουν για την ασφάλεια του εξοπλισμού υποσταθμών και πολλά είναι υπό ανάπτυξη. Για τη γενική αξιολόγηση της ασφάλειας, ο τυποποιημένος ISO 27001 χρησιμοποιείται ευρέως και διευκρινίζει την αξιολόγηση των κινδύνων για ένα σύστημα οποιουδήποτε είδους και τη στρατηγική για το σύστημα ασφάλειας για να μετριάσει τους κινδύνους. Επιπλέον, ο ISO 28000 διευκρινίζει τη διαχείριση ασφάλειας συγκεκριμένα για ένα σύστημα αλυσίδων ανεφοδιασμού [9].

8.12.1 IEEE 1686: Τα IEEE πρότυπα για τις ευφυείς ηλεκτρονικές δυνατοτητες ασφαλειας υποσταθμων (IEDS)

Αυτά τα πρότυπα προήλθαν από μια προσπάθεια ασφάλειας IED του NERC CIP (North America Electric Reliability Corporation). Τα πρότυπα ισχύουν σε οποιοδήποτε IED όπου ο χρήστης απαιτεί «την ασφάλεια, την υπευθυνότητα, και την ακουστική ικανότητα στη διαμόρφωση και τη συντήρηση του IED».

> Τα πρότυπα προτείνουν τους διαφορετικούς μηχανισμούς για να προστατεύσουν IEDs. Το IED:[9]

- προστατεύεται από το μοναδικό χρήστη - συνδυασμοί ταυτότητας και κωδικού πρόσβασης. Ο κωδικός πρόσβασης πρέπει να είναι το ελάχιστο 8 χαρακτήρες και συνδυασμό αριθμών και γραμμάτων
- Δε πρέπει να έχει οποιαδήποτε μέσα να σπάσει ή να παρακάμψει το δημιουργημένο από το χρήστη ID/password. Οι μηχανισμοί όπως ο «ενσωματωμένος κύριος κωδικός πρόσβασης, ή η παράκαμψη υλικού των κωδικών πρόσβασης όπως οι άλτες και οι τοποθετήσεις διακοπτών» δεν θα πρέπει να είναι παρόντες.
- υποστηρίζει το διαφορετικό επίπεδο χρησιμοποίησης των λειτουργιών IED και των χαρακτηριστικών γνωρισμάτων βασισμένων στους μεμονωμένους χρήστες-δημιουργημένους συνδυασμούς ID/password.
- έχει ένα χαρακτηριστικό γνώρισμα διαλείμματος που αποσυνδέει αυτόματα έναν χρήστη.
- καταχωρεί σε έναν διαδοχικό κυκλικό απομονωτή τα γεγονότα του ελέγχου διαδρομών λιστών με τη σειρά στην οποία εμφανίζονται.
- ελέγχει τη σχετική με την ασφάλεια δραστηριότητα και καταστεί τις πληροφορίες διαθέσιμες μέσω ενός πρωτοκόλλου επικοινωνίας σε πραγματικό χρόνο για τη μετάδοση σε SCADA».

8.12.2 IEC 62351: Διαχειριση συστηματων δυναμης και σχετικη ανταλλαγη πληροφοριων

Το IEC 62351 είναι μια σειρά εγγράφων ασφάλειας στοιχείων και επικοινωνιών που διευκρινίζει τους τύπους μέτρων ασφάλειας για τα δίκτυα επικοινωνίας και συστημάτων συμπεριλαμβανομένων των σχεδιαγραμμάτων όπως TCP/IP, τις κατασκευαστικές προδιαγραφές μηνυμάτων (MMS) και το IEC 61850. Μερικά μέτρα ασφάλειας που περιλαμβάνονται στα πρότυπα είναι [9]:

- ✓ επικύρωση των οντοτήτων μέσω των ψηφιακών υπογραφών
- ✓ εμπιστευτικότητα των κλειδιών και των μηνυμάτων επικύρωσης μέσω της κρυπτογράφησης
- ✓ ανίχνευση πλαστογραφήσεων
- ✓ πρόληψη της αναπαραγωγής ήχου και εξαπάτησης
- ✓ έλεγχος επικοινωνιών της ίδια της υποδομής.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το έξυπνο ηλεκτρικό δίκτυο έρχεται για να εκσυγχρονίσει το υπάρχον απαρχαιωμένο ηλεκτρικό δίκτυο το οποίο δεν μπορεί να ανταποκριθεί στις ανάγκες του σημερινού καταναλωτή και δεν έχει την υποδομή να υποστηρίξει τις δυνατότητες που μπορούν να μας δώσουν οι σημερινές τεχνολογίες. Το έξυπνο ηλεκτρικό δίκτυο αξιοποιώντας και ενσωματώνοντας τις νέες τεχνολογίες επικοινωνιών και πληροφορικής σε καίρια σημεία του δικτύου προσφέρει πολλά πλεονεκτήματα για την κοινωνία, την οικονομία και το περιβάλλον. Η ενσωμάτωση των νέων αυτών τεχνολογιών και ειδικότερα αυτών που σχετίζονται με το διαδίκτυο εισάγουν νέες απειλές για την ασφάλεια του έξυπνου πλέγματος. Στη παρούσα διπλωματική εντοπίσαμε κινδύνους που μπορούν να προκύψουν κατά την αλληλεπίδραση των οντοτήτων του έξυπνου πλέγματος και παρουσιάσαμε τρόπους αντιμετώπισης για πολλούς από αυτούς. Το ζήτημα της ασφάλειας των έξυπνων δικτύων θα πρέπει να αποτελέσει μείζον θέμα και θα πρέπει να το θωρακίσουμε με τεχνικές που θα το κάνουν ακόμα πιο ασφαλές στο άμεσο μέλλον κυρίως από επιθέσεις που προέρχονται από το χώρο του διαδικτύου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] http://el.wikipedia.org/wiki/Ηλεκρικό_δίκτυο

[2] The Smart Grid: An Introduction, Διαθέσιμο: http://energy.gov/oe/downloads/smart-grid-introduction-0

[3] ‘’Ten Steps to a Smarter Grid’’, Steven E. Collier. Industry Applications Magazine, IEEE 2010

[4] ‘’Διαχείριση της ηλεκτρικής ζήτησης: Προκλήσεις και πλεονεκτήματα’’, Ιωάννης Παναπακίδης, Νικόλαος Τσιαντούλας. Τεχνικό επιμελητήριο Ελλάδος, Τμήμα Κεντρικής Μακεδονίας-Μόνιμη Επιτροπή Ενέργειας- Θεσσαλονίκη 2012.
(είναι για τις τεχνολογιες εξυπνου δικτυου)

[5] Survey of regulatory and technological developments concerning smart metering in the European Union electricity market,Jorge Vasconcelos. Διαθέσιμο:

http://cadmus.eui.eu/bitstream/handle/1814/9267/RSCAS_PP_08_01.pdf?sequence=2

[6] Chun-Hao Lo, Nirwan Ansari, “The Progressive Smart Grid System from Both Power and Communications Aspects”, *IEEE Communications Surveys & Tutorial*, vol. 14, no. 3, pp. 799-821, 2012

[7] IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 7, NO. 4, NOVEMBER 2011
Smart Grid Technologies: 1CommunicationTechnologies and Standards
1Vehbi C. Güngör*, Member, IEEE*, Dilan Sahin, Taskin Kocak, Salih Ergüt,
1Concettina Buccella*, Senior Member, IEEE*, Carlo Cecati*, Fellow, IEEE*, and
1Gerhard P. Hancke*, Senior Member, IEEE. Διαθέσιμο:*

http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6011696&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F9424%2F6056501%2F06011696.pdf%3Farnumber%3D6011696

[8[http://el.wikipedia.org/wiki/SCADA

[9] J. Ekanayake, K. Liyanage, et al, ''Smart Grid - Technology and Applications'', Wiley & Sons, 2012

[10] Smart grid security, Jorge Cuella, Berlin, Germany, December 3, 2012,

[11] https://www.dei.gr/el/tin-texnologia-tis-tilemetrisis-eisagei-sta-diktua-tis-i-dei-ae

[12]http://en.wikipedia.org/wiki/Smart_grid#Historical_development_of_the_electricity_grid

[13] Σύγχρονες Τεχνολογίες Πρόσβασης και Διαδικτύου σε Έξυπνα Δίκτυα (Smart Grids) ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ Ευφροσύνη Θ. Ζώτου

[14] www.smartgrid.gov advanced metering infrastuctare

[15] https://www.dei.gr/el/tin-texnologia-tis-tilemetrisis-eisagei-sta-diktua-tis-i-dei-ae

[16] IEEE ICSET 2010 6-9 Dec 2010, Kandy, Sri Lanka, Smart Grid - Technologies for its realization, Mahesh Sooriyabandara, Janake Ekanayake

[17] http://energy.gov/oe/downloads/what-smart-grid-means-americans

[18] Swapna Iyer ,Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616-3793, USA, Volume 2011, Article ID 372020 Academic Editor: Pierangela Samarati

[19] Tony Flick, Justin Morehouse "Securing The Smart Grid, Next Generation Power Grid Security"

[20]European Union Smart Grid policy, Διαθέσιμο: http://smartgrid.ieee.org/resources/public-policy/european-union

[21]The United States' Smart Grid policy, Διαθέσιμο: http://smartgrid.ieee.org/resources/public-policy/united-states

[22]The Federal Smart Grid Task Force, Διαθέσιμο:http://energy.gov/oe/technology-development/smart-grid/federal-smart-grid-task-force

[23]https://el.wikipedia.org/wiki/χακερ

[24]Θέματα Ασφάλειας και Συνεργατικών Υπηρεσιών σε Δίκτυα Smart Grid Χρήστος Τσιράκης 2012

[25]Ανίχνευση εισβολών σε δίκτυα υπολογιστών με αλγόριθμους μηχανικής μάθησης. Αικατερίνη Β. Μητροκώτσα, Διδακτορική διατριβή 2007

[26]OWASP, «HTTP Post,» 2010 November 2010. [Ηλεκτρονικό]. Available: https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf.

[27]"After Stuxnet The new rules of cyberwar - Computerworld." [Online]. Available: http://www.computerworld.com/s/article/9233158/After_Stuxnet_The_new_rules_of_cyberwar

[28] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, A. C. Alvaro, and W. H. Sanders, “AMI Threats , Intrusion Detection Requirements and Deployment Recommendations.

[29]http://www.computer-network-security-training.com/what-is-a-spoofing-attack/

[30]Rose Tsang “Cyberthreats, Vulnerabilities and Attacks on SCADA Networks”, Διαθέσιμο: http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf

[31]D. P. P. M. Stephen McLaughlin, «Energy Theft in the Advanced Metering Infrastructure,» Systems and Internet Infrastructure Security Laboratory (SIIS), 2009.

[32] D. P. S. M. A. D. P. M. S. McLaughlin, «Multi-vendor Penetration Testing in the Advanced Metering Infrastructure,» Department of Computer Science and Engineering, Pennsylvania State University, 2010

[33]J. A. J. e. al., «Lest We Remember: Cold Boot Attacks on Encryption Keys,» σε *Proc. 200 Security Symposium*, San Jose, 2008.

[34]P. Kocher, «Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,» σε *CRYPTO '96*, New York, 1996.

[35]J. J. B. J. P. Kocher, «Differential Power Analysis,» σε *19th Annual International Cryptology Conference (CRYPTO)*, New York, 1999.

[36]B. A. J. R. P. R. D. Agrawal, «The EM Side–Channel(s):Attacks and Assessment,» σε *Cryptographic Hardware and Embedded Systems, CHES 2002*, Redwood Shores, California, 2002.

[37]A. S. E. T. D. Genkin, «RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis,» 2013

[38]D. P. S. A. A. F. Todd E. Humphreys, «Evaluation of the vulnerability of phasor measurement units to GPS Spoofing attacks,» *International Journal of Critical Infrastructure Protection,* τόμ. 5, αρ. 3-4, pp. 146-153, December 2012.

[39] Ασφάλεια πληροφοριών στα smart grid, Αναστάσιος-Διονύσιος Καραγιαννης

[40]Smart Grid and Smart Home Security, Ελένη Φιλίππου

41)Julie Greensmith, Uwe Aickelin “Firewalls, Intrusion Detection Systems and Anti-Virus Scanners”, 2005

42)Αθηνά Μπίρδα, Θέματα Ασφαλείας Δεδομένων Ευφυών Δικτύων Διανομής Ηλεκτρικής Ενέργειας

43)Δημήτρης Εργαζάκης, Κρυπτογραφία Διαθέσιμο: http://www.comsol.gr/dat/04FFDD5A/file.pdf

44]YAN, Ye; QIAN, Yi; SHARIF, Hamid. A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. In: Wireless Communications and Networking Conference (WCNC), 2011 IEEE. IEEE, 2011. p. 909-914.

45)Εθνική Επιτροπή Τηλεπικοινωνίων και Ταχυδρομείων. Διαθέσιμο: http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

46) IDS over firewall. Διαθέσιμο http://thecybersaviours.com/intrusion-detection-system-ids

47) Εργαλείο Ανίχνευσης Εισβολής, Παπαδοπούλου Κυριακή

48]MO, Yilin, et al. Cyber–physical security of a smart grid infrastructure. Proceedings of the IEEE, 2012, 100.1: 195-209

49)]Θέματα Ασφάλειας και Συνεργατικών Υπηρεσιών σε Δίκτυα Smart Grid Χρήστος Τσιράκης 2012

50) KHURANA, Himanshu, et al. Smart-grid security issues. IEEE Security & Privacy, 2010, 1: 81-85.

51) Paul Innella and Oba McMillan, An Introduction to Intrusion Detection Systems, Tetrad Digital Integrity, LLC last updated December 6, 2001. Διαθέσιμο: http://www.symantec.com/connect/articles/introduction-ids

52) http://bastionnux.wordpress.com/2011/04/06/ips-intrustion-prevention-systems-your-2nd-line-of-defense/

53) Karen Scarfone, Peter Mell, NIST "Guide to Intrusion Detection and Prevention Systems", 2007, Διαθέσιμο: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

54) B. W. F. K. Holcomb D, «Initial SRAM state as a fingerprint and source of true random numbers for RFID tags,» σε *Conference on RFID Security*, 2007

55) S. G.-J. S. B. v. G. J. V. N. W. R. Tuyls P, «Read-proof hardware from protective coatings,» σε *Cryptographic Hardware and Embedded Systems*, 2006

56) C. D. v. D. M. D. S. Gassend B, «Controlled physical random functions,» σε *Annual Computer Security Applications*, 2002

57) R. D. A. C. Xi Chen, «Operating System Controlled Processor–Memory Bus Encryption,» March 2008. [Ηλεκτρονικό]. Available: http://robertdick.org/publications/chen08mar-a.pdf.

58) K. R. a. R. K. -. N. Poly, «Attacks and Defences for JTAG,» January/February 2010. [Ηλεκτρονικό]. Available: http://isis.poly.edu/~securejtag/design_and_test_final.pdf

59) DDoS Επιθέσεις από Δίκτυα Botnet σε Κρίσιμες Υποδομές του Έξυπνου Δικτύου, Αβραάμ Κυριακίδη

60]ALOULA, Fadi, et al. Smart grid security: Threats, vulnerabilities and solutions. International Journal of Smart Grid and Clean Energy, 2012, 1.1: 1-6.

61]Grid Security Exercise (GridEx II), After-Action Report, March 2014 available at
http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20Public%20Report.pdf

62) http://wikipedia.qwika.com/en2el/DNP3

63)Securing Analysis of the Non –Aggressive Challenge Response of the DNP3 Protocol using a CPN Model, Raphael Amouh, Sariadi Sariadi ,Seyit Camtepe , Ernesto Foo, information security discipline Science and Engineering Faculty
Queensland University of Technology Australia

64)Security Solution For SCADA Protocols communication during Multicasting and Polling Scenario
A. Shahzad,S.Musa and M. Irfan
Malaysian Institute of Information Technology (MIIT), Jalan Sultan Ismail , University Kuala Malaysia

65) Συστήματα παρακολούθησης και καταγραφής ενέργειας για την ενεργειακή διαχείριση κτηρίων και εξαγωγή καμπύλων εκτίμησης κατανάλωσης, Δημήτριος Αλεξόπουλος

66) Συλλογή δεδομένων και εποπτικός έλεγχος στο περιβάλλον Cimplicity της GeFanuc, Χούντρα Θεοδώρου

67) C.W.S. Skorobogatov " In the Blink of an eye: There goes your AES keys", IACR Cryptology ePrint Archive, 2012

68) G. L. L. R. T. A. Bucci M, «Three-phase dual-rail pre-charge logic,» σε *Cryptographic Hardware Embeded System*, 2006.

69) M. K. Menendez E, «A high-performance, low-overhead, power-analysis-resistant, single-rail logic style,» σε *Hardware-Oriented Security and Trust*, Anaheim, CA, 2008