Ατομική Διπλωματική Εργασία

SMART GRID AND SMART HOME SECURITY

Ελένη Φιλίππου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2013

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Smart Grid and Smart Home Security

Ελένη Φιλίππου

Επιβλέπων Καθηγητής
Αντρέας Πιτσιλλίδης

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2013

Ευχαριστίες

Η ολοκλήρωση της παρούσας διπλωματικής εργασίας δε θα ήταν δυνατή χωρίς τη στήριξη και την καθοδήγηση ατόμων που με στήριξαν από την αρχή μέχρι το τέλος. Στα άτομα αυτά οφείλω ένα μεγάλο ευχαριστώ.

Καταρχάς, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στον επιβλέποντα καθηγητή μου, Δρ. Αντρέα Πιτσιλλίδη, τη στήριξη του οποίου δε θα ξεχάσω ποτέ. Στον άνθρωπο αυτό οφείλω ένα μεγάλο ευχαριστώ για το προσωπικό ενδιαφέρον που επέδειξε για εμένα και τη δουλειά μου από την πρώτη στιγμή λαμβάνοντας υπόψη τα ειδικά μου ενδιαφέροντα κατά τη διατύπωση του θέματος της παρούσας μελέτης. Τον ευχαριστώ επίσης για όλο το χρόνο που διέθεσε για την ανάγνωση αυτής της εργασίας, αποτέλεσμα του οποίου υπήρξαν οι χρήσιμες συμβουλές και συστάσεις του που βοήθησαν στη βελτίωση της ποιότητάς της.

Ευγνωμοσύνη, οφείλω επίσης και στον Δρ. Νίκο Κομνηνό, χωρίς την πολύτιμη εμπειρία του οποίου η διπλωματική αυτή δε θα ήταν ίδια. Ένα θερμό ευχαριστώ, για όλες τις ώρες που μου αφιέρωνε, σχεδόν κάθε βδομάδα μέσα στον περασμένο χρόνο, για εποικοδομητικό διάλογο και πολύτιμη καθοδήγηση όχι μόνο για θέματα που εμπίπτουν στο πλαίσιο της παρούσας μελέτης, αλλά και για θέματα που αφορούν στη μετέπειτα ακαδημαϊκή ζωή μου. Ο ενθουσιασμός, η αφοσίωση και η μεθοδικότητα του αποτέλεσαν για μένα έμπνευση, ενώ οι ιδέες και οι εισηγήσεις του συνέβαλαν σε μεγάλο βαθμό στη διαμόρφωση της παρούσας διπλωματικής ως έχει.

Τις ειλικρινείς ευχαριστίες μου, οφείλω και στο Δρ. Αντρέα Καμηλάρη, ο οποίος στάθηκε δίπλα μου κατά τη διάρκεια εκπόνησης της συγκεκριμένης διπλωματικής εργασίας, προσφέροντάς μου πολύτιμες συμβουλές και εισηγήσεις για τη βελτίωση του περιεχομένου της.

Κλείνοντας, θα ήθελα να εκφράσω ένα πολύ μεγάλο ευχαριστώ στη μητέρα και τον πατέρα μου, για όλη τους την αγάπη, τη συμπαράσταση και την πίστη σε εμένα όλα αυτά τα χρόνια. Ευχαριστώ ακόμα την αδερφή μου, Άντρια ,με τη υποστήριξη, την ειλικρίνεια και το χιούμορ της οποίας κατάφερα να διατηρήσω πολύτιμες ισορροπίες όλο αυτό το διάστημα.

Τέλος, ευχαριστώ τον Γιώργο για όλη την αγάπη, την κατανόηση και τη στήριξη του σε αυτή την προσπάθεια.

Περίληψη

Η βιομηχανία παραγωγής ηλεκτρικής ενέργειας βρίσκεται πλέον στο κατώφλι μιας νέας εποχής. Μιας εποχής, που υπόσχεται μέσα από τη μετεξέλιξη των υφιστάμενων δικτύων ηλεκτροδότησης σε Smart Grids, αποδοτικότερη και αποτελεσματικότερη διαχείριση ενέργειας, μεγαλύτερη αξιοπιστία, μειωμένο κόστος παραγωγής και διαδικασίες πιο φιλικές προς το περιβάλλον ως αποτέλεσμα της αξιοποίησης εναλλακτικών και ανανεώσιμων πηγών ενέργειας. Αργά ή γρήγορα τα Smart Grids θα αποτελούν τη νέα μας πραγματικότητα. Ήδη, ανά το παγκόσμιο, πολλές πρωτοβουλίες και πιλοτικά προγράμματα εφαρμόζονται για την αξιολόγηση των πλεονεκτημάτων και τον εντοπισμό ενδεχόμενων κινδύνων που ενέχονται στην μετεξέλιξη των υφιστάμενων δικτύων σε Smart Grids. Τέτοια δίκτυα, αποτελούν κρίσιμες υποδομές για κάθε χώρα μαζί με τα δίκτυα υδροδότησης, τα δίκτυα τηλεπικοινωνιών, τα οδικά δίκτυα, τα δίκτυα δημόσιας υγείας, τον τραπεζικό τομέα κλπ.. Η ασφάλειά τους λοιπόν, γίνεται συνώνυμη με την εύρυθμη λειτουργία κάθε κοινωνίας. Η μελέτη αυτή επικεντρώνεται σε θέματα που αφορούν στην ασφάλεια του Smart Grid περιβάλλοντος και των Smart Homes, τα οποία θα αποτελέσουν μελλοντικά αναπόσπαστο κομμάτι του. Μέσα από αυτή τη μελέτ,η επιχειρούμε να παρουσιάσουμε μερικούς από τους πιο αντιπροσωπευτικούς κινδύνους που απειλούν το Smart Home/Smart Grid περιβάλλον. Οι κίνδυνοι αυτοί, εντοπίστηκαν στη βάση σεναρίων που αντιπροσωπεύουν τις κυριότερες αλληλεπιδράσεις μεταξύ των οντοτήτων του Smart Home/Smart Grid περιβάλλοντος και κατηγοριοποιήθηκαν με βάση στόχους ασφάλειας που τέθηκαν για το σύστημα. Για κάθε ένα από αυτούς τους στόχους, αναζητούμε μέσα από τη σύγχρονη βιβλιογραφία, τρόπους αντιμετώπισης. Γεγονός, που μας επιτρέπει να εντοπίσουμε ανοικτές προκλήσεις και άλυτα προβλήματα ασφάλειας των Smart Homes/Smart Grids, τα οποία παρουσιάζουμε ως ανοικτούς τομείς έρευνας για το μέλλον.

Περιεχόμενα

Λίστα Σχεδιαγραμμάτων

Σχεδιάγραμμα

Λίστα Πινάκων

Πίνακας

Λίστα Ακρωνύμων

AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
AODV	Ad hoc On-Demand Distance Vector
ASKMA	Advanced SCADA Key Management Architecture
BAN	Business Area Networks
BPSK	Binary Phase Shift Keying
CA	Certification Authority
CFB	Cipher Feedback
CIS	Customer Information System
COSEM	Companion Specification for Energy Metering
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier sense multiple access with collision avoidance
CSWG	Cyber Security Work Group
CTR	Counter
CUSUM	Cumulative Sum
DAP	Distribution Access Points
DER	Distributed Energy Resources
DES	Data Encryption Standard
DKMF	Dedicated Key Management Functions
DLMS	Device Language Message Specification
DoE	Department Of Energy
DoS	Denial of Service

DRMS	Demand Response Management System
DSS	Digital Signature Standard
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
EIBC	Extensible Identity Based Cryptography
EMS	Energy Management System
ERPI	Electric Power Research Institute
ESI	Energy Services Interface
FACTS	Flexible AC Transmission Systems
FAN	Field Area Network
GSM	Global System for Mobile Communications
HAN	Home Area Network
HMAC	Hash Message Authentication Code
HMI	Human Machine Interface
HTTP	HyperText Transfer Protocol
IAN	Industrial Area Networks
IBC	Identity Based Cryptography
IDP	Identity Provider
IDS/IPS	Intrusion Detection System/ 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

KDC	Key Distribution Centre
LAN	Local Area Network
LMS	Load Management System
MAC	Message Authentication Code
MAC layer	Medium Access Control
MDMS	Meter Data Management System
MKB	Media Key Blocks
MTU	Master Terminal Unit
NAN	Neighbourhood Area Network
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OMS	Outage Management System
PCT	Programmable Communicating Thermostat
PDC	Phasor Data Concentrator
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PET	Privacy Enhancing Technology
PEV	Plug In Electrical Vehicle
PHEV	Plug In Hybrid Electrical Vehicle
PKG	Private Key Generator
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
PMU	Phasor Measurement Units
PSTN	Public Switched Telephone Network
QoS	Quality of Service

QPSK	Quadrature Phase Shift Keying
RA	Registration Authority
REST	Representational State Transfer
RP	Relaying Party
RSA	Rivest Shamir Adleman
RTU	Remote Terminal Unit
S/MIME	Secure/Multipurpose Internet Mail Extensions
SA	Security Association
SAML	Security Assertion Markup Language
SCADA	Supervisory Control And Data Acquisition system
SG-CG	Smart Grid Coordination Group
SHA	Secure Hash Algorithm
SKE	SCADA Key Establishment
SKMA	SCADA Key Management Architecture
SOAP	Simple Object Access Protocol
SPK	Signature Proof of Knowledge
SSH	Secure Shell
SSL	Secure Sockets Layer
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TSO	Transmission System Operator
TTP	Third Trusted Party
UKMF	Unified Key Management Functions
URI	Universal Resource Identifier
VA	Validation Authority

WAKE	Wide Area Measurements Key Management
WS	Web Services
WSDL	Web Services Description Language
XACML	eXtensible Access Control Markup Language
ZKP	Zero Knowledge Protocols/Proofs

Κεφάλαιο 1

Εισαγωγή

Ότι έχουμε καταφέρει να δημιουργήσουμε μέχρι σήμερα, όλος ο σύγχρονος τεχνολογικός πολιτισμός, η πρόοδος που έχουμε εξασφαλίσει για τις κοινωνίες μας αλλά και κάθε μας προσπάθεια για οικονομική ανάπτυξη και ευημερία, στηρίχθηκαν και εξακολουθούν να στηρίζονται σε μια από τις πιο κρίσιμες υποδομές που κατασκεύασε ποτέ ο άνθρωπος – τα δίκτυα ηλεκτροδότησης.

Για πολλά χρόνια τα δίκτυα αυτά, τα οποία ελάχιστα έχουν αλλάξει μέχρι σήμερα, κατάφερναν να ικανοποιούν τις ανάγκες μας, όμως, καθώς προχωρούν τα χρόνια, οι απαιτήσεις μας γίνονται ολοένα και πιο σύνθετες. Πλέον δε μας αρκεί η απλή παραγωγή και μεταφορά ενέργειας. Χρειαζόμαστε δίκτυα που θα εξυπηρετήσουν τους νέους μας στόχους για πιο αποδοτική αξιοποίηση των ανανεώσιμων πηγών ενέργειας, προστασία του περιβάλλοντος, μεγαλύτερη αξιοπιστία, και ανάπτυξη μιας εσωτερικής αγοράς ενέργειας στην οποία ο καταναλωτής θα λαμβάνει πλέον ενεργά μέρος.

Η μετεξέλιξη των υφιστάμενων δικτύων ηλεκτροδότησης, θεωρείται πια αναπόδραστη. Ήδη ανά το παγκόσμιο βλέπουμε πολλές πρωτοβουλίες επιχειρηματικού αλλά και ακαδημαϊκού χαρακτήρα, για εκσυγχρονισμό του υφιστάμενου δικτύου ηλεκτροδότησης, να αρχίζουν να λαμβάνουν ολοένα και μεγαλύτερες διαστάσεις[1]. Στην Ευρωπαϊκή Ένωση μόνο μπορούμε να εντοπίσουμε περισσότερα από 200 τέτοια projects τα οποία βρίσκονται υπό εξέλιξη σήμερα, ενώ όπως φαίνεται και στην εικόνα 1.1, ανάλογο ενδιαφέρον επιδεικνύεται και στον υπόλοιπο κόσμο. Οι πρωτοβουλίες αυτές επιχειρούν να καταστήσουν ομαλή τη μετάβαση από το απλό grid σ’ ένα smarter grid, το οποίο αναμένουμε να εξελιχθεί στο προσεχές μέλλον σε ένα γνήσιο Smart Grid. Ένα δίκτυο, η άνευ προηγουμένου ευφυΐα του οποίου υπόσχεται να αλλάξει ριζικά τον τρόπο με τον οποίο σκεφτόμαστε σήμερα τα δίκτυα ηλεκτρικής ενέργειας.

Μια υποδομή με τόσες πολλές νέες δυνατότητες, όσες το Smart Grid, αποκτά προφανώς ένα πολύ πιο κρίσιμο χαρακτήρα από ένα τυπικό δίκτυο ηλεκτροδότησης. Η ασφάλεια, της νέας αυτής υποδομής, και η προστασία της έναντι της πληθώρας κινδύνων που θα μπορούσαν να προκύψουν από την κακόβουλη αξιοποίηση των δυνατοτήτων που παρέχει, αποτελούν αναμφίβολα ένα από τους σημαντικότερους στόχους που πρέπει να θέσουμε για αυτήν. Άλλωστε πρόκειται για την κρισιμότερη υποδομή που διαθέτουμε, δε μπορούμε να ρισκάρουμε τη διαθεσιμότητα και την αξιοπιστία της γιατί κάτι τέτοιο μπορεί να κοστίσει ακόμα και ζωές.

Παρά την κρισιμότητά της, η έρευνα για θέματα ασφάλειας σε Smart Grid και Smart Home περιβάλλοντα, βρίσκεται σήμερα σε αρχικά στάδια. Το γεγονός αυτό, αποτέλεσε για εμάς κίνητρο να εργαστούμε τόσο για τον εντοπισμό αντιπροσωπευτικών κινδύνων που μπορούν να προκύψουν κάτω από τα βασικότερα σενάρια αλληλεπίδρασης οντοτήτων του Smart Grid, όσο και για την αναζήτηση προτεινόμενων τρόπων αντιμετώπισης των κινδύνων αυτών, μέσα στη σύγχρονη βιβλιογραφία.

Σχεδιάγραμμα 1.1 Πρωτοβουλίες ανά το παγκόσμιο για θέματα που αφορούν σε Smart Grids.

1.1 Συμβολή της παρούσας μελέτης

Η παρούσα μελέτη έρχεται να ενισχύσει την ήδη υπάρχουσα βιβλιογραφία για θέματα ασφάλειας σε Smart Home/Smart Grid περιβάλλοντα. Η συμβολή της, θα μπορούσε να συνοψισθεί στα εξής τρία σημεία :

- Η μελέτη αυτή υιοθετεί ένα διαφορετικό τρόπο παρουσίασης των θεμάτων ασφάλειας στο Smart Grid περιβάλλον . Έναν τρόπο πιο συνολικό, ο οποίος θεωρούμε ότι επιτρέπει στον αναγνώστη να εκτιμήσει βαθύτερα τη σημασία της ασφάλειας στο

Smart Grid. Απομακρυνόμαστε από τα τυπικά δείγματα της βιβλιογραφίας σε αυτό τον τομέα, κοιτάζοντας το θέμα της ασφάλειας όχι αποσπασματικά, στα πλαίσια συγκεκριμένων υποσυστημάτων του Smart Grid, αλλά συνολικά, από την παραγωγή μέχρι την κατανάλωση, με στόχο να κατανοήσουμε καλύτερα τη συστημικότητα των κινδύνων στο Smart Grid.

Η προσέγγισή μας, στηρίχθηκε στον εντοπισμό των βασικότερων σεναρίων αλληλεπίδρασης μεταξύ των κυρίαρχων οντοτήτων του Smart Grid που προτείνονται από τη σύγχρονη βιβλιογραφία. Στόχος μας ήταν, μέσα από τα σενάρια αυτά, να εντοπίσουμε αδυναμίες και ενδεχόμενους κινδύνους αλλά και τις συνέπειες αυτών τόσο στο υποσύστημα στο οποίο εντάσσονται όσο και στο Smart Grid ευρύτερα. Οι κίνδυνοι που εντοπίσαμε, κατηγοριοποιήθηκαν βάσει της κατηγορίας αλληλεπίδρασης στην οποία ανήκαν και του στόχου ασφάλειας τον οποίον παραβίαζαν, ενώ αξιολογήθηκε επίσης και η κρισιμότητά τους στο πλαίσιο του Smart Grid.

- Μέσα από τη μελέτη αυτή, επιχειρούμε επίσης μια επισκόπηση της βιβλιογραφίας των τελευταίων χρόνων (2011-2013), για τρόπους αντιμετώπισης των κινδύνων κατά της ασφάλειας στο πλαίσιο του Smart Home/Smart Grid περιβάλλοντος, η οποία αποτελεί εξ' όσων γνωρίζουμε τη μοναδική στο είδος της. Μέσα από αυτήν εντοπίζουμε ορισμένα από τα πιο ενδιαφέροντα δείγματα βιβλιογραφίας, τα οποία παρουσιάζουμε και κατηγοριοποιούμε βάσει του στόχου ασφάλειας τον οποίο επιδιώκουν να εξασφαλίσουν.
- Τέλος, μέσα από τη μελέτη αυτή, εντοπίζουμε ανοικτές προκλήσεις στον τομέα της ασφάλειας των Smart Grids και μια πληθώρα από θέματα τα οποία θεωρούμε πως θα μπορούσαν να αποτελέσουν ανοικτές περιοχές για έρευνα και δημιουργία προτύπων μέσα στα επόμενα χρόνια.

1.2 Οργάνωση της μελέτης

Η εργασία αυτή οργανώνεται σε έξι κεφάλαια :

Στο δεύτερο κεφάλαιο επιχειρούμε μέσα από μια σύντομη γνωριμία με το τρέχον δίκτυο ηλεκτροδότησης, να εντοπίσουμε τις αδυναμίες του προκειμένου να προβάλουμε την ανάγκη που μας οδήγησε στην ιδέα ενός Smart Grid. Μια αφαιρετική περιγραφή της αρχιτεκτονικής ενός Smart Grid που στόχο της έχει να συνδυάσει βασικές έννοιες που θα χρησιμοποιήσουμε

στη συνέχεια όπως HAN, NAN, AMI, Smart Meter κτλ., εντάσσεται επίσης σε αυτό το κεφάλαιο, το οποίο καταλήγει με μια μικρή ενότητα που εισάγει κάποιους πρώτους προβληματισμούς για θέματα ασφάλειας σε Smart Grids.

Στο τρίτο κεφάλαιο εισάγεται η έννοια του Smart Home και πιο συγκεκριμένα των χαρακτηριστικών που το καθιστούν Energy Aware. Αναφερόμαστε στην αρχιτεκτονική του κάνοντας ένα διαχωρισμό μεταξύ αυτής που του επιτρέπει την εξωτερική αλληλεπίδραση με το Smart Grid και αυτής που του επιτρέπει την εσωτερική αλληλεπίδραση με τα υποσυστήματα του. Ακολουθεί, μια μεγάλη ενότητα στην οποία παρουσιάζουμε μερικές από τις επικρατέστερες τεχνολογίες αυτοματοποίησης και επικοινωνίας που υπάρχουν σήμερα οι οποίες θα μπορούσαν να χρησιμοποιηθούν για το σύστημα επικοινωνίας ηλεκτρικών συσκευών – μετρητή και επιμέρους μετρητών- μετρητή στο εσωτερικό περιβάλλον του Smart Home. Σε ότι αφορά στην εξασφάλιση της επικοινωνίας του Smart Home με το εξωτερικό του περιβάλλον η ενότητα αυτή παρουσιάζει πώς το Web θα μπορούσε να λειτουργήσει ως integration platform μεταξύ Smart Home – Smart Grid. Το κεφάλαιο κλείνει με την αναφορά δυνατοτήτων και ωφελημάτων που μπορεί να μας προσφέρει η διασύνδεση του Smart Home με το Smart Grid.

Στο τέταρτο κεφάλαιο ορίζουμε με σαφήνεια τους στόχους ασφάλειας στους οποίους αναμένουμε να ανταποκρίνεται το Smart Home/Smart Grid περιβάλλον ενώ παρουσιάζουμε παράλληλα και το μοντέλο βάσει του οποίου επιχειρείται η αξιολόγηση των διαφόρων κινδύνων που εντοπίζουμε στη συγκεκριμένη ενότητα. Ο εντοπισμός των κινδύνων επιχειρείται στη βάση σεναρίων που ορίσαμε με στόχο να αντιπροσωπεύσουμε ένα ευρύ φάσμα λειτουργιών τις οποίες θα καλείται να επιτελέσει το Smart Home/ Smart Grid περιβάλλον. Για σκοπούς καλύτερης οργάνωσης θεωρήσαμε θεμιτό να εντοπίσουμε κινδύνους που προκύπτουν είτε αποκλειστικά από οντότητες του Smart Grid επηρεάζοντας οντότητες του Smart Grid, είτε από οντότητες του Smart Home επηρεάζοντας το Smart Home είτε από οντότητες του ενός συστήματος – επηρεάζοντας το άλλο.

Στο πέμπτο κεφάλαιο, επιχειρούμε μια επισκόπηση της σύγχρονης βιβλιογραφίας ψάχνοντας τρόπους με τους οποίους θα μπορούσαμε να εξασφαλίσουμε τους στόχους ασφάλειας που τέθηκαν για το Smart Home/Smart Grid περιβάλλον στην προηγούμενη ενότητα. Μέσα από αυτή την ενότητα παρουσιάζουμε τρόπους με τους οποίους ήδη υφιστάμενοι μηχανισμοί ασφάλειας θα μπορούσαν να συνδυαστούν ώστε να επιτύχουμε τη διαφύλαξη εμπιστευτικότητας και ιδιωτικότητας και τη διασφάλιση διαθεσιμότητας, αυθεντικότητας,

ακεραιότητας και μη αποποίησης ευθύνης στο πλαίσιο του Smart Home/Smart Grid περιβάλλοντος.

Στο έκτο και τελευταίο κεφάλαιο, εντοπίζουμε και παρουσιάζουμε ανοικτά θέματα και προκλήσεις στον τομέα της ασφάλειας στα Smart Home/Smart Grid περιβάλλοντα , οι οποίες θα μπορούσαν να αποτελέσουν θέματα μελλοντικής έρευνας στο πεδίο αυτό.

Κεφάλαιο 2

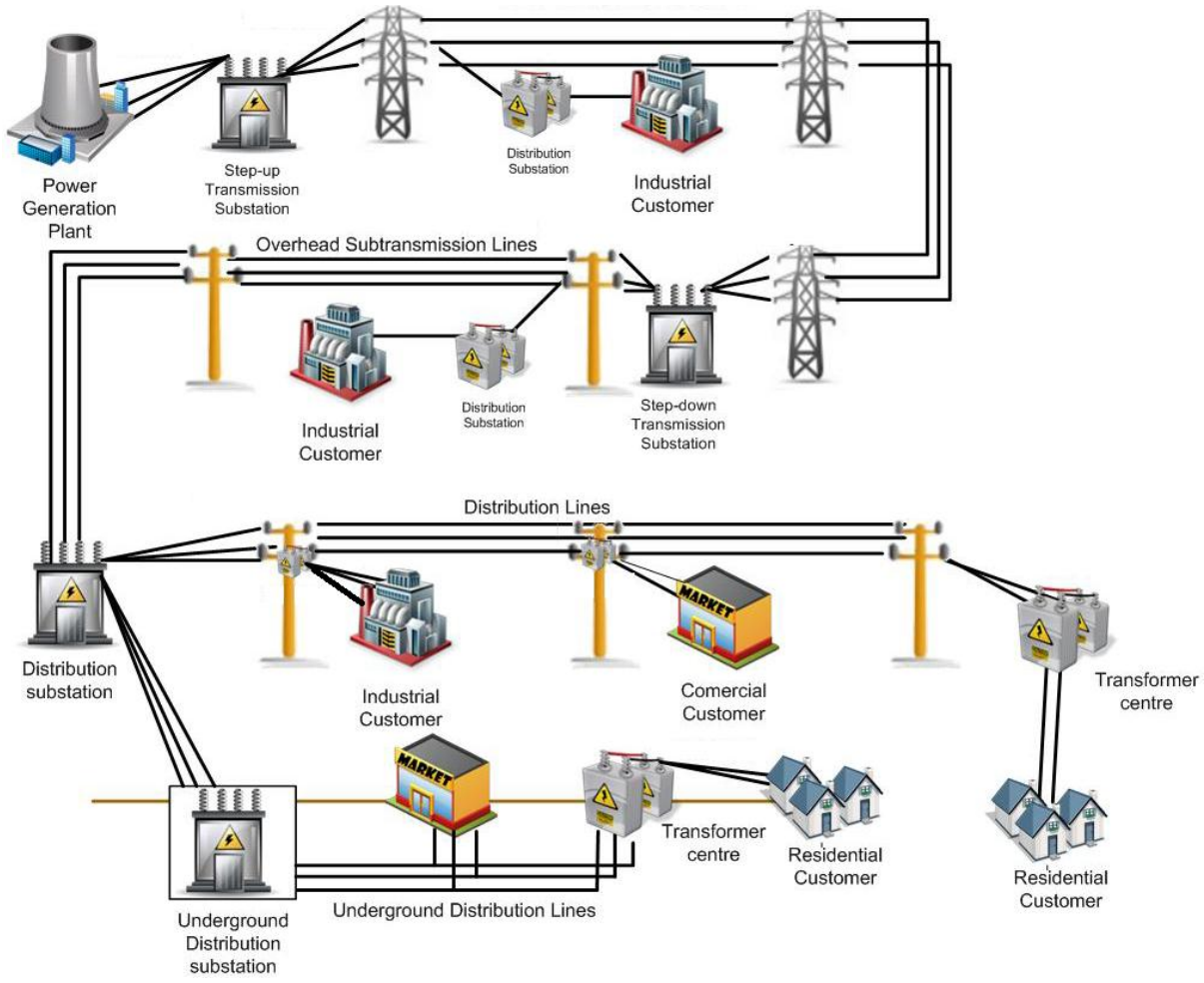
The Smart Grid

2.1 Τα ηλεκτρικά δίκτυα σήμερα

Ηλεκτρισμός. Ένα αναπόσπαστο κομμάτι της ζωής μας. Τόσο άρρηκτα συνδεδεμένο με κάθε τομέα της ανθρώπινης δραστηριότητας που δε θα ήταν υπερβολή να πούμε πως είναι η κινητήριος δύναμη ολόκληρου του κόσμου και ο ουσιαστικότερος φορέας εξέλιξης και προόδου σήμερα. Από τον Nicola Tesla ο οποίος παρουσίασε στις 16 Μαΐου του 1888 στο Αμερικανικό Ινστιτούτο Ηλεκτρομηχανικής μια πρωτοποριακή ιδέα για «το Νέο Σύστημα Κινητήρων και Μετασχηματισμών Εναλλασσόμενου Ρεύματος» [2], μέχρι τις αρχές του 20^{ου} αιώνα και τη δημιουργία των πρώτων ηλεκτρικών δικτύων μεταφοράς ρεύματος τα οποία χαρακτηρίστηκαν ως το σπουδαιότερο επίτευγμα του αιώνα από την Εθνική Ακαδημία Μηχανικών (National Academy of Engineers) [3], αλλά και μέχρι τις μέρες μας, ο ηλεκτρισμός εξακολουθεί να αλλάζει σημαντικά τη ζωή μας .

Στην ουσία ένα ηλεκτρικό δίκτυο σήμερα καθιστά εφικτή την παραγωγή , μεταφορά και διανομή ηλεκτρικής ενέργειας από τον σταθμό παραγωγής στον καταναλωτή [4][5]. Ένα τυπικό ηλεκτρικό δίκτυο [6][7][8], αποτελείται από ηλεκτροπαραγωγούς σταθμούς (power plants), υποσταθμούς μεταφοράς ανύψωσης τάσης (step-up transmission substations), υποσταθμούς μεταφοράς υψηλής τάσης και υποβιβασμού της σε μέση τάση (step-down transmission substations), υποσταθμούς διανομής μέσης τάσης και υποβιβασμού σε χαμηλή τάση (distribution substations) και γραμμές διανομής υψηλής, μέσης και χαμηλής τάσης (transmission and distribution lines). Η ενέργεια η οποία παράγεται στους ηλεκτροπαραγωγούς σταθμούς προέρχεται από ανανεώσιμες ή μη πηγές ενέργειας. Οι ανανεώσιμες πηγές ενέργειας κατατάσσονται συνήθως σε δύο κατηγορίες τις μεταβλητές

(ηλιακή, αιολική ενέργεια) και τις μη μεταβλητές πηγές ενέργειας (υδροηλεκτρική, βιομάζα, γεωθερμική ενέργεια). Οι μη ανανεώσιμες (και μη μεταβλητές) πηγές ενέργειας αφορούν συνήθως στα ορυκτά καύσιμα (κάρβουνο, πετρέλαιο, φυσικό αέριο) ή την πυρηνική ενέργεια[6]. Όπως και να παράγεται όμως η ενέργεια στους ηλεκτροπαραγωγούς σταθμούς το επόμενο βήμα είναι το ίδιο και έχει να κάνει με τη μεταφορά της, μέσω μετασχηματιστών, σε υψηλές τάσεις πριν από την εισαγωγή της στο δίκτυο μεταφοράς ώστε να ελαχιστοποιηθούν οι απώλειες λόγω του φαινομένου του Joule. Μέσω των γραμμών μεταφοράς υψηλής τάσης η ενέργεια αυτή φτάνει σε υποσταθμούς μεταφοράς η οποίοι μετασχηματίζουν την υψηλή τάση σε μέση τάση για να συνεχίσει να μεταφέρεται μέσω των γραμμών μεταφοράς προς τους υποσταθμούς διανομής οι οποίοι μετασχηματίζοντας τη μέση τάση σε χαμηλή, παραδίδουν πλέον την ενέργεια σε γραμμές διανομής χαμηλής τάσης οι οποίες συνδέονται με τα υποστατικά μας. Το Σχεδιάγραμμα 2.1 αποτελεί την αναπαράσταση της συγκεκριμένης διαδικασίας.



Σχεδιάγραμμα 2.1
Η μεταφορά και διάδοση της ηλεκτρικής ενέργειας από την παραγωγή στην κατανάλωση.

Οι υποσταθμοί μεταφοράς ηλεκτρικής ενέργειας βέβαια πέρα από τον ρόλο που διαδραματίζουν για τον μετασχηματισμό τάσης σχεδιάζονται στις πλείστες των περιπτώσεων με τρόπο τέτοιο που να εξασφαλίζονται διασυνδέσεις εναλλακτικής τροφοδοσίας από υφιστάμενους υποσταθμούς σε περιπτώσεις κατά τις οποίες ένας υποσταθμός δε μπορεί να χρησιμοποιηθεί για κάποιο λόγο (π.χ. εργασίες συντήρησης) πράγμα που αυξάνει την αξιοπιστία του δικτύου μεταφοράς ηλεκτρικής ενέργειας. Παράλληλα, μέσα στους υποσταθμούς μεταφοράς εντοπίζονται μεταξύ άλλων διακόπτες κυκλωμάτων (circuit breakers) οι οποίοι αξιοποιούνται για αποσύνδεση από το σύστημα μεταφοράς (για απομόνωση των εγκαταστάσεων ή/και των μηχανημάτων) αλλά και μονάδες συλλογής δεδομένων του υποσταθμού για αποστολή τους σε ένα κέντρο ελέγχου ενέργειας [7].

Η μεταφορά της ηλεκτρικής ισχύος από την παραγωγή στο δίκτυο διανομής μέσω των υποσταθμών μεταφοράς είναι μια διαδικασία τον έλεγχο της οποίας αναλαμβάνει συνήθως ένας Διαχειριστής Συστήματος Μεταφοράς (Transmission System Operator – TSO). Βασικός στόχος του κάθε Διαχειριστή Συστήματος Μεταφοράς είναι μεταξύ άλλων, η εξασφάλιση της ομαλής και αποδοτικής λειτουργίας του ηλεκτρικού δικτύου. Ουσιαστικής σημασίας για την επίτευξή της, είναι η ύπαρξη των κατάλληλων συστημάτων και εξοπλισμού προκειμένου να επιτυγχάνεται η διαρκής παρακολούθηση του δικτύου για την όσο το δυνατό πιο άμεση αποκατάσταση παροχής ηλεκτρικής ενέργειας μετά από περιστατικά διακοπής και την όσο το δυνατό πιο ακριβή πρόβλεψη της ζήτησης για ισοζυγισμό της παραγωγής [6][7][8]. Το βασικό σύστημα πίσω από αυτή τη διαδικασία σήμερα είναι γνωστό σαν Σύστημα Τηλελέγχου και Διαχείρισης Ενέργειας (Supervisory Control and Data Acquisition system – SCADA). Ένα τέτοιο σύστημα εκτελεί στην πραγματικότητα 4 βασικές λειτουργίες : συλλογή, επεξεργασία και παρουσίαση δεδομένων και έλεγχο του συστήματος [9]. Η συλλογή δεδομένων από ολόκληρο το δίκτυο μεταφοράς καθίσταται δυνατή μέσω εξοπλισμού ο οποίος περιλαμβάνει αισθητήρες και τηλετερματικό εξοπλισμό (Remote Terminal Units – RTUs) ο οποίος μετατρέπει τα σήματα των αισθητήρων σε ψηφιακή πληροφορία την οποία μεταφέρει στο σύστημα επεξεργασίας δεδομένων μέσω τηλεπικοινωνιακών διασυνδέσεων [6]. Η επεξεργασία γίνεται από ένα σύνολο συστημάτων μεγάλης υπολογιστικής ισχύος τα οποία παρουσιάζουν την πληροφορία που προέκυψε από τα δεδομένα σε μια μορφή που αποκτά νόημα για τους τεχνικούς που είναι υπεύθυνοι για την παρακολούθηση του δικτύου μέσω της διεπαφής (Human Machine Interface – HMI) που διαθέτει κάθε σύστημα SCADA. Η διεπαφή αυτή, παρουσιάζει σε κατανοητή μορφή την πληροφορία που αφορά στην κατάσταση του δικτύου δίνοντας ουσιαστικά τη δυνατότητα στον ελεγκτή της να έχει άμεση πληροφόρηση για ότι αφορά στο δίκτυο, τη θέση των

διακοπτών , τη φόρτιση των γραμμών, τα επίπεδα τάσης, τα επίπεδα παραγωγής από όλες τις μονάδες, την κατάσταση του εξοπλισμού, τη θερμοκρασία εντός των υποσταθμών κτλ.. Μέσω αυτής καθίσταται δυνατός ο εντοπισμός προβληματικών καταστάσεων οι οποίες απειλούν την ομαλή λειτουργία του ηλεκτρικού δικτύου, και οι οποίες ταξινομούνται από το σύστημα βάσει της επικινδυνότητας τους με τις πιο σοβαρές να αξιολογούνται ως ύψιστης προτεραιότητας, πράγμα το οποίο συμβάλλει στην όσο το δυνατό πιο άμεση ανταπόκριση. Τα συστήματα αυτά παρέχουν επιπρόσθετα και τη δυνατότητα ελέγχου και τηλεχειρισμού του εξοπλισμού ο οποίος βρίσκεται στους υποσταθμούς πράγμα το οποίο σε πολλές περιπτώσεις έχει ως αποτέλεσμα την αποκατάσταση μιας βλάβης χωρίς να χρειαστεί φυσική παρουσία τεχνικού στον υποσταθμό που αντιμετώπισε το πρόβλημα.

Ένα ολοκληρωμένο SCADA σύστημα συνεργάζεται πάντα με ένα Σύστημα Διαχείρισης Ενέργειας (Energy Management System -EMS)[9]. Το EMS αποτελείται στην πραγματικότητα από ένα σύνολο εφαρμογών οι οποίες ως στόχο τους έχουν την βελτιστοποίηση της διαδικασία παραγωγής και μεταφοράς ώστε να είναι όσο το δυνατό πιο αποδοτική , ασφαλής και οικονομική. Ένα EMS σύστημα είναι υπεύθυνο για την πρόβλεψη διακύμανσης ζήτησης ηλεκτρικής ενέργειας για την επόμενη μέρα, πρόβλεψη η οποία γίνεται εφικτή βάσει ενός ιστορικού ζήτησης ηλεκτρικής ενέργειας σε μέρες συγκρίσιμες με την αυριανή (π.χ. μέρες με τις ίδιες καιρικές συνθήκες, την ίδια εποχή, στις ίδιες ώρες). Μετά την πρόβλεψη το σύστημα οφείλει να προχωρήσει στην εισήγηση του καλύτερου τρόπου αξιοποίησης των μονάδων παραγωγής βάσει της πρόβλεψης ζήτησης και βάσει της πιο συμφέρουσας οικονομικά λύσης. Παράλληλα, η δυνατότητα προσομοίωσης της κατάστασης του δικτύου σε περίπτωση αποσύνδεσης εξοπλισμού προκειμένου να λαμβάνονται μέτρα πριν από προγραμματισμένες ενέργειες, εμπίπτει επίσης στις δυνατότητες ενός EMS [10].

2.2 Οι αδυναμίες του τρέχοντος ηλεκτρικού δικτύου

Κάπως έτσι η ηλεκτρική ενέργεια παράγεται και φτάνει στα σπίτια μας. Με μια διαδικασία η οποία ελάχιστα άλλαξε μέσα στα τελευταία 100 χρόνια[4]. Η εξέλιξη της τεχνολογίας έχει φέρει προφανώς την αυτοματοποίηση στην παραγωγή της ηλεκτρικής ενέργειας και στα συστήματα ελέγχου της, ωστόσο σε καμία περίπτωση δε μπορούμε να πούμε ότι έφερε την επανάσταση στον τομέα αυτό, όπως έχει κάνει σε τόσους άλλους τομείς της βιομηχανίας. Καθώς όμως τα χρόνια περνούν οι απαιτήσεις μας αλλάζουν πράγμα το οποίο απαιτεί και τα συστήματά μας να μπορούν να συμβαδίζουν και να ανταποκρίνονται σε αυτές. Έχουμε πλέον αρχίσει να αντιλαμβανόμαστε τις αδυναμίες του παρόντος ηλεκτρικού δικτύου.

Προφανώς, ένα δίκτυο το οποίο λειτουργεί βασισμένο σε μεγάλους κεντρικούς ηλεκτροπαραγωγούς σταθμούς χτισμένους σε στρατηγικά σημεία και συνδεδεμένους με συστήματα μεταφοράς υψηλής τάσης για να στηρίζουν την ηλεκτροδότηση μεγάλων περιοχών, στηρίζεται στη διακίνηση ενός τεράστιου όγκου πληροφορίας από και προς τα κέντρα παραγωγής, με αποτέλεσμα η πληροφορία αυτή να φτάνει πολλές φορές με καθυστερήσεις στον προορισμό (high data latency) γεγονός το οποίο στερεί τη δυνατότητα στο σύστημα να διενεργεί έλεγχο σε πραγματικό κι όχι σε σχεδόν πραγματικό χρόνο [11].

Την ίδια στιγμή μια άλλη αδυναμία του τρέχοντος δικτύου ηλεκτροδότησης έγκειται στη μονόπλευρη φύση της επικοινωνίας και διανομής ενέργειας, η οποία υπαγορεύει πως ενέργεια μεταφέρεται μόνο από τον ηλεκτροπαραγωγό σταθμό στο δίκτυο και κατά συνέπεια στον πελάτη, χωρίς ο πελάτης να μπορεί να συμβάλει στη βελτίωση της αποδοτικότητας του δικτύου εισάγοντας σε αυτό δικές του πηγές ενέργειας (ηλιακή ενέργεια, αιολική ενέργεια από ιδιόκτητες εγκαταστάσεις)[11].

Αυτή η αδυναμία του τρέχοντος ηλεκτρικού δικτύου να ενσωματώσει με επιτυχία τις εναλλακτικές πηγές ενέργειας (οι οποίες εξαρτούνται από τοπικές και καιρικές συνθήκες) στο δίκτυο με τρόπο που να μην επηρεάζει την αξιοπιστία του συστήματος (η οποία τώρα εξασφαλίζεται από την επεξεργασία των μη ανανεώσιμων μη μεταβλητών πηγών ενέργειας οι οποίες εγγυημένα θα δώσουν το ζητούμενο ποσοστό ηλεκτρικής ενέργειας) έχει παράλληλα και σημαντικές επιπτώσεις στο περιβάλλον η ρύπανση του οποίου αποτελεί ένα σημαντικό πρόβλημα σήμερα[12].

Πέραν όλων αυτών βέβαια, άλλο ένα σημαντικό μειονέκτημα του τρέχοντος ηλεκτρικού δικτύου έχει να κάνει με την αδυναμία να αποθηκεύσουμε την ηλεκτρική ισχύ με εύκολο τρόπο[13] (για περισσότερες πληροφορίες για τρόπους με τους οποίους μπορούμε να αποθηκεύσουμε την ηλεκτρική ενέργεια προτείνουμε το [14]), πράγμα το οποίο έχει ως αποτέλεσμα το τρέχον δίκτυο προκειμένου να μπορεί να ανταποκριθεί στις απαιτήσεις της επόμενης ημέρας (χωρίς να διαθέτει απόθεμα ενέργειας), να κάνει μια πρόβλεψη για την ζήτηση ηλεκτρικής ενέργειας της επόμενης ημέρας. Παρά τις προσπάθειες για εξασφάλιση όσο το δυνατό μεγαλύτερης ακρίβειας σε αυτές τις προβλέψεις η ζήτηση δε μπορεί ποτέ να προβλεφθεί με απόλυτη επιτυχία. Αυτό έχει πολύ συχνά ως αποτέλεσμα είτε την παραγωγή περισσότερης ενέργειας από όσης πραγματικά θα χρειαστεί με αποτέλεσμα η επιπλέον αυτή ενέργεια να μη χρησιμοποιείται πουθενά (αλλά το κόστος της παραγωγής της να επιβαρύνει τον πελάτη). Είτε τη διακοπή ρεύματος (rolling blackouts) λόγω μιας κακής εκτίμησης η

οποία είχε ως αποτέλεσμα την παραγωγή λιγότερης ενέργειας από αυτή που πραγματικά ζητήθηκε την επόμενη μέρα[12].

Όλα αυτά έρχονται φυσικά να επιβαρυνθούν και από το γεγονός ότι το τρέχον σύστημα χρειάζεται τη φυσική παρέμβαση ενός χειριστή προκειμένου να μπορέσει να επανέλθει σε κατάσταση λειτουργίας κατόπιν οποιασδήποτε βλάβης [15].

Φτάσαμε λοιπόν, σε ένα σημείο όπου η αδυναμία του τρέχοντος ηλεκτρικού δικτύου να ανταποκριθεί στις ολοένα αυξανόμενες απαιτήσεις μας, δημιούργησε την ανάγκη για ένα πιο έξυπνο επανασχεδιασμό του ηλεκτρικού δικτύου του 21^{ου} αιώνα. Στο νέο αυτό δίκτυο οι τεχνολογίες της επικοινωνίας και της πληροφορίας θα διαδραματίζουν κεντρικό ρόλο σε όλα τα επιμέρους στάδια από την παραγωγή μέχρι την κατανάλωση. Κάπως έτσι γεννήθηκε η ιδέα του Smart Grid!

2.3 Smart Grid - Ένα έξυπνο ηλεκτρικό δίκτυο

2.3.1 Ορίζοντας το Smart Grid

Σύμφωνα με το Electric Power Research Institute (ERPI) το Smart Grid παρουσιάζεται ως «μία ευφυής υποδομή παροχής ηλεκτρικής ενέργειας η οποία υποστηρίζεται από τις τελευταίες τεχνολογίες στον τομέα της επικοινωνίας, του υπολογισμού και της ηλεκτρονικής προκειμένου να ανταποκριθεί στις μελλοντικές απαιτήσεις της κοινωνίας σε ηλεκτρική ενέργεια»[4]. Σε μια άλλη εκδοχή, το Γραφείο Μεταφοράς και Διανομής Ενέργειας του Department of Energy (DoE) των ΗΠΑ, ορίζει το Smart Grid ως τη λύση που «θα εξασφαλίσει την αξιοπιστία, την ασφάλεια και την αποδοτικότητα του ηλεκτρικού συστήματος μέσω ανταλλαγής πληροφοριών, κατανεμημένης παραγωγής και αποθήκευσης της ενέργειας». Η Ευρωπαϊκή Επιτροπή, μέσω του COM(2011) 202 “Smart Grids: from innovation to deployment” [16] παρουσιάζει το Smart Grid ως «ένα εξελιγμένο ηλεκτρικό δίκτυο, του οποίου αναπόσπαστο κομμάτι είναι η αμφίδρομη επικοινωνία μεταξύ παραγωγού και καταναλωτή και τα ευφυή συστήματα μέτρησης και παρακολούθησης της λειτουργίας του.» Ενώ το European Commission Task Force for Smart Grid [17]ορίζει το έξυπνο δίκτυο ως «ένα ηλεκτρικό δίκτυο το οποίο με αποδοτικό τρόπο μπορεί να ενσωματώσει τη συμπεριφορά και τις δράσεις όλων των παραγόντων που βρίσκονται συνδεδεμένοι σε αυτό – παραγωγοί, καταναλωτές ή και καταναλωτές που παράγουν ενέργεια – ώστε να διασφαλίσει ένα οικονομικά αποδοτικό, βιώσιμο σύστημα ενέργειας με χαμηλές απώλειες και υψηλής ποιότητας υπηρεσία , σε ένα ασφαλές και αξιόπιστο δίκτυο»

Από τους πιο πάνω ορισμούς μπορεί κανείς να καταλάβει πως ένα Smart Grid δεν είναι τίποτα άλλο παρά η μετεξέλιξη του τρέχοντος ηλεκτρικού δικτύου σε ένα δίκτυο στο οποίο η τεχνολογία της πληροφορίας θα έχει τον πρώτιστο ρόλο. Στην ουσία, η τεχνολογία της πληροφορίας θα επιτρέπει πλέον τον απομακρυσμένο έλεγχο όλων των σταδίων από την παραγωγή στην κατανάλωση, την επικοινωνία διπλής κατεύθυνσης μεταξύ παραγωγής και κατανάλωσης (δίνοντας την ευκαιρία στον καταναλωτή να μετέχει και στην παραγωγή ως prosumer), την εξασφάλιση βιωσιμότητας (sustainability) και ποιότητας υπηρεσιών, την κατανεμημένη (distributed) παραγωγή ηλεκτρικής ενέργειας, την επεξεργασία της πληροφορίας σε τοπικό επίπεδο (χωρίς να απαιτείται αποστολή της σε ένα κεντρικό σημείο), την αποθήκευσή της παραγόμενης ενέργειας και την έξυπνη μέτρηση της κατανάλωσής της. Όλα αυτά έχοντας ως κυρίαρχο στόχο την εξασφάλιση αξιοπιστίας, αποδοτικότητας και ασφάλειας.

- Αξιοπιστίας μέσω του σχεδιασμού του συστήματος με τέτοιο τρόπο ώστε να μπορεί να λειτουργεί αυτοάνοσα – ανιχνεύοντας την αιτία των προβλημάτων του και διορθώνοντάς τα, βρίσκοντας παράλληλα εναλλακτικούς τρόπους τροφοδότησης σε περιπτώσεις που οι υφιστάμενοι δεν μπορούν να ανταποκριθούν στις απαιτήσεις. Κάτι τέτοιο προφανώς μειώνει και τον κίνδυνο για blackouts τα οποία έχουν σημαντικό αντίκτυπο σε οικονομικό αλλά και σε κοινωνικό επίπεδο.
- Αποδοτικότητας, μέσω της αξιοποίησης εναλλακτικών μορφών ενέργειας για τη βελτιστοποίηση της διαδικασίας παραγωγής-μεταφοράς και διάδοσης ενέργειας αλλά και μέσω της εμπλοκής του πελάτη στη διαδικασία εξοικονόμησης ενέργειας πράγμα το οποίο μπορεί να επιτευχθεί μέσω ευέλικτων προγραμμάτων demand-response.
- Και ασφάλειας μέσω πιο προσεγμένου ελέγχου και παρακολούθησης της διαδικασίας ηλεκτροδότησης[11].

2.3.2 Τα αναμενόμενα πλεονεκτήματα ενός «Έξυπνου» Δικτύου

Στις 13 Σεπτεμβρίου του 2011 το Τμήμα Εμπορίου του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογιών (National Institute of Standards and Technology - NIST) των ΗΠΑ και η Συντονιστική Επιτροπή για δίκτυα Smart Grids της Ευρωπαϊκής Ένωσης (Smart Grid Coordination Group - SG-CG)[1] σε κοινή τους ανακοίνωση δήλωσαν την πρόθεσή τους να συνεργαστούν για την ανάπτυξη κοινών προτύπων για τη σχεδίαση και λειτουργία των Smart Grids, ώστε να επιτευχθεί η μεταξύ τους διαλειτουργικότητα [18][19]. Οι δύο αυτοί οργανισμοί εκδίδουν κατά καιρούς διάφορες αναφορές. Χρησιμοποιώντας τις [20] και

[21]μπορούμε να συνοψίσουμε ένα σύνολο από πλεονεκτήματα τα οποία αναμένουμε να μας παρέχει το έξυπνο δίκτυο ηλεκτροδότησης.

- Μεγαλύτερη αξιοπιστία και καλύτερη ποιότητα υπηρεσίας (Μέσω υιοθέτησης ενός κατανεμημένου μοντέλου παραγωγής ενέργειας).
- Καλύτερη αξιοποίηση της υφιστάμενης υποδομής και των εναλλακτικών μορφών ενέργειας προκειμένου να μη χρειάζεται πλέον η χρήση απαρχαιωμένων ηλεκτροπαραγωγών σταθμών (που μολύνουν το περιβάλλουν) για κάλυψη της ζήτησης.
- Ευέλικτος σχεδιασμός που να επιτρέπει στο σύστημα να λειτουργεί αυτοάνοσα σε περιπτώσεις βλάβης.
- Προστασία του περιβάλλοντος μέσω της αξιοποίησης εναλλακτικών μορφών ενέργειας που έχει ως αποτέλεσμα την μείωση εκπομπής ρυπογόνων παραγόντων στην ατμόσφαιρα
- Ενεργός συμμετοχή του καταναλωτή στην προσπάθεια για εξοικονόμηση ενέργειας (μέσω προγραμμάτων demand response και δυναμικής χρέωσης κιλοβατώρων αναλόγως της ώρας της ημέρας).
- Δυνατότητα πιο ακριβούς πρόβλεψης της ζήτησης μέσω επεξεργασίας δεδομένων που λαμβάνονται από έξυπνους μετρητές (πράγμα το οποίο συνεπάγεται μειωμένη σπατάλη ενέργειας και μικρότερο ρίσκο για διακοπές παροχής).

Καταλήξαμε λοιπόν στην ιδέα ενός Smart Grid το οποίο μέσω της ψηφιοποίησης του θα λειτουργεί πιο έξυπνα και γρήγορα. Ένα δίκτυο ευέλικτο με την έννοια της συμβατότητας του με το υφιστάμενο αλλά και της δυνατότητας να το επεκτείνουμε και να το αναπροσαρμόσουμε ώστε να ικανοποιεί τις ανάγκες μας. Το δίκτυο αυτό αναμένουμε να είναι ευφυές, ανθεκτικό απέναντι στις οποιεσδήποτε επιθέσεις εναντίον του και την ίδια στιγμή προσαρμόσιμο ώστε να μπορεί να ικανοποιεί εξειδικευμένα τις ανάγκες των πελατών. Ποια είναι όμως τα συστατικά στοιχεία ενός Smart Grid;

1 Ως αντιπρόσωπος τριών οργανισμών European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI).

2.4 Η αρχιτεκτονική ενός Smart Grid

2.4.1 Σύντομη επισκόπηση αρχιτεκτονικών για τα Smart Grids.

Υπάρχει μια πληθώρα τρόπων με τους οποίους μπορεί κανείς να περιγράψει ένα Smart Grid. Ένας τρόπος ο οποίος αξιοποιείται συχνά στη βιβλιογραφία [21], [22] αφορά στην απεικόνιση του Smart Grid ως ενός συνόλου από οντότητες οι οποίες επικοινωνούν μεταξύ τους. Ο τρόπος αυτός όπως προτάθηκε για πρώτη φορά από τον οργανισμό NIST, προσφέρει μια αφαιρετική απεικόνιση του Smart Grid σε ψηλό επίπεδο χωρίζοντάς το σε επτά συνεργαζόμενους τομείς-δίκτυα κάθε ένα από τα οποία περιλαμβάνει μια ή περισσότερες οντότητες - συσκευές, συστήματα ή προγράμματα (όπως π.χ. smart meters, συστήματα SCADA κτλ..) τα οποία ανταλλάζουν πληροφορίες και λαμβάνουν αποφάσεις για την εξασφάλιση της εύρυθμης λειτουργίας του. Όπως φαίνεται και στο Σχεδιάγραμμα 2.2 οι επτά τομείς στους οποίους μπορούμε να χωρίσουμε ένα Smart Grid είναι οι Πελάτες, οι Αγορές, οι Πάροχοι Υπηρεσιών, οι Λειτουργίες, η Παραγωγή, η Μεταφορά και η Διανομή. Ακολουθεί μια περιγραφή των οντοτήτων τις οποίες περιλαμβάνει κάθε τομέας του μοντέλου όπως προκύπτει από το [21].

- Πελάτες : Τομέας που περιλαμβάνει τόσο τους καταναλωτές όσο και τις συσκευές που αυτοί διαθέτουν για να παράγουν, να αποθηκεύουν και να διαχειρίζονται την ενέργεια. Τυπικά αναφερόμαστε σε τρείς τύπους πελατών. Πελάτες του δικτύου με σκοπό την οικιακή χρήση ηλεκτρισμού, πελάτες με σκοπό την εμπορική χρήση και πελάτες με σκοπό τη βιομηχανική χρήση.

- Αγορές : Τομέας που περιλαμβάνει τους λειτουργούς και τους συμμετέχοντες στην αγορά ενέργειας.

- Πάροχοι Υπηρεσιών: Τομέας που αφορά στους οργανισμούς οι οποίοι προσφέρουν υπηρεσίες παροχής ηλεκτρικής ενέργειας σε πελάτες αλλά και παρόχους άλλων υπηρεσιών.

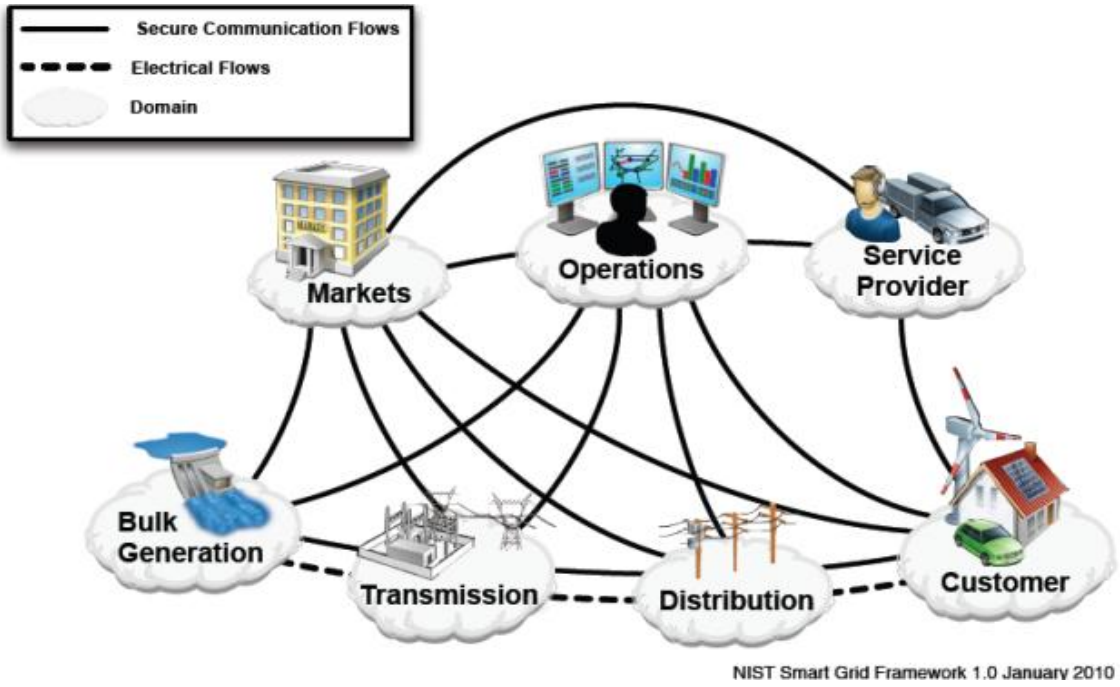
- Λειτουργίες : Τομέας που έχει να κάνει με τους διαχειριστές της διακίνησης ηλεκτρικής ενέργειας μεταξύ δικτύων.

- Παραγωγή: Τομέας που περιλαμβάνει το σύνολο των γεννητριών και ηλεκτροπαραγωγών σταθμών που παράγουν ενέργεια σε μεγάλες ποσότητες και τις μονάδες αποθήκευσης ενέργειας για διάθεση σε κατοπινό στάδιο.

- Μεταφορά : Τομέας που αναφέρεται στην η υποδομή για μεταφορά ηλεκτρικής ενέργειας σε μακρινές αποστάσεις. Ενδεχομένως να περιλαμβάνει μέσα για την αποθήκευση ή παραγωγή ενέργειας κατά τόπους.

- Διανομή : Τομέας που έχει να κάνει με την υποδομή που υπάρχει για διανομή ηλεκτρικής ενέργειας από και προς πελάτες ο οποίος ενδεχομένως να περιλαμβάνει και την αποθήκευση ενέργειας ή την παραγωγή της.

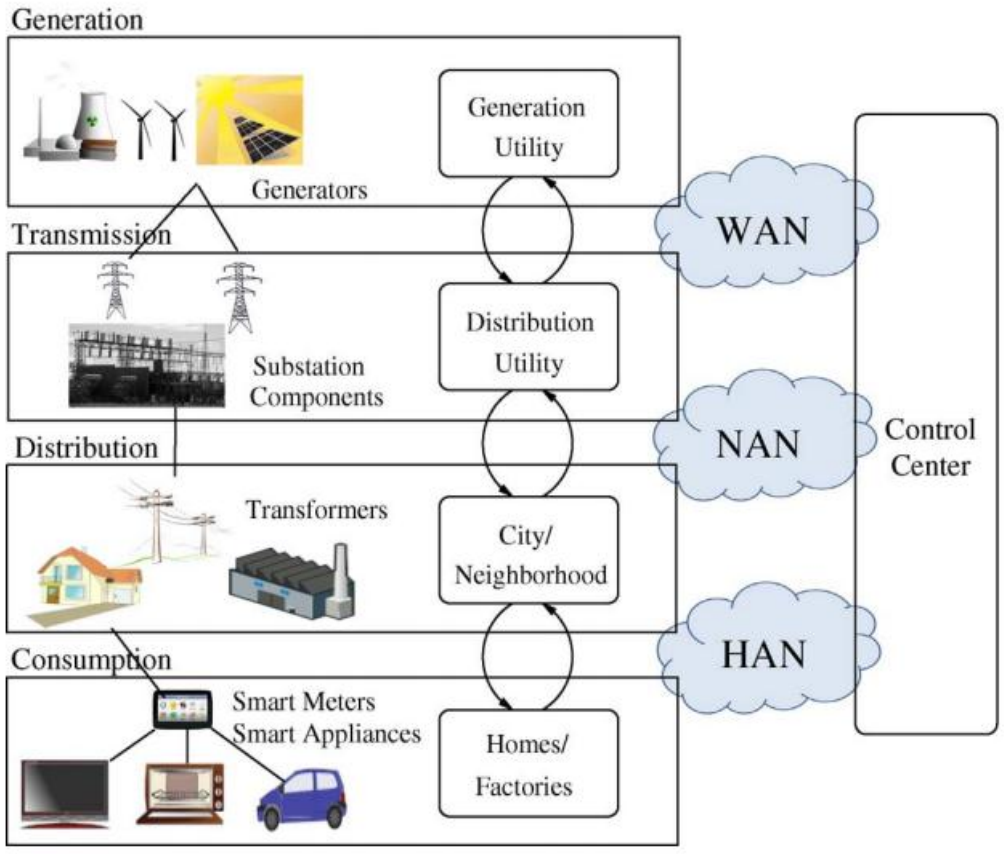
Γενικά οι οντότητες σε κάθε τομέα έχουν κοινούς στόχους και για να τους επιτύχουν πρέπει να συνεργαστούν τόσο μεταξύ τους όσο και με οντότητες άλλων τομέων. Στο σημείο αυτό σημειώνουμε ότι ο διαχωρισμός των οντοτήτων σε τομείς δεν είναι απόλυτος καθότι σε πολλές περιπτώσεις μια οντότητα μπορεί να επιτελεί λειτουργία βασισμένη σε πληροφορία από άλλους τομείς (π.χ. Το δίκτυο διανομής αφορά και τον τομέα Διανομής αλλά και τον τομέα Λειτουργιών (αφού εκεί εμπίπτουν τα συστήματα διαχείρισης δικτύων διανομής).



Σχεδιάγραμμα 2.2 Το αφαιρετικό μοντέλο του NIST το οποίο απεικονίζει το Smart Grid ως ένα σύνολο οντοτήτων που αλληλεπιδρούν μεταξύ τους.

Εκτός από το εννοιολογικό μοντέλο του NIST βέβαια, η βιβλιογραφία έχει να προτείνει κι άλλους τρόπους με τους οποίους μπορεί κανείς να αντιληφθεί την αρχιτεκτονική ενός Smart Grid.

Συγκεκριμένα στο [15] τα Smart Grids μελετούνται ως δίκτυα τα οποία αποτελούνται από τρία θεμελιώδη και αλληλοσυνεργαζόμενα συστήματα, το έξυπνο σύστημα υποδομής (υπεύθυνο για την παραγωγή, μεταφορά και διανομή της ενέργειας με όλα τα υποσυστήματα που ελέγχουν και διαχειρίζονται αυτή τη διαδικασία), το έξυπνο σύστημα διαχείρισης (το οποίο παρέχει υπηρεσίες διαχείρισης και ελέγχου που έχουν να κάνουν με την αποδοτικότερη διαχείριση ενέργειας και την πιο σωστή πρόβλεψη ζήτησης) και το έξυπνο σύστημα ασφάλειας (υπεύθυνο για την εξασφάλιση της εύρυθμης και αξιόπιστης λειτουργίας του δικτύου, μακριά από κακόβουλες επιθέσεις ή καταστροφικά σφάλματα και βάσει των αρχών διαφύλαξης της ιδιωτικότητας των πελατών). Από την άλλη υπάρχουν μελέτες που έχουν προτείνει και αρχιτεκτονικές των Smart Grids οι οποίες τα διαχωρίζουν σε επίπεδα Παραγωγής, Μεταφοράς, Διανομής και Κατανάλωσης της ηλεκτρικής ενέργειας τα οποία μέσω δικτύων (HAN, NAN, WAN) συνδέονται με ένα κέντρο ελέγχου [23] [24]. Ένα τέτοιο μοντέλο παρουσιάζεται στο Σχεδιάγραμμα 2.3.

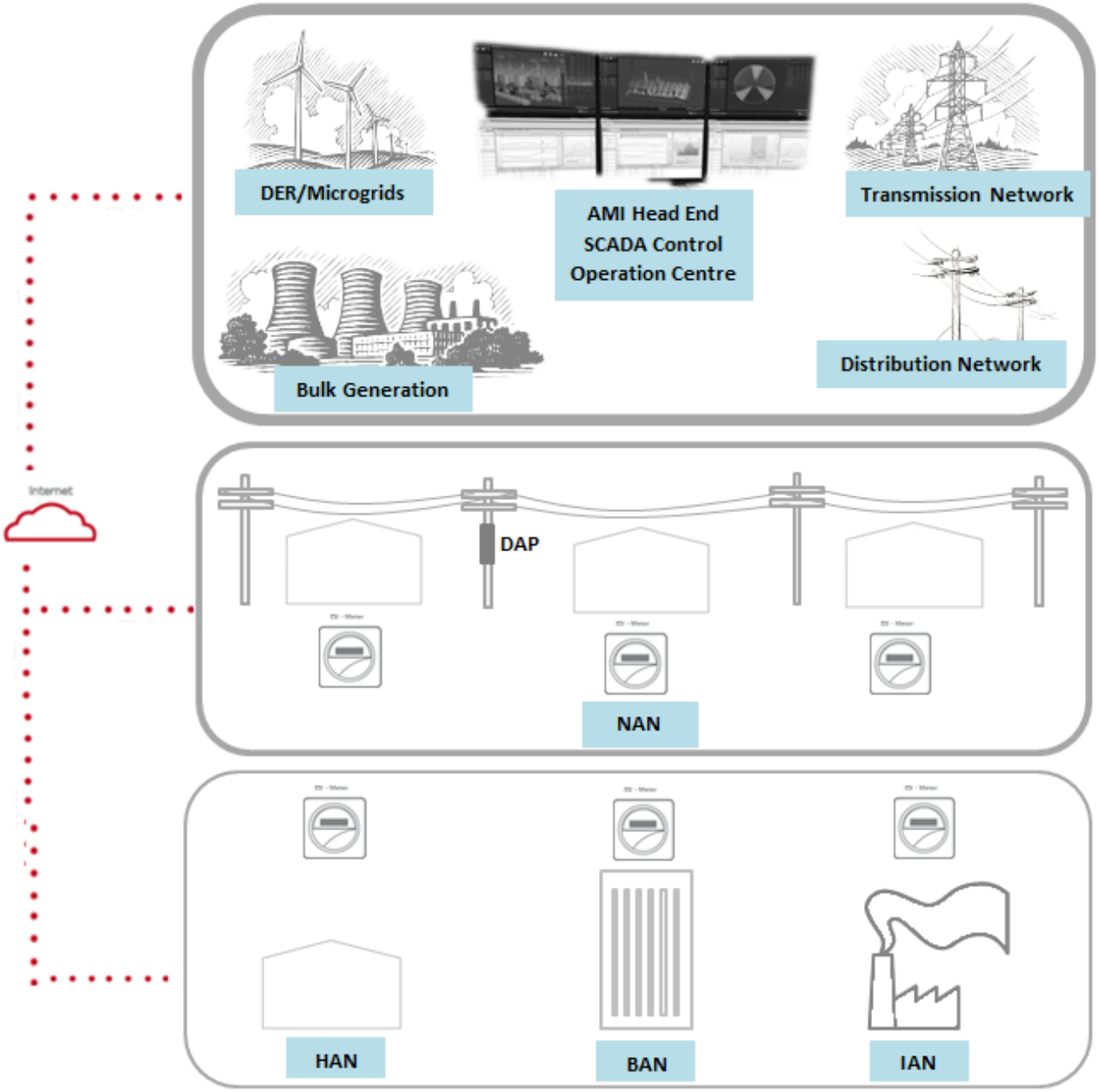


Σχεδιάγραμμα 2.3
Μια σχηματική απεικόνιση της αρχιτεκτονικής ενός Smart Grid, η οποία συνδέει κάθε ένα από τα συστατικά στοιχεία του δικτύου με ένα κεντρικό σημείο ελέγχου το οποίο είναι υπεύθυνο για τον έλεγχο ολόκληρης της διαδικασίας από την παραγωγή στην κατανάλωση.

Πέραν όλων αυτών βέβαια υπάρχουν στη βιβλιογραφία και παρουσιάσεις ενός Smart Grid ως ένα σύνολο αλληλοσυνεργαζόμενων οντοτήτων με σαφέστατα καθορισμένους ρόλους και καθορισμένα μονοπάτια επικοινωνίας [25] μοντέλο το οποίο προτάθηκε από την IEEE στα πλαίσια της κίνησης IEEE Standard 2030 (για εγκαθίδρυση ενός πλαισίου κοινώς αποδεκτών πρακτικών για εξασφάλιση διαλειτουργικότητας στα Smart Grids) για να υιοθετηθεί από μελετητές των Smart Grids [6].

2.3.2 Μια multi-layered προσέγγιση

Για τους σκοπούς αυτής της διπλωματικής εργασίας θα υιοθετήσουμε ένα μοντέλο εμπνευσμένο από τα [11], [26] και [27]. Το μοντέλο αυτό αναπαριστά ένα Smart Grid ως ένα δίκτυο από αλληλοσυνεργαζόμενα δίκτυα και θα λειτουργήσει ως το σημείο αναφοράς μας κατά την μελέτη των θεμάτων ασφάλειας των Smart Grids.



Σχεδιάγραμμα 2.4
Μια multi-layered αρχιτεκτονική για τα Smart Grids

Πρόκειται ουσιαστικά, για ένα μοντέλο το οποίο χωρίζει τα δίκτυα αυτά σε τρία επίπεδα βάσει μιας απλής λογικής η οποία έχει να κάνει με τα χαρακτηριστικά του κάθε ενός από αυτά.

Στο χαμηλότερο επίπεδό συναντάμε τρεις τύπους δικτύων,τα HAN (Home Area Networks), BAN (Business Area Networks) και IAN(Industrial Area Networks) όπου :

- HAN είναι ο όρος που χρησιμοποιούμε για την περιγραφή δικτύων τα οποία διασυνδέουν μεταξύ τους τις ηλεκτρονικές συσκευές αλλά και τις έξυπνες ηλεκτρικές συσκευές ενός σπιτιού (τηλεόραση, ψυγείο, πλυντήριο,smart meter). Η λειτουργία των συσκευών στα δίκτυα αυτά μπορεί να προγραμματιστεί για τις ώρες εκείνες στις οποίες η κατανάλωση ενέργειας κοστίζει λιγότερα από ότι συνήθως, μέσω προγραμμάτων demand-response. Για παράδειγμα, το πλυντήριο μας θα μπορούσε να τίθεται σε λειτουργία κατά τις βραδινές ώρες όταν η ζήτηση είναι πιο περιορισμένη. Την ίδια στιγμή, στα δίκτυα αυτά εμπίπτουν και συσκευές όπως ανεμογεννήτριες και φωτοβολταϊκά, μέσω των οποίων ο καταναλωτής θα μπορεί να μετατραπεί και σε παραγωγό ηλεκτρικής ενέργειας στο δίκτυο[6].
- BAN είναι ο όρος που χρησιμοποιούμε για δίκτυα τα οποία τα οποία διασυνδέουν μεταξύ τους τον εξοπλισμό ενός οργανισμού. Διαφέρουν από τα HAN, λόγω μεγέθους (είναι μεγαλύτερα) και λόγω των διαφορετικών αναγκών τις οποίες έχουν οι οργανισμοί (διαφορετικές ώρες αιχμής, μεγαλύτερες ανάγκες σε ενέργεια, δυνατότητες για διαχείριση της παραγωγής ενέργειας σε τοπικό επίπεδο κτλ.) [6].
- IAN είναι ο όρος που χρησιμοποιούμε για δίκτυα τα οποία παρέχουν την υποδομή που χρειάζεται για επικοινωνία, διασύνδεση αλλά και έλεγχο όλων των συσκευών και μηχανικού εξοπλισμού που είναι απαραίτητος για τη λειτουργία μιας βιομηχανίας, περιλαμβάνοντας πέρα από το υλικό και το λογισμικό[6].

Τα δίκτυα στο χαμηλότερο επίπεδο της ιεραρχίας μας, τοποθετήθηκαν μαζί έχοντας ως κοινό χαρακτηριστικό την άμεση επαφή τους με τον πελάτη. Στην ουσία στο επίπεδο αυτό συσκευές που ονομάζονται Smart Meters συλλέγουν πληροφορίες για τα μοτίβα κατανάλωσης των πελατών με σκοπό να τις διαβιβάσουν στα πιο πάνω επίπεδα. Όλα τα επίπεδα επικοινωνούν μεταξύ τους ανταλλάζοντας πληροφορίες γεγονός που επιτρέπει την αμφίδρομη επικοινωνία μεταξύ του πελάτη και της παραγωγής. Πιο συγκεκριμένα, ο πελάτης μπορεί ανά πάσα στιγμή να γνωρίζει τις λεπτομέρειες της κατανάλωσης του και η εταιρεία

να αποστέλλει σήματα ελέγχου για σύνδεση/αποσύνδεση συσκευών, για σκοπούς καλύτερης κατανομής του φορτίου[11].

Στο αμέσως επόμενο επίπεδο το οποίο βρίσκεται πάνω από το επίπεδο που μόλις έχουμε περιγράψει τοποθετούμε τα δίκτυα τύπου NAN :

- Με τον όρο NAN (Neighbourhood Area Networks) αναφερόμαστε σε δίκτυα τα οποία συνδέουν τους έξυπνους μετρητές των σπιτιών (HAN), οργανισμών (BAN) και βιομηχανιών (IAN) μιας μικρής γεωγραφικής περιοχής με συσκευές που ονομάζονται Distribution Access Points – DAP [25]. Οι συσκευές αυτές λειτουργούν ως διεπαφή μεταξύ του χαμηλότερου και του ψηλότερου επιπέδου επιτρέποντας τη μεταξύ τους επικοινωνία. Την ίδια στιγμή μέρος ενός NAN δικτύου είναι και συσκευές όπως RTUs (Remote Terminal Units) και PMUs (Phasor Measurement Units) οι οποίες είναι υπεύθυνες για τη συλλογή πληροφοριών για την κατάσταση του δικτύου ηλεκτροδότησης της μικρής γεωγραφικής περιοχής.

Στο ψηλότερο επίπεδο της ιεραρχίας μας θα τοποθετήσουμε δίκτυα ευρύτερης περιοχής (Regional Networks) τα οποία συνδέουν μεταξύ τους πολλαπλά NANs με το κεντρικό δίκτυο παραγωγής ηλεκτρικής ενέργειας (bulk generation networks), τα επιμέρους δίκτυα παραγωγής ενέργειας (DERs/microgrids), τα δίκτυα μεταφοράς ενέργειας, τα δίκτυα διανομής ενέργειας και τα δίκτυα ελέγχου και διαχείρισης όλων αυτών των λειτουργιών (Utility LANs). (Τα δίκτυα αυτά μπορούν να τοποθετηθούν και σε ευρύτερες ομάδες δικτύων αντί να αναφέρονται το κάθε ένα ξεχωριστά. Ορισμένα δείγματα βιβλιογραφίας που ακολουθούν το μοντέλο της IEEE [25],[22] για παράδειγμα, παρουσιάζουν τα επιμέρους δίκτυα παραγωγής ενέργειας, να διασυνδέονται με το δίκτυο διανομής ενέργειας σε ένα άλλο τύπου δικτύου που καλείται Field Area Network - FAN).

Για τους σκοπούς του δικού μας μοντέλου θεωρούμε ότι κάθε δίκτυο ευρύτερης περιοχής διαθέτει το δικό του κέντρο ελέγχου ώστε να αποκτήσουμε ένα πιο ευέλικτο και αξιόπιστο σχεδιασμό του έξυπνου δικτύου. Στο επίπεδο αυτό, αναμένουμε να παραδίδονται τα δεδομένα τα οποία οι εξειδικευμένες συσκευές εντός του δικτύου μας (smart meters, customer gateways, RTUs, PMUs) κατέγραψαν για την κατάσταση του δικτύου, και τα μοτίβα κατανάλωσης του κάθε πελάτη. Στο επίπεδο αυτό, αναμένουμε επίσης να γίνεται ο προγραμματισμός που αφορά στη βελτιστοποίηση της διαδικασίας παραγωγής και η προσπάθεια γρήγορης ανταπόκρισης σε προβλήματα τα οποία προκύπτουν.

Εδώ, αξίζει να κάνουμε μια σύντομη αναφορά σε έναν τύπο υποδομής που αναφέρεται συχνά στη βιβλιογραφία και αφορά σε αυτό που ονομάζουμε Advanced Metering Infrastructure (AMI). Με τον όρο AMI αναφερόμαστε σε έναν τύπο δικτύου ο οποίος απαρτίζεται ουσιαστικά από 4 είδη οντοτήτων:

- Τους έξυπνους μετρητές (Smart Meters) ηλεκτρικής και όχι μόνο κατανάλωσης.
- Το Customer Gateway υπεύθυνο να λειτουργήσει ως η διεπαφή μεταξύ του δικτύου επικοινωνίας AMI και του πελάτη.
- Το δίκτυο επικοινωνίας AMI μέσω του οποίου ανταλλάσουν πληροφορίες τα Smart Meters με το AMI Head End.
- Και το AMI Head End, το σύστημα δηλαδή που αναλαμβάνει την επεξεργασία των δεδομένων και την αποστολή κατάλληλων μηνυμάτων και σημάτων προς τον καταναλωτή [4] [28].

Όλα τα δίκτυα που αναφέρθηκαν πιο πάνω (NANs,το κεντρικό δίκτυο παραγωγής ηλεκτρικής ενέργειας, τα επιμέρους δίκτυα παραγωγής ενέργειας, τα δίκτυα μεταφοράς ενέργειας, τα δίκτυα διανομής ενέργειας και τα δίκτυα ελέγχου και διαχείρισης όλων αυτών των λειτουργιών) μεταφέρουν ή λαμβάνουν πληροφορίες λόγω της διασύνδεσής τους με το backhaul network. Το δίκτυο αυτό έρχεται να συνδέσει το δίκτυο του ελέγχου/λειτουργιών του οργανισμού κοινής ωφέλειας (συμπεριλαμβανομένου και του AMI) με τα δίκτυα DER/microgrids, FANs, και NANs (Distribution Access Points).

Σημαντικός είναι επίσης ο ρόλος που έχει να διαδραματίσει το Internet στην επικοινωνία μεταξύ των διαφόρων οντοτήτων στα επίπεδα της ιεραρχίας μας. Η ανταλλαγή δεδομένων μεταξύ των δικτύων μεταφοράς και διανομής, ή μεταξύ του κέντρου ελέγχου και των επιμέρους δικτύων θα μπορούσε να γίνει εφικτή τόσο μέσα από ιδιωτικά δίκτυα όσο και μέσω του Διαδικτύου. Την ίδια στιγμή το Διαδίκτυο θα μπορούσε να αποτελέσει ένα αποτελεσματικό κανάλι επικοινωνίας του Smart Grid με τον πελάτη (αφού μέσω αυτού μπορούν να φτάνουν στον πελάτη λεπτομερείς πληροφορίες για την κατανάλωσή του) αλλά και του πελάτη με το Smart Grid (αφού μέσω Διαδικτύου αναμένουμε να μπορεί ο πελάτης να έχει απομακρυσμένο έλεγχο των συσκευών του) [6].

2.5 Γιατί χρειάζεται ασφάλεια;

Έχουμε πλέον πάρει μια γεύση σχετικά με το τι είναι ένα Smart Grid πόσο διαφέρει σε σχέση με το παραδοσιακό δίκτυο ηλεκτροδότησης και ποια πλεονεκτήματα αναμένουμε από αυτό. Εντούτοις, μέχρι τώρα μιλώντας για τα Smart Grids μιλούσαμε μόνο για αποδοτικότητα,

αξιοπιστία, βελτιστοποίηση της διαδικασίας παραγωγής, οικονομικότερο ηλεκτρισμό, χωρίς να μας απασχολήσει καθόλου ένα βασικό θέμα – αυτό της ασφάλειας.

Η ασφάλεια όμως ενός δικτύου τόσο νευραλγικού όσο το δίκτυο ηλεκτροδότησης μιας χώρας, είναι ένα θέμα που δε μπορούμε να αγνοήσουμε. Ιδιαίτερα τώρα που τα δίκτυα ηλεκτροδότησής μας θα αποτελούνται στο 70% από τεχνολογίες της πληροφορικής και δίκτυα επικοινωνιών ανοικτά προς το Διαδίκτυο[22].

Τι θα μπορούσε να συμβεί; Τα σενάρια είναι πάρα πολλά και δυστυχώς στις πλείστες των περιπτώσεων έχουν σημαντικές προεκτάσεις.

Σ’ ένα Smart Grid διακινούνται τεράστιοι όγκοι δεδομένων οι οποίοι αφορούν μοτίβα κατανάλωσης των πελατών, με στόχο την καλύτερη πρόβλεψη ζήτησης για τον ισοζυγισμό της παραγωγής και το να βοηθήσουμε τον πελάτη δίνοντας του κάποιες κατευθυντήριες γραμμές και εισηγήσεις σχετικά με το πότε είναι πιο οικονομικά συμφέρον για τον ίδιο να προγραμματίσει ορισμένες δουλειές του πιο ενεργειακά δαπανηρές.

Αρκεί μόνο να σκεφτούμε πόση πληροφορία μπορούμε να εξάγουμε για τους ενοίκους ενός σπιτιού ή τους υπαλλήλους μιας εταιρείας, μόνο και μόνο μελετώντας τα καθημερινά αυτά μοτίβα κατανάλωσης, για να αντιληφθούμε πόσο επικίνδυνο είναι να αμελήσουμε την ασφάλεια ενός Έξυπνου δικτύου.

Ποιες συσκευές χρησιμοποιούνται; Σε ποιο δωμάτιο βρίσκονται οι ένοικοι; Πόσοι ένοικοι ζουν στο σπίτι; ποιες είναι οι συνήθειές τους (πότε κοιμούνται; πότε τρώνε; πότε απουσιάζουν όλοι από το σπίτι;). Αυτές είναι μόνο μερικές από τις πληροφορίες που μπορούμε να λάβουμε συνδυάζοντας ακόμη και τα ανώνυμα δεδομένα ενός μετρητή [29]. Και σα να μη φτάνει αυτό, από τα δεδομένα τα οποία συλλέγονται φορτίζοντας κατά τόπους τα PEV (Plug-In Electric Vehicles), τα ηλεκτρικά δηλαδή αυτοκίνητα τα οποία αναμένουμε να αρχίσουν να εμφανίζονται και να εδραιώνονται με τα Smart Grids, μπορούμε να καθορίσουμε πού βρίσκεται ο οδηγός ανά πάσα στιγμή, αν ακολουθεί τις συγκεκριμένες διαδρομές κάθε μέρα, προς τα πού πηγαίνει και ένα σύνολο άλλων καθαρά ευαίσθητων ιδιωτικών πληροφοριών[30].

Την ίδια στιγμή, δεν είναι απόμακρο το ενδεχόμενο μιας παρείσφρησης στο δίκτυο ενός κακόβουλου χρήστη ο οποίος εκμεταλλευόμενος την απουσία κρυπτογράφησης της

πληροφορίας στο AMI δίκτυο ή της απουσίας αυθεντικοποίησης πριν να επιτραπεί η αποστολή πληροφορίας, καταφέρνει να προσποιηθεί πως είναι το κέντρο ελέγχου που αποστέλλει πληροφορία προς το μετρητή μας . Με τον τρόπο αυτό μπορεί να διαβάσει δεδομένα που αποστέλλονται από το σπίτι μας στο κέντρο ελέγχου ή να αποστείλει ψευδή μηνύματα προς τον μετρητή του σπιτιού μας ότι οι ώρες που ακολουθούν είναι ώρες μειωμένης κατανάλωσης και χρεώνονται λιγότερο, πράγμα το οποίο δεν ισχύει.

Άλλοι ενδεχόμενοι κίνδυνοι οι οποίοι προκύπτουν έχουν να κάνουν με τη λογική των ενημερώσεων του λογισμικού στα κέντρα ελέγχου και τα επιμέρους τμήματα του δικτύου. Από τη μια, η δυνατότητα ενημέρωσης της έκδοσης ενός λογισμικού μας επιτρέπει να εμπλουτίσουμε το λογισμικό ακόμα και μετά την κυκλοφορία του πράγμα το οποίο θεωρητικά μας καθιστά πιο προετοιμασμένους να αντιμετωπίσουμε νέες απειλές. Από την άλλη όμως, αυτό μπορεί να αποτελέσει μια από τις σημαντικότερες αδυναμίες του δικτύου. Ο λόγος είναι απλός. Ένας κακόβουλος χρήστης ο οποίος ανεβάζει στο δίκτυο μια «ενημέρωση» ενός συγκεκριμένου λογισμικού, η οποία δεν είναι τίποτα περισσότερο από επιβλαβές λογισμικό, θέτει σε κίνδυνο ολόκληρο το δίκτυο.

Ο ιός Stuxnet ο οποίος δημιουργήθηκε το 2010 για να επιμολύνει SCADA συστήματα κατασκευασμένα από τη SIEMENS στο Ιράν είναι ένα τέτοιο παράδειγμα. Στην ουσία από τη στιγμή της εγκατάστασής του ο ιός εντόπιζε PLC (Programmable Logic Controllers) της SIEMENS μέσα στο δίκτυο και εγκαθίστατο σε αυτά. Οι συνέπειες αν ο ιός αυτός αναλάμβανε δράση θα μπορούσαν να είναι καταστροφικές κι αυτό γιατί ο ιός είχε ως στόχο όχι να «κλέψει» πληροφορία αλλά να επέμβει στις ρυθμίσεις του δικτύου. Θεωρητικά επεμβαίνοντας στα ρολόγια ρύθμισης ροής αερίου που ελέγχουν τη ροή αερίου στις σωλήνες που το μεταφέρουν θα μπορούσαν να υπάρξουν εκρήξεις, ενώ μεταβάλλοντας στοιχεία που καθορίζουν πως ακριβώς γίνεται η φυγοκέντρηση στους ηλεκτροπαραγωγούς σταθμούς πυρηνικής ενέργειας, ο σταθμός θα μπορούσε να παραμείνει ανενεργός[31].

Είναι προφανές πως οποιαδήποτε αδυναμία του δικτύου ηλεκτροδότησης να ανταποκριθεί στις απαιτήσεις των καταναλωτών μπορεί να οδηγήσει σε διακοπές στην παροχή ηλεκτροδότησης. Κάτι τέτοιο είτε προέλθει από κακόβουλη ενέργεια (όπως ο Stuxnet (2010) ή κάποια μετεξέλιξή του Duqu (2011), Flame (2012) [32]) είτε απροσχεδίαστα μπορεί να προκαλέσει ανυπολόγιστες ζημιές στην κοινωνία (π.χ. σε υπηρεσίες υγείας όπου η απουσία παροχής μπορεί να κοστίσει ζωές) αλλά και στην οικονομία. Σε βιομηχανίες των ΗΠΑ το κόστος διακοπής της ηλεκτροδότησης εκτιμάται στα $80δις κάθε χρόνο με τα 2/3 των

διακοπών αυτών να διήρκεσαν μόλις μερικά λεπτά [33]. Ο ηλεκτρισμός σήμερα είναι η κινητήριος δύναμη μιας χώρας πράγμα το οποίο τον καθιστά ως το νούμερο ένα στόχο για τρομοκρατικά κτυπήματα, κακόβουλες επιθέσεις και κατασκοπία. Ας θυμηθούμε περιστατικά του 2008 στην Αμερική όταν εντοπίστηκαν ίχνη Κινέζων και Ρώσων κατασκόπων οι οποίοι κατάφεραν να διεισδύσουν στο δίκτυο ηλεκτροδότησης των ΗΠΑ [34]. Μια επιτυχημένη έκβαση της υπόθεσης θα μπορούσε κυριολεκτικά να παραλύσει τις ΗΠΑ, αφού το δίκτυο παραγωγής πυρηνικής ενέργειας, το δίκτυο υδροδότησης και το δίκτυο απομάκρυνσης λυμάτων όλα σχετίζονται άμεσα με το δίκτυο ηλεκτροδότησης.

Ο τελευταίος κίνδυνος που θα αναφέρουμε στα πλαίσια αυτής της σύντομης εισαγωγής έχει να κάνει με το γνωστό είδος επιθέσεων Denial Of Service. Οι επιθέσεις αυτές υπερφορτώνουν το δίκτυο και τα επιμέρους τμήματά του ώστε αυτό να μη μπορεί να ανταποκριθεί στις απαιτήσεις των πραγματικών χρηστών του. Τέτοιες επιθέσεις στο νέο αυτό δίκτυο θα μπορούσαν να εστιάζονται πάνω στους αισθητήρες που καταγράφουν την κατάσταση του δικτύου ανά πάσα στιγμή με στόχο την εξάντληση της μπαταρίας πάνω στην οποία στηρίζουν τη λειτουργία τους. Κάτι τέτοιο αυτόματα συνεπάγεται ελλιπούς αντίληψη της κατάστασης του δικτύου με όλες τις συνέπειες που αυτό μπορεί επιφέρει.

Κάποτε κτίζαμε δίκτυα με πρώτιστο στόχο την απόδοση και τελευταίο την ασφάλεια. Σήμερα όμως οι συνθήκες είναι τέτοιες που τα πράγματα έχουν αλλάξει. Οι κίνδυνοι που ελλοχεύουν πλέον είναι πάρα πολλοί και οι συνέπειες τους δεν είναι αμελητέες. Το θέμα της ασφάλειας των Smart Grids έρχεται λοιπόν στο προσκήνιο και αποτελεί έναν από τους σημαντικότερους στόχους των σχεδιαστών του συγκεκριμένου τύπου δικτύου.

Κεφάλαιο 3

The Energy Aware Smart Home

3.1 Ένα έξυπνο σπίτι με ενεργειακή επίγνωση

Στο προηγούμενο κεφάλαιο γνωρίσαμε το όραμα για ένα έξυπνο δίκτυο ηλεκτροδότησης το οποίο ενσωματώνοντας τεχνολογίες ακριβούς μέτρησης (synchrophasors, optical sensors), δίκτυα επικοινωνίας, ανανεώσιμες πηγές ενέργειας κτλ., αναμένεται να επηρεάσει τον τρόπο με τον οποίο διαχειριζόμαστε σήμερα την ενέργεια. Παρουσιάσαμε την ιδέα ενός Advanced Metering Infrastructure (AMI) το οποίο επιτρέποντας την αμφίπλευρη επικοινωνία μεταξύ του καταναλωτή και του δικτύου παραγωγής – μεταφοράς και διανομής ενέργειας, θα εξασφαλίσει πέρα από το διαρκή έλεγχο του δικτύου, τη λειτουργία του κατά τρόπο που να ανταποκρίνεται στη ζήτηση με τη λιγότερη δυνατή επιβάρυνση για τον καταναλωτή και το περιβάλλον.

Εξασφαλίζοντας την επικοινωνία μεταξύ μετρητή και κέντρου ελέγχου του εκάστοτε οργανισμού ηλεκτροδότησης , αλλά και την επικοινωνία μεταξύ όλων των συσκευών ενός υποστατικού με το μετρητή, δίνουμε στο Smart Grid τεράστιες δυνατότητες. Μια εξ' αυτών η δυνατότητα για demand-side management η οποία θα επιτρέπει στις εταιρείες ηλεκτροδότησης παρακολουθώντας τα μοτίβα κατανάλωσης να στέλνουν μηνύματα στο AMI δίκτυο, με στόχο την πληροφόρηση του καταναλωτή/ ή ακόμα και τον απομακρυσμένο έλεγχο κάποιων συσκευών του. Την ίδια στιγμή, αυτή η επικοινωνία καθιστά δυνατή τη δυναμική χρέωση με βάση το κόστος της ενέργειας ανά πάσα στιγμή επιτρέποντας στους καταναλωτές να επιλέγουν πότε είναι πιο οικονομικά συμφέρον για τους ίδιους να θέσουν σε λειτουργία τις συσκευές τους – συμβάλλοντας έτσι και στην καλύτερη διαχείριση ενέργειας.

Για την ακρίβεια, η μείωση των ποσοστών ενέργειας που καταναλώνεται σε σπίτια και υποστατικά πρέπει να αποτελεί έναν από τους βασικότερους στόχους μας. Πρόσφατες μελέτες καταδεικνύουν ότι η ενεργειακή κατανάλωση σπιτιών και κτηρίων είναι υπεύθυνη για το 40% της συνολικής ενεργειακής κατανάλωσης στην Ευρωπαϊκή Ένωση[35], ως επίσης και για το 36% των συνολικών εκπομπών διοξειδίου του άνθρακα στην ατμόσφαιρα. Το αντίστοιχο ποσοστό ενεργειακής κατανάλωσης του τομέα αυτού στις ΗΠΑ φτάνει στο 41% [36], ενώ στην Κίνα υπολογίζεται πως ξεπερνά το 40% με τα ποσοστά διοξειδίου του άνθρακα να υπερβαίνουν το 30% και στις δύο περιπτώσεις[37].

Κι ενώ το κόστος όλης αυτής της ενέργειας το επωμίζεται ο καταναλωτής, πράγμα που μας κάνει να αναμένουμε ότι η πληροφόρηση του σχετικά με τις ώρες που η ενέργεια κοστίζει λιγότερο θα τον ευαισθητοποιήσει σημαντικά, μελέτες δείχνουν ότι τα πράγματα δεν είναι τόσο απλά. Στην πραγματικότητα όσο μικρότερη είναι η ανάγκη για ανθρώπινη επέμβαση τόσο πιο ελκυστικό γίνεται το πλάνο της δυναμικής χρέωσης για τον καταναλωτή και άρα τόσο καλύτερα αναμένουμε να γίνεται η διαχείριση ενέργειας. Αφού λοιπόν δε μπορούμε να βασιστούμε απόλυτα στον ίδιο τον καταναλωτή για να μειώσει την ενέργεια που καταναλώνει στο σπίτι του, γιατί να μη βασιστούμε στο ίδιο το σπίτι;

Η ιδέα για ένα «έξυπνο» σπίτι προέκυψε για πρώτη φορά γύρω στο 1980[38]. Από τότε μέχρι και σήμερα το «έξυπνο σπίτι» εξακολουθεί να αποτελεί αντικείμενο μελέτης πάρα πολλών μελετητών οι οποίοι μάλιστα ασχολήθηκαν μεταξύ άλλων με το πώς «έξυπνα» σπίτια μπορούν να συμβάλουν καθοριστικά στη βελτίωση της ποιότητας ζωής ασθενών ή ανθρώπων με αναπηρίες.

Τι θεωρούμε όμως «έξυπνο» σπίτι; Η αλήθεια είναι πως θα μπορούσαμε να δώσουμε μια πληθώρα ορισμών. Για την ακρίβεια μέχρι το 2002 οι Wigginton και Harris, συμπεριέλαβαν στο βιβλίο τους Intelligent Skins (ISBN:0750648473) πάνω από 30 ορισμούς για «ευφυή» κτήρια. Συνδυάζοντας ορισμένους από αυτούς αλλά και κάποιους πιο σύγχρονους[39] θα μπορούσαμε να ορίσουμε το Smart Home ως ένα έξυπνο σπίτι το οποίο ενσωματώνοντας τεχνολογίες δικτύωσης στο σχεδιασμό του θα μπορεί να εξασφαλίσει την επικοινωνία μεταξύ των συσκευών και συστημάτων του, δίνοντας στο χρήστη τη δυνατότητα απομακρυσμένου ελέγχου και χειρισμού τους. Ένα τέτοιο σπίτι, θα μπορεί να συμβάλει στην αναβάθμιση της ποιότητας ζωής των κατοίκων του εξασφαλίζοντας τους πιο ασφαλείς, άνετες και υγιεινές συνθήκες διαβίωσης, ενώ παράλληλα θα συμβάλλει στην αποδοτικότερη διαχείριση ενέργειας προστατεύοντας έτσι και το περιβάλλον!

Αναφερόμαστε λοιπόν όχι απλά σε ένα έξυπνο σπίτι αλλά σε ένα έξυπνο σπίτι με ενεργειακή επίγνωση, ένα Energy Aware Smart Home, το οποίο θα διαθέτει τον έξυπνο μετρητή του, τις έξυπνες ηλεκτρικές του συσκευές ή τις έξυπνες πρίζες του οι οποίες θα του επιτρέπουν να αναπροσαρμόζει το ενεργειακό του προφίλ με δυναμικό τρόπο με βάση τα σήματα που θα λαμβάνει από το Smart Grid.

Ένα τέτοιο σπίτι θα μπορεί για παράδειγμα λαμβάνοντας πληροφόρηση από το Smart Grid για τη χρέωση της ενέργειας ανά πάσα στιγμή να αποφασίζει μόνο του πότε είναι πιο συμφέρον να θέσει σε λειτουργία διάφορες ηλεκτρικές συσκευές. Την ίδια στιγμή, εκμεταλλευόμενο την τεχνολογία με την οποία είναι εξοπλισμένο, θα μπορεί να λαμβάνει πληροφόρηση σε σχεδόν πραγματικό χρόνο για την τοποθεσία των ενοίκων του προκειμένου να ελέγχει πιο αποδοτικά τόσο το σύστημα φωτισμού όσο και το σύστημα κλιματισμού και θέρμανσης. Έτσι τα φώτα θα μπορούν να σβήνουν όταν δεν ανιχνεύεται κίνηση στο δωμάτιο για κάποιο προκαθορισμένο χρονικό διάστημα. Ενώ η θερμοκρασία του δωματίου θα μειώνεται αυτόματα τις ώρες που ο ένοικος δε βρίσκεται στο σπίτι.

Κάτι τέτοιο ενδεχομένως να μας φαίνεται ασήμαντο εντούτοις είναι πραγματικά εντυπωσιακό το πόση ενέργεια μπορεί να εξοικονομηθεί μόνο και μόνο από την αποδοτικότερη χρήση συστημάτων κλιματισμού και θέρμανσης! Ο κλιματισμός και η θέρμανση ενός σπιτιού είναι η αιτία για το 43% της ενεργειακής κατανάλωσης σε σπίτια στις ΗΠΑ και για το 61% στον Καναδά και το Ηνωμένο Βασίλειο όπου η μέση θερμοκρασία διατηρείται σε χαμηλότερα επίπεδα ολόκληρο το χρόνο[40]. Συνεπώς, αν καταφέρουμε να πετύχουμε αισθητές μειώσεις της κατανάλωσης στον τομέα αυτό, προσφέρουμε ήδη σημαντικά στο Smart Grid.

Τα Energy Aware Smart Homes θα αποτελέσουν αναμφίβολα αναπόσπαστο κομμάτι του Smart Grid με το οποίο θα βρίσκονται σε διαρκή επικοινωνία. Από την πρώτη στιγμή λοιπόν της σχεδίασής τους αυτό είναι κάτι που πρέπει να λάβουμε σοβαρά υπόψη.

3.2 Η αρχιτεκτονική ενός Smart Home

Ένα Energy Aware Smart Home, θα βρίσκεται σε διαρκή αλληλεπίδραση με το εξωτερικό και το εσωτερικό του περιβάλλον :

- Ως **εξωτερικό περιβάλλον** ενός Smart Home, θα μπορούσαμε να περιγράψουμε τόσο το ίδιο το Smart Grid όσο και τους τρόπους διασύνδεσης Smart Home/Smart Grid οι οποίοι επιτρέπουν τη διαχείριση της ενέργειας βάσει των δυνατοτήτων του δικτύου.

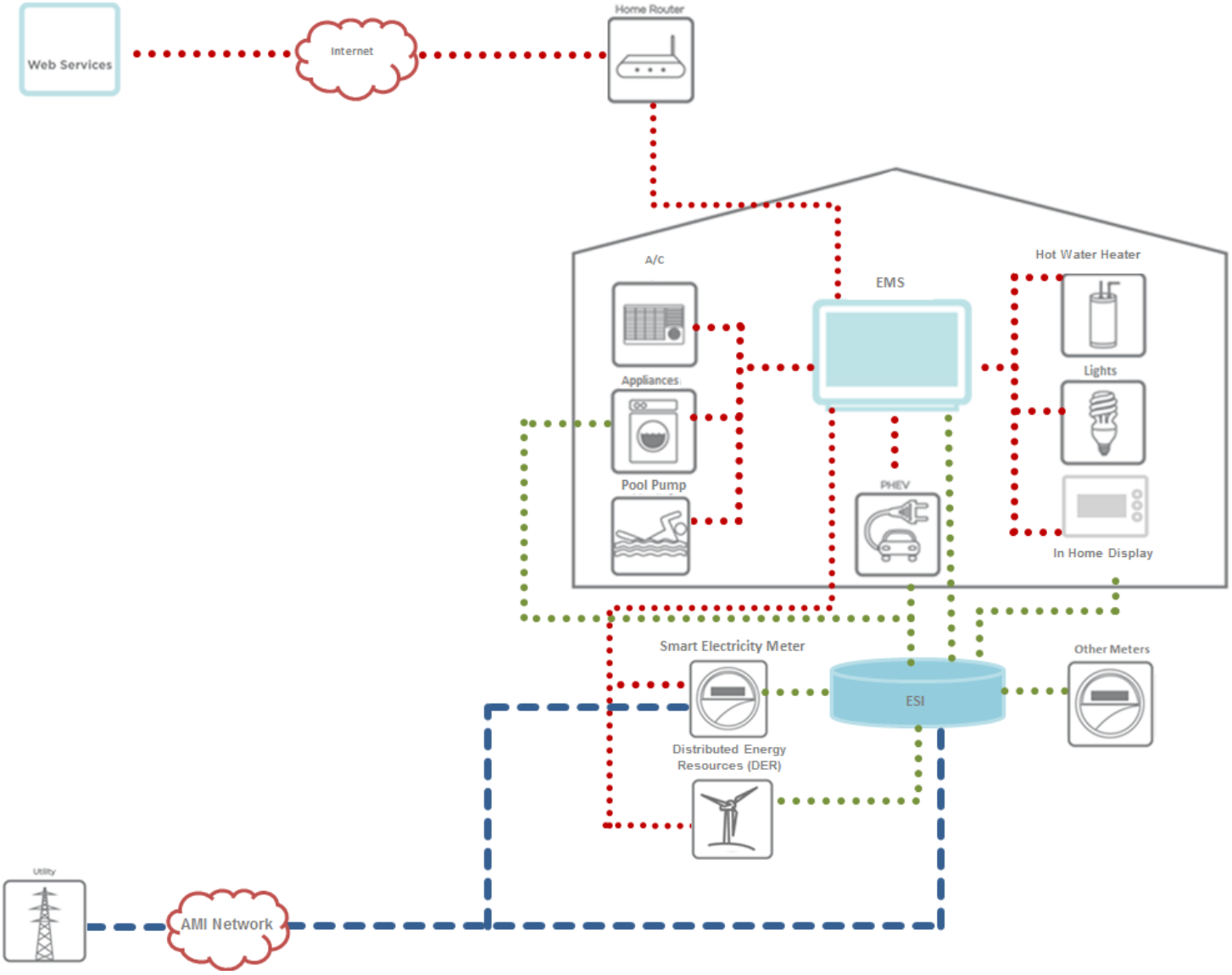
- Ενώ ως **εσωτερικό περιβάλλον** ενός Smart Home θα μπορούσαμε να χαρακτηρίσουμε το περιβάλλον εκείνο στο οποίο ο τρόπος διαχείρισης της ενέργειας καθορίζεται από τη συμπεριφορά, τις συνήθειες αλλά και την παρουσία των ενοίκων στο σπίτι.

Η ύπαρξη των δύο αυτών περιβαλλόντων μας προδιαθέτει για την ύπαρξη δύο σημαντικών οντοτήτων στο κάθε Home Area Network. Μιας οντότητας η οποία θα αναλαμβάνει τη διασύνδεση Smart Home/Smart Grid και μιας η οποία θα αφορά στη διαχείριση του εσωτερικού περιβάλλοντος. Ένα τέτοιο μοντέλο έξυπνου σπιτιού που διαθέτει τις δύο αυτές κυρίαρχες οντότητες προτάθηκε στη βιβλιογραφία από τα μέλη του UtilityAMI OpenHAN Task Force Core Development Team[41]. Το μοντέλο αυτό έρχεται να παρουσιάσει το ESI – Energy Services Interface ως την οντότητα η οποία καθιστά δυνατή την υποστήριξη αμφίδρομης επικοινωνίας μεταξύ Smart Home/ Smart Grid και το EMS – Energy Management System ως την εφαρμογή που καθιστά δυνατή τη διαχείριση του εσωτερικού περιβάλλοντος του Smart Home.

Μιλώντας για το ESI σύστημα αναφερόμαστε ουσιαστικά στη διεπαφή μεταξύ Smart Home/Smart Grid η οποία καθιστά εφικτά μεταξύ άλλων, τον απομακρυσμένο έλεγχο συσκευών, την υποστήριξη προγραμμάτων Demand Response, την παρακολούθηση των Κατανεμημένων Πηγών Ενέργειας (DER) τις οποίες ενδεχομένως διαθέτουμε σπίτι μας, την ανάγνωση και προώθηση μετρήσεων που προέρχονται από διάφορους μετρητές (όχι μόνο μετρητές ενέργειας), τη φόρτιση PEV κτλ.. Ένα Smart Home μπορεί να διαθέτει περισσότερα του ενός ESI συστήματα με το κάθε ένα να διαχειρίζεται το δικό του ανεξάρτητο δίκτυο.

Από την άλλη ως EMS σύστημα ορίζεται η εφαρμογή εκείνη που μας δίνει τη δυνατότητα ελέγχου πολλαπλών συσκευών (ιδιαίτερα αυτών που ανήκουν στην κατηγορία 3 και 4 όπως για παράδειγμα Θερμοστάτες, Διακόπτες Φωτισμού, Αντλίες Πισινών, PEV κτλ.). Η εφαρμογή αυτή μπορεί να βρίσκεται εντός οποιασδήποτε HAN συσκευής (In-Home Display, Computer κτλ.) ή να υπάρχει ως μια ξεχωριστή φυσική οντότητα.

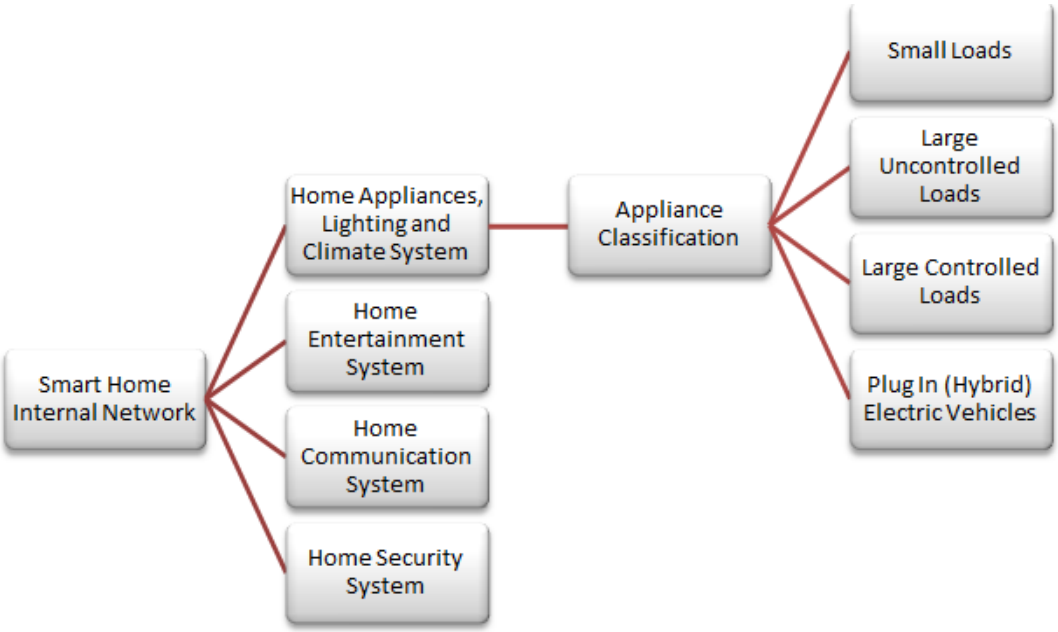
Τα EMS και ESI είναι προφανώς και μεταξύ τους συνδεδεμένα, προκειμένου να διασφαλιστεί η επικοινωνία εσωτερικού και εξωτερικού περιβάλλοντος. Μια αναπαράσταση των δύο αυτών οντοτήτων δίδεται στο Σχεδιάγραμμα 3.1.



Σχεδιάγραμμα 3.1 Τα συστήματα ESI και EMS. Το σύστημα ESI σήμερα αποτελεί συχνά μέρος του Smart Meter. Υπάρχει όμως ένας λογικός διαχωρισμός μεταξύ μετρητή και ESI παρά την ενδεχόμενη φυσική τους συνύπαρξη. Το ESI σύστημα αναλαμβάνει την επικοινωνία μεταξύ Smart Home και Υπηρεσίας Παροχής Ηλεκτρικής Ενέργειας. Ο μετρητής από την άλλη μετρά και καταγράφει την ενεργειακή μας κατανάλωση και αναλαμβάνει την επικοινωνία μεταξύ Distribution Network και Smart Home.

Στο EMS σύστημα μπορούν να συνδεθούν τα τέσσερα βασικότερα υποσυστήματα που απαρτίζουν Smart Home όπως εντοπίζονται από το [42]. Τα υποσυστήματα αυτά είναι το σύστημα ηλεκτρικών συσκευών, φωτισμού, κλιματισμού και θέρμανσης (Home Appliances/ Lighting and Climate System), το υποσύστημα ψυχαγωγίας (Home Entertainment System) το οποίο περιλαμβάνει τηλεοράσεις, ηχοσυστήματα, καλωδιακή , surround sound systems, DVD players κτλ., το υποσύστημα επικοινωνίας (Home Communication System) το οποίο

περιλαμβάνει PCs, smart phones, tablets, εκτυπωτές, VoIP τηλέφωνα, και το υποσύστημα ασφάλειας (Home Security System) το οποίο αφορά σε κλειστά κυκλώματα παρακολούθησης, αισθητήρες κίνησης/καπνού, ηλεκτρικά παράθυρα, συστήματα παρακολούθησης υγείας ασθενών κτλ..



Σχεδιάγραμμα 3.2 Τα υποσυστήματα του Smart Home και οι κατηγορίες ηλεκτρικών συσκευών

Ιδιαίτερου ενδιαφέροντος για εμάς είναι το πρώτο υποσύστημα στο οποίο μπορούμε να εντοπίσουμε μεταξύ άλλων και τις διάφορες ηλεκτρικές συσκευές ενός σπιτιού. Προφανώς εδώ χρειάζεται μια κατηγοριοποίηση των οικιακών συσκευών οι οποίες παρουσιάζουν διαφορετικές ανάγκες επικοινωνίας με το EMS. Η κατηγοριοποίηση που παρουσιάζεται στη βιβλιογραφία[43] προτείνει την ύπαρξη τεσσάρων διακριτών ομάδων συσκευών.

- Στην πρώτη κατηγορία (Small Loads) εντάσσονται οι συσκευές των οποίων η ενεργειακή κατανάλωση είναι τόσο μικρή που η προσπάθεια να τη μειώσουμε θα εισήγαγε traffic στο δίκτυο έχοντας όμως πολύ μικρό αντίκτυπο στο συνολικό ενεργειακό φορτίο του σπιτιού – καθιστώντας έτσι την επικοινωνία με αυτές πραγματικά ασύμφορη. Συσκευές που εντάσσουμε στην πρώτη κατηγορία είναι π.χ. οι λαμπτήρες φωτισμού, οι φορτιστές κινητών τηλεφώνων, οι φορητοί υπολογιστές κτλ..

- Στη δεύτερη κατηγορία (Large Uncontrolled Loads) εντάσσουμε ηλεκτρικές συσκευές οι οποίες έχουν μεγάλη ενεργειακή κατανάλωση όπως για παράδειγμα μια ηλεκτρική κουζίνα, οι οποίες όμως δε μπορούν να ανήκουν στην κατηγορία των

άμεσα ελεγχόμενων από το Smart Grid συσκευών ακριβώς λόγω του ότι ο ένοικος απαιτεί να είναι διαθέσιμες ανά πάσα στιγμή και δε μπορεί να αναβάλει την ανάγκη του για χρήση τους σε μετέπειτα στάδιο.

- Στην τρίτη κατηγορία (Large Controlled Loads), τοποθετούνται οι συσκευές μεγάλης ενεργειακής κατανάλωσης τις οποίες όμως μπορούμε να ελέγξουμε από το Smart Grid, μεταθέτοντας τη χρήση τους σε κάποια μελλοντική χρονική στιγμή. Τέτοιες συσκευές είναι για παράδειγμα τα πλυντήρια πιάτων και ρούχων, τα κλιματιστικά κτλ.. Οι συσκευές αυτής της κατηγορίας αναμένουμε να στέλνουν τις περισσότερες πληροφορίες στο EMS σε ότι αφορά στο χρόνο λειτουργίας τους, στην αναμενόμενη κατανάλωση τους κτλ.. Την ίδια στιγμή οι συσκευές αυτές αναμένουμε και να λαμβάνουν πληροφορία από το EMS ώστε να μπορούν να προγραμματίσουν πότε θα τεθούν σε λειτουργία.

- Στην τέταρτη και τελευταία κατηγορία εντάσσουμε το PEV/PHEV[44] (Plug-In Electrical Vehicle – Plug In Hybrid Electrical Vehicle) το οποίο θεωρείται μια από τις σημαντικότερες καινοτομίες που εισάγονται στο Smart Grid. Τα αυτοκίνητα αυτά, υβριδικά ή όχι (το υβριδικό plug-in διαθέτει και μπαταρίες για επαναφόρτιση και εσωτερικό κινητήρα καύσης για τις περιπτώσεις όπου η μπαταρία εξαντλείται) θεωρούνται πιο φιλικά στο περιβάλλον με χαμηλές ή καθόλου εκπομπές ρίπων. Ο ρόλος τους δε στο Smart Grid είναι ρόλος κλειδί. Αφού θα φορτίζονται δημόσια ή ιδιωτικά σε ώρες που η κατανάλωση είναι περιορισμένη σε χαμηλά επίπεδα, ενώ θα μπορούν να προσφέρουν ενέργεια πίσω στο Grid σε στιγμές που το Grid τη χρειάζεται. Τοποθετούνται σε μια κατηγορία ξεχωριστή από τις υπόλοιπες, ακριβώς διότι οι ανάγκες τους για επικοινωνία με το EMS και κατ’ επέκταση με το Smart Grid είναι ιδιαίτερα μεγάλες.

3.3 Τεχνολογίες για Αυτοματοποίηση και Επικοινωνία

Παρουσιάζοντας την αρχιτεκτονική του Smart Grid στην ενότητα 2.4 είχαμε μιλήσει για μια πληθώρα από δίκτυα ανομοιόμορφα μεταξύ τους τα οποία όμως βρίσκονται σε διαρκή επικοινωνία. Στην ενότητα αυτή παρουσιάζουμε τεχνολογίες οι οποίες θα μπορούσαν να μας επιτρέψουν να εδραιώσουμε την επικοινωνία στο εσωτερικό περιβάλλον ενός Smart Home εξασφαλίζοντας παράλληλα και την επικοινωνία του με το Smart Grid.

Στην πραγματικότητα οι τεχνολογίες που υπάρχουν σήμερα διαθέσιμες θα μπορούσαν να χωριστούν σε δύο ευρύτερες κατηγορίες. Τις ενσύρματες και τις ασύρματες τεχνολογίες. Στην κατηγορία των ενσύρματων τεχνολογιών τοποθετούμε τόσο τεχνολογίες οι οποίες θεωρούμε πως αποτελούν μέρος της συνηθισμένης καλωδίωσης ενός σπιτιού, όπως οι γραμμές ηλεκτροδότησης, οι τηλεφωνικές γραμμές, τα ομοαξονικά καλώδια καθώς και τα twisted pairs όσο και νέες ενσύρματες τεχνολογίες δικτύωσης όπως τεχνολογίες της οικογένειας Ethernet (802.11.3) πάνω από διάφορα ενσύρματα μέσα. Στις ασύρματες τεχνολογίες εντάσσουμε ουσιαστικά όλες τις τεχνολογίες δικτύωσης οι οποίες μπορούν να επικοινωνήσουν μεταξύ τους με τρόπο που δεν απαιτεί την ύπαρξη ενσύρματης υποδομής.
Προφανώς, κάθε μια από τις δύο κατηγορίες τεχνολογιών διαθέτει τα υπέρ και τα κατά της, ενώ δεν υπάρχει μια τεχνολογία κατάλληλη για να καλύψει τις απαιτήσεις ολόκληρου του Smart Grid. Η ετερογένεια των δικτύων που απαρτίζουν το Smart Grid, η οποία καθορίζει προφανώς και τις διακριτές τους ανάγκες, επιβάλλει τη χρήση διαφορετικών τεχνολογιών πολλές φορές ακόμα και στα πλαίσια του ίδιου δικτύου.

Οι ενσύρματες τεχνολογίες γνωστές από το 1900 και την εμφάνιση του τηλεφωνικού δικτύου, μας προσφέρουν την αξιόπιστη διάδοση της πληροφορίας από τον αποστολέα στον παραλήπτη και θεωρούνται πιο ασφαλείς από τις ασύρματες υπό την έννοια ότι το ασύρματο σήμα μπορεί να αλλοιωθεί, να υποκλαπεί ή να μη φτάσει ποτέ στον προορισμό. Την ίδια στιγμή, η ενσύρματη τεχνολογία έρχεται να προσφέρει συνδεσιμότητα της οποίας η εμβέλεια δεν περιορίζεται σε μερικά μόλις μέτρα όπως στα πλείστα ασύρματα δίκτυα, ενώ οι ταχύτητες διάδοσης στα ενσύρματα είναι πολύ μεγαλύτερες από ότι στα ασύρματα μέσα[42].

Από την άλλη, οι ασύρματες τεχνολογίες μας απαλλάσσουν από την ανάγκη ύπαρξης μιας υποδομής, η οποία πολλές φορές χρειάζεται προσεκτικό σχεδιασμό και εγκατάσταση από εξειδικευμένα άτομα – κάτι που προφανώς κοστίζει. Παράλληλα, η μεγάλη ευελιξία των ασύρματων τεχνολογιών, η δυνατότητα τους να υποστηρίζουν την κινητικότητα των χρηστών και η επεκτασιμότητα που τις χαρακτηρίζει τις καθιστούν ιδιαίτερα ελκυστικές.

3.3.1 Η επικοινωνία στα πλαίσια του Smart Home

Σε ένα Smart Home μπορούμε να παρατηρήσουμε στην ουσία την ύπαρξη δύο συστημάτων επικοινωνίας.

- Το σύστημα επικοινωνίας μεταξύ έξυπνων ηλεκτρικών συσκευών και κεντρικού έξυπνου μετρητή και

- Το σύστημα επικοινωνίας μεταξύ επιμέρους μετρητών (γκαζιού, νερού κτλ.) με τον κεντρικό έξυπνο μετρητή του σπιτιού μας

Πιο κάτω εντοπίζουμε μερικές από τις πιο συχνά προτεινόμενες στη βιβλιογραφία τεχνολογίες οι οποίες μας επιτρέπουν να επιτύχουμε την επικοινωνία μεταξύ των ηλεκτρικών συσκευών μας και του έξυπνου μετρητή.

3.3.1.1 Πρωτόκολλα Επικοινωνίας μεταξύ ηλεκτρικών συσκευών και έξυπνου μετρητή.

Από την κατηγορία των ενσύρματων τεχνολογιών θα σταθούμε ιδιαίτερα σε αυτές που κάνουν χρήση της ήδη υπάρχουσας υποδομής καλωδίων μεταφοράς ηλεκτρικού ρεύματος (Power Line Technologies) . Αυτό που καθιστά αυτού του είδους τεχνολογίες πιο ελκυστικές σε σχέση με άλλες ενσύρματες, είναι το γεγονός ότι μας απαλλάσσουν από την ανάγκη για εγκατάσταση νέας υποδομής, αφού μας επιτρέπουν να χρησιμοποιήσουμε τις γραμμές που υπάρχουν ήδη στο σπίτι μας για σκοπούς ηλεκτροδότησης, για να μεταφέρουμε πληροφορία.

Οι τεχνολογίες power line μπορούν να χρησιμοποιηθούν σε διάφορα υποσυστήματα ενός Smart Home. Μεταξύ αυτών το υποσύστημα ηλεκτρικών συσκευών, φωτισμού, κλιματισμού και θέρμανσης και το υποσύστημα ασφάλειας. Τα δίκτυα αυτά σχεδιάστηκαν βέβαια με στόχο τη μεταφορά ενέργειας και όχι πληροφορίας κάτι το οποίο έχει προφανώς τις συνέπειες του[45]. Η πληροφορία που μπορεί να μεταφερθεί από τα powerline δίκτυα, είναι σχετικά περιορισμένη και μεταφέρεται υπό μορφή τάσης ή φορτίου το οποίο εισάγεται στις γραμμές. Γεγονός που έχει ως αποτέλεσμα την αύξηση της πολυπλοκότητας του transceiver ο οποίος θα λαμβάνει την πληροφορία, αν θέλουμε να εξασφαλίσουμε μια όσο το δυνατό μεγαλύτερη πιθανότητα επικοινωνίας. Παράλληλα, το γεγονός ότι η ποιότητα του μεταδιδόμενου σήματος εξαρτάται από τον τύπο και τον αριθμό των ηλεκτρικών συσκευών που βρίσκονται συνδεδεμένες στο δίκτυο σε συνδυασμό με το γεγονός ότι όσο μεγαλύτερες είναι οι αποστάσεις στις οποίες αναμένουμε να διαδοθεί το σήμα τόσο μεγαλύτερη είναι η εξασθένισή του είναι ορισμένες από τις αδυναμίες των powerline τεχνολογιών.

Ορισμένες από τις πιο γνωστές τεχνολογίες για powerline επικοινωνία στα πλαίσια ενός Smart Home είναι οι HomePlug, X10, KNX και LonWorks. Πιο κάτω επιχειρούμε μια συνοπτική παρουσίασή τους.

- HomePlug

Με την πρώτη του έκδοση να κυκλοφορεί το 2001 από το HomePlug Power Line Alliance, το HomePlug[46] είναι ένα πρότυπο που επιτρέπει την επικοινωνία πάνω από γραμμές ηλεκτροδότησης . Αποτελεί μια από τις πρώτες τεχνολογίες που κατάφεραν να ξεπεράσουν φυσικούς περιορισμούς του μέσου παρέχοντας εύκολη εγκατάσταση, υψηλές ταχύτητες και αξιοπιστία και ένα από τα λίγα πρωτόκολλα που πέτυχαν την προτυποποίησή τους (IEEE P1901 – Σεμπτέμβριος 2010). Το HomePlug απαρτίζεται από διάφορες κατηγορίες προτύπων. Μια ιδιαίτερα ενδιαφέρουσα για εμάς, είναι η κατηγορία HomePlug Command & Control η οποία δημιουργήθηκε για τον έλεγχο του υποσυστήματος ηλεκτρικών συσκευών, φωτισμού, κλιματισμού και θέρμανσης αλλά και η κατηγορία HomePlug Green PHY (GP). Οι δύο αυτές κατηγορίες θα μπορούσαν κάλλιστα να εξυπηρετήσουν την ανάγκη ελέγχου των συσκευών μας στο Smart Home. Πολύ περισσότερο τώρα, που η HomePlug Alliance προχώρησε σε συνεργασία με τη ZigBee Alliance για την ανάπτυξη του ZigBee Smart Energy Profile το οποίο έχει τη δυνατότητα υποστήριξης HomePlug και 6LowPAN RF δίκτυα[47].

- X10

Αποτελεί ένα από τα παλαιότερα ανοικτά πρότυπα για αυτοματοποίηση και επικοινωνία μεταξύ συσκευών, μέσω γραμμών ηλεκτροδότησης αφού αναπτύχθηκε το 1975 από την Pico Electronics. Τα δεδομένα στο πρωτόκολλο αυτό κωδικοποιούνται σε μια συχνότητα φέροντος των 120kHz και μεταδίδονται ακολουθώντας μια προτυποποιημένη μέθοδο (IEC 61334) που χρησιμοποιείται επίσης και για μετρητές ηλεκτρισμού, νερού και από SCADA[47]. Μπορεί να υποστηρίξει data rates το πολύ 20bps, πράγμα το οποίο σημαίνει πως στην πραγματικότητα το πρωτόκολλο αυτό μπορεί να μεταφέρει μόνο μηνύματα ενεργοποίησης και απενεργοποίησης συσκευών. Στην πραγματικότητα κάθε πακέτο που μεταφέρεται μέσω X10 αποτελείται από 4bit τα οποία αντιπροσωπεύουν ένα κωδικό σπιτιού (A-P), τα οποία ακολουθούνται από 4bit που αφορούν στον κωδικό συσκευής(0-15), για να τελειώσουμε με 4bit τα οποία αντιπροσωπεύουν την εντολή. Κάθε συσκευή του συστήματος είναι ρυθμισμένη ώστε να αντιστοιχεί σε μια από τις 256 πιθανές διευθύνσεις. Γειτονικά σπίτια δε θέλουμε να έχουν τον ίδιο κωδικό σπιτιού αλλά γενικότερα οι κωδικοί επαναχρησιμοποιούνται.

- KNX

Ένα ακόμα ώριμο πρότυπο το οποίο φτιάχτηκε για σκοπούς επικοινωνίας και ελέγχου στα πλαίσια ενός αυτοματοποιημένου σπιτιού, είναι το KNX[48] από την KNX Association μέλη της οποίας είναι ορισμένοι από τους γνωστότερους κολοσσούς σήμερα (ABB, Bosch, Cisco Systems, Philips, Siemens, Fujitsu κ.α.). Αποτελεί το διάδοχο τριών ξεχωριστών προτύπων, των European Home Systems Protocol (EHS), BatiBUS και Instabus των οποίων συνδυάζει τα χαρακτηριστικά. Το πρότυπο αυτό είναι ιδιωτικό, πράγμα το οποίο συνεπάγεται την ύπαρξη κάποιου κόστους για την απόκτησή του. Έχει οριστεί όμως πάνω από διάφορα φυσικά μέσα μεταξύ των οποίων twisted pair, powerline, radio, infrared και Ethernet. Το KNX powerline λειτουργεί στις συχνότητες μεταξύ 90 και 120kHz με bit rate το οποίο φτάνει τα 1200bps. Η εγκατάστασή του είναι απλή και αυτό γιατί οποιαδήποτε συσκευή από ένα 8bit microcontroller μέχρι ένα PC μπορούν να χρησιμοποιηθούν για να το εγκαταστήσουν και να το ελέγχουν σε όλα τα επίπεδα. Για τη διαχείρηση των πόρων του KNX δικτύου χρησιμοποιείται τόσο point-to-point όσο και multicast επικοινωνία. Στην ουσία, μόλις μια συσκεύη ανακοινώσει την πρόθεσή της να στείλει κάτι στο δίκτυο, της ανατίθεται μια multicast group διεύθυνση. Όταν κάποια άλλη συσκευή εντός group λάβει την πληροφορία τότε θα μπορεί να ενημερώσει την τοπική εφαρμογή. Σαν πρότυπο το KNX έχει πάρει μια σειρά από πιστοποιήσεις μεταξύ των οποίων οι ISO/IEC 14543-3 και CENELEC EN 50090.

- LonWorks /LonTalk

Η LonWorks είναι μια πλατφόρμα δικτύωσης η οποία δημιουργήθηκε με στόχο τη διασύνδεση και τον έλεγχο συσκευών. Φτιάχτηκε από την Echelon Corporation και διατίθεται προεραιτικά ως μια ολόκληρη πλατφόρμα με hardware (Neuron chips) , firmware και tools (Neuron Ainsi C) – γεγονός που επιτρέπει την ευκολότερη εγκατάστασή του. Το πρωτόκολλο LonTalk, το οποίο δημιουργήθηκε ώστε να επιτρέπει την επικοινωνία point-to-point ανεξάρτητα από το φυσικό μέσο, είναι ένα σημαντικό κομμάτι της πλατφόρμας αυτής. Σε ότι αφορά στα επίπεδα που υλοποιεί, από το MAC Layer και πάνω, αυτά στηρίζονται στο πρότυπο ANSI-CEA-709.1 , ενώ το φυσικό μέσο μπορεί να είναι είτε twisted pair, είτε powerline είτε fibre optics είτε RF[47]. Από το 2008, οι ISO /IEC επέτρεψαν την προτυποποίηση του LonWorks (ISO/IEC 14908 -1/2/3/4), το οποίο μέχρι το

2010 κατάφερε να διεισδύσει για τα καλά στην αγορά με 90 εκατομμύρια συσκευές να διαθέτουν τεχνολογία LonWorks[49].

Η εναλλακτική λύση στις ενσύρματες τεχνολογίες, είναι οι ασύρματες τεχνολογίες. Οι οποίες μας προσφέρουν την ευελιξία που συνεπάγεται της απουσίας ενσύρματης υποδομής, την απαλλαγή από το κόστος εγκατάστασης της υποδομής αυτής , τη δυναμικότητα και επεκτασιμότητα. Οι ασύρματες τεχνολογίες αποτελούν επίσης ενδεχόμενη μέθοδο διασύνδεσης συσκευών στα πλαίσια του Smart Home.

Πιο κάτω παρουσιάζουμε ορισμένες από τις πιο γνωστές τεχνολογίες για ασύρματη επικοινωνία στα πλαίσια ενός Smart Home. Συγκεκριμένα θα μιλήσουμε για τα πρωτόκολλα ZigBee, Zwave και INSTEON.

- ZigBee

  Πρόκειται για ένα πρότυπο χαμηλής ενεργειακής κατανάλωσης για ασύρματη δικτύωση που αναπτύχθηκε από την εταιρεία ZigBee Alliance[50], για να διευκολύνει τη διαχείριση, τον έλεγχο και την επικοινωνία μεταξύ διάφορων συσκευών. Αξιοποιεί την ιδέα μιας στοίβας τεσσάρων επιπέδων η οποία περιλαμβάνει Physical Layer, MAC Layer, Network Layer και Application Layer με τα δύο χαμηλότερα επίπεδα να καθορίζονται από το πρότυπο IEEE 802.15.4 και τα δύο ψηλότερα από το ZigBee specification. Λειτουργεί στις συχνότητες των 868MHz στην Ευρώπη όπου δίνει data rate 20kbps , 915MHz στη Βόρεια Αμερική με data rate 40kbps και 2.4GHz στον υπόλοιπο κόσμο με data rate 250kbps. Για τα πρώτα δύο bands συχνοτήτων χρησιμοποιείται το BPSK ως τεχνική διαμόρφωσης ενώ για το band των 2.4GHz , χρησιμοποιείται Orthogonal – QPSK. Σε ότι αφορά στον έλεγχο πρόσβασης στο μέσο υπάρχουν δύο τρόποι να καθοριστεί. Είτε με την ύπαρξη κεντρικού συντονιστή ο οποίος θα αποστέλλει beacons στο δίκτυο (CSMA/CA with beacons) για να συντονίζει την πρόσβαση των επιμέρους κόμβων στο μέσο, ή χωρίς αυτόν, με κλασσικό CSMA/CA τρόπο, όπου οι κόμβοι ανταγωνίζονται για πρόσβαση στο μέσο. Ένα σημαντικό χαρακτηριστικό του πρωτοκόλλου αυτού έχει να κάνει με την υποστήριξη στο επίπεδο δικτύου δενδροειδών και mesh τοπολογιών. Στη mesh τοπολογία τα μονοπάτια μπορούν να δημιουργηθούν on-demand με τη χρήση του αλγορίθμου δρομολόγησης AODV ο οποίος υπαγορεύει τον τρόπο διεξαγωγής της point to point επικοινωνίας. Το γεγονός αυτό δίνει στο δίκτυό μας την ευκαιρία να λειτουργήσει αυτοάνοσα. Πέρα από όλα αυτά βέβαια, το ZigBee έρχεται να

καθορίσει και application profiles για τα ασύρματα Home Area Networks. Τα δύο γνωστότερα τέτοιου τύπου profiles είναι το ZigBee Home Automation Public Application Profile και το ZigBee Smart Energy Profile[51]. Το τελευταίο μας ενδιαφέρει ιδιαίτερα, αφού δημιουργήθηκε κατόπιν συνεργασίας της ZigBee Alliance με τη HomePlug Alliance για να περιγράψει συσκευές οι οποίες διενεργούν meter-reading, να καθορίσει τρόπους υλοποίησης Demand Response, φόρτισης PEV κτλ. [52].

- Z-wave

  Το πρωτόκολλο Z-wave[53] έχει αναπτυχθεί από την ZenSys επίσης για σκοπούς αυτοματοποίησης. Κύριος στόχος του συγκεκριμένου πρωτοκόλλου είναι η εξασφάλιση αξιόπιστης διάδοσης μηνυμάτων μεταξύ κόμβων στο δίκτυο και κεντρικού σημείου ελέγχου. Η οργάνωση του πρωτοκόλλου στηρίζεται σε μια στοίβα πέντε επιπέδων το Physical Layer, το MAC Layer, το Transfer layer, το Routing Layer και το Application Layer. Χρησιμοποιεί, όπως και το ZigBee, τις συχνότητες των 868MHz στην Ευρώπη όπου δίνει data rate 20kbps και 915MHz στις ΗΠΑ, ενώ επιτρέπει και μετάδοση στα 9.6 και 40kbps κάνοντας χρήση BFSK τεχνικής διαμόρφωσης. Πρόσφατη προσθήκη στην οικογένεια Z-Wave, το Z-Wave 400 series on a single chip υποστηρίζει και το band των 2,4GHz, εξασφαλίζοντας ρυθμούς μετάδοσης δεδομένων γύρω στα 200kbps [50]. Σε ότι αφορά στο μηχανισμό πρόσβασης στο μέσο που υλοποιεί το Z-wave, πρόκειται για έναν Collision Avoidance μηχανισμό ο οποίος επιτρέπει την αποστολή πακέτων όταν το δίκτυο είναι διαθέσιμο αξιοποιώντας έναν μηχανισμό που για σκοπούς fairness υλοποιεί ένα random backoff timer. Το πρωτόκολλο αυτό, υλοποιεί δε και μηχανισμό ο οποίος αναλαμβάνει προαιρετικά το retransmission πακέτων βάσει των ACKs που έχουμε πάρει. Η δρομολόγηση πακέτων στο Z-wave γίνεται βάση του αποστολέα, αφού πρωτού ένα πακέτο αποσταλεί στο δίκτυο ο αποστολέας καθορίζει πλήρως τη διαδρομή που αυτό θα ακολουθήσει μέχρι τον προορισμό. Οι συσκευές σε ένα τέτοιο δίκτυο επικοινωνούν μεταξύ τους χρησιμοποιώντας ενδιάμεσους κόμβους. Αυτό είναι θετικό, διότι μπορούμε να επικοινωνήσουμε σε μεγαλύτερο range, αν και η αλήθεια είναι πως όσα περισσότερα intermediate nodes προσπεράσουμε τόσο μεγαλύτερο latency θα έχουμε.

- INSTEON

  Το πρωτόκολλο INSTEON[54] δημιουργήθηκε από τα SmartLabs με στόχο, όπως και τα δύο προηγούμενα πρωτόκολλα, την αυτοματοποίηση σπιτιού. Διακριτό χαρακτηριστικό του INSTEON είναι το γεγονός ότι καθορίζει μια mesh τοπολογία που συνδυάζει RF τεχνολογίες και powerline τεχνολογίες. Σε ότι αφορά στις RF τεχνολογίες, το INSTEON αξιοποιεί FSK διαμόρφωση με τα 904MHz ως κεντρική συχνότητα, δίνοντας data rate 38.4kbps[50]. Οι συσκευές σε ένα INSTEON δίκτυο μπορούν να αποστέλλουν, να προωθούν ή να λαμβάνουν μηνύματα. Με τον όρο προώθηση, αναφερόμαστε ουσιωδώς στην έννοια της multihop επικοινωνίας η οποία, όπως υλοποιείται από το INSTEON διαφέρει από το παραδοσιακό multihop που γνωρίζουμε. Όλες οι συσκευές του δικτύου που δεν είναι ο προορισμός ενός πακέτου το κάνουν retransmit. Ένα πακέτο μπορεί να ταξιδέψει το πολύ μέχρι 4 hops. Ο τρόπος με τον οποίο επιτυγχάνεται η multihop επικοινωνία έχει να κάνει με ένα slot synchronization scheme, στο οποίο οι μεταδόσεις επιτρέπονται σε συγκεκριμένα slots με τις συσκευές που βρίσκονται εντός της ίδιας εμβέλειας να μη μπορούν να μεταδώσουν διαφορετικά μηνύματα την ίδια στιγμή. Οι RF συσκευές που δε συνδέονται στο powerline δίκτυο μπορούν να μεταδίδουν ασύγχρονα ακόμα και το ίδιο μήνυμα (simulcast) αλλά τα μηνύματα που σχετίζονται μεταξύ τους πρέπει να μεταδίδονται συγχρονισμένα από τις ραδιοσυχνότητες που συνδέονται στο powerline.

Οι τεχνολογίες και τα πρωτόκολλα που υπάρχουν για την επικοινωνία των συσκευών με τον έξυπνο μετρητή στο πλαίσιο του Smart Home είναι φυσικά πολύ περισσότερες από αυτές που έχουμε αναφέρει πιο πάνω. Εντούτοις, μια εκτενέστερη αναφορά στα πρωτόκολλα αυτά βρίσκεται έξω από τους στόχους αυτής της έρευνας και για το λόγο αυτό έχει παραληφθεί.

3.3.1.2 Πρωτόκολλα Επικοινωνίας μεταξύ μετρητών

Έχοντας ήδη μελετήσει πρωτόκολλα επικοινωνίας μεταξύ έξυπνων ηλεκτρικών συσκευών και κεντρικού έξυπνου μετρητή, σε αυτή την ενότητα θα παρουσιάσουμε πρότυπα για την εξασφάλιση της ανταλλαγής πληροφορίας μεταξύ των επιμέρους μετρητών του Smart Home με το κεντρικό smart meter. Παρουσιάζουμε πιο κάτω δύο από τα πιο γνωστά πρότυπα τα οποία μπορούν να χρησιμοποιήσουν το DLMS/COSEM ως το κοινό πρωτόκολλο επικοινωνίας για το Application Layer, τα IEC 62056-21 και EM13757.

Το πρωτόκολλο DLMS/COSEM[52] συνδυάζει το μοντέλο δεδομένων COSEM, το σύστημα κωδικών αναγνώρισης OBIS και τις υπηρεσίες ανταλλαγής μηνυμάτων και επικοινωνίας

πάνω από διάφορα μέσα, του DLMS. Το DLMS (Device Language Message Specification) είναι ένα πρωτόκολλο του επιπέδου εφαρμογών το οποίο καθορίζει γενικές έννοιες που μπορούν να χρησιμοποιηθούν για τη μοντελοποίηση διαφόρων υπηρεσιών που σχετίζονται με αντικείμενα (objects), ενώ το COSEM (Companion Specification for Energy Metering) είναι ο τρόπος ορισμού κλάσεων διεπαφής, των οποίων τα instances λέγονται COSEM-objects και περιλαμβάνουν χαρακτηριστικά και μεθόδους για να περιγράψουν τη λειτουργία διάφορων μετρητών ενέργειας. Τα αντικείμενα αυτά διαθέτουν ένα OBIS (Object Identification System) αυτοπεριγραφικό όνομα για να μπορούν να χρησιμοποιηθούν από το DLMSx που καθορίζει πώς να έχουμε πρόσβαση σε χαρακτηριστικά και μεθόδους COSEM-objects μέσω DLMS. Στην ουσία το COSEM μας παρέχει τις διεπαφές που μπορούμε να χρησιμοποιήσουμε για τη μοντελοποίηση ακόμη και πολύπλοκων μετρητών, οι οποίοι αποτελούνται από ένα σύνολο οντοτήτων τα χαρακτηριστικά των οποίων είναι προσβάσιμα μέσω DLMSx υπηρεσιών και μετατρέπονται σε byte streams όταν διαβάζονται.

Το DLMS/COSEM υποστηρίζει την ανταλλαγή δεδομένων μεταξύ μετρητών είτε σε τοπικό επίπεδο είτε μέσω αμφίδρομης επικοινωνίας σε μακρινές αποστάσεις[55] και χρησιμοποιείται από διάφορα πρότυπα που υποστηρίζουν την ανταλλαγή δεδομένων μεταξύ μετρητών όπως τα δύο που παρουσιάζουμε πιο κάτω.

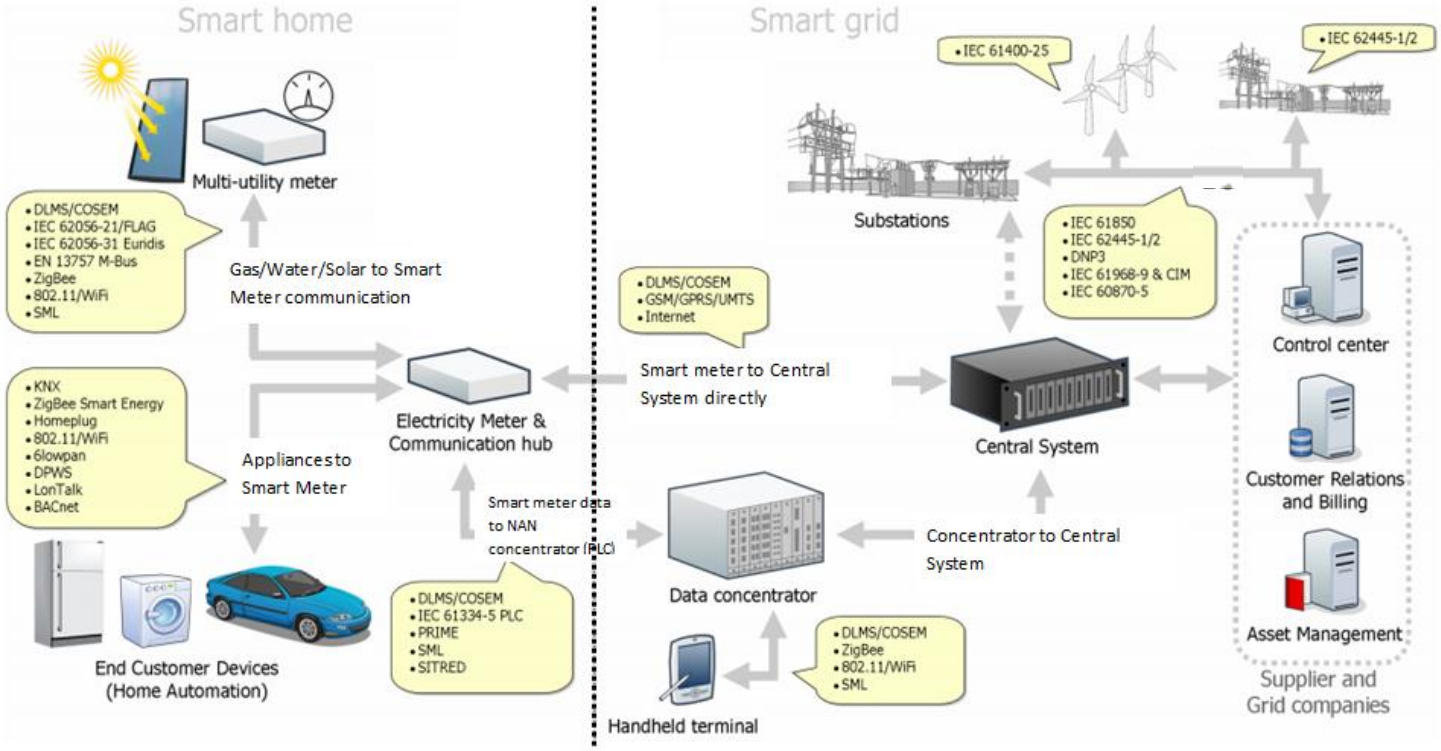
- IEC 62056-21

  Το πρότυπο IEC 62056-21[56] αλλιώς γνωστό και ως «FLAG» παρουσιάζει ομοιότητες με το Αμερικάνικο πρότυπο ANSI C12.18 ορίζοντας μια σειρά πρωτοκόλλων λογισμικού και υλικού που επιτρέπουν την ανταλλαγή δεδομένων μεταξύ μετρητών τόσο σε τοπικό όσο και μη τοπικό επίπεδο (μέσω PSTN/GSM modems). Διαθέτει πέντε ξεχωριστές ρυθμίσεις επικοινωνίας, οι οποίες διαφέρουν μεταξύ τους σε ότι αφορά ασφάλεια και κατεύθυνση επικοινωνίας, με την πέμπτη (E) να διαθέτει τη δυνατότητα υποστήριξης DLMS/COSEM. Αποτέλεσε ένα από τα πρώτα πρότυπα για ανταλλαγή πληροφορίας μεταξύ μετρητών και χρησιμοποιείται ευρέως ανά το παγκόσμιο κυρίως για σκοπούς ανταλλαγής πληροφορίας μεταξύ μετρητών σε τοπικό επίπεδο.

- M-Bus / EN13757

  Το Ευρωπαϊκό πρότυπο M-Bus[57], αλλιώς γνωστό ως EN13757 δημιουργήθηκε για να υποστηρίξει τη μονόδρομη και αμφίδρομη επικοινωνία μεταξύ μετρητών (όχι μόνο ηλεκτρικής κατανάλωσης), ενώ μπορεί να χρησιμοποιηθεί επίσης και από ποικιλία αισθητήρων και actuators. Σαν πρότυπο, ορίζει την επικοινωνία πάνω από διάφορα φυσικά μέσα (twisted pairs,radio) και πρωτόκολλα αλλά και πάνω από το μοντέλο δεδομένων COSEM. Στηρίζει τη λειτουργία του στην ιδέα μιας στοίβας τριών επιπέδων η

οποία περιλαμβάνει μόνο τα Physical Layer, MAC Layer και Application Layer. Στο επίπεδο εφαρμογών μπορεί να χρησιμοποιήσει είτε το δικό του M-Bus application layer είτε το DLMS/COSEM. Το πρωτόκολλο είναι βελτιστοποιημένο ώστε από πλευράς μετρητή να επιτρέπει απλή χαμηλού κόστους εγκατάσταση και μεγαλύτερη διάρκεια ζωής της μπαταρίας ενώ υποστηρίζει encryption με DES/AES αλλά όχι authentication.



Σχεδιάγραμμα 3.3 Πρότυπα επικοινωνίας και η τοποθέτησή τους στο Smart Grid

3.3.2 Η επικοινωνία έξω από τα πλαίσια του Smart Home

Στη προηγούμενη ενότητα παρουσιάσαμε ορισμένες από τις ήδη υπάρχουσες τεχνολογίες οι οποίες θα μπορούσαν να αξιοποιηθούν για την εξασφάλιση επικοινωνίας μεταξύ έξυπνων ηλεκτρικών συσκευών και κεντρικού έξυπνου μετρητή αλλά και μεταξύ επιμέρους μετρητών με τον κεντρικό έξυπνο μετρητή. Στην ενότητα αυτή, ξεφεύγουμε πλέον από τα θέματα επικοινωνίας στα πλαίσια του Smart Home για να επικεντρώσουμε το ενδιαφέρον μας στη διασύνδεση του με το Smart Grid. Μια διασύνδεση μέσω της οποίας εξασφαλίζεται η διαρκής αλληλεπίδραση του Smart Home τόσο με τους ενοίκους του, όσο και με το ίδιο το Smart Grid.

Όταν πια τα Smart Homes θα είναι σε θέση να ανταποκρίνονται σε μηνύματα που λαμβάνουν από το Smart Grid, δίνοντας στους ενοίκους τους το δικαίωμα της έγκυρης και έγκαιρης πληροφόρησης τότε θα βρισκόμαστε ένα βήμα πιο κοντά στην ικανοποίηση μιας

από τις σημαντικότερες ανάγκες που γέννησαν την ιδέα του Smart Grid. Της ανάγκης για αποδοτικότερη διαχείριση ενέργειας. Μέσα από την αλληλεπίδραση Smart Home - Smart Grid καθίσταται εφικτή[58] η ενημέρωση του καταναλωτή για τις τρέχουσες τιμές ηλεκτρικής ενέργειας, τον τρέχον φόρτο του δικτύου ως επίσης και τη διαθεσιμότητα ενέργειας που προέρχεται από ανανεώσιμες πηγές. Παράλληλα, χάρη στη διασύνδεση αυτή ο καταναλωτής μπορεί ανά πάσα στιγμή να γνωρίζει πόση είναι η κατανάλωσή του (και η κατανομή της ανάμεσα στις διάφορες ηλεκτρικές συσκευές που χρησιμοποιεί), να λαμβάνει πιθανόν, εξατομικευμένες συμβουλές για τη μείωσή της και γιατί όχι να τη συγκρίνει με αυτήν άλλων ανθρώπων.

Όλα τα πιο πάνω, αποτελούν αναμφίβολα, έννοιες κλειδιά για την επιτυχία του Smart Grid. Έννοιες οι οποίες συνεπάγονται πέρα από την αλληλεπίδραση και την επικοινωνία μεταξύ ηλεκτρικών συσκευών στα πλαίσια ενός Smart Home, την αλληλεπίδραση και επικοινωνία μεταξύ Smart Home και Smart Grid.

Η βαθειά ετερογένεια του Smart Grid αλλά και η φύση του η οποία προστάζει να είναι ευέλικτο και επεκτάσιμο φέρνουν στο μυαλό μας ένα δίκτυο το οποίο ήδη πληροί αυτά τα κριτήρια και το οποίο αποτελεί ίσως μια από τις καταλληλότερες τεχνολογίες για αυτή τη διασύνδεση· το Διαδίκτυο. Προσεγγίσεις οι οποίες βασίζονται στο Διαδίκτυο έρχονται να μας εγγυηθούν πως μπορούμε να γεφυρώσουμε μεταξύ τους τα τόσα διαφορετικά δίκτυα του Smart Grid, εξασφαλίζοντας τη διαλειτουργικότητα τους όχι μόνο σε τεχνικής φύσεως κομμάτια αλλά και σε συντακτικό και σημασιολογικό επίπεδο.
Η διασύνδεση μεταξύ Smart Home και Smart Grid μπορεί να γίνει μέσω διαδικτυακών υπηρεσιών (Web Services – WS)[59], [60]. Το World Wide Web Consortium (W3C) ορίζει τον όρο «διαδικτυακή υπηρεσία» ως ένα software system το οποίο έχει σχεδιαστεί με στόχο να υποστηρίξει την αλληλεπίδραση μηχανής προς μηχανή, πάνω από ένα δίκτυο[61]. Οι διαδικτυακές υπηρεσίες ανήκουν είτε στην κατηγορία των Big Web Services (WS-*, SOAP, WSDL) είτε σε αυτήν των RESTful Web Services.

Η πρώτη κατηγορία[62] υπηρεσιών αξιοποιεί το SOAP, μια XML γλώσσα η οποία καθορίζει τη σύνταξη των μηνυμάτων που ανταλλάζονται μεταξύ service consumer και service provider. Το SOAP έρχεται να ορίσει την έννοια του envelope , ενός αντικειμένου το οποίο διαθέτει header, που χρησιμοποιείται για θέματα δρομολόγησης του μηνύματος και για σκοπούς καθορισμού των παραμέτρων ποιότητας υπηρεσίας και ασφάλειας, και σώμα, στο οποίο εντοπίζουμε το μήνυμα. Σε τέτοια συστήματα αξιοποιείται συχνά και μια γλώσσα

όπως η WSDL (Web Services Description Language) η οποία είναι επίσης XML based αλλά χρησιμοποιείται για το συντακτικό καθορισμό των interfaces τα οποία καθορίζουν πώς καλούμε μια υπηρεσία, τι παραμέτρους λαμβάνει αυτή η υπηρεσία και τι αναμένουμε να επιστρέψει. Για τη WSDL μια υπηρεσία είναι μια συλλογή από ports – endpoints τα οποία διαθέτουν το δικό τους URI (Universal Resource Identifier) αν διευθυνσιοδοτούνται από το transport layer. Πολλά από τα πλεονεκτήματα της στοίβας WS-* οφείλονται στις δύο αυτές τεχνολογίες. Τέτοια πλεονεκτήματα είναι λόγου χάρη η ανεξαρτησία της από οποιοδήποτε πρωτόκολλο που της προσφέρει το SOAP, αφού μηνύματα αυτής της μορφής μπορούν να μεταφερθούν πάνω από πληθώρα πρωτοκόλλων HTTP – based ή όχι, αλλά και η αφαιρετικότητα που προσφέρει η WSDL μέσω των διεπαφών της που αποκρύπτουν συγκεκριμένες πληροφορίες υλοποίησης. Στα μειονεκτήματα αυτής της κατηγορίας υπηρεσιών, συγκαταλέγονται ο μεγάλος χρόνος απόκρισης και η ενεργειακή τους κατανάλωση.

Στη δεύτερη κατηγορία υπηρεσιών ανήκουν οι λεγόμενες RESTful υπηρεσίες. Το REST (Representational State Transfer) αποτελεί μια πιο ελαφριά αρχιτεκτονική που μπορεί να υποστηρίξει τις ανάγκες κατανεμημένων hypermedia συστημάτων μεγάλης κλίμακας όπως ο Παγκόσμιος Ιστός[59]. Σαν αρχιτεκτονική ανήκει στην κατηγορία των Resource Oriented Αρχιτεκτονικών στις οποίες τα δεδομένα του συστήματος αποτελούν τους πόρους του. Οι πόροι αυτοί, αναγνωρίζονται μοναδικά μέσω ενός URI. Το interface της REST αρχιτεκτονικής περιορίζεται στην υποστήριξη τεσσάρων βασικών λειτουργιών που έρχονται να μας θυμίσουν το HTTP πρωτόκολλο. Οι βασικές αυτές λειτουργίες είναι[63] η GET μέσω της οποίας ανακτούμε την τρέχουσα κατάσταση ενός πόρου, η PUT για τη δημιουργία νέων πόρων, η DELETE για τη διαγραφή τους και η POST για τη μεταφορά μιας νέας κατάστασης σε ένα πόρο. Οι RESTful υπηρεσίες είναι stateless ενώ διαθέτουν επίσης δυνατότητα αποσύνδεσής της πληροφορίας τους από μια συγκεκριμένη αναπαράσταση κάτι που κάνει το περιεχόμενο τους προσβάσιμο από ένα σύνολο διαφορετικών τεχνολογιών αναπαράστασης π.χ. HTTP, XML, PDF, JPEG κτλ.. Στα βασικά πλεονεκτήματα των RESTful υπηρεσιών συγκαταλέγονται η απλότητα, το ανάλαφρο interface, η ευκολία με την οποία μπορούμε να φτιάξουμε υπηρεσίες που να το αξιοποιούν και να τις δοκιμάσουμε απευθείας πάνω από οποιονδήποτε Web Browser χωρίς να χρειάζεται εξειδικευμένα προγράμματα και η επεκτασιμότητα σε ότι αφορά στον αριθμό χρηστών που μπορούν να λαμβάνουν μια υπηρεσία[62]. Σε ότι αφορά στα μειονεκτήματα τους, εντοπίζουμε μεταξύ άλλων, το γεγονός ότι σε ορισμένες περιπτώσεις proxies και firewalls στο δίκτυο δεν επιτρέπουν εντολές τύπου PUT και DELETE άρα τα POST και GET χρησιμοποιούνται

συχνότερα, με το GET να περιορίζεται σε ότι αφορά στην είσοδο που μπορεί να δεχτεί στα 4KB μόνο, με αποτέλεσμα για μεγαλύτερα requests ο server είτε να απορρίπτει το request είτε να καταρρέει! Άλλο ένα μειονέκτημα, έχει να κάνει με την έλλειψη προτύπων για την υποστήριξη ασφαλούς επικοινωνίας στα πλαίσια του REST γεγονός που αναγκάζει τους developers να ασχοληθούν με τα προβλήματα αυτά στο Transport Layer.

3.4 Δυνατότητες και Οφέλη από τη συνεργασία Smart Home/Smart Grid

Στη προηγούμενη ενότητα μιλήσαμε μεταξύ άλλων για τη διασύνδεση των Energy Aware Smart Homes με το Smart Grid καταλήγοντας στο συμπέρασμα πως μια τέτοια αλληλεπίδραση αποτελεί κλειδί για την επιτυχία του Smart Grid. Η ενότητα αυτή είναι αφιερωμένη σε εφαρμογές που αναμένουμε να στηριχθούν πάνω σε αυτή τη διασύνδεση και στα οφέλη που μπορούν να προκύψουν από αυτές.

3.4.1 Demand Response και Load Shedding

Στο δεύτερο κεφάλαιο είχαμε δει πως προκειμένου ένα δίκτυο ηλεκτροδότησης να μπορεί να ανταποκρίνεται στη ζήτηση ενέργειας, αξιοποιεί ορισμένα μοντέλα πρόβλεψης ζήτησης για να ρυθμίζει την παραγωγή. Τα μοντέλα αυτά, όπως είχαμε πει και τότε, δεν είναι πάντοτε σε θέση να μας δώσουν μια ακριβή εκτίμηση ζήτησης, κι αυτό γιατί αστάθμητοι παράγοντες μπορούν να δημιουργήσουν αλλαγές στη ζήτηση ανά πάσα στιγμή. Όταν αυτή η αλλαγή είναι μια απροσδόκητη αύξηση ζήτησης για παράδειγμα, το παραδοσιακό δίκτυο μη μπορώντας να τη διαχειριστεί άμεσα, στις πλείστες των περιπτώσεων καταρρέει. Προφανώς, κάτι τέτοιο δεν πρέπει να αποτελεί καν επιλογή για το «έξυπνο» μας δίκτυο το οποίο οφείλει να αναζητήσει άμεσα τρόπους μείωσης του φόρτου του. Δύο τέτοιοι τρόποι είναι τα προγράμματα Demand Response και η λογική του Load Shedding που παρουσιάζονται πιο κάτω.

Ως Demand Response Program θα μπορούσαμε να χαρακτηρίσουμε ουσιαστικά τη συμφωνία που διεξάγεται μεταξύ της εταιρείας παροχής ηλεκτρικής ενέργειας και του καταναλωτή, ώστε ο καταναλωτής να απολαμβάνει π.χ. μειωμένες χρεώσεις ηλεκτρικής ενέργειας ή εκπτώσεις στον τελικό λογαριασμό ηλεκτρικού ρεύματος, δεδομένου ότι συμφωνεί να συνεργάζεται οποιαδήποτε στιγμή του ζητηθεί από την εταιρεία παροχής, περιορίζοντας το φορτίο που ο ίδιος προσθέτει στο δίκτυο. Η λογική πίσω από αυτή την ιδέα είναι πως αν πολλοί καταναλωτές συμβάλουν μειώνοντας λίγο ο καθένας το φορτίο με το οποίο επιβαρύνουν το δίκτυο, τότε η ενέργεια θα είναι αρκετή για όλους[64].

Σήμερα, υπάρχει μια πληθώρα διαφορετικών προγραμμάτων Demand Response τα οποία διαφέρουν ελαφρώς το ένα από το άλλο σε ότι αφορά π.χ. στους τρόπους επιβράβευσης του καταναλωτή για τη συνεργασία, στο κατά πόσο η συνεργασία του καταναλωτή γίνεται πάνω σε υποχρεωτική ή εθελοντική βάση, στους τρόπους διαχείρισης των περιπτώσεων που ένας πελάτης που συμφώνησε συνεργασία σε υποχρεωτική βάση επιλέγει να μη συνεργαστεί όταν του ζητηθεί κτλ.[65]. Παρόλα αυτά όλα τα προγράμματα Demand Response στηρίζονται σε κάποιας μορφής προγραμματισμό ώστε να μπορεί ο καταναλωτής (αφού ενημερωθεί μέσω π.χ. e-mail, fax ή ακόμα και τηλεφωνικώς) να γνωρίζει έγκαιρα πότε χρειάζεται να συνδράμει. Ενώ επίσης όλες οι εταιρείες που υποστηρίζουν τέτοιου είδους προγράμματα διαθέτουν μεταξύ άλλων λογισμικό για σκοπούς καταγραφής της κατανάλωσης πελατών με συμβόλαιο συνεργασίας.

Το βασικότερο πλεονέκτημα που προκύπτει από την εφαρμογή Demand Response προγραμμάτων είναι ο ορθότερος ισοζυγισμός μεταξύ παραγωγής και ζήτησης. Χάρη σε αυτόν πολλά επιμέρους προβλήματα του Smart Grid μπορούν να επιλυθούν. Τέτοια προβλήματα[64] είναι για παράδειγμα :

- *Η αστάθεια που δημιουργείται στο Smart Grid όταν η παραγόμενη ενέργεια από μη-κεντρικούς σταθμούς παραγωγής ξεπεράσει συγκεκριμένα ποσοστά*, κάτι που μετά τον καλύτερο ισοζυγισμό δε θα υφίσταται επιτρέποντάς μας να αξιοποιήσουμε περισσότερο τη μη-κεντρικοποιημένη παραγωγή ενέργειας.
- *Οι περιπτώσεις όπου υπάρχουν peaks ζήτησης με αποτέλεσμα να αναγκαζόμαστε να θέσουμε σε λειτουργία πεπαλαιωμένους σταθμούς παραγωγής ενέργειας προκειμένου να ανταποκριθούμε στη ζήτηση*, κάτι που δε θα υφίσταται μετά από ορθότερο προγραμματισμό.
- *Οι απώλειες κατά τη μεταφορά ενέργεια*, κάτι που επίσης δε θα υφίσταται λόγω της μείωσης της ποσότητας ενέργειας που θα χρειάζεται μεταφορά πάνω από μεγάλες αποστάσεις αφού πλέον θα υπάρχει δυνατότητα αξιοποίησης της τοπικής παραγωγής και
- *Θέματα συμφόρησης του δικτύου*, τα οποία πλέον μέσω μηχανισμών Demand Supply θα βρίσκονται υπό έλεγχο.

Ο άλλος τρόπος μέσω του οποίου το Smart Grid αναμένεται να επιχειρήσει να περιορίσει το φόρτο του σε κάποια δεδομένη στιγμή, καλείται Load Shedding[66]. Load Shedding είναι η ορολογία που χρησιμοποιούμε για να περιγράψουμε την εσκεμμένη διακοπή παροχής ηλεκτρικής ενέργειας σε τμήματα του δικτύου ηλεκτροδότησης, στην οποία αναγκαζόμαστε

να καταφύγουμε σε περιπτώσεις όπου για οποιοδήποτε λόγο παρατηρούνται ανεπαρκή ποσοστά ενέργειας σε σχέση με αυτά που χρειάζονται για να ανταποκριθούμε στη ζήτηση. Σε τέτοιες περιπτώσεις, ρισκάρουμε την κατάρρευση ολόκληρου του δικτύου ηλεκτροδότησης εάν δεν καταφέρουμε να μειώσουμε άμεσα τη ζήτηση σε λογικά επίπεδα, κατά συνέπεια το Load Shedding είναι αναπόφευκτο.

Το Load Shedding γίνεται συνήθως με δύο τρόπους αυτόματα ή επιλεκτικά. Μιλώντας για αυτόματο Load Shedding αναφερόμαστε σε περιπτώσεις στις οποίες αυτόματα κάποια κομμάτια του δικτύου ηλεκτροδότησης απενεργοποιούνται έχοντας εντοπίσει πολλαπλές βλάβες σε σημεία του δικτύου παραγωγής και μετάδοσης του Smart Grid, οι οποίες θα μπορούσαν να προκαλέσουν cascading ή total blackouts σε ολόκληρες πόλεις. Το αυτόματο Load Shedding είναι όσο το δυνατό πιο άμεσο έχοντας σα στόχο να προλάβει τη διάδοση του προβλήματος σε ολόκληρο το δίκτυο. Το επιλεκτικό Load Shedding από την άλλη, συμβαίνει συνήθως όταν υπάρχει ένα χρονικό περιθώριο πριν την διακοπή. Συνήθως στο χρονικό αυτό περιθώριο αποφασίζουμε σε ποια περιοχή θα υπάρξει διακοπή ρεύματος λαμβάνοντας υπόψη ορισμένα κριτήρια[67] π.χ. αν η περιοχή έχει νοσοκομεία, αεροδρόμια, μέσα μαζικής μεταφοράς που στηρίζονται σε ηλεκτρικό ρεύμα, αν σε αυτήν βρίσκεται το σύστημα παροχής νερού/ το σύστημα απομάκρυνσης λυμάτων κτλ.. Τις περισσότερες φορές, περιοχές όπως τις πιο πάνω θεωρούνται υψηλής προτεραιότητας και γι' αυτό το ρεύμα σε τέτοιες περιοχές διακόπτεται σε εξαιρετικά έκτακτες περιπτώσεις (είναι οι τελευταίες περιοχές που θα χάσουν την ηλεκτροδότηση και οι πρώτες που θα τη λάβουν)

3.4.2 Feedback - Peak Shaving και «Χρηματιστήρια» Ενέργειας

Η δυνατότητα αλληλεπίδρασης με τον καταναλωτή αποτελεί ίσως ένα από τα σπουδαιότερα χαρακτηριστικά που προκύπτουν από την αλληλεπίδραση Smart Home και Smart Grid κι αυτό γιατί μέσω αυτής της αλληλεπίδρασης επιτρέπουμε στον καταναλωτή να αποκτήσει συναίσθηση του πώς η ενεργειακή του συμπεριφορά επηρεάζει τον ίδιο και το περιβάλλον του.

Το 2006, το Environmental Change Institute του πανεπιστημίου της Οξφόρδης, διεξήγαγε την έρευνα «The Effectiveness of Feedback on Energy Consumption»[68] με στόχο να μελετήσει πώς η ενημέρωση του καταναλωτή για την ενεργειακή του συμπεριφορά, μπορεί να συμβάλει στη διαδικασία μείωσης της ενεργειακής του κατανάλωσης. Μέσα από την έρευνα προκύπτει πως ένας από τους βασικότερους λόγους που ωθούν τον κόσμο σήμερα στη σπατάλη ενέργειας είναι η αδυναμία αντίληψης του πόση ενέργεια καταναλώνεται από

το κάθε τι. Φυσικά, θα μπορούσε κάποιος να εισηγηθεί πως ο λογαριασμός που λαμβάνουμε σε τακτά χρονικά διαστήματα είναι κι αυτός ένας τρόπος ενημέρωσης για την κατανάλωσή μας ο οποίος εντούτοις δε φαίνεται να μας κάνει να καταναλώνουμε λιγότερα – μήπως αυτό σημαίνει πως τελικά το feedback δεν είναι τόσο σημαντικό όσο το προβάλλουμε να είναι; Το θέμα είναι, όπως εισηγείται η μελέτη, όχι απλώς η ύπαρξη του feedback αλλά και το πόσο κατανοητό και χρήσιμο είναι αυτό τη δεδομένη στιγμή στον καταναλωτή. Ένας λογαριασμός από μόνος του δε λέει πολλά στον απλό καταναλωτή όπως παρατήρησαν οι Kempton και Layne ήδη από το 1994[69] χρησιμοποιώντας την εύστοχη αναλογία «Φανταστείτε ότι βρίσκεστε σε ένα μανάβικο όπου όλα τα φρούτα και λαχανικά δεν έχουν τιμές εσείς παίρνετε ότι θέλετε και στο τέλος του μήνα φτάνει σπίτι σας ένας λογαριασμός που γράφει μόνο το ποσό που χρωστάτε για το μήνα που πέρασε – π.χ. $527 για 2362 μονάδες φαγητού κατά το μήνα Απρίλιο. Πώς θα μπορούσατε να κάνετε οικονομία σε ένα τέτοιο κόσμο;». Αν τώρα σε συνδυασμό με το λογαριασμό μας (ο οποίος θα μπορούσε να γίνει ακόμα πιο περιεκτικός και κατανοητός), λαμβάναμε επίσης ενημέρωση για την κατανάλωσή μας ανά πάσα στιγμή, σε μια οθόνη μέσα στο σπίτι μας όχι σε κιλοβατώρες αλλά σε κάτι άμεσα κατανοητό σε όλους μας π.χ. σε euro δε θα μας βοηθούσε αυτό να αποκτήσουμε καλύτερη αντίληψη του πόση ενέργεια καταναλώνουμε; Εάν δε αυτή η ένδειξη συνοδευόταν και από κάποια εισήγηση για μείωση της ενέργειας, αυτό δε θα γινόταν ακόμα καλύτερο; Η μελέτη αυτή εισηγείται ότι ακόμα και μέσω της απευθείας πληροφόρησης μόνο, μπορούμε να μειώσουμε τα ποσοστά ενέργειας που σπαταλούνται κατά 5-15% δίνοντας μας έτσι να καταλάβουμε τη σημασία που έχει η σωστή ενημέρωση.

Η αλληλεπίδραση με τον καταναλωτή φυσικά μας αφήνει περιθώρια και για άλλου τύπου εφαρμογές όπως για παράδειγμα την υποστήριξη προγραμμάτων δυναμικής χρέωσης[66] τα οποία θα ανακοινώνονται στους καταναλωτές κάθε μέρα για την επόμενη, περιλαμβάνοντας χρεώσεις που αντανακλούν την κατάσταση της αγοράς ενέργειας[70] (με φθηνότερη ενέργεια σε ώρες μειωμένης ζήτησης και ακριβότερη ενέργεια σε ώρες αιχμής). Κάτι τέτοιο θα μπορούσε να αποτελέσει έναυσμα για την υποστήριξη διαδικασιών Peak Shaving εντός του Grid. Μιλώντας για Peak Shaving, αναφερόμαστε στη διαδικασία που εφαρμόζεται προκειμένου να εξομαλυνθούν οι απότομες αιχμές στη ζήτηση, μέσω καλύτερης κατανομής της ζήτησης σε όλες τις ώρες της ημέρας[71]. Το Peak Shaving επιτυγχάνεται συνήθως απενεργοποιώντας συσκευές κατηγορίας 3 σε ώρες αιχμής και επαναπρογραμματίζοντας τη λειτουργία τους για αργότερα.

Τέλος, σενάρια στα οποία ο καταναλωτής συμμετέχει στο δίκτυο και ως παραγωγός ενέργειας γίνονται επίσης εφικτά μέσω αυτής της αλληλεπίδρασης δικτύου-καταναλωτή. Αφού ο καταναλωτής θα μπορεί πλέον να πουλά ενέργεια (από τα φωτοβολταϊκά του, ή τις ανεμογεννήτριες του) τη στιγμή που το Grid τη χρειάζεται[59]. Δε θα ήταν παράξενο δε, να μιλάμε στο μέλλον για ένα «χρηματιστήριο» ενέργειας μεταξύ Smart Homes και Smart Grid, όπου η ενέργεια θα πωλείται και θα αγοράζεται σε ανταγωνιστικές τιμές που καθορίζονται από τη ζήτηση.

3.4.3 Αξιοπιστία και Ανοχή Σφαλμάτων

Ένα ακόμα σημαντικό χαρακτηριστικό το οποίο προκύπτει απ' την επικοινωνία μεταξύ Smart Home και Smart Grid έχει να κάνει με τη γρηγορότερη ανίχνευση προβληματικών καταστάσεων ή παράξενων μοτίβων κατανάλωσης ενέργειας χρηστών τα οποία θα μπορούσαν να χρησιμοποιηθούν ώστε το σύστημα να αποκτά εγκαίρως μια όσο το δυνατό ακριβέστερη εικόνα της κατάστασης του σε διάφορα σημεία. Ακόμα και η αδυναμία του Smart Home να ανταποκριθεί σε εντολές που του αποστέλλονται μπορούν να μας αποκαλύψει πληροφορίες όπως για παράδειγμα ενδεχόμενη βλάβη στο δίκτυο του πελάτη, με αποτέλεσμα η εταιρεία ηλεκτροδότησης πλέον, να είναι σε θέση να ανταποκριθεί άμεσα με αποκατάσταση της βλάβης. Η όλη διαδικασία εξυπηρετεί βέβαια, πέρα από τον καταναλωτή και τις ίδιες τις εταιρείες ηλεκτροδότησης[59], αφού ο δείκτης αξιοπιστίας και ποιότητας υπηρεσίας τους ανεβαίνει απ' τη στιγμή που η οποιαδήποτε βλάβη στο δίκτυο εντοπίζεται και αποκαθίσταται άμεσα ενώ παράλληλα συμβάλλει στη διατήρηση της γενικότερης ευρωστίας του δικτύου.

Κεφάλαιο 4

Smart Home and Smart Grid Security Issues

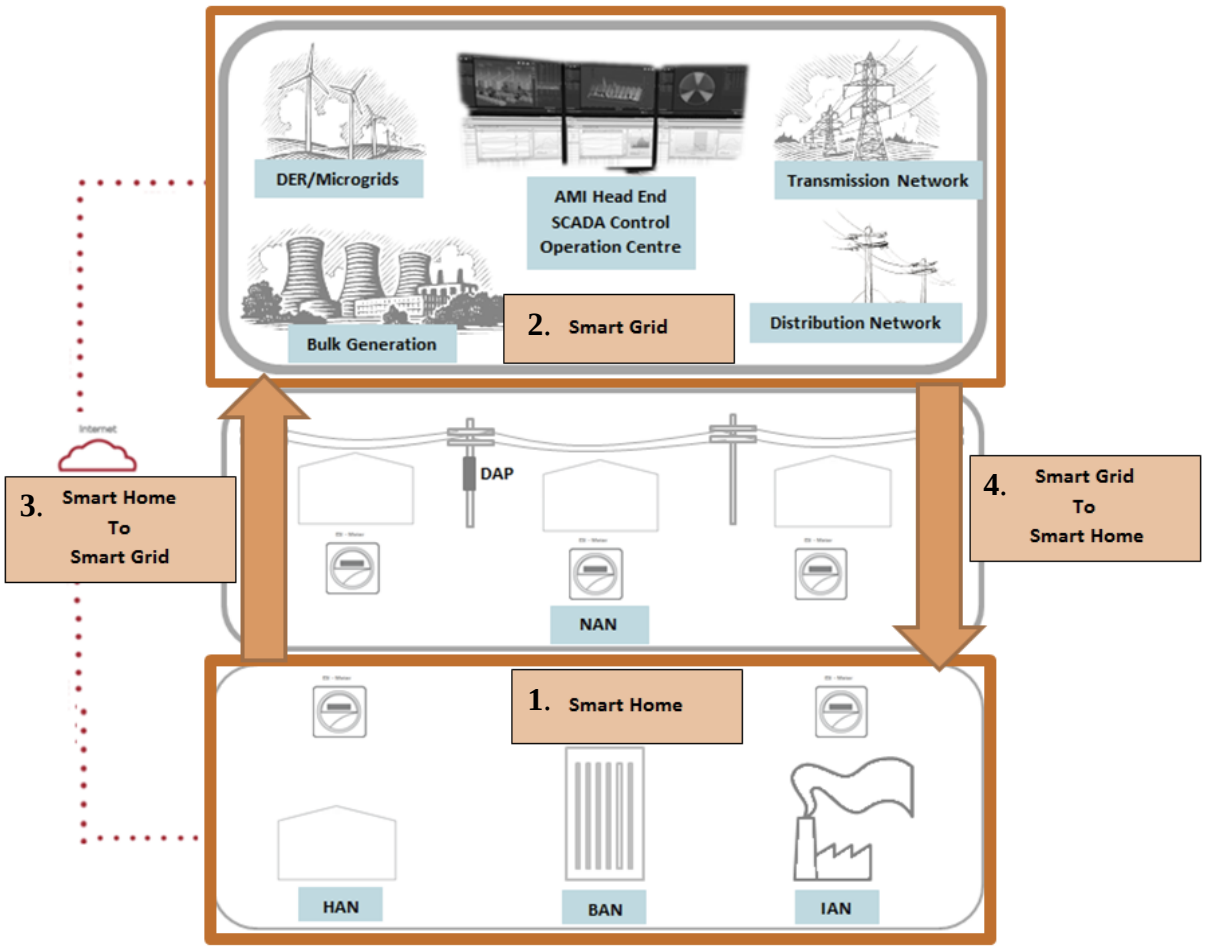
Με τα προηγούμενα δύο κεφάλαια κλείνουμε ουσιαστικά μια μεγάλη νοηματική ενότητα. Μια ενότητα η οποία μας βοήθησε να γνωρίσουμε τα Smart Grids ως τη μετεξέλιξη του τρέχοντος δικτύου ηλεκτροδότησης και τα Energy Aware Smart Homes ως τη μετεξέλιξη της ιδέας του Smart Home σε ένα ενεργειακά αποδοτικότερο περιβάλλον. Μέσα από τα κεφάλαια αυτά, μας δόθηκε η ευκαιρία να εντοπίσουμε ορισμένα από τα σπουδαιότερα πλεονεκτήματα που προκύπτουν τόσο μέσα από τη μετάβαση από το τρέχον δίκτυο ηλεκτροδότησης στα Smart Grids, όσο και μέσα από την αμφίδρομη επικοινωνία μεταξύ Smart Grid και Energy Aware Smart Homes.

Με το κεφάλαιο αυτό, εγκαινιάζουμε τη δεύτερη και πιο μεγάλη νοηματική ενότητα της μελέτης αυτής. Στην ενότητα αυτή θα εντοπίσουμε πολλά από τα θέματα ασφάλειας που καλείται να αντιμετωπίσει το Smart Grid, και τρόπους με τους οποίους τα θέματα αυτά θα μπορούσαν να αντιμετωπιστούν για να αποφύγουμε κινδύνους που θα μπορούσαν να έχουν καταστροφικές συνέπειες για το δίκτυο μας.

Το κεφάλαιο αυτό, επικεντρώνεται σε θέματα ασφάλειας σε Smart Homes και Smart Grids. Στόχος του είναι, μέσα από τη μελέτη ορισμένων από τα βασικότερα σενάρια κάτω από τα οποία αλληλεπιδρούν μεταξύ τους οι σπουδαιότερες οντότητες σε Smart Home και Smart Grids, να εντοπίσει ορισμένους από τους αντιπροσωπευτικότερους κινδύνους που απειλούν τόσο τις οντότητες αυτές, όσο και τη μεταξύ τους επικοινωνία. Στο δεύτερο κεφάλαιο είχαμε εισάγει με μια multi-layered προσέγγιση για τη περιγραφή της αρχιτεκτονικής ενός Smart Grid. Στο κεφάλαιο αυτό, αξιοποιώντας αυτή ακριβώς την προσέγγιση προσπαθούμε να

εντοπίσουμε τους κινδύνους που απειλούν τα Smart Grids. Έτσι σε πρώτη φάση μας απασχολούν οι κίνδυνοι που προκύπτουν από την αλληλεπίδραση οντοτήτων αποκλειστικά στα πλαίσια του Smart Home. Σε επόμενη φάση εντοπίζουμε τους κινδύνους που αφορούν στην επικοινωνία μεταξύ οντοτήτων του Smart Grid, ενώ τελειώνοντας μελετάμε κινδύνους που προκαλούνται από επιθέσεις σε οντότητες των Smart Homes με αντίκτυπο στο Smart Grid, και κινδύνους που προκαλούνται από επιθέσεις σε οντότητες του Smart Grid με αντίκτυπο στο Smart Home.

Σχηματικά η πιο πάνω προσέγγιση παρουσιάζεται στο Σχεδιάγραμμα 4.1.



Σχεδιάγραμμα 4.1 Τα τέσσερα βασικά περιβάλλοντα στα οποία θα μελετήσουμε σενάρια αλληλεπίδρασης οντοτήτων για καθορισμό των κινδύνων ασφαλείας στα Smart Grids.

Τονίζουμε ότι παρόλο που τα HAN/BAN/IAN θεωρούνται και αυτά οντότητες του Smart Grid δικτύου, εντούτοις για σκοπούς ορθότερης ανάλυσης των κινδύνων, μελετάμε τα περιβάλλοντα αυτά ως ξεχωριστές οντότητες πριν κάνουμε λόγο για την επικοινωνία τους με το Smart Grid. Άρα η έννοια του Smart Grid σε αυτό το κεφάλαιο αφορά στην ουσία το δίκτυο διανομής και μεταφοράς ενέργειας, τους παροχείς υπηρεσιών, τον τομέα λειτουργιών στο AMI Head End και τις αγορές ενέργειας.

Σε κάθε ένα από τα σενάρια που θα παρουσιαστούν στις ενότητες που ακολουθούν, εντοπίζουμε ορισμένους από τους κινδύνους που θα μπορούσαν να προκύψουν κάνοντας λόγο και για τις ενδεχόμενες συνέπειες τους. Ακολούθως, εντοπίζουμε ποιοι από τους στόχους ασφάλειας παραβιάζονται μέσω αυτών των κινδύνων και αξιολογούμε το βαθμό στον οποίο αυτή η παραβίαση θα μπορούσε να επηρεάσει την ομαλή και εύρυθμη λειτουργία τόσο του Smart Grid όσο και του Smart Home, με ό,τι αυτό συνεπάγεται.

Η αξιολόγηση των κινδύνων στηρίζεται στο μοντέλο αξιολόγησης επιπτώσεων που προκύπτουν από την παραβίαση της ασφάλειας πληροφορικών συστημάτων όπως παρουσιάζεται στο Federal Information Processing Standard [72] του NIST. Οι επιπτώσεις αυτές όπως προκύπτουν από την παραβίαση των στόχων ασφαλείας του θα μπορούσαν να αξιολογηθούν ως :

Low:

- Στην περίπτωση εκείνη που περιορίζουν τη δυνατότητα ενός συστήματος να επιτελέσει ορισμένες από τις λειτουργίες του για τέτοιο χρονικό διάστημα και σε τέτοιο βαθμό που ενώ ακόμα μπορεί να επιτελεί τις βασικές του λειτουργίες, εντούτοις είναι αισθητή η μείωση της αποδοτικότητας του.
- Στην περίπτωση που μπορούν να προκαλέσουν περιορισμένη ζημιά σε μέρη του συστήματος.
- Στην περίπτωση που μπορούν να προκαλέσουν περιορισμένη οικονομική επιβάρυνση/ζημιά.
- Στην περίπτωση που μπορούν να έχουν περιορισμένες συνέπειες στα άτομα με τα οποία αλληλεπιδρούν.

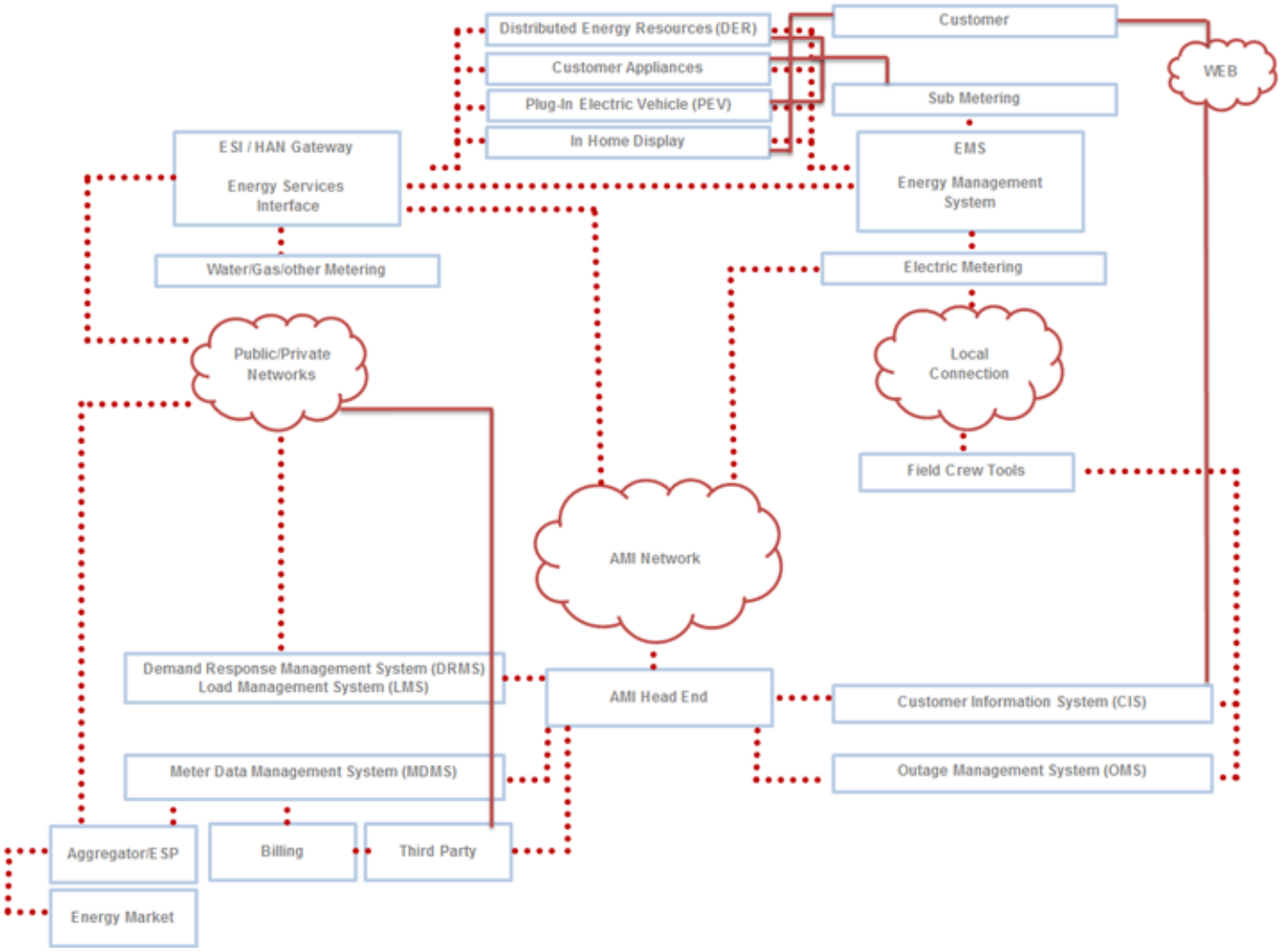
Moderate:

- Στην περίπτωση εκείνη που περιορίζουν τη δυνατότητα ενός συστήματος να επιτελέσει ορισμένες από τις λειτουργίες του για τέτοιο χρονικό διάστημα και σε τέτοιο βαθμό που ενώ ακόμα μπορεί να επιτελεί τις βασικές του λειτουργίες, εντούτοις είναι αισθητή η σημαντική μείωση της αποδοτικότητας του.
- Στην περίπτωση που μπορούν να προκαλέσουν σημαντική ζημιά σε μέρη του συστήματος.
- Στην περίπτωση που μπορούν να προκαλέσουν σημαντική οικονομική επιβάρυνση/ζημιά.
- Στην περίπτωση που μπορούν να έχουν σημαντικές συνέπειες στα άτομα με τα οποία αλληλεπιδρούν (μη συμπεριλαμβανομένου του θανάτου των ατόμων)

High:

- Στην περίπτωση εκείνη που περιορίζουν τη δυνατότητα ενός συστήματος να επιτελέσει ακόμα και βασικές λειτουργίες του.
- Στην περίπτωση που μπορούν να προκαλέσουν εκτεταμένη ζημιά σε μέρη του συστήματος.
- Στην περίπτωση που μπορούν να προκαλέσουν εκτεταμένη οικονομική επιβάρυνση/ζημιά.
- Στην περίπτωση που μπορούν να έχουν καταστροφικές συνέπειες στα άτομα με τα οποία αλληλεπιδρούν κοστίζοντας ακόμα και τη ζωή τους.

Πριν προχωρήσουμε όμως στον ορισμό των στόχων ασφάλειας για τα Smart Grids, παρουσιάζουμε ένα τελευταίο αλλά πολύ χρήσιμο διάγραμμα (Σχεδιάγραμμα 4.2). Στο διάγραμμα αυτό διαφαίνονται οι βασικότερες οντότητες στα Smart Home και Smart Grid περιβάλλοντα και τα μονοπάτια αλληλεπίδρασης και επικοινωνίας μεταξύ τους. Το διάγραμμα αυτό, αποτελεί και το βασικότερο διάγραμμα πάνω στο οποίο θα στηριχθούμε για την παρουσίαση των θεμάτων ασφάλειας στα Smart Home/Smart Grid περιβάλλοντα.



Σχεδιάγραμμα 4.2
Οι βασικότερες οντότητες σε Smart Homes (πάνω) και σε Smart Grid (κάτω), τα δίκτυα και τα μονοπάτια αλληλεπίδρασης μεταξύ τους. Το διάγραμμα αυτό προέκυψε συνδυάζοντας πληροφορίες για τα 22 communicating interfaces του Smart Grid, όπως εντοπίστηκαν από το NIST [73].

4.1 Στόχοι Ασφάλειας σε Smart Homes/Smart Grids

Οι στόχοι ασφάλειας που ένα Smart Home/Smart Grid περιβάλλον καλείται να πληροί, προκειμένου να θεωρούμε ότι εξασφαλίζεται η εύρυθμη λειτουργία του, παρουσιάζονται σε μια πληθώρα μελετών της σύγχρονης βιβλιογραφίας[42], [43], [74] με ελαφρές διαφοροποιήσεις ως προς τον ορισμό, γεγονός που σε κάποιες περιπτώσεις αφήνει περιθώρια για την παρουσίαση επιπρόσθετων στόχων ασφάλειας. Για τους σκοπούς της δικής μας μελέτης επιλέξαμε αυτούς που θεωρούμε αντιπροσωπευτικότερους για Smart Home/Smart Grid περιβάλλοντα. Οι στόχοι αυτοί δεν είναι άλλοι από την εξασφάλιση:

- **Εμπιστευτικότητας (Confidentiality):** Όπου ως εμπιστευτικότητα ορίζουμε την διαβεβαίωση πως μόνο εξουσιοδοτημένες οντότητες μπορούν να ανταλλάζουν και να έχουν πρόσβαση σε συγκεκριμένα δεδομένα.
- **Ακεραιότητας (Integrity):** Όπου ως ακεραιότητα ορίζουμε τη διαβεβαίωση πως τα δεδομένα που ανταλλάζονται μεταξύ εξουσιοδοτημένων οντοτήτων είναι ορθά, συνεπή και χρονικά έγκυρα. Δηλαδή, δεν έχουν επιδεχθεί οποιαδήποτε αλλοίωση (προσθήκες/διαγραφές περιεχομένου) και δεν έχουν υποστεί καταστροφή ή απώλεια κατά τη διάδοση τους, την αποθήκευσή τους ή την ανάκτησή τους.
- **Διαθεσιμότητας (Availability):** Όπου ως διαθεσιμότητα ορίζουμε τη διαβεβαίωση ότι οι οποιοιδήποτε πόροι του δικτύου (δεδομένα / bandwidth / συστήματα συνδεμένα με αυτό), είναι πάντοτε διαθέσιμοι για κάθε εξουσιοδοτημένη οντότητα, όποτε η οντότητα αυτή τους χρειαστεί, και προστατευμένοι έναντι οποιουδήποτε περιστατικού μπορεί να επηρεάσει την άμεση διαθεσιμότητα τους.
- **Αυθεντικότητας (Authenticity):** Όπου ως αυθεντικότητα ορίζουμε την πιστοποίηση ότι μια οντότητα είναι πράγματι αυτή που ισχυρίζεται πως είναι και πως ένα μήνυμα το οποίο αποστέλλεται από αυτήν πράγματι έχει αποσταλεί από αυτήν.
- **Εξουσιοδότησης (Authorization) :** Όπου ως εξουσιοδότηση ορίζουμε τη διαβεβαίωση ότι τα δικαιώματα της κάθε οντότητας στο Smart Home/Smart Grid περιβάλλον είναι σαφέστατα καθορισμένα και πως καμία οντότητα δε θα καταφέρει να έχει πρόσβαση σε επίπεδα που βρίσκονται πέραν τον δικών της δικαιωμάτων.
- **Μη αποποίησης ευθύνης (Non repudiation) :** Όπου ως μη αποποίηση ευθύνης ορίζεται η διαβεβαίωση της προστασίας έναντι της οποιαδήποτε προσπάθειας άρνησης της αποστολής ή της παραλαβής ενός μηνύματος ή της πρόσβασης ή μη σε μια συγκεκριμένη υπηρεσία από μια οποιαδήποτε οντότητα συμμετέχει στην επικοινωνία. (Στο σημείο αυτό είναι σημαντικό να επισημάνουμε πως η αρχή αυτή δε μας εγγυάται τη μη αποποίηση (ότι κανείς δε θα αρνηθεί κάτι που συνέβη ή να

ισχυριστεί ότι κάτι συνέβη ενώ αυτό δεν συνέβηκε ποτέ). Αυτό που μας εγγυάται είναι ότι για οποιοδήποτε ισχυρισμό μιας οντότητας, θα μπορούμε να αποδείξουμε κατά πόσο ο ισχυρισμός αυτός ευσταθεί ή όχι).

Έχοντας πλέον καθορίσει με σαφήνεια τους στόχους ασφάλειας που αναμένουμε να πληρούνται από το Smart Home/Smart Grid περιβάλλον είμαστε πια έτοιμοι να εντοπίσουμε μερικούς από τους κινδύνους που θα μπορούσαν να προκύψουν σε ορισμένα από τα πιο αντιπροσωπευτικά σενάρια αλληλεπίδρασης μεταξύ οντοτήτων του Smart Home/Smart Grid περιβάλλοντος. Οι επόμενες ενότητες αφιερώνονται ακριβώς σε αυτό.

4.2 Θέματα Ασφάλειας στα Smart Homes

Περιγράφοντας την αρχιτεκτονική ενός Energy Aware Smart Home στο κεφάλαιο 3 προχωρήσαμε σε ένα διαχωρισμό μεταξύ εξωτερικού και εσωτερικού περιβάλλοντος. Ως εσωτερικό περιβάλλον είχαμε ορίσει το περιβάλλον εκείνο στο οποίο ο ίδιος ο πελάτης καθορίζει μέσω των συνηθειών του και των απαιτήσεών του, τον τρόπο με τον οποίο το σπίτι του θα διαχειρίζεται την ενέργεια. Το περιβάλλον, στο οποίο αντιπροσωπευτικότερη οντότητα είναι το σύστημα διαχείρισης ενέργειας EMS. Στο σύστημα αυτό, όπως είχαμε πει και τότε συνδέονται τα τέσσερα βασικότερα υποσυστήματα κάθε Energy Aware Smart Home, ενώ το ίδιο είναι ταυτόχρονα συνδεδεμένο με το ESI/HAN Gateway, τη διεπαφή ενός Smart Home προς το εξωτερικό περιβάλλον. Η ενότητα αυτή ως στόχο της έχει, μέσα από διάφορα σενάρια στα οποία οι οντότητες του εσωτερικού περιβάλλοντος αλληλεπιδρούν μεταξύ τους, να εντοπίσει ενδεχόμενες απειλές προς τους στόχους ασφάλειας που παρουσιάσαμε προηγουμένως.

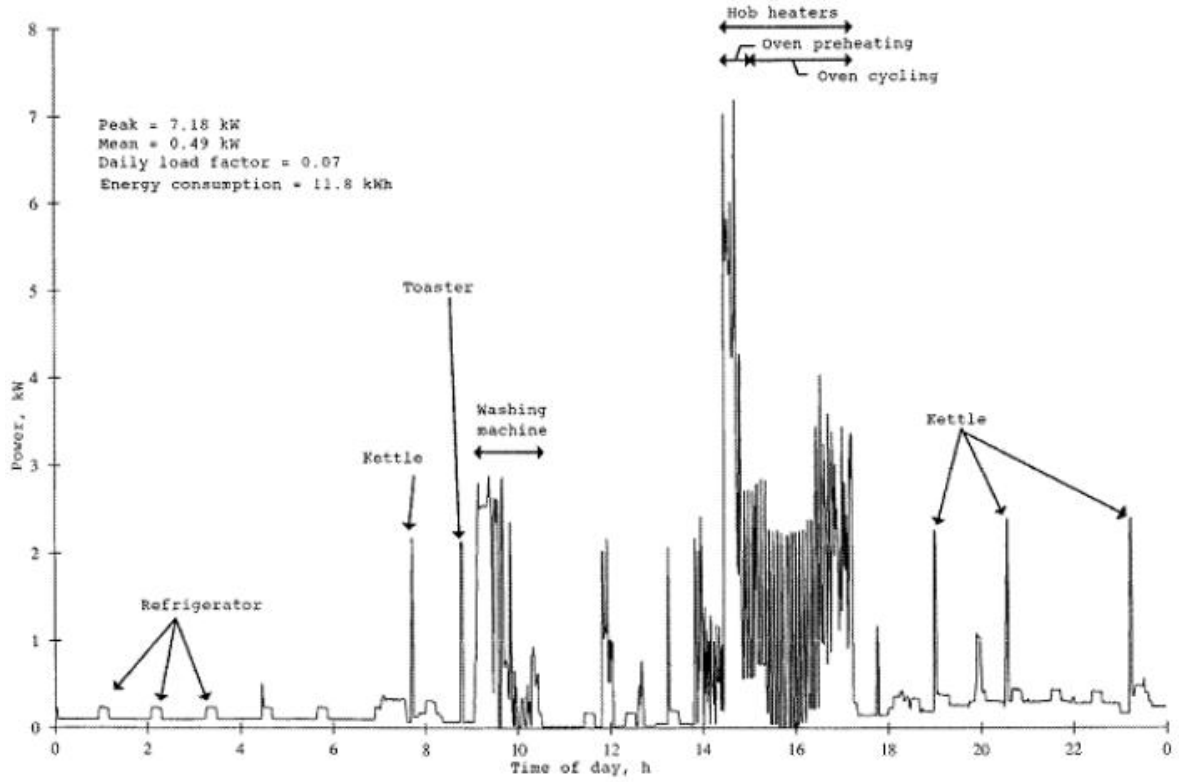
4.2.1 Μεταφορά στοιχείων ενεργειακής κατανάλωσης από μια συσκευή στο EMS.

Σενάριο

Οι συσκευές που βρίσκονται μέσα στα πλαίσια του Smart Home διαθέτουν τη δυνατότητα καταμέτρησης της δικής τους ενεργειακής κατανάλωσης (μέσω sub metering συσκευών) και αποστολής των στοιχείων που αφορούν σε αυτήν στο EMS σύστημα με το οποίο συνδέονται ώστε αυτό να αναλάβει την προώθηση της κατάλληλης πληροφορίας στο Smart Meter.

Οι κίνδυνοι που θα μπορούσαν να προκύψουν κάτω από ένα τέτοιο σενάριο αφορούν περισσότερο σε θέματα παραβίασης της ιδιωτικότητας των καταναλωτών. Δεδομένα τα οποία εμείς θεωρούμε «ανώνυμα», πολλές φορές μπορούν να αποκαλύψουν πολλά

περισσότερα για εμάς από όσα οι ίδιοι πιστεύουμε. Αρκεί μόνο να σκεφτούμε πως τα Smart Meters θα συλλέγουν επαρκείς πληροφορίες από τις συσκευές ώστε να είναι σε θέση να ενημερώνουν το Smart Grid ανά διαστήματα των 15 λεπτών[73] (και όχι του ενός μηνός όπως ήταν μέχρι τώρα). Κάτι τέτοιο προφανώς συνεπάγεται τη συλλογή πολύ περισσότερης πληροφορίας. Πληροφορίας, η οποία μέσα από την κατάλληλη επεξεργασία από αλγόριθμους Load Signature μπορεί να μας φανερώσει ακόμα και ποια συσκευή χρησιμοποιείται ανά πάσα στιγμή[75]. Τέτοιοι αλγόριθμοι οι οποίοι λειτουργούν αναγνωρίζοντας μεταξύ άλλων και διαφορετικούς τύπους φορτίου (μη γραμμικοί αντιστάτες για θερμάστρες/λαμπτήρες, επαγωγικοί αντιστάτες για ηλεκτρικούς κινητήρες, άεργοι αντιστάτες για φούρνους μικροκυμάτων και αντιστάτες υπό μορφή διόδων για led φωτισμό), μπορούν να μας βοηθήσουν να κατασκευάσουμε ενεργειακά προφίλ κατανάλωσης για τις διάφορες συσκευές όπως αυτά που παρουσιάζονται πιο κάτω.



Σχεδιάγραμμα 4.3 Εντοπισμός συσκευών που τίθενται σε λειτουργία ανά πάσα στιγμή μέσω του ενεργειακού τους προφίλ.

Με τη συλλογή τέτοιων ενεργειακών προφίλ για μικρά χρονικά διαστήματα, ένας επιτιθέμενος θα μπορούσε να αποκτήσει πληθώρα γνώσεων σε ότι αφορά τις συνήθειες, τη ρουτίνα και τις συμπεριφορές των ενοίκων ενός υποστατικού[73]. Να καθορίσει 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.. Τέτοια πληροφορία

θα μπορούσε κάλλιστα να αξιοποιηθεί για την οργάνωση σοβαρότερων επιθέσεων με στόχο τους ίδιους τους καταναλωτές ή την περιουσία τους.

Ενδεχόμενες επιθέσεις οι οποίες θα μπορούσαν να επιτρέψουν σε έναν κακόβουλο χρήστη να αποκτήσει αυτή την πληροφορία θα μπορούσαν να έχουν να κάνουν με [28]Eavesdropping, υποκλοπή δηλαδή της πληροφορίας κατανάλωσης που αποστέλλει η συσκευή προς το Smart Meter. Ή με Traffic Analysis[42] όταν το Eavesdropping δεν είναι εφικτό. Επιθέσεις τύπου Traffic Analysis αναλύουν όχι τα μηνύματα που αποστέλλονται αυτά καθαυτά αλλά τα μοτίβα αποστολής μηνυμάτων προς τους μετρητές. Ακόμα και χωρίς πρόσβαση στο περιεχόμενο των μηνυμάτων ένα Traffic Analysis attack αρκεί για να καθορίσει εάν οι ένοικοι βρίσκονται εκτός του σπιτιού ή όχι αφού δεν αναμένουμε όλες οι συσκευές να αποστέλλουν ενημερώσεις σε τόσο τακτά διαστήματα όταν δε θα χρησιμοποιούνται.

Πέραν αυτού βέβαια, εξίσου πιθανός είναι και ο κίνδυνος ενός Man-In-The-Middle Attack[28] σε τέτοιες περιπτώσεις. Σε ένα τέτοιο είδος επίθεσης ο επιτιθέμενος μιμείται τη συσκευή και εισάγει δικά του μηνύματα κατανάλωσης/ επαναλαμβάνει παλαιότερα ή κάνει drop τα νέα, ενώ παράλληλα προσωποποιεί και το μετρητή στη συσκευή, ώστε αυτή να θεωρεί ότι η ενημέρωση που έστειλε παραλήφθηκε επιτυχώς από αυτόν (δε χρειάζεται retransmission). Με τον τρόπο αυτό, η συσκευή λανθασμένα θεωρεί ότι έχει ενημερώσει το μετρητή και ο μετρητής λανθασμένα θεωρεί ότι έχει λάβει τη σωστή πληροφόρηση από τη συσκευή. Κάτι τέτοιο έχει ως αποτέλεσμα ο Smart Meter να προωθεί τη λανθασμένη πληροφορία που συνέλεξε και προς το Grid επηρεάζοντάς τον τρόπο λειτουργίας του σε διάφορους τομείς (πολύ περισσότερο αν τέτοιες επιθέσεις λάβουν μαζικό χαρακτήρα).

4.2.2 Μηνύματα για μεταφορά ενέργειας στο ή απορρόφηση ενέργειας από το Smart Grid.

Όπως έχουμε ήδη πει, το Smart Grid δίνει την ευκαιρία στον καταναλωτή, πέρα από το να καταναλώνει ενέργεια, να μετέχει ενεργά στην όλη διαδικασία διαχείρισης ενέργειας είτε προσφέροντας στο Grid ενέργεια από το δικό του ενεργειακό απόθεμα είτε απορροφώντας ενέργεια από το Smart Grid όταν αυτό κριθεί απαραίτητο. Για να γίνει κάτι τέτοιο, χρειάζεται πρωτίστως ο καταναλωτής να διαθέτει τις δικές του μονάδες παραγωγής και αποθήκευσης ενέργειας (ηλιακά, ανεμογεννήτριες κτλ.) κι έπειτα να διαθέτει τη δυνατότητα να τις διαχειρίζεται. Αυτό το τελευταίο φυσικά θα ήταν ενδεχομένως δύσκολο δεδομένης της απειρίας του πελάτη και της έλλειψης σχετικών γνώσεων, για το λόγο αυτό εκείνο που αναμένουμε να μπορεί να γίνεται είναι ο πελάτης να συνάπτει μια συμφωνία με έναν

παροχέα υπηρεσιών της επιλογής του ώστε ο παροχέας αυτός να αναλαμβάνει τη διαχείριση των μονάδων ενέργειας του πελάτη έναντι κάποιου ποσοστού[76].

Σενάριο

Ένα μήνυμα ελέγχου για προσφορά/ αποθήκευση ενέργειας παραλαμβάνεται από το ESI/HAN Gateway το οποίο το επεξεργάζεται και δρομολογεί τις κατάλληλες εντολές προς DER/PEV.

Μια ενδεχόμενη αλλοίωση του μηνύματος[42] από έναν κακόβουλο χρήστη ο οποίος προσωποποιεί είτε το ESI/HAN Gateway είτε τις συσκευές DER/PEV, υποκλέπτοντας τα μηνύματα και αλλοιώνοντας το περιεχόμενό τους προκειμένου να αναγράφουν διαφορετικά ποσοστά ενέργειας προς απορρόφηση/προσφορά ή να αλλοιωθεί ο βαθμός κρισιμότητας της αίτησης, θα μπορούσε να έχει αρνητικές συνέπειες. Αφού μια μαζική λανθασμένη προσφορά ενέργειας σε ένα ήδη βεβαρυμμένο δίκτυο ηλεκτροδότησης θα μπορούσε πρωτίστως να θέσει σε κίνδυνο τον εξοπλισμό του Smart Grid κι έπειτα να προκαλέσει αλυσιδωτά φαινόμενα load-shedding σε μεγάλες περιοχές στερώντας τους έτσι την ηλεκτρική παροχή. Παρόμοια αποτελέσματα, θα μπορούσε να έχει και ένα Replay Attack[42] υποκινούμενο από ένα κακόβουλο χρήστη, το οποίο θα μπορούσε να εξελιχθεί αναμεταδίδοντας μηνύματα αποφόρτισης PEV/DER σε ώρες υπερφόρτωσης και μηνύματα απορρόφησης ενέργειας σε ώρες αυξημένης ζήτησης γεγονός που θα μπορούσε να κινητοποιήσει προγράμματα Demand Response/Load Shedding (που μπορούν να προκαλέσουν ταλαιπωρία και σε κάποιες περιπτώσεις χρηματική επιβάρυνση στον καταναλωτή) χωρίς κάτι τέτοιο να χρειάζεται πραγματικά.

Τονίζουμε ότι στην περίπτωση που ένας παροχέας ηλεκτρικής ενέργειας (ESP) αναλαμβάνει τη διαχείριση των DER ενός Smart Home, η συμφωνία που διεξάγεται μεταξύ αυτού και του πελάτη πρέπει να προστατεύεται από περιπτώσεις στις οποίες ο πελάτης ισχυρίζεται ότι δεν έχει αποδεχθεί ποτέ μια τέτοια συνεργασία/ ή περιπτώσεις στις οποίες ο πελάτης ισχυρίζεται ότι ο παροχέας δεν έδρασε σε κάποια περίπτωση που έπρεπε ή έδρασε σε μια περίπτωση που δεν έπρεπε επιβαρύνοντάς τον οικονομικά.

4.2.3 Πρόκληση φυσικής ζημιάς στο μετρητή.

Ακόμα και στην προ Smart Grid εποχή παρατηρούμε σε αρκετές περιπτώσεις προσπάθειες για πρόκληση φυσικής ζημιάς/αλλοίωσης του μετρητή ηλεκτρικής ενέργειας ενός υποστατικού από τους ενοίκους του, σε μια προσπάθεια μείωσης του προσωπικού τους

λογαριασμού[74],[77]. Τέτοιου είδους επιθέσεις, προφανώς δεν αναμένουμε να σταματήσουν να υφίστανται στα Smart Grid δίκτυα. Κατ' ακρίβεια περιμένουμε ακριβώς το αντίθετο. Δηλαδή περισσότερες προσπάθειες φυσικής αλλοίωσης του μετρητή, οι οποίες θα εκμεταλλεύονται τις νέες αδυναμίες που εισάγονται λόγω της ψηφιοποίησης του.

Σενάριο

Ο πελάτης επιχειρεί να αποσυνδέσει το μετρητή από το υποστατικό του ή να τον τροποποιήσει ώστε να ξεκινήσει να μετράει αντίστροφα, να τον παραποιήσει ώστε να μετρά με διαφορετικούς ρυθμούς κτλ.. Ενδεχόμενες επιθέσεις αυτής της μορφής είναι και οι επιθέσεις στις οποίες επιχειρείται η παράνομη τροποποίηση ή ενημέρωση του λογισμικού που τρέχει ο μετρητής η οποία θα μπορούσε να υλοποιηθεί με την προσωποποίηση μιας νόμιμης οντότητας.

Τέτοιου είδους σενάρια θέτουν σε κίνδυνο τους στόχους της ακεραιότητας των μετρήσεων του συστήματος καθώς επίσης και τους στόχους διαθεσιμότητας του μετρητή και της αυθεντικότητας του αποστολέα του software update.

4.2.4 Απομακρυσμένος έλεγχος συσκευών και συστημάτων από τον πελάτη

Μια από τις σπουδαιότερες δυνατότητες που μας παρέχει το Smart Grid είναι αναμφίβολα, η δυνατότητα απομακρυσμένου ελέγχου των συσκευών και συστημάτων στο Smart Home μας με την αποστολή μηνυμάτων προς το ESI/HAN Gateway[76].

Σενάριο

Ο πελάτης βρίσκεται εκτός εσωτερικού περιβάλλοντος και αποστέλλει μηνύματα ελέγχου προς το ESI/HAN Gateway με στόχο τον έλεγχο των συσκευών του.

Είναι προφανές πως μια προσωποποίηση του πελάτη από πλευράς ενός κακόβουλου χρήστη θα μπορούσε να έχει απρόβλεπτα αποτελέσματα σε μια τέτοια περίπτωση[42]. Ο κακόβουλος χρήστης θα μπορούσε για παράδειγμα να αποστείλει μηνύματα ελέγχου με στόχο όλες οι οικιακές συσκευές του σπιτιού να τεθούν σε λειτουργία (γεγονός που αναμφίβολα θα επιβάρυνε τον πελάτη οικονομικά σε μεγάλο βαθμό – ή ακόμα και το τοπικό Grid λόγω απρόσμενης αύξησης της ζήτησης). Παρόμοια, ο κακόβουλος χρήστης θα μπορούσε να στείλει ένα μήνυμα για απενεργοποίηση όλων των συσκευών στο σπίτι (κάτι το οποίο θα μπορούσε να κοστίσει ακόμα και ζωές σε περίπτωση που ανάμεσα σε αυτές τις συσκευές είναι και συσκευές υποστήριξης υγείας/ζωής κτλ.). Πέραν όλων αυτών, ο

επιτιθέμενος θα μπορούσε ακόμα, προσποιούμενος τον πελάτη να επιτρέψει την εγκατάσταση ενός κακόβουλου λογισμικού στον κεντρικό έξυπνο μετρητή του σπιτιού.

Σε ένα άλλο ενδεχόμενο, ο κακόβουλος χρήστης θα μπορούσε να οργανώσει ένα Device Impersonation Attack[43], το οποίο θα είχε ως αποτέλεσμα ενώ ο πελάτης θεωρεί ότι ελέγχει απομακρυσμένα μια συσκευή να ελέγχει μια άλλη. Κάτι τέτοιο θα μπορούσε να προκαλέσει τα πάντα από μια απλή ταλαιπωρία μέχρι ένα πολύ σοβαρότερο πρόβλημα αν π.χ. αντί ο φούρνος στους 160◦C τεθεί η σάουνα (στις σάουνες οι μέγιστες θερμοκρασίες δε ξεπερνούν κατά πολύ τους 100◦C) .

Παρόμοια αποτελέσματα θα μπορούσε να έχει και η παρεμβολή, τροποποίηση(Message Modification) και επαναποστολή ενός μηνύματος του πελάτη προς το ESI/HAN Gateway του σπιτιού του. Σε ένα τέτοιο ενδεχόμενο ο επιτιθέμενος θα μπορούσε π.χ.. να θέσει σε λειτουργία το αυτόματο σύστημα ποτίσματος αντί για 30 λεπτά, για 4 ώρες κάτι που θα μπορούσε ενδεχομένως να έχει καταστροφικές συνέπειες.

Ο κίνδυνος του Replay Attack είναι επίσης ορατός κάτω αυτό το σενάριο, στο οποίο ένας κακόβουλος χρήστης θα μπορούσε για σκοπούς επιβάρυνσης του λογαριασμού του πελάτη (ή ακόμα και για πλάκα) να υποκλέπτει τα μηνύματα του πελάτη προς το ESI/HAN Gateway να τα καταγράφει και να τα αναμεταδίδει σε μετέπειτα χρονικές στιγμές με αποτέλεσμα τα ρούχα στο πλυντήριο να ξαναπληθούν, τα ρούχα στο στεγνωτήριο να ξαναστεγνώσουν κτλ..

Σημαντικό είναι και σε αυτή την περίπτωση ο πελάτης να μη μπορεί να αποποιηθεί της αποστολής ενός μηνύματος απομακρυσμένου ελέγχου ενώ το έχει στείλει ή να ισχυριστεί αποστολή ενός απομακρυσμένου μηνύματος ενώ δεν το έστειλε.

4.2.5 Ο πελάτης ζητά να λάβει τα στοιχεία που αφορούν στην ενεργειακή του κατανάλωση από την εταιρεία παροχής ενέργειας.

Από τη στιγμή που τα δεδομένα ενεργειακής κατανάλωσης ενός υποστατικού μεταφέρονται στο MDMS σύστημα και οι κατάλληλες χρεώσεις εφαρμόζονται, ένας πελάτης διαθέτει το δικαίωμα να ζητήσει να δει τα στοιχεία που αφορούν στη δική του κατανάλωση[76]. Όπως είχαμε πει και στο προηγούμενο κεφάλαιο, κάτι τέτοιο θα μπορούσε να ήταν μια καλή ευκαιρία για την εταιρεία παροχής ηλεκτρικής ενέργειας, να δώσει χρήσιμο feedback και συμβουλές στον καταναλωτή, προκειμένου να πετύχει τη μεγαλύτερη ευαισθητοποίησή του σε θέματα ενέργειας.

Σενάριο

Ο πελάτης ζητά τα στοιχεία που αφορούν στη δική του κατανάλωση (ή σύγκριση της δικής του κατανάλωσης με αυτήν γειτονικών ή παρόμοιων υποστατικών). Το αίτημα δρομολογείται στο CIS/MDMS το οποίο αποστέλλει τη ζητούμενη πληροφορία με το κατάλληλο feedback στο In-Home Display του πελάτη.

Ενδεχόμενες απειλές σ' ένα τέτοιο σενάριο θα μπορούσαν να έχουν να κάνουν για παράδειγμα με την προσωποποίηση ενός πελάτη, από έναν κακόβουλο χρήστη, προκειμένου ο χρήστης αυτός να αποκτήσει πρόσβαση σε στατιστικά στοιχεία που αφορούν στην ενεργειακή κατανάλωση ενός υποστατικού και ενδεχομένως και των γειτονικών του υποστατικών, στο ιστορικό χρεώσεων κτλ.. Κάτι τέτοιο θα μπορούσε να έχει ως αποτέλεσμα τη συλλογή πληροφορίας η οποία θα μπορούσε για παράδειγμα να καταμαρτυρεί την οικονομική κατάσταση του χρήστη/ το μέγεθος του σπιτιού του / τον αριθμό διαμερίσματος κτλ. με συνέπεια ο κακόβουλος χρήστης να έχει όλη τη γνώση που χρειάζεται προκειμένου να σχεδιάσει ένα μελλοντικό χτύπημα.

Κάτω από το ίδιο πρίσμα, ευαίσθητα δεδομένα θα μπορούσαν να παραπέσουν στα χέρια ενός κακόβουλου χρήστη ο οποίος επιχειρεί να παρακούσει τη συνομιλία μεταξύ CIS/MDMS και In-Home Display. Σε μια τέτοια επίθεση (Eavesdropping) η παρουσία του κακόβουλου χρήστη δε γίνεται αντιληπτή από τις δύο οντότητες που συμμετέχουν στην επικοινωνία. Ο κακόβουλος χρήστης όμως μπορεί να παρακολουθεί ότι ακριβώς κυκλοφορεί στο δίκτυο με αποτέλεσμα να μπορεί να λάβει ακόμη και ευαίσθητα προσωπικά δεδομένα.

Ως επέκταση της απλής παθητικής παρουσίας του κακόβουλου χρήστη βέβαια, κάποιος θα μπορούσε να επιχειρήσει να τροποποιήσει το περιεχόμενο των αιτήσεων του πελάτη προκειμένου να λάβει περισσότερη πληροφορία για τον πελάτη.

4.2.6 Ο πελάτης δίδει την έγκριση του ώστε τα προσωπικά δεδομένα κατανάλωσής του να διατίθενται στον παροχέα υπηρεσιών με τον οποίο συνεργάζεται.

Σε πολλές περιπτώσεις ένας πελάτης μπορεί να επιλέξει τη συνεργασία με τους παροχείς υπηρεσιών της επιλογής του. Σε τέτοιες περιπτώσεις συνήθως, τα δεδομένα κατανάλωσής του πελάτη αποθηκεύονται στο κεντρικό σύστημα κάποιου συγκεκριμένου παροχέα και ο άλλος παροχέας (π.χ.. αυτός που αναλαμβάνει τη λιανική πώληση ενέργειας για χάρη του πελάτη) λαμβάνει δεδομένα από τον κεντρικό. Για να γίνει κάτι τέτοιο βέβαια ο πελάτης πρέπει να δώσει την έγκριση του[73].

Σενάριο

Ο πελάτης επιθυμεί να εξουσιοδοτήσει κάποιον παροχέα υπηρεσιών που εμπιστεύεται (π.χ.. για τη λιανική πώληση ενέργειας) , να λαμβάνει ότι πληροφορία χρειάζεται σχετικά με την κατανάλωση του, από το κεντρικό σύστημα κάποιου συγκεκριμένου παροχέα.

Σε ένα τέτοιο σενάριο παρουσιάζεται ο κίνδυνος επιθέσεων του τύπου Man In The Middle Attack στις οποίες ο επιτιθέμενος προσποιείται το ένα άκρο επικοινωνίας στο άλλο, με στόχο να αποσπάσει την πληροφορία που μεταφέρεται. Μια τέτοια επίθεση, αν συνδυαστεί για παράδειγμα με μια επίθεση αλλοίωσης μηνυμάτων θα μπορούσε να οδηγήσει στην εξουσιοδότηση μιας κακόβουλης οντότητας να λαμβάνει τα ευαίσθητα προσωπικά δεδομένα του πελάτη με όλες τις συνέπειες που κάτι τέτοιο συνεπάγεται.

Επίσης, επικίνδυνο σε αυτό το σενάριο είναι και το ενδεχόμενο ο πελάτης να επιχειρήσει να αποποιηθεί της εξουσιοδότησης μιας οντότητας να λαμβάνει τα δικά του προσωπικά δεδομένα – απειλή που θα μπορούσε κάλλιστα να λάβει νομικό χαρακτήρα.

Σε αυτή την ενότητα, μας δόθηκε η ευκαιρία να εξετάσουμε πολλούς από τους ενδεχόμενους κινδύνους που θα μπορούσαν να επηρεάσουν τους στόχους ασφάλειας του συστήματός μας στα πλαίσια του Smart Home. Ο πίνακας 4.1 αποτελεί μια συνοπτική αναφορά στα σενάρια που μελετήσαμε και στους κινδύνους που εντοπίσαμε στο κάθε ένα από αυτά.

Smart Home Security				
Security Issue : Devices transferring energy consumption data to Customer EMS				
Systems Involved	Description	Possible Threads	Security Goals Compromised	Degree of Impact
Appliances/ DER/ PEV ↕ Sub metering/ Customer EMS ↕ Electric Metering	Device-related consumption patterns and data are propagated from Sub metering devices or the appliances as such to the Customer EMS which forwards it to the Electric Smart Meter.	• Eavesdropping • Traffic Analysis • Man-In-The-Middle attack • Message Modification • Replay Attack • Device Impersonation	• Confidentiality • Integrity • Authenticity	Low-Moderate
Security Issue: Control signals for Smart Home energy residue exporting/importing energy				
Systems Involved	Description	Possible Threads	Security Goals Compromised	Degree of Impact
ESI/HAN ↕ Customer EMS ↕ DER/PEV	Control Signals to allow the exporting of stored energy residue from Smart Home environment to Smart Grid.	• Repudiation • Message Modification	• Non repudiation • Integrity • Authentication	Moderate
Security Issue: Physical Meter Tampering/Reversal/Removal				
Systems Involved	Description	Possible Threads	Security Goals Compromised	Degree of Impact
Electric Meter	The customer may indulge in the illegal action of meter tampering, reversal or removal in an effort to relief himself from the financial burdens of electricity bills	• Tampering/Reversal/ Removal of Meter • Illegal Software Modification/Update	• Authentication • Integrity	Low – Moderate (if massive)
Security Issue: Remote Customer Access to and Control Devices				
Systems Involved	Description	Possible Threads	Security Goals Compromised	Degree of Impact
Customer at Remote Location ↕ ESI/HAN ↕ Customer Appliances and Metering Equipment	Customers will be able to remotely access and control their appliances (by sending signals for switching devices on/off etc.)	• Impersonation of a customer • Device Impersonation • Message Modification • Replay attack • Repudiation	• Integrity • Non Repudiation • Authentication	Low-High (risk life)
Security Issue :Customer Requesting Energy Usage Data from the Utility				
Systems Involved	Description	Possible Threads	Security Goals Compromised	Degree of Impact
Customer ↕ CIS/MDMS ↕ AMI Head End ↕ ESI/HAN ↕ In-Home Display	Once metering data has been validated and priced, energy usage information can and will be sent to the customer upon request in a meaningful representation (in terms of feedback/personalized advice/comparisons with other homes etc) This feedback is intended for aiding consumers in becoming more aware of their consumption.	• Impersonation of a customer • Eavesdropping/Message Interception • Message Modification	• Confidentiality • Integrity • Authenticity	Low –Moderate (If data is exploited)
Security Issue: Authorization for Usage of his Data from Retail Energy Service Provider				
Systems Involved	Description	Possible Threads	Security Goals Compromised	Degree of Impact
Customer ↕ CIS ↕ MDMS ↕ Aggregator/ESP	Customer wishes to authorize the transfer of his private energy-consumption-related data from Utilities to third party ESPs as part of an agreement he forms with the ESP for the direct control of his appliances and equipment.	• Repudiation • Man in the Middle	• Integrity • Confidentiality • Authenticity	Low-Moderate(if data us exploited)

Πίνακας 4.1: Η παρουσίαση και αξιολόγηση των κινδύνων στο Smart Home περιβάλλον.

4.3 Θέματα Ασφάλειας στα Smart Grids

Αφήνοντας πίσω μας τα θέματα ασφάλειας που προκύπτουν στο πλαίσιο του Smart Home επικεντρωνόμαστε τώρα σε θέματα ασφάλειας που προκύπτουν σε οντότητες του υπόλοιπου Smart Grid. Όπως θα παρατηρήσουμε στη συνέχεια, η επιτυχία μιας κακόβουλης επίθεσης σε αυτό το επίπεδο, μπορεί να προσλάβει τεράστιες διαστάσεις, αφού επηρεάζει άμεσα κάθε υποστατικό, επιχείρηση ή βιομηχανία που βρίσκεται συνδεδεμένη με το Smart Grid.

4.3.1 Επιθέσεις με στόχο την κατάρρευση του συστήματος

Η ομαλή λειτουργία του Smart Grid εξαρτάται σε μεγάλο βαθμό από διάφορα συστήματα όπως για παράδειγμα τα SCADA/EMS, DRMS/LMS, MDMS κτλ.. Πίσω από τα συστήματα αυτά μια πληθώρα από servers αναλαμβάνει να διεκπεραιώσει όλες τις καίριας σημασίας εργασίες για το Smart Grid π.χ. το DRMS σύστημα διαχειρίζεται τα θέματα που αφορούν σε προγράμματα Demand Response, το LMS σύστημα διαχειρίζεται τα θέματα που αφορούν σε διαχείριση φορτίου (π.χ. load shedding κτλ.), το MDMS σύστημα είναι υπεύθυνο για τη συλλογή δεδομένων από τους μετρητές διάφορων υποστατικών προκειμένου να επιβάλει τις απαραίτητες χρεώσεις, ενώ τέλος τα SCADA συστήματα είναι υπεύθυνα για τη συλλογή, την επεξεργασία, την παρουσίαση και τον έλεγχο της κατάστασης του συστήματος σε κάθε σημείο του κ.ο.κ. [73]. Χωρίς τα συστήματα αυτά, στην ουσία δε θα μπορούσαμε καν να μιλάμε για Smart Grids κατά συνέπεια η ασφάλειά τους ανάγεται σε έναν από τους ουσιαστικότερους στόχους μας.

Σενάριο

Ένας κακόβουλος χρήστης αξιοποιεί μια οποιαδήποτε τεχνική τον εξυπηρετεί για να ρίξει έναν ή περισσότερους servers του συστήματος[77]**.**

Τέτοιες επιθέσεις θα μπορούσαν να έχουν ως αποτέλεσμα ολόκληρες περιοχές η μια μετά την άλλη βυθίζονται στο απόλυτο σκοτάδι, με τις συνέπειες να είναι καταστροφικές τόσο για την οικονομία όσο και για την κοινωνία μιας χώρας. Για την ακρίβεια δε θα ήταν υπερβολή να πούμε πως τον ενδεχόμενο τέτοιων επιθέσεων δίνει στην τρομοκρατία σήμερα άλλο ένα πρόσωπο[78]. Δε χρειάζονται πλέον όπλα μαζικής καταστροφής για να σπείρει κανείς το χάος προκαλώντας ζημιές σε εγκαταστάσεις δισεκατομμυρίων. Ένα κομμάτι κώδικα είναι αρκετό!

Πώς όμως θα μπορούσε ένας κακόβουλος χρήστης να ρίξει τους servers που στηρίζουν το σύστημα;
Ένα ενδεχόμενο θα ήταν η αξιοποίηση πληροφοριών οι οποίες είναι διαθέσιμες στο ευρύ κοινό (π.χ. μέσω μιας ιστοσελίδας με πληροφορίες που αφορούν στο εταιρικό δίκτυο ενός παροχέα υπηρεσιών, ονόματα υπαλλήλων/διευθύνσεις ηλεκτρονικού ταχυδρομείου κτλ..)[28]. Τέτοιες πληροφορίες μπορούν να χρησιμοποιηθούν κάλλιστα με έξυπνο τρόπο για να προδώσουν συνθηματικά πρόσβασης στο σύστημα. Προσβάσεις στο οποίο, αφήνουν ανοικτό το ενδεχόμενο για διαγραφή ή τροποποίηση αρχείων συστήματος που θα μπορούσαν να κοστίσουν τη διαθεσιμότητά του. Για του λόγου το αληθές, το 2003 ένας διδακτορικός φοιτητής με το όνομα Sean Gorman, κατέθεσε στο πανεπιστήμιο George Mason όπου φοιτούσε, μια διατριβή η οποία προκάλεσε τότε την προσοχή πολλών, αναγκάζοντας μάλιστα κυβερνητικά στελέχη και μυστικές υπηρεσίες να προχωρήσουν στην κατηγοριοποίηση της ως απόρρητο έγγραφο του κράτους και να απαγορεύσουν τη δημοσιοποίηση των λεπτομερών αποτελεσμάτων της[79]. Ο λόγος; Απλός. Ο Sean Gorman κατάφερε, αξιοποιώντας πληροφορία κοινά διαθέσιμη στο Internet, να χαρτογραφήσει λεπτομερώς, κάθε επιχείρηση και βιομηχανικό τομέα της Αμερικανικής οικονομίας στο δίκτυο οπτικών ινών που τις συνδέει.
Κάτι τέτοιο θα μπορούσε κάλλιστα να γίνει εφικτό και σε Smart Grid δίκτυα δημιουργώντας έναν πλήρες χάρτη για οποιονδήποτε ενδιαφέρεται να επιτεθεί στο σύστημα!

Παράλληλα, πρόσβαση στο σύστημα μπορεί να επιτευχθεί και αξιοποιώντας αδυναμίες στα platform configurations του συστήματος[28], [80]. Αδυναμίες που μπορούν να αφορούν σε κακά ορισμένες πολιτικές δικαιωμάτων που δίνουν στους χρήστες περισσότερα δικαιώματα από αυτά που απαιτούνται για το ρόλο που επιτελούν, σε ακατάλληλους ή ανεπαρκής τρόπους αυθεντικοποίησης χρήστη, σε κακά ορισμένες πολιτικές καθορισμού συνθηματικών πρόσβασης, σε μη κρυπτογραφημένα μηνύματα τα οποία μπορεί να περιλαμβάνουν ακόμα και τους κωδικούς πρόσβασης των χρηστών που μπορούν να πέσουν στα χέρια ενός κακόβουλου χρήστη ακόμα και μ’ ένα απλό sniffing των πακέτων μέσω ενός λογισμικού που διατίθεται δωρεάν όπως το Wireshark[12].

Τέτοιες αδυναμίες στα platform configurations ή ακόμα και στο ίδιο το λειτουργικό σύστημα και το λογισμικό που χρησιμοποιείται από τους υπολογιστές του συγκεκριμένου δικτύου, θα μπορούσαν να τύχουν εκμετάλλευσης ακόμα ευκολότερα, αν συνοδεύονται από ανεπαρκείς πολιτικές ασφάλειας του δικτύου της εταιρείας[73], [80]. Ελλιπή configurations, αδύναμοι κανόνες στα firewalls, κακή σχεδίαση του δικτύου και σωρεία άλλων αδυναμιών, μπορούν

εύκολα να αφήσουν περιθώρια για port scanning και ping sweeps με εργαλεία διαθέσιμα δωρεάν όπως το Nmap τα οποία θα μπορούσαν να εντοπίσουν τους active hosts, τα network services που αυτοί χρησιμοποιούν, στοιχεία που να προδίδουν το λειτουργικό τους σύστημα και τα οποία θα μπορούσαν σε συνδυασμό με ένα πρόγραμμα εντοπισμού αδυναμιών συστήματος όπως το Nessus να προδώσουν πολλά από τα τρωτά σημεία του συστήματος που θα μπορούσαν να αποτελέσουν στόχο ενός κακόβουλου χρήστη[12].

Έχοντας συλλέξει πολύτιμη πληροφορία για το σύστημα, ένας επιτιθέμενος θα μπορούσε επίσης να αξιοποιήσει τρωτά σημεία ή bugs που εντοπίζονται στο λογισμικό που τρέχει σε αυτούς τους servers (ή και η εκμετάλλευση της απουσίας IDS/IPS συστημάτων) προκειμένου να επιτύχει π.χ. μια επίθεση τύπου Denial of Service Attack[28]. Τέτοιες επιθέσεις καθιστούν αμέσως τους servers που δέχονται επίθεση ανίκανους να εξυπηρετήσουν τους κανονικούς χρήστες του συστήματος, λόγω υπερφόρτωσης η οποία προκαλείται από τον κακόβουλο χρήστη που βομβαρδίζει με ψεύτικες αιτήσεις το σύστημα. Πολλές φορές τέτοιου τύπου επιθέσεις οδηγούν σε κατάρρευση του συστήματος γεγονός που βοηθά τον χρήστη να πετύχει το σκοπό του ακόμα και χωρίς να επιτύχει πρόσβαση στο σύστημα.

Παράλληλα, η επιμόλυνση του συστήματος με ένα επιβλαβές κομμάτι λογισμικού[24] το οποίο διεισδύει στο σύστημα χωρίς να γίνεται αντιληπτό και λειτουργεί σβήνοντας αρχεία, τροποποιώντας αποθηκευμένα αρχεία, μειώνοντας την απόδοση του υπολογιστή κτλ., θα μπορούσε επίσης να οδηγήσει σε κατάρρευση του συστήματος. Τέτοιου τύπου λογισμικά κρίνονται ιδιαιτέρως επικίνδυνα κυρίως αν λάβουμε υπόψη το γεγονός ότι μπορούν να εκμεταλλευτούν την απουσία μηχανισμών ασφάλειας στο δίκτυο της εταιρείας (π.χ. network segmentation) για να διαδοθούν και σε άλλα συστήματα καίριας σημασίας.

Επίσης επικίνδυνο ενδεχόμενο για την κατάρρευση του συστήματος θα μπορούσε να αποτελεί μια επίθεση με τη βοήθεια κάποιου από το εσωτερικό δίκτυο[28], ή ενός δυσαρεστημένου από την εταιρεία υπαλλήλου ο οποίος θα μπορούσε να έχει και το κίνητρο και τις γνώσεις που χρειάζονται για να καταφέρει πλήγματα στη διαθεσιμότητα των συστημάτων της.

4.3.2 Επιθέσεις με στόχο τον έλεγχο του συστήματος.

Εξίσου επικίνδυνες με τις επιθέσεις που στοχεύουν στην κατάρρευση του συστήματος θα μπορούσαμε να θεωρήσουμε και τις επιθέσεις που θέτουν ως στόχο τους τον έλεγχο του συστήματος[77]. Σε τέτοιου είδους επιθέσεις, ο επιτιθέμενος καταφέρνει να αποκτήσει τον

έλεγχο του συστήματος ή ενός μέρους του συστήματος κι έπειτα χρησιμοποιεί το σύστημα με όποιο τρόπο θεωρεί ότι εξυπηρετούνται καλύτερα οι στόχοι του. Τέτοιου είδους επιθέσεις μπορούν κάλλιστα να προσλάβουν διαστάσεις τρομοκρατικού κτυπήματος προκαλώντας κοινωνικό χάος και οικονομική ύφεση σε μια χώρα.

Σενάριο

Ένας κακόβουλος χρήστης επιτυγχάνει να πάρει στα χέρια του τον έλεγχο του συστήματος, το οποίο χρησιμοποιεί στη συνέχεια για να εξυπηρετήσει τους στόχους του.

Το να πάρει κάποιος τον έλεγχο ενός συστήματος στα χέρια του, έστω και αν μιλάμε για ένα μόνο κομμάτι του συγκεκριμένου συστήματος θα μπορούσε να συμβεί με διάφορους τρόπους. Ένας εξ' αυτών, η αξιοποίηση όπως είχαμε πει και προηγουμένως, πληροφορίας άμεσα διαθέσιμης στο ευρύ κοινό, η οποία θα μπορούσε να διευκολύνει σημαντικά την προσπάθεια πρόσβασης στο σύστημα (προσφέροντας στον επιτιθέμενο γνώσεις και πληροφορίες που θα μπορούσαν να διευκολύνουν την προσπάθεια του για απόκτηση κωδικών πρόσβασης, αναζήτηση αδυναμιών στις πολιτικές καθορισμού κωδικών πρόσβασης/δικαιωμάτων πρόσβασης χρηστών κτλ.).

Την ίδια στιγμή, μέσω της επιμόλυνσης του συστήματος με επιβλαβές λογισμικό (τύπου worms/Trojans κτλ.) το οποίο ενδεχομένως λειτουργεί κατά τρόπο που αναγκάζει π.χ. SCADA servers να επιτεθούν στους υπόλοιπους servers με τους οποίους συνεργάζονται, ένας κακόβουλος χρήστης θα μπορούσε να επιτύχει το στόχο του για απόκτηση ελέγχου πάνω στο σύστημα. Ήδη έχουν σημειωθεί περιστατικά επιμόλυνσης SCADA συστημάτων με επιβλαβές λογισμικό[81–83] με δυνατότητες όχι μόνο καταγραφής όλων των πληκτρολογούμενων εντολών που καταχωρήθηκαν στο σύστημα από τη στιγμή της επιμόλυνσης, αλλά και κλοπής digital certificates(που συνδέουν το δημόσιο κλειδί της εταιρείας με την ίδια), ή διαγραφής των πληροφοριών που καταγράφηκαν πρόσφατα στο ιστορικό του συστήματος ή ακόμα και διαγραφής των περιεχομένων στους σκληρούς δίσκους του συστήματος. Τέτοια είδη λογισμικού επιτρέπουν σε κάποιες περιπτώσεις στο χρήστη και την αλλοίωση δεδομένων που έχουν καταχωρηθεί στο σύστημα, γεγονός που σημαίνει πως ένας κακόβουλος χρήστης θα μπορούσε να συγκαλύψει την επίθεση του εισάγοντας ή τροποποιώντας το ιστορικό προσβάσεων και αλλαγών που διατηρεί η εταιρεία, ώστε να κατηγορηθεί κάποιος αθώος για τη ζημιά που ο ίδιος επιχειρεί να προκαλέσει.

Ένα ακόμα είδος επίθεσης, το οποίο θα μπορούσε να επιτρέψει σε μια κακόβουλη οντότητα να προκαλέσει σημαντικά προβλήματα στο σύστημα είναι μια επίθεση παθητικής αναγνώρισης του δικτύου (Passive Network Reconnaissance)[28][84]. Σε μια επίθεση αυτής της μορφής, ο επιτιθέμενος αποκτά τη δυνατότητα παρακολουθώντας την κίνηση μέσα σε ένα δίκτυο, να αρχίσει να αναγνωρίζει βασικές οντότητες που βρίσκονται συνδεδεμένες σε αυτό, το λειτουργικό σύστημα που τρέχουν, τους τύπους μηνυμάτων που αυτές ανταλλάζουν μεταξύ τους, στοιχεία που αφορούν στην τοπολογία του δικτύου κτλ.. Όλη αυτή η πληροφορία, αν συνδυαστεί σωστά με την οποιαδήποτε άλλη γνώση για το σύστημα της εταιρείας μπορεί να φέρει τον επιτιθέμενο ένα βήμα πιο κοντά στο να επιτεθεί στοχευμένα στο σύστημα, με στόχο να αποκτήσει τον έλεγχό του.

Τέλος, αξίζει τον κόπο να αναφέρουμε ότι μια πρόσβαση στο σύστημα με στόχο τον έλεγχό του θα μπορούσε να επιτευχθεί και μέσα από την επίθεση ενός δυσαρεστημένου υπαλλήλου απέναντι στην εταιρεία.

Όλα τα πιο πάνω ενδεχόμενα παρουσίασαν μια πληθώρα τρόπων απόκτησης είτε άμεσης πρόσβασης στο σύστημα είτε γνώσεων ώστε να επιχειρηθεί μελλοντικά μια πρόσβαση στο σύστημα. Μια επιτυχημένη έκβαση κάποιας απ’ τις πιο πάνω επιθέσεις, θα μπορούσε να έχει απρόβλεπτες συνέπειες αφού με την απόκτηση πρόσβασης σε servers DRMS/LMS, MDMS, SCADA κτλ. ένας κακόβουλος χρήστης θα μπορούσε να προχωρήσει στη δημιουργία και αποστολή ψεύτικων μηνυμάτων (message fabrication) στους πελάτες της εταιρείας ή σε υποσταθμούς και άλλο βοηθητικό εξοπλισμό του Smart Grid (RTUs, PMUs), ή στην αναμετάδοση παλαιότερων μηνυμάτων που έχουν ήδη σταλεί (replay attack).Κάτι τέτοιο θα μπορούσε να επηρεάσει τόσο τους πελάτες όσο και το ίδιο το δίκτυο, αφού οι πελάτες ή τα συστήματα ESI στα υποστατικά τους θα ανταποκρίνονται σε άκυρα μηνύματα τα οποία δεν αντιστοιχούν στην κατάσταση του δικτύου, επιβαρύνοντάς το. Παράλληλα, σ’ ένα εξίσου πιθανό σενάριο ένας κακόβουλος χρήστης θα μπορούσε να επιχειρήσει να τροποποιήσει δεδομένα που αφορούν σε χρεώσεις πελατών με στόχο τη χρηματική επιβάρυνσή τους ή απλώς για πλάκα.

4.3.3 Επιθέσεις με στόχο την κλοπή εταιρικών δεδομένων

Η επιτυχία του Smart Grid στηρίζεται σε μεγάλο βαθμό στη δυνατότητά του να διαχειρίζεται ορθά τον τεράστιο όγκο δεδομένων που συλλέγει. Δεδομένα, τα οποία δεν περιλαμβάνουν μόνο την πληροφορία που συλλέγεται από τα Smart Meters αλλά και όλες τις μετρήσεις που λαμβάνονται από διάφορους αισθητήρες, PMUs και PLCs που τοποθετούνται σε διάφορα

σημεία του δικτύου για να λαμβάνουν μετρήσεις που βοηθούν να ανιχνεύσουμε την κατάσταση του Smart Grid.

Τέτοιου τύπου αλλά και άλλες πληροφορίες που αφορούν σε μια εταιρεία παροχής ηλεκτρικής ενέργειας, δε θα ήταν απίθανο να αποτελέσουν στόχο για ένα ακόμα είδος επίθεσης. Μια επίθεση με σκοπό να αποσπάσει όσο το δυνατό περισσότερες πληροφορίες από τα συστήματα μιας εταιρείας. Τέτοιες επιθέσεις, θα μπορούσαν να υποκινούνται από άλλες εταιρείες παροχής για σκοπούς απόκτησης ανταγωνιστικού πλεονεκτήματος ή ακόμα και για σκοπούς υποβάθμισης της αξιοπιστίας της υπό-επίθεση εταιρείας.

Σενάριο

Ένας κακόβουλος χρήστης, αποκτά τη δυνατότητα κλοπής δεδομένων που αποτελούν περιουσία ενός συγκεκριμένου παροχέα ηλεκτρικής ενέργειας[76]**.**

Όπως έχουμε πει και προηγουμένως, ένας ενδεχόμενος τρόπος ο κακόβουλος χρήστης να αποκτήσει δυνατότητες ανάκτησης δεδομένων που βρίσκονται αποθηκευμένα στο σύστημα (σε βάσεις δεδομένων κτλ.), θα ήταν μέσω συλλογής πληροφοριών που δόθηκαν στη δημοσιότητα από την ίδια την εταιρεία, ή/και εκμεταλλευόμενος διάφορες ελλείψεις στις πολιτικές ασφαλείας της εταιρείας οι οποίες θα μπορούσαν να αφήσουν ανοικτές διάφορες οδούς για πρόσβαση στο κεντρικό σύστημα.

Πέραν αυτού, κλοπή δεδομένων θα μπορούσε να συμβεί και εγκαθιστώντας κακόβουλο λογισμικό στα συστήματα μιας εταιρείας παροχής. Ήδη στο πρόσφατο παρελθόν, έχουν αναφερθεί παραδείγματα επιμόλυνσης συστημάτων με κακόβουλο λογισμικό ειδικά φτιαγμένο για SCADA συστήματα. Όπως μας έχει αποδείξει η ιστορία, τέτοιο λογισμικό μπορεί να διαθέτει τεράστιες ικανότητες, οι οποίες δε χρειάζεται κατ’ ανάγκη να έχουν καταστρεπτικό χαρακτήρα. Λογισμικά για παράδειγμα όπως το Duqu[82] ή το Flame με μοναδικό στόχο τη συλλογή πληροφοριών από το σύστημα και όχι τη διαγραφή ή την τροποποίησή τους έχουν ήδη κάνει την εμφάνισή τους. Τέτοιου είδους λογισμικά, εκμεταλλευόμενα συνήθως επιθέσεις τύπου Zero-Day Attacks (επιθέσεις που εκμεταλλεύονται τρωτά σημεία στο σύστημα τα οποία δεν είναι γνωστά στους developers ώστε να μπορέσουν να τα αντιμετωπίσουν), εγκαθιστούν rootkits (μετά από την εξασφάλιση πρόσβασης στο σύστημα από μια τρύπα ασφάλειας/ ή το σπάσιμο ενός κωδικού πρόσβασης) τα οποία τρυπώνουν στις βάσεις δεδομένων των SCADA συστημάτων, ξετρυπώνοντας αρχεία με δεδομένα που αφορούν στο ακριβές σχέδιο του ηλεκτρικού δικτύου, τα σημεία

ελέγχου του κτλ. ενώ παράλληλα, κάνουν sniffing της κίνησης από και προς τα συστήματα αυτά, λαμβάνουν screenshots, ηχογραφούν οποιεσδήποτε συζητήσεις και κλήσεις, καταγράφουν οτιδήποτε καταχωρήθηκε στο σύστημα μέσω του keyboard και διαθέτουν τη δυνατότητα να ενεργοποιούν το Bluetooth σε συσκευές που βρίσκονται σε κοντινή απόσταση προκειμένου να υποκλέπτουν τις επαφές των συσκευών αυτών. Σε πολλές περιπτώσεις δε, τέτοιου τύπου συστήματα διαθέτουν την ικανότητα να λειτουργούν υπό απόλυτη μυστικότητα (stealthy attack)[81] ανιχνεύοντας το anti-virus που χρησιμοποιείται από το σύστημα και αναπροσαρμόζοντας δυναμικά τη δομή των αρχείων τους ώστε να μη γίνονται στόχος.

Επίσης, πιθανό είναι βέβαια και το ενδεχόμενο που έχουμε αναφέρει και στις πιο πάνω περιπτώσεις, ένας δυσαρεστημένος με την εταιρεία υπάλληλος να αποφασίσει να χρησιμοποιήσει τις γνώσεις του κατά της εταιρείας παροχής αξιοποιώντας τα δικά του δικαιώματα πρόσβασης, ή καταφέρνοντας να αποκτήσει περαιτέρω δικαιώματα που θα μπορούσαν να του εξασφαλίσουν πρόσβαση σε δεδομένα, τα οποία θα ήταν δυνατό να φέρει στο φως της δημοσιότητας (ώστε να πλήξει την αξιοπιστία της εταιρείας κτλ.).

4.3.4 Επιθέσεις κατά των Field Devices του Smart Grid

Τελειώνοντας, θα κάνουμε αναφορά σε είδη επίθεσης οι οποίες έχουν ως στόχο τους να πλήξουν το Smart Grid όχι επηρεάζοντας τα κεντρικά συστήματα που ελέγχουν τη λειτουργία του αλλά «μαγειρεύοντας» τα δεδομένα και τις μετρήσεις που συλλέγονται από τα διάφορα επιμέρους συστήματα του Smart Grid όπως αισθητήρες, RTUs, PMUs κτλ.. Τέτοιες επιθέσεις έχουν ως αποτέλεσμα να εισάγονται στο Smart Grid λανθασμένες πληροφορίες, γεγονός που σημαίνει ότι το σύστημα αποκτά λανθασμένη εικόνα για την κατάσταση του δικτύου. Κάτι, που προφανώς έχει αντίκτυπο και στο όλο δίκτυο, και στις αγορές ενέργειας και στους ίδιους τους καταναλωτές.

Σενάριο

Ένας κακόβουλος χρήστης επιχειρεί να εισάγει λανθασμένη πληροφορία στο Smart Grid ελέγχοντας τις περιφερειακές συσκευές που χρησιμοποιεί για να λαμβάνει μετρήσεις.

Μια επίθεση προς αυτή την κατεύθυνση θα μπορούσε να λάβει τη μορφή ενός False Data Injection Attack[85], [86] πράγμα το οποίο θα σήμαινε πως ένας κακόβουλος χρήστης, τροποποιώντας τις μετρήσεις που λήφθηκαν από διάφορα PMUs και υλοποιώντας π.χ. Denial of Service Attacks στους αισθητήρες του δικτύου (γεγονός που θα μπορούσε εύκολα

να εξαντλήσει το ενεργειακό τους απόθεμα), θα μπορούσε κάλλιστα να καταφέρει με τρόπο που δε μπορεί να γίνει εύκολα αντιληπτός να επηρεάσει το σύστημα σε μεγάλο βαθμό. Ο λόγος είναι απλός κι έχει να κάνει με τον αλγόριθμο ο οποίος χρησιμοποιείται για την πρόβλεψη ζήτησης της επόμενης ημέρας. Ο αλγόριθμος αυτός, λαμβάνει υπόψη του την κατάσταση του δικτύου και τα επίπεδα ζήτησης της προηγούμενης μέρας, με αποτέλεσμα η εισαγωγή λανθασμένων δεδομένων να επηρεάζει εν μέρει την ακρίβεια του αποτελέσματος. Κάτι τέτοιο θα μπορούσε να σημαίνει μεγαλύτερες αστάθειες στο δίκτυο την επόμενη μέρα, και ενδεχομένως διακοπές στην παροχή ηλεκτρικού ρεύματος.
Στη σφαίρα αυτών των επιθέσεων θα μπορούσαμε να εντάξουμε και επιθέσεις κατά του τοπικού Automatic Voltage Regulator[80], της οντότητας στο υποσύστημα παραγωγής που αναλαμβάνει τη διατήρηση της ισορροπίας στο ηλεκτρικό δίκτυο, ελέγχοντας τα ποσοστά του reactive power που απορροφά ή δέχεται το σύστημα όπως αυτά καταγράφονται από τερματικά. Ή και τις επιθέσεις εναντίον του τοπικού Governor Control, της οντότητας δηλαδή, που αναλαμβάνει τον έλεγχο συχνότητας στο δίκτυο. Ο έλεγχος αυτός, καθίσταται εφικτός μέσα από αισθητήρες οι οποίοι ανιχνεύουν αλλαγές στη συχνότητα που συνοδεύουν τα διάφορα μη φυσιολογικά φαινόμενα ώστε να αναπροσαρμόζεται δυναμικά την ισχύ εξόδου των μονάδων παραγωγής. Και οι δύο αυτές οντότητες θα μπορούσαν να επιμολυνθούν με ένα κακόβουλο λογισμικό το οποίο θα μπορούσε να φτάσει σε αυτές μέσα από το ίδιο το κεντρικό σύστημα ελέγχου.

Με παρόμοιο τρόπο σε αυτή την κατηγορία θα μπορούσαμε να εντάξουμε και κινδύνους κατά του εξοπλισμού FACTS[80] (Flexible AC Transmission Systems) του δικτύου μεταφοράς. Ο εξοπλισμός αυτός που στόχο του έχει να ελέγχει το ποσοστό του reactive power που εισάγεται ή απορροφάται από το σύστημα, προκειμένου να βελτιώσει το σύστημα μεταφοράς, θα μπορούσε να επηρεαστεί με διάφορους τρόπους. Μεταξύ αυτών θα μπορούσαμε να εντάξουμε το Denial of Cooperation, μια επίθεση δηλαδή με στόχο να πλήξει την επικοινωνία μεταξύ τέτοιων συσκευών, προκαλώντας απώλειες κρίσιμης πληροφορίας η οποία θα μπορούσε να επηρεάσει τις δυνατότητες ελέγχου του συστήματος. Επιθέσεις οι οποίες επιχειρούν να διαταράξουν την ομαλή λειτουργία των FACTS, επηρεάζοντας της πληροφορίες για συγχρονισμό του εξοπλισμού αλλά και επιθέσεις τύπου False Data Injection οι οποίες εισάγουν στο δίκτυο ψευδή δεδομένα για την κατάσταση του συστήματος ή ψευδή μηνύματα ελέγχου, με κίνδυνο να επηρεάσουν την ομαλή λειτουργία του συστήματος.

Σε αυτή την ενότητα, μας δόθηκε η ευκαιρία να εξετάσουμε πολλούς από τους ενδεχόμενους κινδύνους που θα μπορούσαν να επηρεάσουν τους στόχους ασφάλειας του συστήματός μας

στα πλαίσια του Smart Grid. Ο πίνακας 4.2 αποτελεί μια συνοπτική αναφορά στα σενάρια που μελετήσαμε και στους κινδύνους που εντοπίσαμε στο κάθε ένα από αυτά.

Smart Grid Security				
Security Issue : Taking Down The Server				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
AMI HeadEnd (SCADA servers) Or DRMS/LMS server Or MDMS server (or any other server situated in the Utility side The networks to them and between them.	An adversary could deploy a variety of techniques for taking down servers situated in the Utility resulting in rolling blackouts of massive scale able to cripple a county's economy and heavily impact the quality of life of its population / if not putting it at peril risk. These sorts of attacks form a new king of terrorism and are amongst the most serious attacks that can occur in the Smart Grid	• Exploiting publicly available information • Platform configuration software vulnerabilities to gain access to the system • Denial of Service Attacks • Malware • Insider Attack	• Confidentiality • Integrity • Availability • Authenticity • Authorization	High
Security Issue: Gaining Control over the System				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
AMI HeadEnd (SCADA servers) Or DRMS/LMS server Or MDMS server (or any other server situated in the Utility side The networks to them and between them.	An adversary could deploy a variety of techniques for gaining control over the systems in the Utility side to utilize them in any way he pleases. These sorts of attacks form a new king of terrorism and are amongst the most serious attacks that can occur in the Smart Grid.	• Exploiting publicly available information weak platform configuration software vulnerabilities to gain access to the system • Malware and other • Passive Network Reconnaissance • Exploiting the control over DRMS/LMS, MDMS or AMI Head End – Fabricated Messages/Replay attacks • Fiddling with billing	• Confidentiality • Integrity • Availability • Authorization • Non repudiation • Authenticity	Moderate-High
Security Issue: Stealing corporate data(Adversaries or Rival Companies)				
Systems Involved	Description	Possible Threads	Security Goals Compromised	Degree of Impact
AMI HeadEnd (SCADA servers) Or DRMS/LMS server Or MDMS server (or any other server situated in the Utility side The networks to them and between them.	An adversary who has gained access to the system attempts to steal important data about customers or the Utility to either harm the customers somehow, or harm the Utility's reliability.	• Exploiting publicly available information and platform configuration or software vulnerabilities to gain access to the system • Malware • Insider attacks	• Confidentiality • Integrity • Availability • Authorization • Authenticity	Moderate -High
Security Issue : Interaction with Field Devices				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
Sensors/ RTUs/PMUs AVR/FACTS Governor Control	Fiddling with data collected by smart grid's field devices can result in the SCADA system getting a false impression of the grid's status thereby making the wrong decisions for its manipulation. Such attacks could also affect energy markets.	• False Data Injection Attacks • Malware	• Integrity • Availability	Moderate-High

Πίνακας 4.2 . Η παρουσίαση και αξιολόγηση των κινδύνων στο Smart Grid Περιβάλλον.

4.4 Θέματα Ασφάλειας από το Smart Home στο Smart Grid

Έχοντας πλέον αποκτήσει μια πιο σφαιρική εικόνα σε ότι αφορά στους κινδύνους που απειλούν τόσο το Smart Home όσο και το Smart Grid σαν ιδιαίτερες οντότητες, είμαστε πια έτοιμοι να εντοπίσουμε ορισμένες από τις βασικότερες απειλές που θα μπορούσαν να θέσουν ως στόχο τη μεταξύ τους αλληλεπίδραση. Η ενότητα αυτή αφιερώνεται σε απειλές που ξεκινούν επηρεάζοντας ή λαμβάνοντας τον έλεγχο οντοτήτων του Smart Home και καταλήγουν επηρεάζοντας οντότητες του Smart Grid.

4.4.1 Demand Response Σήματα στο Smart Home

Όπως είχαμε πει και στο προηγούμενο κεφάλαιο, η αλληλεπίδραση μεταξύ Energy Aware Smart Home και Smart Grid αφήνει ανοικτό το ενδεχόμενο για την υιοθέτηση προγραμμάτων Demand Response. Ας θυμηθούμε πως τα προγράμματα αυτά στηρίζουν τη λειτουργία τους στην ανταμοιβή του καταναλωτή για την προθυμία του να μειώσει το φόρτο που ο ίδιος προσθέτει στο ηλεκτρικό δίκτυο όταν αυτό του ζητηθεί. Συνήθως σε τέτοια συστήματα, τα σήματα που αποστέλλονται στον πελάτη περιλαμβάνουν μια πληροφορία που αφορά στη χρέωση της ενέργειας, η οποία μπορεί να συμβαίνει είτε με τη λογική του[76] Time of Use Pricing όπου η ενέργεια κοστολογείται με βάση τα χρονικά μπλοκ που χρησιμοποιείται και το κατά πόσο αυτά θεωρούνται ώρες αιχμής ή όχι, είτε με τη λογική του Real Time Pricing, ενός μοντέλου δυναμικής χρέωσης που δίνει την τιμή της ενέργειας ανά πάσα στιγμή, είτε με τη λογική του Critical Peak Pricing το οποίο αξιοποιείται σα μοντέλο μόνο λίγες μέρες το χρόνο όπου το Smart Grid βρίσκεται υπό ακραίες πιέσεις. Τέτοια μηνύματα φτάνουν στον καταναλωτή με τρεις τρόπους. Άμεσα, ώστε αυτός να μπορέσει να λάβει τα απαραίτητα μέτρα προκειμένου να ανταποκριθεί στους όρους της συμφωνίας που έχει συνάψει με την εταιρεία παροχής ηλεκτρικής ενέργειας, μέσω του ESI/HAN Gateway στο σπίτι του πελάτη το οποίο μπορεί να ελέγχει συσκευές κατηγορίας 3 στο πλαίσιο της συμφωνίας πελάτη-εταιρείας παροχής, ή στο ESI/HAN Gateway με στόχο να προωθηθούν προς το EMS σύστημα το οποίο αναλαμβάνει να στείλει τις κατάλληλες εντολές ελέγχου στις συσκευές/συστήματα που πρέπει.

Σε κάθε μια από τις τρεις περιπτώσεις που αναφέραμε πιο πάνω ένα σύνολο κινδύνων μπορούν να εντοπιστούν.

Σενάριο 1^{ο}

Ένα Demand Response (DR) σήμα περιλαμβάνοντας πληροφορίες που αφορούν στην τιμή της ενέργειας, το βαθμό κρισιμότητας (urgency) κτλ., παραλαμβάνεται από το ESI/HAN Gateway και προωθείται στην οθόνη αλληλεπίδρασης χρήστη (In-Home Display) προκειμένου ο χρήστης να ενημερωθεί κατάλληλα, για να ρυθμίσει τις συσκευές του[76]**.**

Σε ένα τέτοιο σενάριο είναι προφανής ο κίνδυνος αλλοίωσης του μηνύματος (αλλοίωση η οποία θα μπορούσε να σημαίνει αλλαγή του βαθμού κρισιμότητας, ή τροποποίηση της ένδειξης χρέωσης ενέργειας). Μια τέτοια αλλοίωση θα μπορούσε να πραγματοποιηθεί από έναν κακόβουλο χρήστη ο οποίος μιμούμενος το ESI/HAN Gateway (ESI/HAN Gateway Impersonation) θα μπορούσε να υποκλέπτει τα μηνύματα που αποστέλλονται προς αυτό, να τα τροποποιεί και να τα προωθεί αλλοιωμένα σε αυτό, ή να τα κατακρατά προκειμένου να τα αποστείλει σε κάποια μελλοντική χρονική στιγμή στην οποία τα μηνύματα αυτά δε θα ανταποκρίνονται πλέον στην πραγματικότητα (Replay Attack). Τέτοια φαινόμενα παραβιάζουν το στόχο που αφορά στην ακεραιότητα των δεδομένων, και το στόχο αυθεντικότητας του αποστολέα. Εξαιτίας αυτών των φαινομένων, ο πελάτης θα μπορούσε να οδηγηθεί στη λήψη λανθασμένων αποφάσεων, θέτοντας τις συσκευές του σε λειτουργία σε ώρες αιχμής όπου η ενέργεια κοστίζει πολύ περισσότερο (νομιζόμενος 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.

Άλλος ένας κίνδυνος ο οποίος θα μπορούσε να μας απασχολήσει σε ένα τέτοιο σενάριο είναι ο κίνδυνος που προκύπτει λόγω της προσπάθειας αποποίησης από πλευράς του πελάτη, της παραλαβής ενός Demand Response μηνύματος, προκειμένου να δικαιολογήσει τη μη τήρηση από πλευράς του των συμφωνηθέντων μεταξύ του και της εταιρείας παροχής ηλεκτρικής ενέργειας. Ένα τέτοιο φαινόμενο θα μπορούσε να προκύψει στην προσπάθεια του πελάτη να γλυτώσει την επιπλέον οικονομική επιβάρυνση/ κύρωση που του επιβάλλεται για τη μη τήρηση της συμφωνίας. Τέτοια φαινόμενα μπορεί να εκλάβουν νομικές διαστάσεις γι’ αυτό καλό θα ήταν τέτοιοι κίνδυνοι να αποτρέπονται.

Σενάριο 2^{ο}

Ένα Demand Response (DR) σήμα περιλαμβάνοντας πληροφορίες που αφορούν στην τιμή της ενέργειας, το βαθμό κρισιμότητας (urgency) κτλ., παραλαμβάνεται από το ESI/HAN Gateway το οποίο ακολούθως είτε το προωθεί απευθείας στα PEV/PCT/DER και τις συσκευές ώστε να ρυθμίσουν τον τρόπο λειτουργίας τους κατάλληλα, είτε το επεξεργάζεται και προωθεί στις οντότητες αυτές κατάλληλες εντολές ώστε να ρυθμίσουν τη λειτουργία τους βάσει αυτών[76]**.**

Στο σενάριο αυτό παρατηρείται και πάλι ο κίνδυνος αλλοίωσης του μηνύματος. Κίνδυνος, ο οποίος εξακολουθεί να αποτελεί απειλή για τις αρχές της ακεραιότητας των δεδομένων και της αυθεντικότητας του αποστολέα, αφού μέσω Impersonation του ESI/HAN Gateway, ο οποιοσδήποτε κακόβουλος χρήστης θα μπορούσε να υποκλέψει τα μηνύματα που παραλαμβάνονται από το ESI/HAN Gateway να τα αλλοιώσει και να τα μεταδώσει στο ESI/HAN τροποποιημένα. Τέτοιες επιθέσεις, θα μπορούσαν να οδηγήσουν το ESI/HAN Gateway στον καθορισμό έπιζήμιων προγραμμάτων λειτουργίας για τα PEV/PCT/DER και τις συσκευές τόσο για τον καταναλωτή όσο και για το Smart Grid. Αρκεί μόνο να σκεφτούμε πως ο λανθασμένος προγραμματισμός θα μπορούσε να έχει ως αποτέλεσμα συσκευές και προγραμματιζόμενοι θερμοστάτες (PCT) να ενεργοποιούνται σε ώρες αυξημένης ζήτησης και να απενεργοποιούνται σε χρονικές στιγμές που λανθασμένα ερμηνεύονται ως ώρες υπερφόρτωσης, για να αντιληφθούμε το μέγεθος της ζημίας που θα μπορούσαν να προκαλέσουν τέτοιες επιθέσεις ιδιαίτερα αν λάβουν μαζικό χαρακτήρα (π.χ. φόρτιση PEV κτλ.).

Παρόμοιου τύπου επίθεση σε ένα τέτοιο σενάριο είναι και η επίθεση του Replay Attack, της παρεμβολής δηλαδή ενός μηνύματος που προορίζεται για το ESI/HAN Gateway και της αναμετάδοσής του σε μια μελλοντική χρονική στιγμή όπου το μήνυμα αυτό δεν θα έχει καμία απολύτως υπόσταση. Τέτοιες επιθέσεις θα μπορούσαν για παράδειγμα να πραγματοποιηθούν αναμεταδίδοντας μηνύματα συγκεκριμένου βαθμού κρισιμότητας (urgency) κατά τις περιόδους που το Smart Grid δε βρίσκεται σε οποιαδήποτε κρίσιμη κατάσταση (με αποτέλεσμα το το ESI/HAN Gateway να διακόπτει λειτουργίες στα PEV/PCT/DER και τις συσκευές προκαλώντας αχρείαστη ταλαιπωρία στους καταναλωτές) ή αναμεταδίδοντας μηνύματα μικρού βαθμού κρισιμότητας σε ώρες που το Smart Grid χρειάζεται πραγματικά επιπλέον ενέργεια. Παράλληλα, τέτοιες επιθέσεις θα μπορούσαν να υλοποιηθούν εναλλάσσοντας τέτοια μηνύματα με το ρίσκο πρόκλησης βλαβών σε συσκευές

(ή και γραμμές παραγωγής σε IAN δίκτυα) λόγω της απρόσμενης διακοπής/επανέναρξης της λειτουργίας τους.

Ένα ακόμα είδος επίθεσης που θα μπορούσε να πραγματοποιηθεί στο σενάριο αυτό αφορά σε αυτό που ονομάζουμε Jamming Attack. Ένα είδος επίθεσης, το οποίο θα μπορούσε να προκύψει όταν ένας κακόβουλος χρήστης ξεκινά τη μετάδοση σημάτων στο ασύρματο μέσο με στόχο τη μείωση της ποιότητας μεταδιδόμενου σήματος ως προς το θόρυβο (SNR), ώστε να διακόψει την επικοινωνία μεταξύ ESI/HAN Gateway και PEV/PCT/DER/συσκευών . Ως αποτέλεσμα μιας τέτοιας επίθεσης το ESI/HAN Gateway θα μπορούσε να απολέσει τη δυνατότητα επικοινωνίας του με τις οντότητες αυτές γεγονός που σε καταστάσεις εκτάκτου ανάγκης θα μπορούσε να επηρεάσει σημαντικά τη διαθεσιμότητα του Smart Grid.

Σενάριο 3^{ο}

Ένα Demand Response (DR) σήμα (περιλαμβάνοντας πληροφορίες που αφορούν στην τιμή της ενέργειας, το βαθμό κρισιμότητας (urgency) κτλ.), παραλαμβάνεται από το ESI/HAN Gateway το οποίο το προωθεί προς το EMS σύστημα. Το EMS, θα ερμηνεύσει το σήμα προκειμένου να στείλει τα ανάλογα μηνύματα στις συσκευές/συστήματα που μπορεί να ελέγξει[76]**.**

Σ' ένα τέτοιο σενάριο, εμφανίζεται και πάλι ο κίνδυνος αλλοίωσης του μηνύματος, ο οποίος θα μπορούσε να προκύψει αυτή τη φορά είτε μέσω Impersonation του ESI/HAN Gateway είτε μέσω impersonation του ίδιου του EMS από έναν κακόβουλο χρήστη. Κάτι τέτοιο θα μπορούσε να συμβεί υποκλέπτοντας τα μηνύματα που αποστέλλονται με στόχο τον ένα ή τον άλλο παραλήπτη, αλλοιώνοντας τα και έπειτα προωθώντας τα εκεί που θα έπρεπε να φτάσουν. Η τροφοδότηση του EMS με λανθασμένη πληροφορία, θα μπορούσε να οδηγήσει στο λανθασμένο προγραμματισμό λειτουργίας των συσκευών/συστημάτων που βρίσκονται σε άμεση επικοινωνία με αυτό. Κάτι τέτοιο, θα μπορούσε να κλονίσει σημαντικά τις ισορροπίες του Smart Grid, ιδιαίτερα αν μαζικά συσκευές αρχίζουν να λειτουργούν/ αποφορτίζουν ενέργεια σε ώρες που το δίκτυο είναι ήδη υπερφορτωμένο κτλ..

Την ίδια στιγμή, εξίσου πιθανή είναι η απειλή ενός Jamming Attack[43], της μετάδοσης δηλαδή, αχρείαστων σημάτων στο ασύρματο μέσο από έναν κακόβουλο χρήστη με στόχο τη μείωση της ποιότητας του μεταδιδόμενου σήματος. Τέτοιες επιθέσεις θα μπορούσαν να θέσουν ως στόχο τους είτε τη διακοπή επικοινωνίας μεταξύ ESI/HAN Gateway και EMS, είτε τη διακοπή επικοινωνίας μεταξύ EMS και συστημάτων/συσκευών που συνδέονται με

αυτό. Μια τέτοια επίθεση θα μπορούσε να επηρεάσει σημαντικά τη διαθεσιμότητα του συστήματος, καθιστώντας το πολύ πιο δύσκολο να ληφθούν διορθωτικά μέτρα σε καταστάσεις έκτακτης ανάγκης· γεγονός που πολλές φορές αυξάνει το ενδεχόμενο διακοπής στην παροχή ηλεκτρικής ενέργειας. Αδυναμία επικοινωνίας με το Smart Home μπορεί να σημαίνει παράλληλα και οικονομική επιβάρυνση του πελάτη (ο οποίος μη μπορώντας να λάβει πληροφόρηση για την κατάσταση του Grid λειτουργεί στα τυφλά, θέτοντας σε λειτουργία τις συσκευές του σε ώρες αιχμής που κοστίζουν πιο ακριβά).

Ένας ακόμα κίνδυνος που θα μπορούσε να προκύψει κάτω από αυτό το σενάριο έχει να κάνει με αυτό ονομάζουμε Device Impersonation δηλαδή με την προσωποποίηση μιας συσκευής από κάποια άλλη. Μια τέτοια επίθεση θα μπορούσε να δρομολογηθεί από έναν πελάτη ο οποίος έχει υπογράψει μια συμφωνία συμμετοχής σε προγράμματα Demand Response, στην προσπάθεια του να ξεγελάσει την εταιρεία παροχής ηλεκτρικής ενέργειας. Κάνοντας ένα ηλεκτρικό βραστήρα νερού να προσποιείται ότι είναι το στεγνωτήριο, ένα μήνυμα που φθάνει από το ESI/HAN Gateway με στόχο την προσωρινή αναβολή της λειτουργίας του στεγνωτηρίου θα είχε ως αποτέλεσμα ο πελάτης να μη μπορεί να χρησιμοποιήσει τον ηλεκτρικό βραστήρα νερού για κάποιο χρονικό διάστημα. Στο διάστημα αυτό η εταιρεία παροχής ηλεκτρικής ενέργειας θεωρεί ότι ο πελάτης δε χρησιμοποιεί το στεγνωτήριο και τον ανταμείβει. Κάτι τέτοιο θα μπορούσε να προκαλέσει αστάθειες στο Smart Grid ιδιαίτερα αν το φαινόμενο αποκτήσει μαζικές διαστάσεις (λόγω της καταχώρησης λανθασμένης πληροφορίας στα συστήματα του Head End.) οι οποίες θα μπορούσαν να αναγκάσουν το Smart Grid να προβεί σε load balancing ενέργειες. Αξίζει να σημειώσουμε πως σε ένα τέτοιο σενάριο οι αστάθειες του Smart Grid φαντάζουν ανεξήγητες στους λειτουργούς του, οι οποίοι βλέπουν πως όλα συμβαίνουν όπως θα έπρεπε.

Πέραν αυτών απειλή θα μπορούσε να αποτελεί στο συγκεκριμένο σενάριο και η προσπάθεια ενός πελάτη να αρνηθεί την παραλαβή ενός DR σήματος στην προσπάθειά του να δικαιολογηθεί για την παραβίαση των όρων της συμφωνίας του με την εταιρεία παροχής, για να γλυτώσει τις κυρώσεις που συνεπάγονται της μη συμμόρφωσης του με τους όρους της συμφωνίας. Ένα τέτοιο ενδεχόμενο απειλεί την αρχή της μη αποποίησης.

4.4.2 Επιθέσεις με στόχο την επικοινωνία μεταξύ μετρητών και NAN aggregators.

Στο κεφάλαιο δύο είχαμε παρουσιάσει το Smart Meter ως μια από τις βασικές οντότητες μέσω των οποίων το σπίτι μας μπορεί να επιτύχει την αμφίδρομη επικοινωνία με το Smart Grid. Το κεφάλαιο τρία, μας παρουσίασε και το ESI/HAN Gateway. Στην πραγματικότητα,

είναι χάρη στις δύο αυτές οντότητες που το Smart Home μας καταφέρνει να βρίσκεται σε διαρκή αλληλεπίδραση με το Smart Grid. Γεγονός, που αποτελεί και τη βασικότερη εξήγηση πίσω από το ότι τα Smart Meters και το ESI/HAN Gateway είναι οι δύο πιο συχνά χρησιμοποιούμενες οντότητες στα σενάρια μας.
Πιθανές επιθέσεις που εμπλέκουν Smart Meters τις οποίες δεν έχουμε αναφέρει έως τώρα, έχουν να κάνουν με επιθέσεις τύπου Eavesdropping 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[87], όσο και την αποκάλυψη στοιχείων που αφορούν στα πρωτόκολλα επικοινωνίας μεταξύ μετρητών και NAN aggregators (δομές μηνυμάτων κτλ.) 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.

Παράλληλα, επιθέσεις που επικεντρώνονται όχι απλά στην παθητική υποκλοπή των μηνυμάτων που αποστέλλονται από τους μετρητές προς τα NAN aggregators , αλλά και στην τροποποίησή τέτοιων μηνυμάτων[88], ή την εισαγωγή άλλων ψευδών στο δίκτυο, μπορούν να λάβουν παρόμοιες διαστάσεις με αυτές που περιγράφηκαν πιο πάνω, αφού και πάλι μέσω τέτοιων επιθέσεων επίπλαστη πληροφορία φθάνει στα κεντρικά συστήματα χωρίς να αντικατοπτρίζει την πραγματική κατάσταση του δικτύου, με αποτέλεσμα λανθασμένες προβλέψεις ζήτησης, λανθασμένη αποστολή μηνυμάτων load shedding, λανθασμένες χρεώσεις κτλ..

Ένα ακόμα πιθανό είδος επίθεσης, θα μπορούσε να είναι μια Man-In-The-Middle Attack. Μια τέτοια επίθεση επιτυγχάνει να προσωποποιήσει το μετρητή στο NAN aggregator και το NAN aggregator στο μετρητή, με αποτέλεσμα η μεταξύ τους επικοινωνία να βρίσκεται εξολοκλήρου στα χέρια ενός κακόβουλου χρήστη. Τέτοιες επιθέσεις, επιτυγχάνουν και πάλι τον επηρεασμό του Smart Grid, ιδιαίτερα αν συμβαίνουν μαζικά (επηρεάζοντας πολλές γειτονιές παράλληλα).

Τέλος, μια ακόμα πιθανή επίθεση θα μπορούσε να αφορά στη χρήση παραδείγματος χάριν του Wireshark ή ενός οποιουδήποτε λογισμικού παρόμοιας λειτουργικότητας για την ανίχνευση των μοτίβων κίνησης που θεωρούνται φυσιολογικά για το δίκτυο μεταξύ μετρητών και NAN aggregators, και η αξιοποίηση σε μετέπειτα στάδιο του εργαλείου Nmap

για την εισαγωγή επιπλέον πακέτων στο δίκτυο αυτό, σε μια προσπάθεια να θέσει τον NAN aggregator εκτός διαθεσιμότητας μέσω ενός Denial of Service Attack[12]. Στο σημείο αυτό, αξίζει να σημειώσουμε πως και τα δύο παραδείγματα λογισμικού που παρουσιάσαμε πιο πάνω είναι δωρεάν διαθέσιμα στο Internet!

4.4.3 Επιθέσεις με στόχο το σύστημα ανίχνευσης και ενημέρωσης διακοπής ρεύματος.

Μια από τις ιδιαίτερα χρήσιμες ιδιότητες ενός Smart Meter έχει να κάνει με την ανίχνευση και την αναφορά στο OMS (Outage Management System) σύστημα τυχόν διακοπών στο σύστημα ηλεκτροδότησης, εντός ενός μικρού χρονικού πλαισίου από τη στιγμή της εκδήλωσής τους. Μέσω του συστήματος αυτού, η υπηρεσία αποκτά σχεδόν άμεση ενημέρωση για τυχόν βλάβες ώστε να μπορεί να αποστείλει επιτόπου προσωπικό για να χειριστεί το περιστατικό[76].

Ενδεχόμενες απειλές σε αυτή την περίπτωση θα μπορούσαν να αφορούν σε προσωποποίηση του μετρητή (Meter Impersonation) από πλευράς ενός κακόβουλου χρήστη και στην υλοποίηση ενός Replay Attack. Σε μια τέτοια περίπτωση, παλαιότερα μηνύματα-αναφορές διακοπής ρεύματος αποστέλλονται στο OMS ακόμα και όταν δεν υπάρχουν διακοπές στην υπηρεσία με αποτέλεσμα προσωπικό να αποστέλλεται σε συγκεκριμένες περιοχές χωρίς να υπάρχει πραγματική ανάγκη. Τέτοιες κακόγουστες «φάρσες» αναμφίβολα αποτελούν ταλαιπωρία για την υπηρεσία η οποία καταβάλλει κάθε προσπάθεια να εξασφαλίσει μια όσο το δυνατό καλύτερη ποιότητα υπηρεσίας για τους πελάτες της.

4.4.4 Επιθέσεις με στόχο το σύστημα επιβεβαίωσης επιτυχούς απομόνωσης δικτύου ή επιτυχούς τερματισμού των DER.

Στο ίδιο μήκος κύματος, όταν διακοπές ρεύματος αρχίζουν να επηρεάζουν διάφορα σημεία του Smart Grid, τα DER κάθε υποστατικού στην πληγείσα περιοχή πρέπει είτε να τερματίζουν τη λειτουργία τους, είτε να αρχίσουν να λειτουργούν απομονώνοντας τον εαυτό τους από το υπόλοιπο grid ώστε να συνεχίσουν να παράγουν και να διοχετεύουν ενέργεια στο δικό τους micro grid μέχρι τα πράγματα να επανέλθουν σε μια υγιή κατάσταση[73]. Και στις δύο πιο πάνω περιπτώσεις είναι ευθύνη του Smart Meter να ενημερώσει το OMS για το τι επιλέγηκε να γίνει (διακοπή ή απομόνωση) και σε ποιο βαθμό ολοκληρώθηκε με επιτυχία.

Η προσωποποίηση του μετρητή και η παραποίηση ή επανάληψη τέτοιων μηνυμάτων από έναν κακόβουλο χρήστη ο οποίος όχι μόνο παρεμβάλλεται στην επικοινωνία αλλά επίσης φροντίζει να κάνει drop τα πακέτα που στέλνει ο μετρητής προκειμένου να τα

αντικαταστήσει με δικά του, θα μπορούσε να λάβει επικίνδυνες προεκτάσεις. Η παραπληροφόρηση της υπηρεσίας για το αν έγινε τερματισμός ή islanding με επιτυχία, δίνει λανθασμένη εικόνα της κατάστασης του συστήματος στο προσωπικό που προσπαθεί να επιληφθεί του προβλήματος, θέτοντάς το ενδεχομένως σε κίνδυνο.

Σε αυτή την ενότητα, μας δόθηκε η ευκαιρία να εξετάσουμε πολλούς από τους ενδεχόμενους κινδύνους που θα μπορούσαν να επηρεάσουν τους στόχους ασφάλειας του συστήματός μας στα πλαίσια του περιβάλλοντος επικοινωνίας Smart Home προς Smart Grid. Ο πίνακας 4.3 αποτελεί μια συνοπτική αναφορά στα σενάρια που μελετήσαμε και στους κινδύνους που εντοπίσαμε στο κάθε ένα από αυτά.

Smart Home to Smart Grid				
Security Issue : Demand Response Signals from ESI/HAN to In-Home Display				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
ESI / HAN ↕ In-Home Display ↕ Customer	The DR signal containing tariff, urgency and other information is transmitted and projected on the In-Home Display. The customer decides on how to respond to the signal (switch devices on/off).	• Message Modification • Repudiation • ESI/HN Impersonation • Replay Attack	• Integrity • Non repudiation • Authenticity	Low – Moderate
Security Issue : Demand Response Signals from ESI/HAN to Appliances/PCT/PEV/DER				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
ESI / HAN ↕ PCT/Appliances/ PEV/DER	The DR signal containing tariff, urgency and other information is transmitted to ESI/HAN which then either forwards the message as such to PCTs/DERs/PEVs and appliances (so that they can determine how to respond) or processes the message to transmit more specific commands to these entities.	• Message Modification • Replay Attacks • Jamming Attacks	• Integrity of message • Availability • Authenticity	Low -High
Security Issue : Demand Response Signals from ESI/HAN to EMS				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
ESI / HAN ↕ Customer EMS ↕ Appliances/ DER/ PEV	The DR signal containing tariff, urgency and other information is transmitted to ESI/HAN which then forwards it to the EMS that interprets the message and sends (on/off/change energy level) commands to specific devices.	• Message Modification • Impersonates the ESI/HAN system • Replay Attacks • Jamming Attacks • Device Impersonation • Repudiation	• Integrity • Availability • Repudiation • Authentication	Low-High
Security Issue : Outage Detection and Reporting				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
Meter ↕ AMI Head End ↕ OMS	Smart meters are able to detect and report outages at customer side, only within a short time of their occurrence and notify the Head End OSI so that personnel can be dispatched locally to tackle the issue.	• Meter Impersonation and Replay attack • Impersonation of the Utility	• Integrity • Availability • Authenticity	Low (Personnel dispatched as part of a prank)
Security Issue : Verification of successful DER shutdown or islanding				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
Meter ↕ AMI Head End ↕ OMS	When outages affecting the Smart Grid in its entirety occur, the DER should either shut down or isolate itself from the rest of the grid, in an effort to keep supplying its micro - grid with energy. In such cases meters have to inform the Head End about the success of the islanding or shutdown operation.	• Meter Impersonation / Message Modification	• Integrity	Low-Moderate
Security Issue : Attacks aiming for the meter-NAN Aggregator communication				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
Smart Meter ↕ NAN Aggregator	Smart Meters collect consumption data & forward it to NAN	• Eavesdropping • Message Meditation • MAN in the Middle Attack	• Confidentiality • Integrity • Authenticity	Low - High

Πίνακας 4.3 . Η παρουσίαση και αξιολόγηση των κινδύνων από Smart Home σε Grid.

4.5 Θέματα Ασφάλειας από το Smart Grid στο Smart Home

Έχοντας πια εντοπίσει ορισμένες από τις αντιπροσωπευτικότερες απειλές που ξεκινούν επηρεάζοντας οντότητες του Smart Home περιβάλλοντος και εξελίσσονται επηρεάζοντας το Smart Grid, είμαστε πλέον έτοιμοι να ασχοληθούμε με μια τελευταία κατηγορία απειλών. Πρόκειται για τις απειλές οι οποίες ξεκινούν επηρεάζοντας οντότητες του Smart Grid αυτή τη φορά, και εξελίσσονται με τέτοιο τρόπο που επηρεάζουν το περιβάλλον του Smart Home.

4.5.1 Σήματα Demand Response από το DRMS/LMS προς το ESI/HAN Gateway.

Αναμφίβολα η υπηρεσία Demand Response, αποτελεί μια από τις βασικότερες για την πλήρωση πολλών από τους στόχους που έχουν τεθεί για τα Smart Grids. Στην προηγούμενη ενότητα, μας δόθηκε η ευκαιρία να μάθουμε πολλά για κινδύνους που θα μπορούσαν να επηρεάσουν αυτή την υπηρεσία από το Smart Home προς το Smart Grid. Σε αυτή την ενότητα, αναζητούμε τις απειλές στην Demand Response υπηρεσία που ξεκινούν στα πλαίσια του Smart Grid.

Μια επίθεση στο Demand Response σύστημα στα πλαίσια του Smart Grid δικτύου, θα μπορούσε να ξεκινά με πλαστοπροσωπία (Impersonation), από πλευράς του επιτιθέμενου, του DRMS συστήματος. Κάτι που θα μπορούσε να είναι το πρώτο βήμα για μια επίθεση επανάληψης παλαιότερων μηνυμάτων του DRMS (Replay Attack) τα οποία συνέλεξε ο επιτιθέμενος. Με αποτέλεσμα την πρόκληση αναστάτωσης του πελάτη, λόγω ανταπόκρισης του ESI/HAN – EMS συστήματος στα ψευδή μηνύματα με την τροποποίηση των προγραμμάτων των διάφορων συσκευών του.

Μια εξέλιξη στο σενάριο αυτό, θα μπορούσε να αφορά στην υποκλοπή και την τροποποίηση των μηνυμάτων που φεύγουν από το DRMS με στόχο το ESI/HAN Gateway των πελατών που λαμβάνουν μέρος στην υπηρεσία. Μια τέτοια επίθεση θα μπορούσε να υλοποιηθεί μεταβάλλοντας το περιεχόμενο των μηνυμάτων (είτε αυτό αφορά σε pricing signals, είτε αφορά στο βαθμό κρισιμότητας κτλ.). Τα αποτελέσματα μιας τέτοιας επίθεσης θα μπορούσαν να ποικίλουν από την απλή οικονομική επιβάρυνση των καταναλωτών που λόγω της λανθασμένης πληροφόρηση για τη χρέωση της ενέργειας θέτουν σε λειτουργία τις συσκευές τους σε ώρες αιχμής, μέχρι την πρόκληση αστάθειας στο δίκτυο σε τοπικά επίπεδα, λόγω υπερφόρτωσης (κάτι τέτοιο θα μπορούσε να συμβεί αν για παράδειγμα το σύστημα κλιματισμού ενός ουρανοξύστη έμπαινε σε λειτουργία λαμβάνοντας την εντολή ενός ESI/HAN Gateway – εξαιτίας ενός ψευδούς DR μηνύματος, σε μια ώρα αιχμής).

Ένα ακόμα είδος επίθεσης θα μπορούσε να είναι π.χ. ένα False Synchronization Attack[89]. Σε μια τέτοια επίθεση ο επιτιθέμενος παράγει λανθασμένα μηνύματα συγχρονισμού της DR υπηρεσίας με το ESI/HAN Gateway με αποτέλεσμα τα μηνύματα που καταφθάνουν να μη βρίσκουν ανταπόκριση εντός του κρίσιμου χρονικού διαστήματος που πρέπει λόγω κακού συγχρονισμού.

4.5.2 Σήματα για Direct Load Shedding από το LMS προς το ESI/HAN

Σε περιπτώσεις έκτακτης ανάγκης για το Grid, όπου η ζήτηση και ο φόρτος του υπερβαίνουν τα προβλεπόμενα όρια, κρίνεται απαραίτητο, προκειμένου να προστατέψουμε τον εξοπλισμό του Smart Grid και να αποφύγουμε την κατάρρευσή του και τα rolling-blackouts που αυτή συνεπάγεται, να βρούμε τρόπους μείωσης της ζήτησης και περιορισμού του φορτίου. Μια λύση σε τέτοιες περιπτώσεις είναι να τεθούν σε εφαρμογή συμφωνίες μεταξύ υπηρεσιών και πελατών για Load Shedding συσκευών της τρίτης κατηγορίας. Κάτι τέτοιο συνεπάγεται την αποστολή κατάλληλων μηνυμάτων από το LMS στο ESI/HAN Gateway, τα οποία θα μπορούσαν μεταξύ άλλων να περιέχουν εντολές απομακρυσμένης απενεργοποίησης συσκευών[73].

Κάτω από ένα τέτοιο σενάριο, πολλοί είναι οι κίνδυνοι που μπορούν να εντοπιστούν. Μεταξύ αυτών, ο κίνδυνος για επιθέσεις τύπου Denial of Service οι οποίες θα μπορούσαν να προκληθούν, λόγου χάριν μέσω Jamming στο μέσο που αξιοποιεί το LMS ή μέσω επιθέσεων που έχουν ως στόχο τον ίδιο τον LMS server. Τέτοιες επιθέσεις θα μπορούσαν να καταστήσουν αδύνατη την επικοινωνία μεταξύ του LMS και του ESI/HAN Gateway, με αποτέλεσμα να καθίσταται πολύ πιο δύσκολο έως και ακατόρθωτο τα μηνύματα για Load Shedding να φτάσουν στα υποστατικά έγκαιρα, προκειμένου να προλάβουμε τη μαζική κατάρρευση του δικτύου και το κόστος που κάτι τέτοιο συνεπάγεται τόσο σε κοινωνικό όσο και σε οικονομικό επίπεδο.

Ανάμεσα στην πληθώρα των δεδομένων που αποθηκεύονται πάνω σε έναν DRMS/LMS server, ανήκουν και τα δεδομένα που αφορούν στον προγραμματισμό των Load Shedding περιστατικών. Όπως είχαμε αναφέρει και στην προηγούμενη ενότητα, το Load Shedding δε συμβαίνει πάντα στις ίδιες περιοχές ή πάντα με την ίδια σειρά στο σύνολο των περιοχών που συμμετέχουν, κυρίως για λόγους μικρότερης ταλαιπωρίας των πελατών που συμμετέχουν στα προγράμματα Demand Response. Βέβαια, δεν έχουν όλες οι περιοχές τον ίδιο βαθμό σπουδαιότητας. Αυτό που συμβαίνει στην πραγματικότητα, είναι πως ένα πρόγραμμα Load Shedding δεν εκδηλώνεται σε όλες τις περιοχές ανεξαιρέτου, εκ περιτροπής· ακριβώς λόγω

της κρισιμότητας των εγκαταστάσεων σε συγκεκριμένες περιοχές (νοσοκομεία, υδατοπρομήθειες κτλ.). Σε αυτές τις περιοχές, καταφεύγουμε σε Load Shedding μόνο την υστάτη αφού πρώτα έχουμε εξαντλήσει κάθε πιθανή προσπάθεια να αποφύγουμε κάτι τέτοιο. Πάνω σε αυτή τη βάση, θα μπορούσαμε λοιπόν να εντοπίσουμε έναν ακόμα κίνδυνο. Τον κίνδυνο που προκύπτει όταν ένας κακόβουλος χρήστης καταφέρει να αποκτήσει πρόσβαση στα αρχεία του DRMS/LMS server που αφορούν σε αυτά τα προγράμματα προτεραιότητας, τροποποιώντας τα στοιχεία τους κατά βούληση. Σε μια τέτοια περίπτωση, τα ενδεχόμενα αποτελέσματα θα μπορούσαν να ξεκινούν από την απλή ταλαιπωρία των ίδιων πελατών για διαδοχικά περιστατικά, μέχρι την πρόκληση διακοπής ρεύματος σε περιοχές κρίσιμης σημασίας η οποία θα μπορούσε να προκαλέσει πολύ σοβαρότερα προβλήματα στον ανθρώπινο παράγοντα.

Πέραν των πιο πάνω, εξίσου πιθανές σε μια τέτοια περίπτωση είναι επιθέσεις της μορφής False Synchronization οι οποίες θα μπορούσαν να ξεκινούν από την αποστολή ανακριβών μηνυμάτων συγχρονισμού συστημάτων μεταξύ DRMS/LMS και ESI/HAN με αποτέλεσμα το Load Shedding να προκύπτει νωρίτερα/αργότερα απ' ότι θα έπρεπε.

Παράλληλα, άλλες ενδεχόμενες επιθέσεις θα μπορούσαν να πάρουν τη μορφή Replay Attack όπου ο επιτιθέμενος υποκλέπτει τα μηνύματα του DRMS/LMS προς το ESI/HAN Gateway. Σε τέτοιες περιπτώσεις, ο επιτιθέμενος θα μπορούσε να αξιοποιήσει τα μηνύματα αυτά, επαναλαμβάνοντάς τα σε ώρες που δεν ανταποκρίνονται σε πραγματική ανάγκη του Grid για Load Shedding, με αποτέλεσμα να προκαλείται ταλαιπωρία στους πελάτες οι οποίοι δε μπορούν να λειτουργήσουν τις συσκευές τους, χωρίς αυτό να εξυπηρετεί κανέναν.

4.5.3 Επιθέσεις με στόχο τις απευθείας εντολές ελέγχου του DRMS/LMS προς τα DER για ενίσχυση του Grid με ενέργεια/ ή απορρόφηση ενέργειας από αυτό.

Όπως έχουμε ήδη πει, ανάμεσα στα βασικότερα χαρακτηριστικά που διαθέτει το Smart Grid είναι η δυνατότητα που παρέχεται στον καταναλωτή να λαμβάνει και ο ίδιος μέρος στην όλη διαδικασία διαχείρισης ενέργειας, μέσω των συστημάτων DER που διαθέτει. Τέτοια συστήματα, συνήθως ελέγχονται όχι από τον ίδιο τον πελάτη αλλά από έναν ESP με τον οποίο ο πελάτης συνάπτει συμφωνία. Μια ενδεχόμενη επίθεση σε τέτοια συστήματα θα μπορούσε να αφορά στην υποκλοπή και την επανάληψη των μηνυμάτων ενίσχυσης/απορρόφησης ενέργειας[76], από έναν επιτιθέμενο με στόχο την πρόκληση ζημιάς στο Smart Grid. Η ζημιά αυτή θα μπορούσε να προκληθεί στέλνοντας για παράδειγμα στα DER, μηνύματα αποφόρτισης ενέργειας στο Smart Grid σε στιγμές που το Smart Grid

βρίσκεται ήδη σε οριακά σημεία, με αποτέλεσμα την κατάρρευσή του και ενδεχομένως την πρόκληση ζημιάς σε εξοπλισμό του, που θα μπορούσε να οδηγήσει υποσταθμούς στο να τερματίσουν τη λειτουργία τους λόγω αδυναμίας να ανταπεξέλθουν στη ζήτηση.

Επίσης ενδεχόμενη επίθεση στο σύστημα, είναι η επίθεση του Message Modification στην οποία ο επιτιθέμενος παρεμβάλλεται στην επικοινωνία DRMS/LMS και DER τροποποιώντας τα μηνύματα που το DRMS/LMS αποστέλλει στον πελάτη, αυξάνοντας π.χ. το ποσοστό ενέργειας που ζητείται να δοθεί στο Grid/ ή μειώνοντας το ποσοστό που πρέπει να απορροφηθεί από αυτό, με αποτέλεσμα τη συμμετοχή των πελατών στη διαδικασία διαχείρισης με μη αναμενόμενο τρόπο. Κάτι τέτοιο θα μπορούσε να επηρεάσει σε μεγάλο βαθμό το Grid, προκαλώντας brownouts/blackouts σε διάφορες περιοχές.

Ένα ακόμα είδος επίθεσης κάτω από τέτοια σενάρια, θα μπορούσε να έχει να κάνει με το Denial of Service attack το οποίο θα μπορούσε είτε να επηρεάσει το σύστημα του πελάτη είτε το σύστημα DRMS/LMS, είτε το κανάλι επικοινωνίας μεταξύ τους, καθιστώντας αδύνατη την επικοινωνία μεταξύ των δύο οντοτήτων, με αποτέλεσμα την αποτροπή του Smart Grid από το να πραγματώσει έναν από τους σημαντικότερους στόχους του το self-healing.

4.5.4 Επιθέσεις κατά των μηνυμάτων ενεργειακής κατανάλωσης ενός πελάτη που μεταφέρονται από έναν κεντρικό σε έναν άλλο ESP.

Με την εξουσιοδότηση του πελάτη, όπως αναφέραμε και σε προηγούμενη ενότητα, ένας δεύτερος ESP διαθέτει το δικαίωμα να λαμβάνει και αυτός τα δεδομένα που αφορούν στην ενεργειακή κατανάλωση ενός πελάτη. Οι κίνδυνοι που προκύπτουν κάτω από τέτοιας φύσης σενάρια, επηρεάζουν σε σημαντικό βαθμό τους στόχους της ακεραιότητας και της εμπιστευτικότητας των πληροφοριών[76].

Ένας κίνδυνος ο οποίος θα μπορούσε να υποσκελίσει την ακεραιότητα των δεδομένων / οντοτήτων στο σύστημα θα μπορούσε να αφορά στην πλαστοπροσωπία από πλευράς ενός επιτιθέμενου, του δεύτερου ESP. Κάτι τέτοιο θα μπορούσε να έχει ως αποτέλεσμα την παραλαβή από πλευράς του επιτιθέμενου των μηνυμάτων εκείνων που αφορούν στην ενεργειακή κατανάλωση του πελάτη και στάλθηκαν προς τον δεύτερο ESP, γεγονός το οποίο όπως ήδη γνωρίζουμε συνιστά παραβίαση της ιδιωτικότητας του αφού τα δεδομένα αυτά, ακόμα και τα ανώνυμης φύσεως μπορούν μετά από κατάλληλη επεξεργασία, να αποκαλύψουν πολλές πληροφορίες για τις συνήθειες και τον τρόπο ζωής διαφόρων ατόμων.

Στο σημείο αυτό αξίζει να σημειώσουμε το εξής : Τέτοιου τύπου επιθέσεις θα μπορούσαν να υποκινούνται από μια πληθώρα οργανισμών για τους οποίους η πληροφορία αυτή είναι καίριας σημασίας (π.χ. ασφαλιστικές εταιρείες οι οποίες μπορούν να εξάγουν στοιχεία για τυχόν προβλήματα υγείας των ενοίκων σε ένα υποστατικό, εταιρείες marketing για σκοπούς έρευνας των συνηθειών των καταναλωτών ώστε οι διαφημίσεις να γίνονται πιο στοχευμένες, ιδιωτικοί ντετέκτιβ και μυστικές υπηρεσίες για την παρακολούθηση ύποπτων ατόμων, ακόμα και δημοσιογράφοι σκανδαλοθηρικού τύπου για την εξαγωγή των συνηθειών δημόσιων προσώπων!)[73].

Σε μια μικρή παραλλαγή της πιο πάνω δραστηριότητας, ένας κακόβουλος χρήστης θα μπορούσε να στοχεύσει στην υποκλοπή του περιεχομένου (με τρόπο που να μη γίνεται αντιληπτός από κανένα από τα δύο μέρη που επικοινωνούν). Επιθέσεις τύπου Eavesdropping, πάλι αφήνουν περιθώριο στον επιτιθέμενο να εξάγει χρήσιμη πληροφορία για τον πελάτη, αφού λαμβάνει περιοδικά, μηνύματα που περιγράφουν τα μοτίβα κατανάλωσής του, τα οποία εν μέρει αποκαλύπτουν συνήθειες και συμπεριφορές.

Σε αυτή την ενότητα, μας δόθηκε η ευκαιρία να εξετάσουμε πολλούς από τους ενδεχόμενους κινδύνους που θα μπορούσαν να επηρεάσουν τους στόχους ασφάλειας του συστήματός μας στα πλαίσια του περιβάλλοντος επικοινωνίας Smart Grid προς Smart Home. Ο πίνακας 4.4 αποτελεί μια συνοπτική αναφορά στα σενάρια που μελετήσαμε και στους κινδύνους που εντοπίσαμε στο κάθε ένα από αυτά.

Smart Grid to Smart Home				
Security Issue : Demand Response Signals from Utility to Customers				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
DRMS/LMS ↕ AMI Head End ↕ ESI/HAN	A DR signal containing tariff and urgency information is sent to a consumer or a group of consumers	• Message Modification • Impersonation of DRMS/LMS • Replay of Previous Messages • False Synchronization Attack	• Integrity • Authenticity	Low – Moderate
Security Issue : Direct Load Shedding				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
DRMS/LMS ↕ AMI Head End ↕ ESI/HAN ↕ Customer EMS/Appliances/ PEV	The DRMS/LMS uses a command that shuts down all controllable devices (which could potentially mean remotely disconnecting the meter as well)	• Denial of Service attacks • Access the DRMs/LMS server • False synchronization attack • Replay attack	• Availability • Integrity • Non repudiation • Authenticity	Moderate - High
Security Issue : Direct Control of DER Generation Levels/ Storage Levels				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
DRMS/LMS ↕ AMI Head End ↕ ESI/HAN ↕ Customer EMS→DER, PEV	Such messages are usually of the form of import/export energy commands that if propagated during wrong times can cause higher load/ strain on the grid (storage is usually used for load shifting whilst export needs to be used on times of increased demand).	• Replay attack • Message Modification Attack • Denial of Service attacks	• Integrity • Availability • Authenticity	Moderate-High
Security Issue : Customer Authorization for Usage of his Data from Retail Energy Service Provider				
Systems Involved	Description	Possible Threats	Security Goals Compromised	Degree of Impact
Customer ↕ CIS ↕ MDMS ↕ Aggregator/ESP	Customer wishes to authorize the transfer of his private energy-consumption-related data from Utilities to third party ESPs as part of an agreement he forms with the ESP for the direct control of his appliances and equipment.	• Aggregator/ESP Impersonation • Eavesdropping	• Integrity • Authenticity • Confidentiality	Low - Moderate

Πίνακας 4.4 . Η παρουσίαση και αξιολόγηση των κινδύνων από Smart Grid σε Home.

Κεφάλαιο 5

Smart Home/Smart Grid Security Countermeasures

5.1 Ασφαλίζοντας το Smart Home /Smart Grid περιβάλλον

Το προηγούμενο κεφάλαιο αποτέλεσε την πρώτη μας γνωριμία με θέματα ασφάλειας στο Smart Home/Smart Grid περιβάλλον. Μέσα από αυτό γνωρίσαμε τους στόχους ασφάλειας που καλείται να πληροί το Smart Home/Smart Grid και εντοπίσαμε πώς αυτοί οι στόχοι θα μπορούσαν να παραβιαστούν, κάτω από διάφορα σενάρια αλληλεπίδρασης των οντοτήτων τους αξιολογώντας παράλληλα, τις συνέπειες σε ολόκληρο το Smart Home/Smart Grid.

Στο κεφάλαιο αυτό, επικεντρωνόμαστε σε πρακτικές με τις οποίες μπορούμε να πετύχουμε τους στόχους ασφάλειας στο Smart Home/Smart Grid περιβάλλον, διασφαλίζοντας την εύρυθμη και αποδοτική λειτουργία του. Στόχος μας είναι, να παρουσιάσουμε τις επικρατέστερες πρακτικές και ορισμένες από τις πιο αντιπροσωπευτικές ιδέες που προτάθηκαν μέσα από άρθρα των τελευταίων χρόνων με στόχο την εξασφάλιση της Εμπιστευτικότητας, Ακεραιότητας, Αυθεντικοποίησης, Μη Αποποίησης Ευθύνης, Διαθεσιμότητας και Εξουσιοδότησης στο πλαίσιο του Smart Home/Smart Grid.

5.1.1 Ασφαλίζοντας ένα δίκτυο διαφορετικό από όσα έχουμε συνηθίσει

Το να εγγυηθεί κανείς ασφάλεια σ’ ένα δίκτυο τόσο μεγάλο και ετερογενές όσο το Smart Grid είναι προφανώς ένα δύσκολο και απαιτητικό έργο. Οι τεχνολογίες του Smart Grid έρχονται να εισάγουν εκατομμύρια νέων έξυπνων συσκευών στο υφιστάμενο δίκτυο ηλεκτροδότησης. Συσκευές, οι οποίες θα επικοινωνούν κατά τρόπους πολύ πιο εξελιγμένους από ό,τι έχουμε συνηθίσει. Για πρώτη φορά στην ιστορία των δικτύων ηλεκτροδότησης μιλάμε για επικοινωνία διπλής κατεύθυνσης, κατανεμημένο έλεγχο σε όλα τα συστατικά στοιχεία του Smart Grid και δυναμική ενημέρωση των ενδιαφερόμενων μελών για την κατάσταση του συστήματος ανά πάσα στιγμή [90]. Όλες αυτές οι εξελίξεις προφανώς δίνουν

στο Smart Grid τη δυνατότητα υποστήριξης πληθώρας νέων λειτουργιών, εντείνουν ωστόσο την ανάγκη για προστασία του.

Η προηγούμενη εμπειρία μας σε σύνθετα δίκτυα αφορά κυρίως πληροφορικά δίκτυα, όπως για παράδειγμα το Διαδίκτυο. Τέτοια δίκτυα παρουσιάζουν προφανώς ομοιότητες με το Smart Grid αφού αποτελούν τμήμα του, εντούτοις οι μέθοδοι ασφάλειας που εφαρμόζονται σε αυτά, σε πολλές περιπτώσεις δε μπορούν να εφαρμοστούν αμετάβλητες σε ολόκληρο το Smart Grid. Ο λόγος, είναι ότι το Smart Grid διαφέρει σε πολλά από ένα τυπικό πληροφορικό δίκτυο με ορισμένες από τις τυπικότερες διαφορές να φαίνονται πιο κάτω [91]:

- **Διαφορά στο τι θεωρούμε σημαντικό να ασφαλίσουμε.** Στα τυπικά δίκτυα, η προσοχή μας επικεντρώνεται κυρίως στη διαφύλαξη της ασφάλειας στο κέντρο του δικτύου παρά στα άκρα, ενώ στα Smart Grids επιδιώκουμε την ασφάλεια τόσο στα άκρα όσο και στο κέντρο του δικτύου.
- **Διαφορά στους τύπους πρωτοκόλλων που αξιοποιούνται.** Στο Smart Grid δε χρησιμοποιούνται πάντα πρωτόκολλα τα οποία συνάδουν με ανοικτά πρότυπα όπως συμβαίνει στα τυπικά δίκτυα. Στο Smart Grid η καθυστέρηση δημιουργίας ενός ολοκληρωμένου προτύπου αρχιτεκτονικής και ασφάλειας άφησε περιθώριο ανάπτυξης ιδιωτικών πρωτοκόλλων τα οποία δεν αποκλείεται να συνεχίσουν να χρησιμοποιούνται.
- **Διαφορά στον ορισμό της ποιότητας υπηρεσίας.** Οι δύο τύποι δικτύων ορίζουν διαφορετικά και την ποιότητα υπηρεσίας (QoS). Για παράδειγμα σ' ένα τυπικό δίκτυο το rebooting θεωρείται αποδεκτό για να ολοκληρωθεί μια ενημέρωση. Στο Smart Grid από την άλλη, κανένας λόγος δε μπορεί να δικαιολογήσει τη μη διαθεσιμότητα του συστήματος έστω και για λίγο. Ενώ επίσης, το Smart Grid θέτει σοβαρότερους χρονικούς περιορισμούς απ' ότι το διαδίκτυο σε πολλές περιπτώσεις.

Στην πραγματικότητα οι διαφορές μεταξύ των Smart Home και Smart Grid είναι πολύ περισσότερες από αυτές που μόλις εντοπίσαμε, εντούτοις ακόμη και αυτές είναι υπεραρκετές για να μας καταδείξουν από τη μια την ανάγκη για αναπροσαρμογή των υφιστάμενων μηχανισμών ασφάλειας που δε συνάδουν με τις ιδιαίτερες απαιτήσεις των Smart Grids και από την άλλη την ανάγκη για δημιουργία νέων μηχανισμών εκεί όπου οι υφιστάμενοι υστερούν.

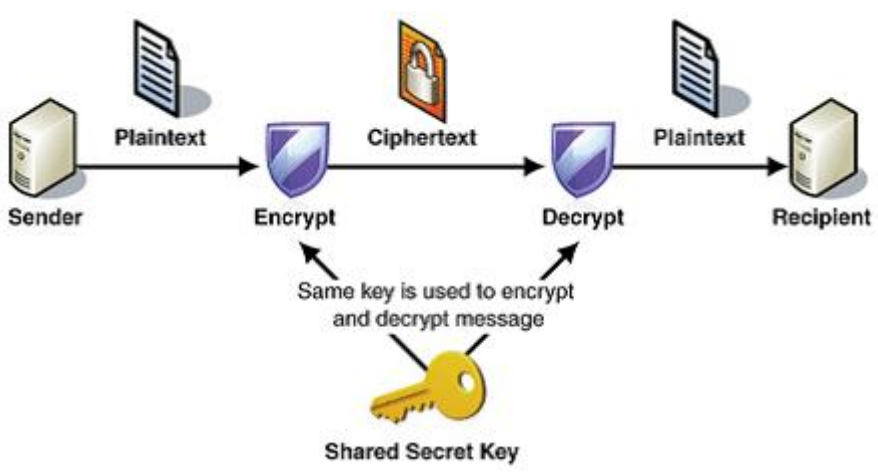
Η αναπροσαρμογή υφιστάμενων ή η ανάπτυξη νέων μηχανισμών ασφάλειας για το Smart Grid είναι βέβαια μια άλλη ιστορία στην οποία καθοριστικό ρόλο διαδραματίζουν οι περιορισμοί που θέτει από τη φύση του το ίδιο το Smart Grid. Ανάμεσα σε αυτούς, ο περιορισμός που θέλει τους μηχανισμούς ασφάλειας να μπορούν να εγκατασταθούν ακόμα και σε συσκευές που διαθέτουν περιορισμένη μνήμη και επεξεργαστική ισχύ (sensors, PMUs, Smart Meters κτλ.), χωρίς να επηρεάζεται η επίδοσή του συστήματος η οποία είναι κρίσιμη για τη λειτουργία του. Όπως επίσης και ο περιορισμός που επιβάλλει ότι τα πρωτόκολλα ασφάλειας που θα αξιοποιεί το Smart Grid πρέπει να είναι ευέλικτα και ευπροσάρμοστα σε αλλαγές με τη λογική πως ο εξοπλισμός δε θα αλλάζει κάθε 2-3 χρόνια (όπως στα πληροφορικά συστήματα) αλλά τουλάχιστον κάθε 10 χρόνια[91][73].

5.2 Εξασφαλίζοντας Εμπιστευτικότητα

Στο προηγούμενο κεφάλαιο παρουσιάσαμε για πρώτη φορά την έννοια του Confidentiality ως τη διαβεβαίωση πως μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση σε ευαίσθητες πληροφορίες. Σε αυτή την ενότητα, παρουσιάζουμε τρόπους με τους οποίους μπορούμε να επιτύχουμε αυτό τον στόχο, διασφαλίζοντας παράλληλα και την ιδιωτικότητα των μηνυμάτων μας.

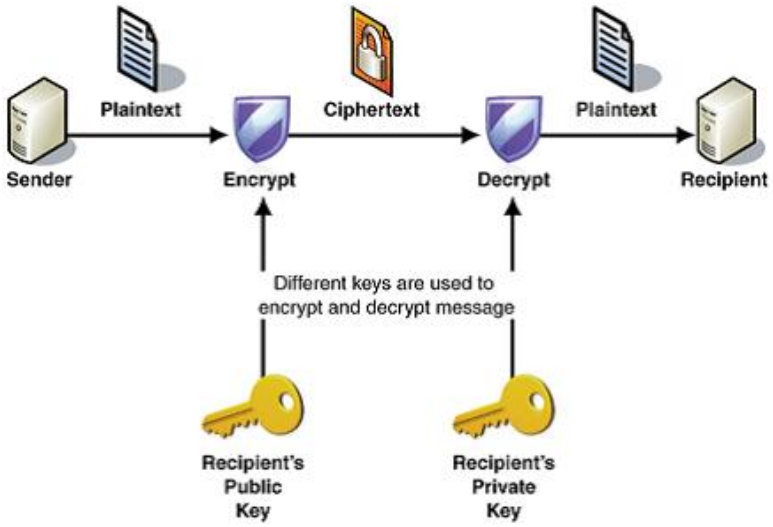
5.2.1 Εξασφαλίζοντας εμπιστευτικότητα μέσω κρυπτογράφησης

Η κρυπτογράφηση είναι ίσως μια από τις ισχυρότερες τεχνικές που διαθέτουμε σήμερα στα χέρια μας για την εξασφάλιση εμπιστευτικότητας, αυθεντικοποίησης και μη αποποίησης. Μέσα από την κρυπτογράφηση ενός μηνύματος επιτυγχάνουμε στην ουσία το μετασχηματισμό του μηνύματος αυτού από έναν αλγόριθμο, σε μια ακατανόητη μορφή, με τρόπο τέτοιο ώστε το μήνυμα να μπορεί να αποκτήσει την αρχική του μορφή μονάχα αφού φτάσει στον νόμιμο παραλήπτη του, ο οποίος είναι ο μόνος που μπορεί να το αποκρυπτογραφήσει. Οι κρυπτογραφικοί αλγόριθμοι κατηγοριοποιούνται ως προς το είδος του κλειδιού που αξιοποιούν σε συμμετρικούς και ασύμμετρους.



Σχεδιάγραμμα 5.1 Σχηματική απεικόνιση συμμετρικής κρυπτογράφησης

- Συμμετρικοί (Σχεδιάγραμμα 5.1) καλούνται οι αλγόριθμοι κρυπτογράφησης στους οποίους ένα κλειδί, κρυφό αλλά κοινό, αξιοποιείται από τα δύο μέρη που εμπλέκονται στην επικοινωνία, τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση της πληροφορίας. Σε αυτή την κατηγορία, ανήκουν τόσο Block Ciphers (αλγόριθμοι δηλαδή που λαμβάνουν το plaintext σε τμήματα και εφαρμόζουν κρυπτογράφηση σε κάθε ένα από αυτά) όσο και Stream Ciphers (οι οποίοι κρυπτογραφούν μια ροή από δεδομένα ένα bit/byte κάθε φορά). Τρόποι με τους οποίους μπορούμε να αξιοποιήσουμε έναν block cipher ως stream cipher υπάρχουν πολλοί, μερικοί εκ των οποίων οι OFB, CFB, CTR, ECB κτλ.. Γνωστοί αλγόριθμοι σε αυτή την κατηγορία είναι οι DES, TDES και AES περισσότερες πληροφορίες για τους οποίους μπορεί κανείς εύκολα να βρει σε ένα οποιοδήποτε εισαγωγικό βιβλίο σε θέματα κρυπτογραφίας. Οι συμμετρικοί αλγόριθμοι χρησιμοποιούνται κυρίως για σκοπούς εξασφάλισης της εμπιστευτικότητας της πληροφορίας[92][93].



Σχεδιάγραμμα 5.2 Σχηματική απεικόνιση ασύμμετρης κρυπτογράφησης

- Ασύμμετροι (Σχεδιάγραμμα 5.2), καλούνται οι αλγόριθμοι κρυπτογράφησης στους οποίους κάθε ένα από τα εμπλεκόμενα μέρη διαθέτει ένα ζεύγος κλειδιών το οποίο αποτελείται από ένα δημόσιο (γνωστό σε όλους) κλειδί και ένα ιδιωτικό κλειδί (μοναδικό και γνωστό μόνο στην οντότητα στην οποία ανήκει). Σε αυτή την κατηγορία αλγορίθμων η κρυπτογράφηση ενός μηνύματος γίνεται με τη χρήση του δημόσιου κλειδιού του παραλήπτη έτσι ώστε μόνο ο παραλήπτης να μπορεί με το ιδιωτικό κλειδί του να έχει πρόσβαση στα περιεχόμενα του μηνύματος. Σε αυτή την κατηγορία αλγορίθμων συναντάμε αλγόριθμους όπως τον RSA ο οποίος βασίζεται στη μαθηματική πολυπλοκότητα που εμπλέκεται στην παραγοντοποίηση μεγάλων

αριθμών. Αυτή η κατηγορία αλγορίθμων παρόλο που μπορεί να εξασφαλίσει την εμπιστευτικότητα της μεταφερόμενης πληροφορίας, τείνει να χρησιμοποιείται περισσότερο για την εξασφάλιση αυθεντικοποίησης, μη αποποίησης και ακεραιότητας δεδομένων[92], [93]. Περισσότερα για το πώς κάτι τέτοιο μπορεί να επιτευχθεί θα παρουσιάσουμε τόσο στην ενότητα που αφιερώνουμε στην ακεραιότητα των δεδομένων όσο και στην ενότητα που αφορά στην αυθεντικοποίηση.

Μέσα στο πλαίσιο της γενικότερης προσπάθειας για εξασφάλιση όσο το δυνατό μεγαλύτερης διαλειτουργικότητας μεταξύ των μηχανισμών ασφάλειας όλων των εμπλεκόμενων φορέων του Smart Grid, το Cyber Security Work Group(CSWG) το οποίο συστάθηκε από το National Institute of Standards (NIST) των ΗΠΑ, αξιολόγησε το 2010 τη χρηστότητα και το προσδόκιμο ζωής, μέσα στο πλαίσιο του Smart Grid, πολλών αλγορίθμων που χρησιμοποιούνται ευρύτατα σήμερα για σκοπούς ασφάλειας. Στο πλαίσιο της διαδικασίας αυτής[72] αξιολογήθηκαν και αλγόριθμοι κρυπτογράφησης, με τους συμμετρικούς που παρουσιάζονται στον πίνακα 5.1 να εμφανίζονται ως η επικρατέστερη λύση για την κρυπτογράφηση μηνυμάτων και τους ασύμμετρους στον πίνακα 5.3 να προτείνονται για σκοπούς ψηφιακής υπογραφής του μηνύματος κάτι για το οποίο θα μιλήσουμε περισσότερο στην ενότητα που αφορά στην αυθεντικοποίηση. Οι πίνακες αυτοί, παρατίθενται αυτούσιοι από το [72].

Algorithm	**Algorithms/Key Lengths for use between 2011-2029**	**Algorithms/Key Lengths for use now and beyond 2030**
Advanced Encryption Standard (AES)	All algorithms/key lengths listed in the next column are Approved during this time.	AES-128,AES-192, and AES-256
Triple-Data Encryption Algorithm(TDEA) or Triple-Data-Encryption-Standard (Triple-DES or TDES)	3-key TDES (Note: 2-key TDES has 80 bits of security strength. All new implementations should have 112 bits of security strength or higher.)	N/A-cannot use TDES beyond 2030 (Note: 2-key TDES and 3-key TDES are not Approved because they have<128 bits of security.)

Πίνακας 5.1 Εγκεκριμένοι Συμμετρικοί Αλγόριθμοι.

5.2.2 Θέματα Διαχείρισης Κλειδιών

Συμμετρική ή Ασύμμετρη η κρυπτογράφηση προϋποθέτει την ύπαρξη ενός τρόπου με τον οποίο τόσο αποστολέας όσο και ο παραλήπτης θα συμφωνούν στο κλειδί ή στα κλειδιά που

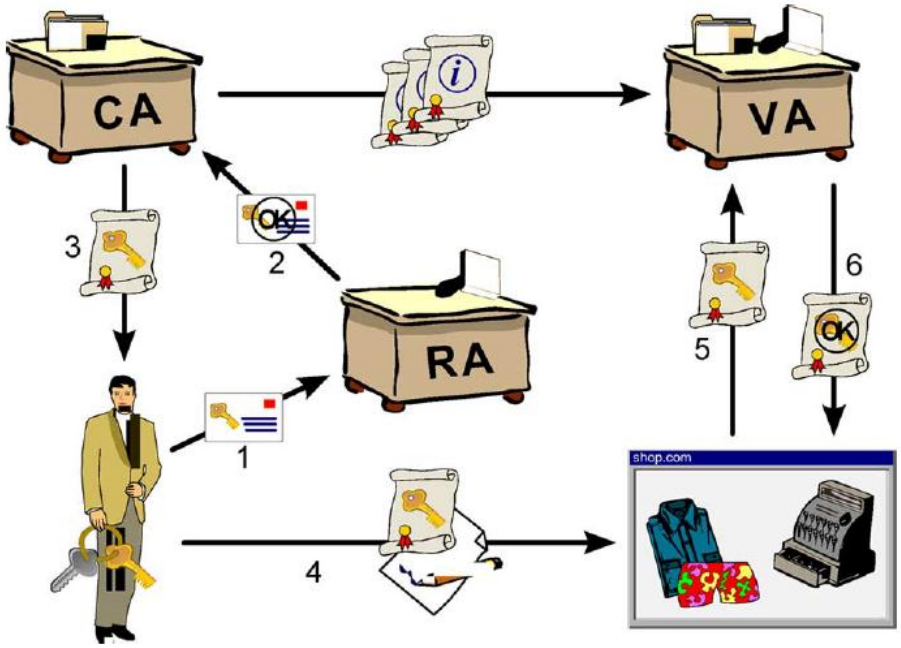
θα χρησιμοποιούν για τη μεταξύ τους επικοινωνία. Κακή διαχείριση κλειδιών, μπορεί να έχει ως αποτέλεσμα τη διαρροή τους ή στοιχείων που μπορούν να οδηγήσουν σε αυτά, υποσκελίζοντας τους στόχους ασφάλειας του Smart Grid[95]. Αυτός ακριβώς είναι και ο λόγος που η σωστή διαχείριση κλειδιών, θεωρείται κρίσιμης σημασίας για το Smart Grid.

Όλα τα πρωτόκολλα ασφάλειας που υπάρχουν σήμερα, στηρίζονται πάνω στην ύπαρξη μιας συσχέτισης ασφάλειας (Security Association – SA) μεταξύ αποστολέα και παραλήπτη, η οποία παρέχει υπηρεσίες ασφάλειας για τις πληροφορίες που διακινούνται πάνω από αυτή [96]. Για τη δημιουργία μιας τέτοιας συσχέτισης απαραίτητη προϋπόθεση είναι τουλάχιστον ένα από τα δύο εμπλεκόμενα μέρη στην επικοινωνία να κατέχει κάποιας μορφής αναγνωριστικό το οποίο να μπορεί να επιβεβαιώσει την ταυτότητά του στις υπόλοιπες οντότητες. Τα αναγνωριστικά αυτά μπορούν να είναι είτε μυστικά κλειδιά τα οποία διαμοιράζονται μεταξύ τους κάποιες οντότητες (secret keys) είτε πιστοποιητικά δημόσιου κλειδιού τα οποία χρησιμοποιούνται για να συνδέσουν χρήστες ή συσκευές σε ένα δημόσιο κλειδί μέσω ενός συστήματος πιστοποίησης όπως π.χ. το PKI(Public Key Infrastructure)[73].

Οι διαδικασίες διαχείρισης κλειδιών που αξιοποιούμε σήμερα μπορούν να διαχωριστούν σε τρείς ξεχωριστές κατηγορίες όπως παρουσιάζονται πιο κάτω :

- **Symmetric Key Management Schemes:** Η διαχείριση κλειδιών στην κατηγορία αυτή επιτυγχάνεται μέσω συμμετρικής κρυπτογράφησης, και αναλαμβάνει την παραγωγή, διανομή, αποθήκευση και ενημέρωση του κλειδιού. Η συγκεκριμένη μέθοδος θεωρείται συνήθως ιδιαίτερα ακριβή και επιρρεπής σε διάφορους κινδύνους. Οι κίνδυνοι αυτοί απορρέουν ουσιωδώς από το γεγονός ότι το κλειδί σε τέτοιες διαδικασίες παράγεται κάπου και πρέπει να μεταφερθεί σε τουλάχιστον μια άλλη οντότητα γεγονός που απαιτεί περισσότερο συντονισμό και επικοινωνία μεταξύ των οντοτήτων που επιθυμούν να επικοινωνήσουν. Φυσικά υπάρχουν και λύσεις βασισμένες στο υλικό οι οποίες θα μπορούσαν να αξιοποιηθούν εντούτοις το κόστος που συνεπάγονται τις καθιστά απαγορευτικές για μικρότερης εμβέλειας συστήματα. Παράλληλα, τεχνικές ανάλογες με αυτές που αξιοποιούνται στο Kerberos ενώ μπορούν να μας απαλλάξουν από το κόστος της όλης διαδικασίας, εντούτοις δε μπορούν να μας παρέχουν τη διαθεσιμότητα που χρειαζόμαστε σε περιπτώσεις όπου δεν είναι δυνατή η επικοινωνία με το Key Distribution Centre[73].
- **Certificate – based Public Key Schemes :** Η διαχείριση κλειδιού στην κατηγορία αυτή επιτυγχάνεται με την αξιοποίηση ψηφιακών πιστοποιητικών, μια λύση η οποία θεωρείται πιο αποδοτική αφού δεν προϋποθέτει τον συγχρονισμό που χρειαζόταν η

συμμετρική μέθοδος. Με τα ψηφιακά πιστοποιητικά κάθε τύπος συσκευής χρειάζεται μόνο ένα πιστοποιητικό και ένα ιδιωτικό κλειδί το οποίο δε θα αποκαλύψει ποτέ. Η τυπική χρήση του Public Key Infrastructure (PKI) παρουσιάζεται στο σχεδιάγραμμα 5.3[97]. Στην ουσία παρατηρούμε ότι η οντότητα που επιθυμεί να επικοινωνήσει με μια ασφαλή οντότητα γνωστή και ως Relaying Party (RP) ξεκινά τη διαδικασία στέλνοντας μια αίτηση σ' ένα Registration Authority (RA), για υπογραφή του πιστοποιητικού της. Το Registration Authority (RA) αξιολογεί το κατά πόσο η αίτηση μπορεί να γίνει αποδεκτή και στην περίπτωση που κάτι τέτοιο μπορεί να γίνει, την υπογράφει και την προωθεί προς το Certification Authority (CA), το οποίο αναλαμβάνει την έκδοση του πιστοποιητικού. Το πιστοποιητικό αυτό θα χρησιμοποιηθεί σε μετέπειτα στάδιο όταν η οντότητα αυτή θα θέλει να επικοινωνήσει με ένα Relaying Party. Σε μια τέτοια περίπτωση, η οντότητα αυτή θα αποστείλει το πιστοποιητικό της στο Relaying Party. Το οποίο θα το ελέγξει για την εγκυρότητά του μέσω ενός Validation Authority (VA). Αν όλα είναι εντάξει τότε οι δύο οντότητες θα μπορούν πλέον να επικοινωνούν.



Σχεδιάγραμμα 5.3 Σχηματική απεικόνιση ενός συστήματος PKI.

- **Identity-based public key schemes :** Η διαχείριση δημόσιου κλειδιού στο μοντέλο αυτό γίνεται με ένα διαφορετικό τρόπο. Στην ουσία το μοντέλο επιτρέπει μοναδικά στοιχεία του χρήστη να χρησιμοποιηθούν ως δημόσια κλειδιά γεγονός που καθιστά τα πιστοποιητικά αχρείαστα. Σε αυτά τα μοντέλα, χρειάζεται μια αξιόπιστη οντότητα

για να παράγει να διανέμει και να ανακαλεί τα ιδιωτικά κλειδιά που θα αντιστοιχούν σε κάθε μοναδικό χαρακτηριστικό (identity)[98].

Μια διαδικασία διαχείρισης κλειδιών οφείλει να πληροί ορισμένες προϋποθέσεις προκειμένου να μπορεί να θεωρείται επιτυχής. Μεταξύ αυτών, η σωστή αξιοποίηση των αλγορίθμων και των παραμέτρων τους (μήκος κλειδιού, διάρκεια ζωής κτλ.), η εξασφάλιση της τυχαιότητας σε ότι αφορά τα κλειδιά, η επεκτασιμότητα, η αποδοτικότητα σε θέματα επίδοσης, μνήμης κτλ. και η αναπροσαρμοστικότητα [95].

5.2.2.1 Μοντέλα διαχείρισης κλειδιού

Όπως ήδη γνωρίζουμε το Smart Grid είναι ένα ετερογενές δίκτυο που αποτελείται από μια πληθώρα διαφορετικών δικτύων επικοινωνίας μεταξύ των οποίων δίκτυα μικρής εμβέλειας (εντός υποσταθμών) και μεγάλης εμβέλειας (όπως το AMI δίκτυο), δίκτυα ενσύρματα και ασύρματα, αλλά και δίκτυα με και χωρίς απαιτήσεις πραγματικού χρόνου[95]. Για την εξασφάλιση της εμπιστευτικότητας της επικοινωνίας μεταξύ των οντοτήτων που ανήκουν σε αυτά τα δίκτυα, χρειαζόμαστε ένα σύστημα διαχείρισης κλειδιών. Η σχεδίαση ενός τέτοιου συστήματος όμως, ενιαίου για ολόκληρο το δίκτυο του Smart Grid, δεν είναι εφικτή, κυρίως για σκοπούς πρακτικότητας. Για το λόγο αυτό καταφεύγουμε στη σχεδίαση επί μέρους συστημάτων διαχείρισης κλειδιών που ανταποκρίνονται στις συγκεκριμένες απαιτήσεις των διάφορων υποσυστημάτων του Smart Grid. Πιο κάτω, παρουσιάζουμε αντιπροσωπευτικά δείγματα συστημάτων διαχείρισης κλειδιών για διάφορα υποσυστήματα του Smart Grid, όπως προτάθηκαν μέσα από τη σύγχρονη βιβλιογραφία.

Αρχή κάνουμε παρουσιάζοντας διάφορες μεθόδους διαχείρισης κλειδιού που προτάθηκαν για SCADA συστήματα. Τέτοια συστήματα αποτελούνται συνήθως από τρία βασικά ήδη οντοτήτων επικοινωνίας :

- Το HMI (Human Machine Interface) που αποτελεί τη διεπαφή του χειριστή με το Σύστημα Τηλελέγχου και Διαχείρισης Ενέργειας.
- Το MTU (Master Terminal Unit) το οποίο ελέγχει τα RTUs και αποτελεί τον τρόπο διασύνδεσής τους με το κεντρικό σύστημα
- Και τέλος τα RTUs (Remote Terminal Units), συσκευές περιορισμένης μνήμης και επεξεργαστικής ισχύος, οι οποίες είναι υπεύθυνες για τη συλλογή δεδομένων που αφορούν στην κατάσταση του συστήματος ανά πάσα στιγμή – εκτελώντας τις εντολές του MTU.

Βάσει των όσων αναφέρονται στο [95] ένα σύστημα διαχείρισης κλειδιού για SCADA συστήματα είναι απαραίτητο να χαρακτηρίζεται από την ικανότητα υποστήριξης broadcasting και multicasting μετάδοσης. Πράγματι, η broadcasting λειτουργία είναι κρίσιμης σημασίας για τις περιπτώσεις στις οποίες το MTU π.χ. θέλει να στείλει σε όλα τα συνδεδεμένα με εκείνο RTUs μήνυμα για επείγον τερματισμό της λειτουργίας του συστήματος (emergency shutdown). Τα μηνύματα αυτά θέλουμε να μπορούν να μεταφέρονται εντός ενός συγκεκριμένου χρονικού πλαισίου, κάτι που το multiple unicasting δε θα μπορούσε να μας επιτρέψει να επιτύχουμε. Σε ότι αφορά τώρα στη multicasting λειτουργία, θεωρείται και αυτή απαραίτητη αφού σε ορισμένες περιπτώσεις παραλήπτες του μηνύματος μπορεί να είναι συγκεκριμένες συσκευές ή συγκεκριμένη κατηγορία συσκευών. Εξίσου σημαντικό χαρακτηριστικό των συστημάτων διαχείρισης κλειδιού για SCADA είναι να λαμβάνουν υπόψη τους περιορισμένους πόρους που διαθέτουν τα RTUs (και άρα την αδυναμία τους να συγκρατούν πολλά κλειδιά) αλλά και την ανάγκη που μπορεί να προκύψει για ενημέρωση κλειδιών εξαιτίας της έκθεσης των RTUs σε φυσικές τοποθεσίες οι οποίες θέτουν σε κίνδυνο τη φυσική ασφάλειά τους.

Το πρώτο σύστημα διαχείρισης κλειδιών που θα μελετήσουμε καλείται SKE (SCADA Key Establishment)[99][95] και προτάθηκε από τα Sandia National Laboratories. Πρόκειται για ένα μηχανισμό ο οποίος θεωρείται ελλιπής λόγω της απουσίας πρόνοιας για broadcasting και multicasting. Σα μηχανισμός, διακρίνει την επικοινωνία εντός ενός SCADA συστήματος σε δύο ειδών : master-slave (η οποία είναι ιδανική για ανταλλαγή συμμετρικών κλειδιών) και peer-to-peer (η οποία μπορεί να αξιοποιηθεί για ασύμμετρα κλειδιά). Όταν το MTU θέλει να προωθήσει μια πληροφορία προς κάποια RTUs οφείλει πρώτα να την κρυπτογραφήσει με τα κλειδιά του κάθε ενός. Ένας MTU στο σχήμα master-slave κρατάει ένα Long-Term Key που μοιράζεται με τα RTUs κι ένα General Seed Key το οποίο του ανήκει. Για να επιτευχθεί ασφαλής επικοινωνία το MTU αποστέλλει το General Seed Key του στα RTUs. Τα οποία το χρησιμοποιούν για να φτιάξουν ένα 128bit hash, που ονομάζεται General Key και χρησιμοποιείται για την παραγωγή του Session Key με το οποίο θα γίνει η κρυπτογράφηση και η αποκρυπτογράφηση.

Ένα παρόμοιο σύστημα διαχείρισης κλειδιών σε SCADA συστήματα, προτάθηκε από το Information Security Institute, του Queensland University of Technology στην Αυστραλία[100]. Το σύστημα αυτό, γνωστό με το όνομα SKMA (SCADA Key Management Architecture), εισάγει ένα KDC(Key Distribution Centre) για τη διατήρηση των Long Term Keys που αναφέραμε πιο πάνω. Όταν μια νέα οντότητα ενταχθεί στο δίκτυο τότε

δημιουργείται ένα node-to-KDC κλειδί μεταξύ της οντότητας και του KDC, το οποίο εγκαθίσταται πάνω στον κόμβο.
Για την επικοινωνία μεταξύ δύο κόμβων, με τη βοήθεια του node-to-KDC κλειδιού, παράγεται ένα node-to-node κλειδί το οποίο χρησιμοποιείται με τη σειρά του για να παράξει το session key που θα χρησιμοποιήσουν στο τέλος οι δύο κόμβοι για τη μεταξύ τους επικοινωνία. Το σύστημα αυτό επίσης δε διαθέτει Broadcasting και Multicasting λειτουργικότητα.

Μερικά χρόνια αργότερα, ένα διαφορετικό σύστημα διαχείρισης κλειδιών για SCADA συστήματα, το ASKMA (Advanced SCADA Key Management Architecture) προτείνεται από τους Choi,Kim,Won και Kim [101], προωθώντας την ιδέα αξιοποίησης λογικών ιεραρχιών από κλειδιά για την επίτευξη αποδοτικότερης διαχείρισης κλειδιών. Το σύστημα αυτό υποστηρίζει broadcasting και multicasting και η επίδοσή του στις node-to-node επικοινωνίες θεωρείται πραγματικά καλή. Βασικό μειονέκτημα του ASKMA είναι παρόλα αυτά, η επίδοση που έχει στις multicast επικοινωνίες.

Αυτό ακριβώς το μειονέκτημα προσπάθησαν να αντιμετωπίσουν στο [102], οι Choi, Lee,Won και Kim, προτείνοντας το ASKMA+, τη μετεξέλιξη του ASKMA . Το ASKMA+ έρχεται να δώσει στο ASKMA την επίδοση που του χρειάζεται στο multicasting, μειώνοντας παράλληλα και το πλήθος των κλειδιών που χρειάζεται να κρατούνται στα RTUs. Για να επιτύχει κάτι τέτοιο το ASKMA+ αξιοποιεί μια λογική ιεραρχία κλειδιών (Logical Key Hierarchy) και επίσης το πλαίσιο Iolus (για καλύτερη διαχείριση του κατανεμημένου δέντρου από κόμβους – RTUs, Sub-MTUs και MTUs).

Σε αυτή την κατηγορία ανήκει και το πιο πρόσφατο παράδειγμα των Saxena,Pal,Saiwan και Saquib [103] που προτείνουν ένα Token-Based σύστημα διαχείρισης κλειδιών για SCADA συστήματα το οποίο χρησιμοποιεί ασύμμετρα κλειδιά και Token fields για να ασφαλίσει την επικοινωνία. Με βάση το σύστημα αυτό κάθε RTU διαθέτει κατά τη φάση της αρχικοποίησης ένα Long Term Key. Το κλειδί αυτό χρησιμοποιείται από το MTU όταν αυτό θα χρειαστεί να διανέμει σε κάθε κόμβο το ζεύγος κλειδιών του (Δημόσιο και Ιδιωτικό) και το δικό του δημόσιο κλειδί. Στην ουσία σε αυτή την αρχιτεκτονική το MTU παράγει Tokens και τα διανέμει στις διάφορες οντότητες που συμμετέχουν στο σύστημά του. Ένα τέτοιο Token χαρακτηρίζεται από κάποιες πληροφορίες όπως για παράδειγμα οι διευθύνσεις αποστολέα και παραλήπτη που θα λάβουν μέρος στην επικοινωνία, η ημερομηνία λήξης αλλά και ένα υπογεγραμμένο hash όλων των πιο πάνω με το ιδιωτικό κλειδί του MTU

(Token fingerprint). Όταν ένα MTU χρειάζεται να επικοινωνήσει με κάποιο κόμβο, το MTU χρειάζεται να παράγει και να αποστείλει το Token για αυτή την επικοινωνία. Από την άλλη όταν ένας κόμβος χρειάζεται να επικοινωνήσει με έναν άλλο κόμβο ή ένα MTU τότε ο κόμβος αυτός χρειάζεται ένα Token από τον MTU για την επικοινωνία, όποιος και αν είναι ο παραλήπτης. Το MTU σε αυτό το σύστημα διαχείρισης κλειδιών, καλείται στην ουσία να διαδραματίσει το ρόλο ενός είδους «Certification Authority» πιστοποιώντας την αυθεντικότητα κάθε κόμβου που συμμετέχει στην επικοινωνία. Συνήθως σε μοντέλα όπως και το πιο πάνω, που εμπνέονται από τη λογική των PKI για την αυθεντικοποίηση, χρησιμοποιούνται πιστοποιητικά. Κάτι τέτοιο όμως στο Smart Grid θεωρείται ανεπιθύμητο κατά τους συγγραφείς, εξαιτίας του ότι τα πιστοποιητικά εισάγουν επιπλέον καθυστερήσεις στο σύστημα. Για το λόγο αυτό οι συγγραφείς προτείνουν την αντικατάσταση των πιστοποιητικών με μοναδικά Tokens τα οποία θα αποδεικνύουν την αυθεντικότητα της κάθε οντότητας. Για να κατανοήσουμε καλύτερα τον τρόπο με τον οποίο τα Tokens αυτά αξιοποιούνται θα περιγράψουμε αφαιρετικά τον τρόπο επικοινωνίας μεταξύ δύο κόμβων κάτω από το συγκεκριμένο μοντέλο ανταλλαγής κλειδιών. Έστω ότι ο κόμβος Α ενδιαφέρεται να επικοινωνήσει με τον κόμβο Β. Το πρώτο βήμα για να μπορέσει να αρχίσει μια τέτοια επικοινωνία, είναι να κοιτάξει ο Α στη βάση δεδομένων που διατηρεί για να εξακριβώσει κατά πόσο γνωρίζει το δημόσιο κλειδί του Β (γεγονός το οποίο θα σήμαινε πως κατέχει ήδη ένα token επικοινωνίας με αυτό). Αν κάτι τέτοιο συμβαίνει τότε ο κόμβος Α κρυπτογραφεί το μήνυμα και το hash του Token με το δημόσιο κλειδί του Β, και το στέλνει σε αυτόν. Αν όμως ο Α δεν έχει το δημόσιο κλειδί του Β και ένα Token για την επικοινωνία μαζί του, τότε τα πράγματα αλλάζουν. Για να επιτευχθεί μια τέτοια επικοινωνία θα πρέπει πρώτα, ο Α να δημιουργήσει ένα μοναδικό αριθμό Ν, να βάλει τη διεύθυνση του Β σ' ένα μήνυμα μαζί με το Ν, να υπογράψει το μήνυμα με το ιδιωτικό κλειδί του, να το κρυπτογραφήσει με το δημόσιο κλειδί του MTU και έπειτα να το αποστείλει σε αυτόν. Με το που λαμβάνει την αίτηση αυτή ο MTU, την αποκρυπτογραφεί με το ιδιωτικό του κλειδί, πιστοποιεί την ταυτότητα του Α ελέγχοντας την υπογραφή του και έπειτα αφού πάρει το Ν, φτιάχνει ένα Token για την επικοινωνία μεταξύ Α και Β το οποίο κρυπτογραφεί με το δημόσιο κλειδί του Α, μαζί με ένα καινούριο μοναδικό αριθμό,και το δημόσιο κλειδί του Β. Όταν ο Α αποκρυπτογραφήσει το μήνυμα και επιβεβαιώσει το Token fingerprint του, στέλνει στο MTU μια επιβεβαίωση, κι έτσι το MTU παράγει ένα νέο Nonce, το βάζει σε ένα μήνυμα μαζί με το δημόσιο κλειδί του Α και το Token και το αποστέλλει κρυπτογραφημένο με το δημόσιο κλειδί του Β. Όταν ο Β λάβει το μήνυμα συγκρίνει το δικό του υπολογισμό του Token hash με το Token fingerprint που έλαβε και αν όλα είναι εντάξει αποστέλλει στον MTU μια επιβεβαίωση. Μετά από αυτή τη διαδικασία οι Α και Β είναι έτοιμοι να

επικοινωνήσουν. Ο Α στέλνει λοιπόν το μήνυμά και το Token fingerprint του στον Β, κρυπτογραφημένο με το δημόσιο κλειδί του Β. Λαμβάνοντάς το ο Β είναι έτοιμος να απαντήσει γιατί ήδη γνωρίζει το δημόσιο κλειδί του Α αλλά και το Token.

Έχοντας γνωρίσει ορισμένα αντιπροσωπευτικά δείγματα των συστημάτων διαχείρισης κλειδιών για SCADA συστήματα, είμαστε πλέον έτοιμοι να προχωρήσουμε στη μελέτη παρόμοιων συστημάτων αυτή τη φορά με στόχο τη διαχείριση και διανομή κλειδιών στα πλαίσια του AMI δικτύου.

Για αρχή παρουσιάζουμε τη δουλειά των Kampto, Qian, Fuller και Attia[104], η οποία αξιοποιεί τη λογική των συμμετρικών κλειδιών και συγκεκριμένα του αλγόριθμου ανταλλαγής κλειδιών Diffie-Helman για να επιτύχει την ασφαλή επικοινωνία μεταξύ οντοτήτων του AMI (HAN). Οι συγγραφείς παρουσιάζουν στο άρθρο τους, μια μέθοδο ανταλλαγής κλειδιών ανάμεσα σε οντότητες του HAN περιβάλλοντος με το εσωτερικό Gateway είτε για επικοινωνία μιας οντότητας του HAN με το Gateway, είτε για επικοινωνία μιας ομάδας συσκευών του Smart Home περιβάλλοντος με το Gateway. Κάθε συσκευή, επικοινωνεί αρχικά με ασφάλεια με ένα Certification Authority το οποίο της δίνει το αναγνωριστικό της, καθορίζει την πολλαπλασιαστική ομάδα τα στοιχεία του οποίου θα αξιοποιήσουμε, έναν τυχαίο πρώτο αριθμό, έναν γεννήτορα, και το Hash Function που θα χρησιμοποιηθεί. Στην περίπτωση που το Gateway εντός του Smart Home, πρέπει να αρχίσει να επικοινωνεί με ένα Smart Meter, το Gateway και το Smart Meter επιλέγουν από ένα τυχαίο αριθμό που ανήκει στο multiplicative group και δημιουργούν τα δημόσια κλειδιά τους (Τα οποία είναι αποτέλεσμα της ύψωσης του τυχαίου πρώτου αριθμού που ορίστηκε ως παράμετρος, στον τυχαίο αριθμό που επιλέγηκε από κάθε οντότητα). Το δημόσιο κλειδί του αποστολέα γίνεται hashed μαζί με το ID του και αποστέλλεται στον παραλήπτη. Τα hashes αυτά χρησιμοποιούνται κατά την αυθεντικοποίηση μετά την οποία και τα δύο εμπλεκόμενα στην επικοινωνία μέρη, παράγουν το κοινό κλειδί που θα χρησιμοποιηθεί για τη μεταξύ τους επικοινωνία ακολουθώντας την τυπική Diffie-Helman διαδικασία. Η παραγωγή ομαδικών κλειδιών (Group Key) τώρα, όπως περιγράφεται από τους Kampto et.al, γίνεται με τη συμμετοχή όλων των κόμβων που ανήκουν στην ομάδα. Συγκεκριμένα κάθε ένας από αυτούς τους κόμβους φτιάχνει το δικό του συμμετρικό κλειδί επικοινωνίας με το Gateway και ακολούθως το aggregate των κλειδιών αυτών αξιοποιείται ως το κοινό κλειδί της ομάδας. Τρόποι ανανέωσης, ανάκλησης και ενημέρωσης των κλειδιών καλύπτονται επίσης μέσα από το συγκεκριμένο άρθρο.

Μια διαφορετική προσέγγιση ακολουθήθηκε από τους συγγραφείς του[105] στο οποίο μελετήθηκαν διάφορες μέθοδοι με τις οποίες Unified Key Management Functions (UKMF) ή Dedicated Key Management Functions (DKMF) ή ακόμα και ένας συνδυασμός των δύο θα μπορούσαν να αξιοποιηθούν προκειμένου να εξασφαλίσουμε τη διαχείριση κλειδιών στο πλαίσιο του Smart Grid. Στην πραγματικότητα το UKMF που προτείνεται από τους συγγραφείς καθορίζει έναν τρόπο παραγωγής κλειδιών κρυπτογράφησης πάνω από διάφορα πρωτόκολλα τα οποία μπορεί να ανήκουν στο ίδιο ή σε διαφορετικό επίπεδο στη στοίβα πρωτοκόλλων επικοινωνίας. Ενώ το DKMF, προτάθηκε ουσιαστικά για τα πρωτόκολλα εκείνα που απαιτούν εξειδικευμένη παραγωγή και διαχείριση κλειδιών την οποία δε μπορεί να τους παρέχει το UKMF. Αν τα πρωτόκολλα επικοινωνίας σε ένα επίπεδο της στοίβας πρωτοκόλλων εξυπηρετούνται από ένα UKMF ενώ τα πρωτόκολλα ενός άλλου επιπέδου εξυπηρετούνται από DKMF (το οποίο μπορεί να τυγχάνει διαχείρισης από το UKMF) τότε το μοντέλο λέγεται partially unified και όχι fully unified όπως θα λεγόταν εάν είχε μόνο UKMF. Οι συγγραφείς του άρθρου θεωρούν ότι το εννοιολογικό μοντέλο που παρουσιάζουν μπορεί κάλλιστα να εφαρμοστεί σε οποιοδήποτε πλαίσιο διαχείρισης κλειδιών, εντούτοις οι ίδιοι επιλέγουν να χρησιμοποιήσουν το EAP (Extensible Authentication Protocol), περιγράφοντας τους τρόπους με τους οποίους το UKMF λαμβάνει τις παραμέτρους που αφορούν στα κλειδιά από έναν EAP peer ή έναν authentication server, για να διανέμει ακολούθως το ίδιο τις παραμέτρους και τα κλειδιά στις εφαρμογές που το χρησιμοποιούν περιγράφοντας παράλληλα με λεπτομέρεια εναλλακτικές μεθόδους διαχείρισης και ανανέωσης κλειδιών.

Μια διαφορετική άποψη εκφράζουν οι Nicafar, Jokar, Beznosov και Leung στο [98] , η οποία αφορά σε ένα Smart Grid Key Management Scheme (SGKM) το οποίο στοχεύει στην αποδοτική διαχείριση κλειδιών αξιοποιώντας τη λογική PKI, όπως αυτή προτείνεται από το NIST [73]. Συγκεκριμένα, η μελέτη αυτή εξελίσσει την ιδέα του Identity Based Cryptography (IBC) προτείνοντας το Enhanced Identity Based Cryptography (EIBC). Στο IBC, ένα Private Key Generator που λειτουργεί ως το Certification Authority παρέχει μια σταθερή, μοναδική μονόδρομη συνάρτηση κατακερματισμού (hash function), F, η οποία μπορεί να χρησιμοποιηθεί για την παραγωγή τόσο του δημόσιου όσο και του ιδιωτικού κλειδιού. Το δημόσιο κλειδί σε τέτοιες περιπτώσει είναι το KPub = F(ID) ενώ το ιδιωτικό προκύπτει από το γινόμενο του F(ID) με έναν τυχαίο αριθμό s (KPriv = s × F(ID)). Η κρυπτογράφηση, η αποκρυπτογράφηση και η επαλήθευση στο IBC, γίνονται όπως ακριβώς θα γίνονταν σε ένα τυπικό PKI σύστημα. Στο EIBC, που προτείνουν οι συγγραφείς του συγκεκριμένου άρθρου, η όλη διαδικασία που μόλις περιγράψαμε διαφοροποιείται, αφού η F παύει πλέον να είναι σταθερή και αποκτά δυναμική μορφή με τον Private Key Generator

(PKG) να παράγει και να αναμεταδίδει περιοδικά, μια νέα συνάρτηση f η οποία χρησιμοποιείται για την ενημέρωση της F (και άρα την ενημέρωση των δημόσιων και ιδιωτικών κλειδιών). Την ίδια στιγμή ο τυχαίος αριθμός s που χρησιμοποιούσαμε προηγουμένως για τη δημιουργία του ιδιωτικού κλειδιού, αντικαθίσταται για τους σκοπούς του EIBC, από δύο αριθμούς ένα τυχαίο και ένα ψευδοτυχαίο, ορισμένες παράμετροι αποκτούν Seed Values και End Values, τα multicast group keys υποστηρίζονται και οι περίοδοι ανανέωσης κλειδιού κατηγοριοποιούνται σε Short Term, Medium Term και Long Term. Η όλη διαδικασία για τη Short Term ανανέωση κλειδιών στην ουσία ξεκινά με την ανανέωση της συνάρτησης f (και των παραμέτρων που σχετίζονται με αυτήν validity time, timestamp κτλ.). Και συνεχίζει με τον Security and Authentication Server να υπολογίζει το συμμετρικό του κλειδί (εφαρμόζοντας τη συνάρτηση κατακερματισμού πάνω στο δημόσιο κλειδί του), να υπογράφει το μήνυμα και μετά να το αποστέλλει. Ο έξυπνος μετρητής που λαμβάνει το μήνυμα, επιβεβαιώνει την εγκυρότητά και αυθεντικότητά του χρησιμοποιώντας την υπογραφή του αποστολέα, υπολογίζει με το δικό του δημόσιο κλειδί το συμμετρικό κλειδί και αποκρυπτογραφεί το πακέτο. Το γεγονός αυτό του επιτρέπει να επιβεβαιώσει κατά πόσο το πακέτο αυτό δεν αποτελεί προϊόν ενός Replay Attack (μέσω ελέγχου του timestamp), ενώ βοηθά (μέσω ελέγχου του validity time) να καθοριστεί επίσης πότε πρέπει να διεξαχθεί η επόμενη ανανέωση κλειδιού. Οι Medium και Long Term τεχνικές διαφέρουν ελάχιστα από την πιο πάνω. Τέλος, οι συγγραφείς του άρθρου αναφέρονται επίσης στον τρόπο με τον οποίο θα μπορούσε να επιτευχθεί Multicasting και Broadcasting.

Έχοντας πάρει μια πρώτη γεύση για τα διάφορα είδη τεχνικών διαχείρισης κλειδιού στο AMI δίκτυο, στρέφουμε τώρα την προσοχή μας σε αντίστοιχες τεχνικές διαχείρισης κλειδιών αυτή τη φορά στο ευρύτερο δίκτυο του Smart Grid, όπου συναντάμε τις περιφερειακές συσκευές που λαμβάνουν μετρήσεις για την κατάσταση του Smart Grid (IEDs, PMUs, PDCs κ.α.).

Ενδεικτικό παράδειγμα σε αυτή την κατηγορία η δουλειά των Zhao et al. [106] στην οποία αξιοποιείται η λογική του Broadcast Encryption, των ελλειπτικών καμπύλων και των media key blocks (MKB) για την διαχείριση συμμετρικών κλειδιών. Το μοντέλο που προτείνεται, αποτελείται ουσιωδώς από δύο υπό-πρωτόκολλα. Το πρώτο εξ' αυτών αναλαμβάνει τη διανομή κλειδιών μεταξύ των διάφορων συσκευών (PMUs, IEDs κτλ.) που θέλουν να επικοινωνήσουν, επιτρέποντας σε ένα ζεύγος συσκευών να μοιράζονται ένα κλειδί για σκοπούς αυθεντικοποιήσης. Η διαδικασία κατά την οποία το κοινό αυτό κλειδί διανέμεται και στα δύο εμπλεκόμενα μέρη εμπλέκει broadcast encryption αφού μια συσκευή μπορεί να

εξάγει το κοινό κλειδί χρησιμοποιώντας το μοναδικό κλειδί της. Το δεύτερο υπό-πρωτόκολλο αφορά αποκλειστικά θέματα αυθεντικοποίησης και χρησιμοποιεί ορισμένους τυχαίους αριθμούς που παράγονται κατά το τρέξιμο του πρώτου υπό-πρωτοκόλλου.

Σε αυτή την κατηγορία εντάσσεται επίσης και το WAKE (Wide Area measurements KEy Management) [107], ένα σύστημα διαχείρισης κλειδιών το οποίο αξιοποιεί γνωστά πρωτόκολλα ασφάλειας για σκοπούς unicasting επικοινωνίας και το TV-HORS πρωτόκολλο για την υποστήριξη multicast επικοινωνίας. Πιο συγκεκριμένα το WAKE χρησιμοποιεί PKI με την εταιρεία παροχής στον ρόλο του Trust Anchor (της ρίζας δηλαδή στο ιεραρχικό δέντρο των διάφορων Certification Authorities) να ακολουθεί το πρότυπο X.509. Για σκοπούς unicast επικοινωνίας, κάθε συσκευή στο δίκτυο κατέχει το δικό της ζεύγος ιδιωτικού και δημόσιου κλειδιού, με το τελευταίο να πιστοποιείται από την υπηρεσία παροχής. Όπως χαρακτηριστικά αναφέρουν οι συγγραφείς, όταν δύο συσκευές στο δίκτυο θέλουν να επικοινωνήσουν, φτιάχνουν ένα ασφαλές κανάλι επικοινωνίας αξιοποιώντας Diffie - Hellman είτε μέσω IKEv2 στο IPSec, είτε μέσω TLS. Σ'ένα τέτοιο κανάλι, τα μηνύματα θα ήταν καλό, κατά τους συγγραφείς, να κρυπτογραφούνται με ένα αλγόριθμο τμημάτων όπως π.χ. ο AES. Ενώ για την αυθεντικότητα των μηνυμάτων προτείνεται η χρήση του CMAC πρωτοκόλλου. Σε ότι αφορά στη multicast επικοινωνία, κατόπιν σύγκρισης μεταξύ TSV+ και TV-HORS, οι συγγραφείς επέλεξαν τελικά το δεύτερο πρωτόκολλο λόγο της μεγαλύτερης αποδοτικότητάς του σε θέματα υπογραφής και πιστοποίησης μηνυμάτων.

Στο σημείο αυτό, φτάσαμε στο τέλος της ενότητας που αφορά σε θέματα διαχείρισης κλειδιών στο Smart Grid/Smart Home περιβάλλον. Η επόμενη ενότητα αφιερώνεται σε κάτι εξίσου σημαντικό και ενδιαφέρον. Στους τρόπους με τους οποίους μπορούμε να εξασφαλίσουμε την ιδιωτικότητα των δεδομένων που διακινούνται στο πλαίσιο του Smart Grid.

5.2.3 Εξασφαλίζοντας ιδιωτικότητα

Αναπόσπαστο κομμάτι του Smart Grid είναι η υποδομή των έξυπνων μετρητών που διαθέτει. Χάρη σε αυτήν μπορούμε να λαμβάνουμε λεπτομερείς εικόνες της κατάστασης του Smart Grid ανά τακτά χρονικά διαστήματα, γεγονός που μας επιτρέπει να προσβλέπουμε μεταξύ άλλων σε μια πιο αποδοτική διαδικασία πρόβλεψης ζήτησης, σε πιο ευέλικτη διαχείριση φορτίου και σε νέα δυναμικά μοντέλα χρέωσης. Η συχνότητα με την οποία το AMI

περιβάλλον μας παρέχει λεπτομερείς πληροφορίες κατανάλωσης εγείρει εντούτοις ορισμένες ανησυχίες. Ήδη, στο προηγούμενο κεφάλαιο, πήραμε μια γεύση των όσων μπορεί κανείς εύκολα να εξάγει για τον τρόπο ζωής μας μέσω μιας απλής διαδικασίας Non-Intrusive Load Monitoring , η οποία μπορεί να αποκαλύψει ποια συσκευή χρησιμοποιείται ανά πάσα στιγμή εντός ενός υποστατικού.

Προφανώς, το Non-Intrusive Load Monitoring δεν είναι ο μόνος τρόπος να εισβάλει κανείς στην ιδιωτική μας ζωή εκμεταλλευόμενος το Smart Grid. Για την ακρίβεια διαδικασίες που αφορούν σε Use Mode Detection, μας παρέχουν την ευκαιρία όχι μόνο να εντοπίσουμε ποια ηλεκτρική συσκευή βρίσκεται σε λειτουργία ανά πάσα στιγμή αλλά και να εξάγουμε συγκεκριμένες πληροφορίες που αφορούν στον τρόπο λειτουργίας της. Αναφέρουμε ως χαρακτηριστικό παράδειγμα τη μελέτη του Greveler et al. [108] η ομάδα του οποίου κατάφερε να αποδείξει ότι συγκεκριμένες πληροφορίες που μπορούν να εξαχθούν από τη λεπτομερή ενεργειακή κατανάλωση τηλεοράσεων σ' ένα διάστημα μόλις δύο δευτερολέπτων, αρκούν για να εντοπίσουμε ποιο κανάλι παίζει στην τηλεόραση. Ενώ πέντε λεπτά διαδοχικής προβολής μιας ταινίας πολλές φορές αποκαλύπτουν ακόμα και το ποια ταινία είναι αυτή!

Συνεπώς, η ανάγκη για διασφάλιση της ιδιωτικότητάς μας γίνεται σήμερα πιο επιτακτική από ποτέ[109]. Προς αυτή την κατεύθυνση χρειαζόμαστε τόσο ένα γερό νομικό πλαίσιο το οποίο να καθορίζει νόμους και πολιτικές που να καλύπτουν τη νέα διάσταση της ιδιωτικότητας στο Smart Grid όσο και ένα γερό τεχνικό πλαίσιο το οποίο να προσπαθεί να αποτρέψει το ενδεχόμενο τέτοιων παραβιάσεων πριν καν προκύψουν.

Στην ενότητα αυτή θα ασχοληθούμε αποκλειστικά με τις διάφορες κατηγορίες τεχνολογιών ενίσχυσης ιδιωτικότητας (Privacy Enhancing Technologies – PETs) όπως αυτές επισημάνθηκαν στο [110] , παρουσιάζοντας αντιπροσωπευτικά δείγματα βιβλιογραφίας που αξιοποιούν μια ή περισσότερες από τις τεχνικές αυτές για να εξασφαλίσουν την ιδιωτικότητα στο Smart Grid. Σε ότι αφορά στη νομική διάσταση της ιδιωτικότητας, θεωρούμε πως μια επισκόπηση των νομικών πλαισίων και πολιτικών που έχουν αρχίσει να διαμορφώνονται από κάθε χώρα για τους σκοπούς του Smart Grid, δεν εμπίπτει άμεσα στους στόχους αυτής της ενότητας.

5.2.3.1Anonymization

Στην πρώτη κατηγορία τεχνολογιών ενίσχυσης ιδιωτικότητας, εντάσσουμε τις τεχνολογίες που επιδιώκουν να εξασφαλίσουν ιδιωτικότητα μέσω ανωνυμοποίησης της μεταφερόμενης πληροφορίας. Ως ανωνυμοποίηση ή αλλιώς anonymization ορίζεται η διαδικασία, μέσω της οποίας με χειροκίνητο ή αυτόματο τρόπο αφαιρούμε ή αντικαθιστούμε με εικονικά δεδομένα, πληροφορίες οι οποίες μπορούν να ταυτοποιήσουν έναν άνθρωπο ή μια ομάδα ανθρώπων, σε μια επικοινωνία, μια βάση δεδομένων ή μια εγγραφή[73]. Με άλλα λόγια, στην περίπτωση του Smart Grid, πρόκειται για τη διαδικασία η οποία εξασφαλίζει στην εταιρεία ηλεκτροδότησης τα στοιχεία που της χρειάζονται προκειμένου να επιτελέσει τις διάφορες λειτουργίες της, αφαιρώντας οτιδήποτε συνδέει τα δεδομένα αυτά με τον μετρητή ή το υποστατικό από το οποίο λήφθηκαν. Η αποτελεσματικότητά του anonymization εξαρτάται σε μεγάλο βαθμό τόσο από τη συχνότητα με την οποία λαμβάνεται η πληροφορία όσο και από τη φύση και την ακρίβεια της πληροφορίας αυτής –παράμετροι οι οποίες μπορούν να αποκαλύψουν σε πολλές περιπτώσεις το δημιουργό της πληροφορίας ακόμα και μετά από anonymization[110].

5.2.3.2 Trusted Aggregator

Στη δεύτερη κατηγορία τεχνολογιών ενίσχυσης ιδιωτικότητας, τοποθετούμε τις τεχνολογίες που στοχεύουν στη διασφάλιση της ιδιωτικότητας αξιοποιώντας τη λογική των μοντέλων εμπιστοσύνης. Σε τέτοια μοντέλα θεωρούμε πως είτε ο ίδιος ο μετρητής είναι αρκετά αξιόπιστος για να αναλάβει τη συγκέντρωση (aggregation) και προώθηση της πληροφορίας με τρόπο που να διαφυλάσσει την ιδιωτικότητά της, είτε εισάγουμε μια τρίτη οντότητα γνωστή ως Third Trusted Party (TTP)[110] , την οποία εμπιστευόμαστε για το έργο της συλλογής και προώθησης της συγκεντρωτικής πληροφορίας. Σε οποιαδήποτε από τις δύο περιπτώσεις αυτό που επιτυγχάνουμε είναι να φθάνει στην εταιρεία παραγωγής ηλεκτρικής ενέργειας μόνο η συγκεντρωτική πληροφορία και όχι οι επιμέρους μετρήσεις που την απαρτίζουν. Κάτι τέτοιο διαφυλάσσει προφανώς την εμπιστευτικότητα παρόλα αυτά, εγείρει ερωτηματικά σε ότι αφορά το τι θεωρούμε αξιόπιστο.

5.2.3.3 Homomorphic Encryption

Η τρίτη κατηγορία απαρτίζεται από τεχνολογίες ενίσχυσης ιδιωτικότητας οι οποίες στηρίζονται στην ομομορφική ιδιότητα διάφορων αλγόριθμων κρυπτογράφησης και μεθόδων ανταλλαγής κλειδιού για να εξασφαλίσουν πως κατά την παραλαβή δεδομένων, η εταιρεία παραγωγής θα μπορεί να αποκρυπτογραφήσει μόνο τη συγκεντρωτική πληροφορία που προκύπτει από τα διάφορα κρυπτογραφήματα ή τα διάφορα secret shares χωρίς τη

δυνατότητα να εξάγει μεμονωμένη πληροφορία που να μπορεί να συνδεθεί με συγκεκριμένους μετρητές/υποστατικά ή πελάτες[110].

5.2.3.4 Perturbation Models

Η τέταρτη κατηγορία τεχνολογιών ενίσχυσης ιδιωτικότητας, περιλαμβάνει τεχνικές εξασφάλισης της ιδιωτικότητας οι οποίες επιχειρούν μέσα από την εισαγωγή θορύβου (perturbation) να αλλοιώσουν τα μεταφερόμενα μηνύματα κατανάλωσης ή τα συγκεντρωτικά αποτελέσματα που προκύπτουν μέσα από την επεξεργασία αυτών. Ορισμένα πρωτόκολλα που ανήκουν σε αυτή την κατηγορία επιχειρούν να εξασφαλίσουν αυτό που ονομάζουμε differential privacy στις συναρτήσεις που αναλαμβάνουν τη συνάθροιση των δεδομένων[110].

5.2.3.5 Verifiable Computation Models

Στην πέμπτη κατηγορία τεχνολογιών ενίσχυσης ιδιωτικότητας ανήκουν μοντέλα επαληθεύσιμου υπολογισμού (verifiable computation) στα οποία η οντότητα που αναλαμβάνει να παράγει τη συγκεντρωτική πληροφορία οφείλει να είναι σε θέση να αποδεικνύει ότι το αποτέλεσμα που προέκυψε προήλθε από έναν πολύ συγκεκριμένο υπολογισμό. Συνήθως η οντότητα αυτή έρχεται να διαδραματίσει το ρόλο του prover σε Zero Knowledge πρωτόκολλα (ZKP) όπου η εταιρεία παροχής ηλεκτρικής ενέργειας είναι ο verifier. Κάτι τέτοιο εξασφαλίζει την ιδιωτικότητα, αφού σε κάθε ZKP ένας verifier προκαλεί τον prover να αποδείξει κατά πόσο έχει τη γνώση που αυτός εισηγείται ότι έχει. Αν όντως ο prover έχει αυτή τη γνώση τότε θα μπορεί να το αποδείξει χωρίς ποτέ ο verifier να μάθει οτιδήποτε περισσότερο από αυτό[111].

5.2.3.6 Data Obfuscation

Η τελευταία κατηγορία τεχνολογιών ενίσχυσης ιδιωτικότητας που θα μελετήσουμε στοχεύει στην εξασφάλιση ιδιωτικότητας μέσω εγκατάστασης επαναφορτιζόμενων μπαταριών στα Smart Homes με στόχο την εξομάλυνση των κορυφών (load peaks) οι οποίες προδίδουν τα ενεργειακά μοτίβα κατανάλωσης χρηστών. Αλγόριθμοι ειδικά σχεδιασμένοι για τη συγκεκριμένη μέθοδο μπορούν να περιορίσουν τις διαρροές ευαίσθητης πληροφορίας αν και θεωρείται πως δεν αρκούν από μόνοι τους να καλύψουν την ανάγκη πλήρους προστασίας της ιδιωτικότητας των καταναλωτών[110].

5.2.3.7 Συνδυάζοντας τις τεχνικές για να πετύχουμε ιδιωτικότητα

Όλες οι πιο πάνω τεχνικές μπορούν να υλοποιηθούν με διάφορους τρόπους και να χρησιμοποιηθούν συνδυαστικά για να επιτύχουν την εξασφάλιση της ιδιωτικότητας των στοιχείων κατανάλωσης μετρητών/υποστατικών. Πιο κάτω παρουσιάζουμε ορισμένα δείγματα της σύγχρονης βιβλιογραφίας τα οποία αξιοποιούν τις συγκεκριμένες τεχνικές με διάφορους τρόπους.

Αρχή κάνουμε με ένα χαρακτηριστικό παράδειγμα τεχνολογίας η οποία αξιοποιεί τη λογική του anonymization για την εξασφάλιση του privacy στο Smart Grid το οποίο προτάθηκε από τους Efthymiou και Kalogirdis στο [112]. Η προσέγγισή τους στηρίζεται στη διάκριση σε δυο τύπους δεδομένων, που θεωρούν ότι καλείται να μεταφέρει ένα Smart Meter, σε δεδομένα χαμηλής συχνότητας (low-frequency data) και δεδομένα υψηλής συχνότητας (high-frequency data). Ως χαμηλής συχνότητας θεωρούνται τα δεδομένα εκείνα που αποστέλλονται πιο σπάνια από έναν μετρητή στην εταιρεία παροχής ηλεκτρικής ενέργειας, για σκοπούς χρέωσης. (Τα δεδομένα αυτά χρειάζεται να μπορούν να αποδοθούν στο δημιουργό τους). Ως υψηλής συχνότητας θεωρούνται τα δεδομένα που αποστέλλονται από το μετρητή κάθε μερικά λεπτά και χρειάζονται για Load Management, Demand Response, Load Shedding/Shifting κτλ.. (Τα δεδομένα αυτά θεωρούνται πιο πιθανό να αποκαλύψουν προσωπικά στοιχεία κάποιου, γι' αυτό επιδιώκουμε να εξασφαλίσουμε την ανωνυμία τους). Οι μετρητές με βάση τους συγγραφείς θα διαθέτουν δύο IDs ένα για High και ένα για Low frequency τα οποία θα χρησιμοποιούνται αναλόγως του τύπου δεδομένων που αποστέλλει ο μετρητής. Το Low Frequency ID θα είναι γνωστό, έτσι ώστε η υπηρεσία να γνωρίζει ότι μιλά με τον συγκεκριμένο μετρητή για σκοπούς χρέωσης, το High Frequency ID εντούτοις, πρέπει να μένει κρυμμένο για σκοπούς ανωνυμοποίησης. Κάτι τέτοιο, εγείρει την ανησυχία για το πώς η εταιρεία παροχής θα γνωρίζει αν το High Frequency ID που έχει λάβει αντιστοιχεί σε κάποιο έγκυρο μετρητή. Για το σκοπό αυτό, μια τρίτη οντότητα – εγγυητής (Third Party Escrow) η οποία γνωρίζει τη σχέση μεταξύ Low και High Frequency ID , αλλά δε θα μπορεί παρόλα αυτά να έχει πρόσβαση στα δεδομένα κατανάλωσης, θα χρησιμοποιείται για την πιστοποίηση της αυθεντικότητας του High Frequency ID .

Συνεχίζουμε, με τη δουλειά των Molina-Markham et al. οι οποίοι παρουσίασαν στο [113] τη δική τους ιδέα για μια αρχιτεκτονική έξυπνων μετρητών η οποία επιτυγχάνει τη διαφύλαξη της ιδιωτικότητας στηριζόμενη στη λογική του Anonymization, και την αξιοποίηση ενός Trusted aggregator και της λογικής του Verifiable Computation. Η αρχιτεκτονική αυτή αποτελείται στην ουσία από τρία βασικά συστατικά: τους έξυπνους μετρητές κάθε

υποστατικού, τα neighbourhood gateways σε κάθε γειτονιά και τους απομακρυσμένους servers της εταιρείας παροχής. Στην αρχιτεκτονική αυτή οι έξυπνοι μετρητές είναι υπεύθυνοι για τη λεπτομερή καταγραφή της ενεργειακής κατανάλωσης του υποστατικού, την οποία αναλαμβάνουν να προωθήσουν με blinded τρόπο προς το neighbourhood gateway με το οποίο είναι συνδεδεμένοι. Ακολούθως το Neighbourhood Gateway λειτουργεί ως ο σύνδεσμος μεταξύ Smart Meters και εταιρείας παροχής, προωθώντας τις μετρήσεις στην εταιρεία παροχής αφού πρώτα αποκρύψει οποιαδήποτε στοιχεία αφορούν στο υποστατικό από το οποίο προήλθε η μέτρηση. Το άρθρο δεν προσδιορίζει το κατά πόσο τα neighbourhood gateways αξιοποιούν οποιοδήποτε τύπου ψευδώνυμο για τους διάφορους μετρητές από τους οποίους λαμβάνονται στοιχειά κατανάλωσης, εντούτοις προτείνει έναν τρόπο με τον οποίο το σύστημα αξιοποιώντας Zero Knowledge Proofs θα μπορούσε να αξιοποιηθεί για συστήματα χρέωσης.

Ένα ακόμα πρωτόκολλο το οποίο συνδυάζει το Anonymization με τεχνικές Verifiable Computation χωρίς όμως να προϋποθέτει την εμπιστοσύνη σε οποιοδήποτε gateway ή Third Trusted Party προτάθηκε από τον Jeske στο [114]. Το πρωτόκολλο του Jeske αποτελείται ουσιωδώς από δύο υπό-πρωτόκολλα τα οποία αφορούν το μεν ένα στην τιμολόγηση ενέργειας (Invoicing), το δε άλλο στην αναφορά κατανάλωσης (Load Reporting). Στο invoicing πρωτόκολλο ο έξυπνος μετρητής αποστέλλει τη συνολική ενεργειακή του κατανάλωτη κρυπτογραφημένη και υπογεγραμμένη με ασύμμετρο τρόπο, στην εταιρεία παροχής. Με αυτό τον τρόπο η εταιρεία παροχής μπορεί να αποδώσει τη συγκεκριμένη κατανάλωση στο υποστατικό στο οποίο ανήκει. Το Load Reporting πρωτόκολλο όμως, στηρίζεται σε μια άλλη λογική. Με βάση αυτήν ο μετρητής κάθε υποστατικού υπάγεται σε ένα group το οποίο έχει ως διαχειριστή του την εταιρεία παροχής. Ο κάθε μετρητής που θέλει να μεταδώσει στοιχεία κατανάλωσής ενός υποστατικού, τα υπογράφει με την υπογραφή του group στο οποίο ανήκει με αποτέλεσμα να εξασφαλίζεται η ανωνυμία του. Το σύστημα που αξιοποιείται για τις ομαδικές υπογραφές στηρίζεται στο μοντέλο Camenisch και Lysyanskaya, η ασφάλεια του οποίου βασίζεται στον αλγόριθμο RSA. Πιο συγκεκριμένα στο μοντέλο αυτό, ο μετρητής αφού αποδείξει με zero-knowledge τρόπο ότι κατέχει ένα ticket το οποίο έχει όντως υπογραφεί από την εταιρεία παροχής και ότι το timestamp των δεδομένων που μεταφέρει με το συγκεκριμένο ticket είναι έγκυρο (Signature Proof of Knowledge – SPK), ζητά από την εταιρεία παροχής, να επιβεβαιώσει την εγκυρότητά του και να του υπογράψει το επόμενο ticket που θα χρειαστεί.

Σ’ ένα εναλλακτικό σενάριο οι Rial et al. στο [115] παρουσιάζουν τη δική τους ιδέα για μια αρχιτεκτονική η οποία εγγυάται τόσο την ιδιωτικότητα όσο και την ακεραιότητα των δεδομένων. Η ιδέα τους βασίζεται σε ένα σύνολο από πρωτόκολλα μεταξύ παροχέα, συσκευής χρήστη και μετρητή. Στην ουσία ο μετρητής λαμβάνει τις ενδείξεις κατανάλωσης, δημιουργεί commitments, υπογράφει πάνω από αυτά και έπειτα προωθεί τα στοιχεία στο user device. Εκείνο λαμβάνοντας από την εταιρεία παροχής τις απαραίτητες χρεώσεις υπολογίζει την τελική χρέωση και προωθεί το λογαριασμό στον παροχέα, μαζί με μια zero-knowledge απόδειξη (ZKP), η οποία παράγεται με τη χρήση Σ-protocols, που επιβεβαιώνει ότι ο υπολογισμός έγινε σωστά και ότι καμία επιπλέον πληροφορία δε διαρρέει.

Ένα δείγμα αρχιτεκτονικής που αξιοποιεί τη λογική των Trusted Aggregators και Cryptographic Computation για τη διασφάλιση της ιδιωτικότητας, εξασφαλίζοντας παράλληλα και access control παρουσιάστηκε από τους Ruj et al. στο [116]. Η αρχιτεκτονική που προτείνουν αποτελείται από HANs στα οποία βρίσκονται εγκατεστημένα smart meter gateways που αναλαμβάνουν τη συλλογή δεδομένων με στόχο την προώθησή τους σε BAN gateways τα οποία συνδυάζουν με τα δικά τους, τα δεδομένα πολλαπλών HANs για να τα στείλουν τελικά σε NAN gateways που τα συλλέγουν και αναλαμβάνουν να προωθήσουν τη συγκεντρωτική πληροφορία που προκύπτει από αυτά, στους πλησιέστερους υποσταθμούς. Στους υποσταθμούς αυτούς Remote Terminal Units (RTUs) αναλαμβάνουν να αποστείλουν τα δεδομένα που έλαβαν σε επί μέρους κέντρα συλλογής δεδομένων της εταιρείας παροχής για αποθήκευση. Η διαδικασία του aggregation της πληροφορίας σε όλα τα στάδια, στηρίζεται στον αλγόριθμο κρυπτογράφησης του Paillier[117]. Ο αλγόριθμος αυτός ανήκει στην κατηγορία αλγορίθμων ομομορφικής κρυπτογράφησης. Μιας μορφής κρυπτογράφησης που δημιουργήθηκε για να εξυπηρετήσει τις περιπτώσεις εκείνες στις οποίες δε θεωρούμε ούτε τον παραλήπτη του μηνύματός μας αξιόπιστο. Ένα απλό παράδειγμα για να κατανοήσουμε το είδος αυτής της κρυπτογράφησης θα μπορούσε να ήταν το εξής : Έστω ότι έχουμε δύο σύνολα. Στο μεν πρώτο οι θετικοί πραγματικοί αριθμοί, στο δε δεύτερο οι λογάριθμοι τους. Τότε, ο πολλαπλασιασμός των πραγματικών αυτών αριθμών και η πρόσθεση των λογαρίθμων τους είναι δύο ομομορφικές πράξεις. Κι αυτό γιατί για κάθε x,y,z στο σύνολο των θετικών πραγματικών αριθμών ισχύει πως αν $x \cdot y = z$ τότε και $\log(x) + \log(y) = \log(z)$. Ο ομομορφισμός αυτός στην ουσία μας επιτρέπει να καταλήξουμε στο z με δύο τρόπους [118] . Αυτή ακριβώς είναι και η βάση της ομομορφικής κρυπτογράφησης η οποία μας επιτρέπει είτε να κάνουμε πράξεις απ’ ευθείας πάνω στα x και y είτε να κρυπτογραφούμε τα x και y, να εφαρμόσουμε μια σειρά πράξεων στα κρυπτογραφήματά τους και έπειτα να αποκρυπτογραφούμε το αποτέλεσμα για να φτάσουμε στην ίδια

απάντηση. Με τον τρόπο αυτό διαφυλάσσουμε και την ιδιωτικότητα των μηνυμάτων μας χωρίς τεχνικές ανωνυμίας (π.χ. mixnets, blind signatures κτλ.). Στην αρχιτεκτονική των Ruj et al. όπως έχουμε ήδη πει αξιοποιείται το ομομορφικό ως προς την πρόσθεση κρυπτοσύστημα του Paillier εξαιτίας του γεγονότος ότι αυτό που θέλουμε να πετύχουμε είναι το aggregation των δεδομένων. Συγκεκριμένα κάθε μετρητής στην αρχιτεκτονική αυτή κρυπτογραφεί τις μετρήσεις που έχει συλλέξει αξιοποιώντας το κρυπτοσύστημα Paillier και το δημόσιο κλειδί της πλησιέστερης σε αυτόν αξιόπιστης οντότητας στη διαδρομή προς τη ρίζα του aggregation tree. Η αξιόπιστη αυτή οντότητα αποκρυπτογραφεί το aggregate των μετρήσεων για κάθε χαρακτηριστικό και έπειτα αξιοποιεί attribute-based- encryption για να εξασφαλίζει και access-control. Περισσότερα για αυτό το είδος κρυπτογράφησης θα παρουσιαστούν στην ενότητα της εξουσιοδότησης.

Στο ίδιο μήκος κύματος κινείται και η προσέγγιση των Li et al. στο [119] η οποία αξιοποιεί aggregation σε όλους τους μετρητές που θα λάβουν μέρος στη δρομολόγηση ενός μηνύματος από τον αποστολέα μετρητή μέχρι την εταιρεία παροχής. Η λογική πίσω από την προσέγγιση των Li et al. στηρίζεται στην κατασκευή ενός aggregation tree το οποίο συνδέει κατά τρόπο αποδοτικό τους κόμβους μιας γειτονιάς. Κάθε κόμβος του δέντρου αυτού, το οποίο ουσιαστικά είναι ένα spanning tree για τον γράφο που απεικονίζει το δίκτυο των διασυνδεδεμένων μετρητών μιας γειτονιάς, συλλέγει δεδομένα από τα παιδιά του, υπολογίζει ένα aggregate των δεδομένων αυτών (μέσω όρο/διασπορά κ.α.) με τα δικά του και ακολούθως δρομολογεί το δικό του ενδιάμεσο αποτέλεσμα στον γονέα του ο οποίος συνεχίζει τη διαδικασία μέχρι το αποτέλεσμα να φτάσει στη ρίζα του δέντρου. Εκεί, συναντάμε τον collector, ο οποίος αναλαμβάνει την επικοινωνία με την εταιρεία παροχής. Η ιδιωτικότητα της πληροφορίας στο μοντέλο αυτό διασφαλίζεται μέσω ομομορφικής κρυπτογράφησης Paillier, γεγονός που επιτρέπει στους ενδιάμεσους μετρητές να συμμετέχουν στη συγχώνευση των δεδομένων χωρίς να γνωρίζουν επί μέρους ή τελικά αποτελέσματα.

Ένα εξίσου ενδιαφέρον σύστημα διασφάλισης της ιδιωτικότητας της επικοινωνίας στο πλαίσιο του Smart Grid, προτάθηκε από τους Chim et al. στο[120]. Στο σύστημα αυτό η ιδιωτικότητα επιτυγχάνεται αξιοποιώντας τη λογική των ανώνυμων διαπιστευτηρίων (anonymous credentials) και τις «τυφλές υπογραφές» (bling signatures). Σε αντίθεση με τα προηγούμενα άρθρα που έχουμε παρουσιάσει, το συγκεκριμένο, ασχολείται με την εξασφάλιση της ιδιωτικότητας όχι κατά τη μεταφορά στοιχείων κατανάλωσης από τον κατ' οίκον μετρητή στην εταιρεία παροχής, αλλά κατά την υποβολή από πλευράς του πελάτη

αίτησης για περισσότερη ενέργεια από αυτήν που του παρέχει η εταιρεία για κάποιο συγκεκριμένο χρονικό διάστημα. Το προτεινόμενο σύστημα αποτελείται από τέσσερα θεμελιώδη επίπεδα. Στο πρώτο, η εταιρεία παροχής επιλέγει ένα RSA ζεύγος δημόσιου-ιδιωτικού κλειδιού για να υπογράφει διαπιστευτήρια και να επιτρέπει στους μετρητές να κρυπτογραφούν μηνύματα προς αυτήν· και έναν αριθμό n ο οποίος θα χρησιμοποιηθεί ακολούθως. Στο επόμενο επίπεδο, κάθε έξυπνος μετρητής (ο οποίος αποκτά το δικό του μοναδικό ID κατά την εισαγωγή του στο δίκτυο) παράγει n φορές περισσότερα διαπιστευτήρια (credentials) από όσα χρειάζονται, με κάθε credential να έχει το δικό του αναγνωριστικό αριθμό και την ημερομηνία κατά την οποία εκδόθηκε. Τα credentials αυτά, υπογράφονται με ένα τυχαίο αριθμό (blinding factor) ο οποίος εξασφαλίζει την ανωνυμία των δεδομένων· και αποστέλλονται στην εταιρεία παροχής. Εκείνη για κάθε n credentials προκαλεί τον μετρητή να ανοίξει n-1 από αυτά και να πιστοποιήσει την πληροφορία. Αν ο μετρητής πιστοποιήσει πως όλα τα credentials που ανοίχτηκαν ήταν έγκυρα, τότε η εταιρεία παροχής υπογράφει το credential που έμεινε. Το credential αυτό αποστέλλεται ακολούθως στον μετρητή και η εταιρεία παροχής αυξάνει τον μετρητή των υπογεγραμμένων διαπιστευτηρίων.

Μετά τις συγκεκριμένες ρυθμίσεις, μια μέρα ή βδομάδα πριν την προγραμματισμένη χρήση ενέργειας οι έξυπνοι μετρητές, κατόπιν επικοινωνίας με τις συσκευές δημιουργούν πίνακες ανάγκης ενέργειας στους οποίους καταγράφουν πότε και πόση επιπλέον ποσότητα ενέργειας θα χρειαστούν. Στη συνέχεια οι έξυπνοι μετρητές κατεβάζουν τις τελευταίες χρεώσεις ενέργειας και αναλόγως αξιοποιούν τα credentials (π.χ. για ενέργεια κατά τη διάρκεια των ωρών αιχμής πρέπει να χρησιμοποιηθούν πιο πολλά credentials). που κατέχουν για να δημιουργήσουν ένα πλάνο χρήσης ενέργειας. Το πλάνο αυτό κρυπτογραφείται με συμμετρικό τρόπο κάνοντας χρήση ενός session key το οποίο κρυπτογραφείται με ασύμμετρο τρόπο χρησιμοποιώντας το δημόσιο κλειδί της εταιρείας παροχής η οποία θα αποκρυπτογραφήσει το μήνυμα, θα επιβεβαιώσει την εγκυρότητα των credentials και θα ανταποκριθεί προγραμματίζοντας την διάθεση ενέργειας στο υποστατικό. Στο τέλος κάθε χρεωστικής περιόδου, ο πελάτης αυθεντικοποιείται στην εταιρεία παροχής παραδίδει τα credentials που δε χρησιμοποίησε και η εταιρεία καθορίζει το ποσό που οφείλει. Μέσα από αυτό το σύστημα εξασφαλίζεται μεταξύ άλλων η εμπιστευτικότητα του μηνύματος μέσω κρυπτογράφησης, η αυθεντικοποίηση κάθε μετρητή ο οποίος κατά την εισαγωγή του στο σύστημα πριν να ζητήσει credentials, πρέπει να πιστοποιήσει τον εαυτό του υπογράφοντας με το ιδιωτικό του κλειδί και η ιδιωτικότητα που διαφυλάχθηκε μέσα από τη χρήση των credentials τα οποία δε μπορούν με κανένα τρόπο να αποδοθούν σε οποιοδήποτε μετρητή/υποστατικό.

Οι Shi et al. στο[121] έρχονται να προτείνουν ένα δικό τους μοντέλο ιδιωτικότητας που στηρίζεται στη λογική του perturbation, το οποίο επιτρέπει σε ένα σύνολο συμμετεχόντων να ανεβάζει κατά περιόδους κρυπτογραφημένα δεδομένα σε έναν aggregator, με τέτοιο τρόπο που για κάθε περίοδο ο aggregator αυτός να μπορεί να αποκρυπτογραφήσει aggregate statistics για τα δεδομένα που έλαβε από όλους τους μετρητές που συνδέονται με αυτόν. Το μοντέλο αυτό θεωρείται aggregator oblivious από τη στιγμή που καμία επιπλέον πληροφορία δεν γνωστοποιείται στον aggregator πέρα από αυτή που ο ίδιος μπορεί να εξάγει από τις γνώσεις του. Με το μοντέλο αυτό κάθε μετρητής μπορεί να ανεβάσει στο σύστημα ένα κρυπτογραφημένο μήνυμα στο οποίο εσκεμμένα εμβάλλει τυχαίο θόρυβο (τον οποίο παράγει μέσω μιας γεωμετρικής κατανομής) που εγγυάται ότι το άθροισμα των τυχαίων θορύβων όλων των μηνυμάτων θα εξασφαλίσει το differential privacy του τελικού αποτελέσματος. Η κρυπτογράφηση των δεδομένων που αποστέλλουν οι μετρητές γίνεται αξιοποιώντας hash λειτουργίες (SHA-256), δύο modular exponentiations και ένα πολλαπλασιασμό σε ένα Diffie-Helman group.Τα κρυπτογραφημένα μηνύματα μεταφέρονται στον aggregator ο οποίος έχει ένα δικό του share με το οποίο κάνει brute-force/ Pollard's lambda method αποκρυπτογράφηση των ιδιωτικών κρυπτογραφημάτων.

Σε μια άλλη προσέγγιση οι Acs και Castellucia στο [122], προτείνουν ένα σύστημα το οποίο διασφαλίζει την ιδιωτικότητα βασισμένο σε ένα ομομορφικό ως προς την πρόσθεση σύστημα κρυπτογράφησης το οποίο εντούτοις δε χρησιμοποιεί τη λογική Paillier (ή άλλους μηχανισμούς για secret sharing οι οποίοι θεωρούνται πιο υπολογιστικά απαιτητικοί). Οι μετρήσεις κατανάλωσης κάθε μετρητή σε αυτό το σύστημα κρυπτογραφούνται με ένα απλό και αποδοτικό κρυπτοσύστημα στο οποίο η κρυπτογράφηση ορίζεται ως το αποτέλεσμα μιας πρόσθεσης της μέτρησης με το κλειδί modulo έναν μεγάλο αριθμό. Το κρυπτοσύστημα αυτό είναι επίσης ομομορφικό ως προς την πρόσθεση γεγονός το οποίο συνεπάγεται πως :

$$E(k_1,m_1) + E(k_2,m_2) = m_1 + k_1 + m_2 + k_2 \bmod n$$
$$= E((k_1+k_2),(m_1+m_2))$$

Στο πρωτόκολλο αυτό οι κόμβοι (Smart Meters) ομαδοποιούνται σε clusters μεγέθους N. Από τη στιγμή της εγκατάστασής του στο δίκτυο ένας κόμβος παρέχει το δικό του Diffie-Hellman component υπογεγραμμένο από τον ίδιο και συνοδευόμενο από το πιστοποιητικό του, στην εταιρεία παροχής. Η οποία για κάθε νέο κόμβο που εισάγεται στο δίκτυο, αναμεταδίδει τα πιστοποιητικά και τα Diffie-Hellman components όλων των κόμβων. Κάθε κόμβος στο cluster μπορεί να υπολογίσει και να διατηρεί ένα pairwise κλειδί με οποιοδήποτε κόμβο εντός του cluster επιθυμεί να επικοινωνεί. Απλοποιώντας λίγο τα πράγματα, ας

υποθέσουμε ότι η Alice επιθυμεί να επικοινωνεί με τον Bob και τον Charlie. Αφού αποφασιστεί κάτι τέτοιο τόσο η Alice όσο και ο Bob τροφοδοτούν με το κοινό κλειδί τους ένα γεννήτορα ψευδοτυχαίων αριθμών και λαμβάνουν ένα τυχαίο αριθμό $r_{1,2}$. Ο αριθμός αυτός θα προστίθεται στις μετρήσεις τις Alice αλλά θα αφαιρείται από τις μετρήσεις του Bob. Η ίδια διαδικασία θα επαναληφθεί και με τον Charlie παράγοντας ένα $r_{1,3}$ το οποίο η Alice θα προσθέτει στις ως τώρα μετρήσεις της, ενώ ο Charlie θ' αφαιρεί. Το τελικό άθροισμα στο οποίο καταλήγει η Alice θα κρυπτογραφηθεί με το κλειδί της εταιρείας παροχής ως ακολούθως :

$$E(K_{AliceUtility}, m_{1,t}) = m_{1,t} + r_{1,2} + r_{1,3} + K_{AliceUtility} \bmod n$$

Με παρόμοιο τρόπο οι Bob και Charlie στέλνουν και αυτοί τα μηνύματά τους στην εταιρεία παροχής κρυπτογραφημένα με το κοινό κλειδί που διατηρεί ο κάθε ένας με αυτήν. Η εταιρεία παροχής υπολογίζει τη συνάθροιση των μετρήσεων που έλαβε και λαμβάνει το άθροισμα των μηνυμάτων σε καθαρό κείμενο αφαιρώντας τα κλειδιά.

$$\begin{aligned} Sum = {} & E(K_{AliceUtility}, m_{1,t}) + E(K_{BobUtility}, m_{2,t}) + E(K_{CharlieUtility}, m_{3,t}) = \\ & (m_{1,t} + r_{1,2} + r_{1,3} + K_{AliceUtility} \bmod n \\ & + m_{2,t} - r_{1,2} + r_{2,3} + K_{BobUtility} \bmod n \\ & + m_{3,t} - r_{1,3} - r_{2,3} + K_{CharlieUtility} \bmod n) \end{aligned}$$

$$= (m_{1,t} + m_{2,t} + m_{3,t} + K_{AliceUtility} + K_{BobUtility} + K_{CharlieUtility}) \bmod n$$

$$Sum - (K_{AliceUtility} + K_{BobUtility} + K_{CharlieUtility}) \bmod n = m_{1,t} + m_{2,t} + m_{3,t} \bmod n$$

Προφανώς με αυτό τον τρόπο οι επι μέρους μετρήσεις δεν αποκαλύπτονται ποτέ στην εταιρεία παροχής η οποία μπορεί να λάβει μόνο το άθροισμά τους. Για την εξασφάλιση της απόκρυψης της πληροφορίας οι Acs και Castellucia επιλέγουν να εφαρμόσουν Laplacian noise πάνω στο τελικό άθροισμα πριν να το κρυπτογραφήσουν (τεχνική η οποία εμπείπτει στη λογική του perturbation). Για να το επιτύχουν αυτό κάθε επιμέρους μετρητής εφαρμόζει ένα gamma noise πάνω στη μέτρησή του πριν να την κρυπτογραφήσει άρα κάθε $m_{i,t}$ που εντοπίσαμε προηγουμένως ήταν το αποτέλεσμα της πρόσθεσης του γνήσιου μηνύματος ($mo_{i,t}$) με δύο τυχαίες τιμές που επιλέγηκαν ανεξάρτητα από την ίδια γάμμα κατανομή.

$$m_{i,t} = mo_{i,t} + G_1(N,\lambda) - G_2(N,\lambda)$$

Τέλος, μια διαφορετική ιδέα για εξασφάλιση ιδιωτικότητας, ακολουθώντας τη λογική του obfuscation, παρουσιάστηκε από τους Varodayan και Khisti στο [123] κι έχει να κάνει με τη χρήση μιας επαναφορτιζόμενης μπαταρίας που θα επιτρέπει σε ένα υποστατικό να αποκρύπτει μερικώς στοιχεία που αφορούν στην κατανάλωσή του διαφυλάσσοντας έτσι την ιδιωτικότητα των ενοίκων του. Η μπαταρία αυτή, χρησιμοποιείται με τέτοιο τρόπο, ώστε να εισέρχεται σε αυτή το aggregate load όλων των συσκευών του υποστατικού και να εξέρχεται από αυτή το συνολικό φορτίο της σε συνδυασμό με το aggregate load, το οποίο ο μετρητής θα αναφέρει στην υπηρεσία. Ανά πάσα στιγμή, το φορτίο που φθάνει από την εταιρεία παροχής στην μπαταρία μπορεί είτε να δρομολογηθεί στις συσκευές του υποστατικού, είτε να αποθηκευτεί για μελλοντική χρήση. Με τον τρόπο αυτό φορτίζοντας και αποφορτίζοντας την μπαταρία μπορούμε να χειριζόμαστε το φορτίο εξόδου και άρα να αποκρύπτουμε μερικώς την πληροφορία του φορτίου εισόδου. Το μοντέλο αυτό λειτουργεί στοχαστικά δηλαδή κάθε απόφαση για αλλαγή της κατάστασης της μπαταρίας (φόρτιση/αποφόρτιση), όταν κάτι τέτοιο επιβάλλεται, μπορεί να προκύψει με συγκεκριμένη πιθανότητα. Ένας αλγόριθμος trellis αξιοποιείται για να υπολογίσει το ρυθμό διαρροής πληροφορίας μεταξύ εισόδου-εξόδου της μπαταρίας.

5.3 Εξασφαλίζοντας Ακεραιότητα, Αυθεντικοποίηση και Μη Αποποίηση Ευθύνης

Πέραν της εμπιστευτικότητας των δεδομένων, εξίσου σημαντική (αν όχι σημαντικότερη) στα πλαίσια του Smart Grid είναι η εξασφάλιση της ακεραιότητας και της αυθεντικότητας των δεδομένων. Η ενότητα αυτή αφιερώνεται ακριβώς σε αυτά τα δύο βασικά θέματα, καταλήγοντας με τρόπους με τους οποίους θα μπορούσαμε να επιτύχουμε και μη αποποίηση ευθύνης.

5.3.1 Εξασφαλίζοντας Ακεραιότητα

Ανάμεσα στις σπουδαιότερες επιθέσεις κατά της ακεραιότητας δεδομένων που εντοπίσαμε στο προηγούμενο κεφάλαιο, ήταν οι επιθέσεις που είχαν να κάνουν με την τροποποίηση του περιεχομένου των μηνυμάτων (Message Modification Attacks).

Μέθοδοι όπως τα Checksums και τα Cyclic Redundancy Checks (CRCs), οι οποίες αξιοποιούνται κάτω από πολλές περιπτώσεις σήμερα για την επικύρωση της ακεραιότητας των μεταφερόμενων δεδομένων, σχεδιάστηκαν για να μπορούν να ανιχνεύσουν αποτελεσματικά, την αλλοίωση των δεδομένων κατά τη μεταφορά τους. Παρόλα αυτά, οι τεχνικές αυτές δε μπορούν να θεωρηθούν ασφαλείς αφού τα μηνύματα μπορούν εύκολα να παραποιηθούν ώστε να παράγουν τα ίδιο checksum ή CRC[92].

Για το λόγο αυτό, προτιμούμε για σκοπούς ακεραιότητας να αξιοποιούμε κρυπτογραφικές τεχνικές κατακερματισμού οι οποίες αν και πιο αργές και υπολογιστικά απαιτητικές, μπορούν να μας εγγυηθούν περισσότερη ασφάλεια. Ορισμένοι από τους πιο διαδεδομένους αλγόριθμους κατακερματισμού χρησιμοποιούνται σε πολλές εφαρμογές και πρωτόκολλα σήμερα όπως τα SSL/TLS, SSH, S/MIME, IPSec κτλ.. Ο πίνακας 5.2 παρουσιάζει τους αλγόριθμους εκείνους που εγκρίθηκαν από το NIST και ανήκουν σε αυτή την κατηγορία όπως περιλαμβάνεται στο [72].

Algorithm	**Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 AND SP 800-131)**	**Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 AND SP 800-131)**
Secure Hash Standard (SHS): Secure Hash Algorithm (SHA)	Sha-224 is Approved for all applications. Additionally, hash functions listed in the next column are Approved during this time.	SHA-256, SHA-384, and SHA-512 are Approved for all applications.

Πίνακας 5.2 Εγκεκριμένοι αλγόριθμοι ασφαλούς κατακερματισμού.

Εντοπίζοντας επιθέσεις κατά της ακεραιότητας δεδομένων στο προηγούμενο κεφάλαιο, αναφερθήκαμε μεταξύ άλλων σε επιθέσεις της μορφής False Data Injection. Τέτοιες επιθέσεις, όπως είχαμε πει και τότε, προέρχονται από την εισαγωγή ψευδών δεδομένων στο Grid από έναν κακόβουλο χρήστη και μπορούν σε πολλές περιπτώσεις να περάσουν εντελώς απαρατήρητες από το σύστημα με αποτέλεσμα τα επίπλαστα δεδομένα τους να χρησιμοποιούνται από κρίσιμης σημασίας αλγόριθμους του Smart Grid (όπως για παράδειγμα τον αλγόριθμο που αναλαμβάνει την πρόβλεψη ζήτησης της επόμενης ημέρας ή το state estimation) επηρεάζοντας σημαντικά τη λειτουργία του.
Αρκετές μελέτες στη σύγχρονη βιβλιογραφία ασχολήθηκαν με τρόπους με τους οποίους θα μπορούσαμε να εντοπίσουμε και να καταπολεμήσουμε τα False Data Injection Attacks. Πιο κάτω παρουσιάζουμε δύο από αυτές.

Αρχή κάνουμε με τη δουλειά των Bhattarai, Ge και Yu στο [124], μέσω της οποίας προτείνεται η αξιοποίηση μιας τεχνικής ψηφιακής υδατογράφησης για τους σκοπούς καταπολέμησης των False Data Injection Attacks. Με τον όρο ψηφιακή υδατογράφηση, αναφερόμαστε στην τεχνική η οποία εισάγει σε ένα μήνυμα ένα υδατογράφημα, δηλαδή επιπλέον ψηφιακά δεδομένα, που μεταφέρουν μοναδική πληροφορία σχετικά με τον

ιδιοκτήτη της συγκεκριμένης πληροφορίας, πληροφορίες εντοπισμού αλλοίωσης κ.α.. Η μέθοδος των Bhattarai, Ge και Yu, έχει να κάνει με τη δημιουργία από πλευράς του μετρητή, δύο όμοιων και συγχρονισμένων υδατογραφημάτων από τα οποία το ένα αξιοποιείται για την υδατογράφηση των δεδομένων που μεταφέρονται προς την εταιρεία παροχής σε πραγματικό χρόνο πάνω από υψηλής ταχύτητας συνδέσεις (που είναι επιρρεπείς σε επιθέσεις) ενώ το άλλο μεταφέρεται από ένα μικρότερου εύρους αλλά μεγαλύτερης ασφάλειας κανάλι προς την εταιρεία παροχής. Η εταιρεία παροχής και άλλες συσκευές του δικτύου (π.χ. aggregators), λαμβάνουν, τόσο τα υδατογραφημένα δεδομένα όσο και το υδατογράφημα, για να ελέγξουν τα δύο μεταξύ τους και να εντοπίσουν τυχόν False Data Injection Attacks.

Αυτού του τύπου επιθέσεις στοχεύουν να αντιμετωπίσουν και οι Huang et. al στο [125], αξιοποιώντας ένα adaptive cumulative sum test για τον εντοπισμό κακόβουλων ενεργειών το συντομότερο δυνατό. Ο δικός τους μηχανισμός έχει ως στόχο τον εντοπισμό bad data injection attacks όσο το δυνατό πιο γρήγορα και με τον μικρότερο δυνατό αριθμό παρατηρήσεων. Για να επιτύχουν το στόχο αυτό αξιοποιούν στατιστική ανάλυση των δεδομένων, προσπαθώντας παράλληλα να περιορίσουν το ποσοστό σφάλματος. Ο αλγόριθμος που αξιοποιούν είναι μια επέκταση του αλγόριθμου CUSUM όπως προτείνεται από τον Page[126] με τη διαφορά ότι ο αλγόριθμος που προτείνουν οι συγγραφείς, μπορεί να λειτουργήσει και κάτω από άγνωστες παραμέτρους επίθεσης.

Παρόμοιου τύπου επιθέσεις, και συγκεκριμένα μη ανιχνεύσιμες επιθέσεις τύπου sparse attacks, στοχεύουν να αντιμετωπίσουν με τη δική τους πρόταση και οι Giani et al. στο [127]. Συγκεκριμένα, έχοντας περιγράψει τον όρο της μη ανιχνεύσιμης επίθεσης ακεραιότητας, ως της επίθεσης κατά την οποία τα στοιχεία κατανάλωσης που καταγράφουν οι μετρητές παραποιούνται με τέτοιο τρόπο που να μην εγείρονται οποιεσδήποτε υποψίες· και υπογραμμίζοντας πως τέτοιου τύπου επιθέσεις χρειάζονται συνήθως των συντονισμό πολύ μικρού αριθμού μετρητών, οι συγγραφείς προτείνουν τη δική τους μέθοδο αντιμετώπισης των επιθέσεων αυτών. Η μέθοδος αυτή, στηρίζεται ουσιαστικά στην τοποθέτηση σε συγκεκριμένους δίαυλους, κάποιων PMUs τα οποία θεωρούνται ασφαλή εξ’ ορισμού, με στόχο την αξιοποίηση των μετρήσεων που λαμβάνουν (phase angles) για ανίχνευση παράξενης συμπεριφοράς. Η εύρεση του ελάχιστου αριθμού των PMUs που πρέπει να τοποθετηθούν για να επιτευχθεί η ανίχνευση μιας τέτοιας επίθεσης, είναι όπως χαρακτηριστικά αναφέρουν οι συγγραφείς του άρθρου, ένα NP-τύπου πρόβλημα. Κατά συνέπεια, αρκούνται στο να εντοπίσουν ποιος αριθμός PMUs θα μπορούσε να ανιχνεύσει επαρκώς ένα σύνολο από μη ανιχνεύσιμες επιθέσεις, καταλήγοντας στο ότι αρκούν p+1

PMUs τοποθετημένα σε συγκεκριμένα σημεία στο δίκτυο για να εντοπιστούν p διαφορετικές μη ανιχνεύσιμες επιθέσεις.

Άλλου τύπου επιθέσεις κατά της ακεραιότητας των δεδομένων που εντοπίσαμε στο προηγούμενο κεφάλαιο είχαν να κάνουν με Device Impersonation Attacks. Τέτοιες επιθέσεις θα μπορούσαν να αντιμετωπιστούν με τη χρήση Load Profiling αλγορίθμων. Μια τέτοια μέθοδος περιγράφεται από τους Aravithan., Namboodiri, Sunku και Jewell στο [43].

Τέλος, μια άλλη κατηγορία επιθέσεων κατά της ακεραιότητας των δεδομένων που παρουσιάσαμε στο προηγούμενο κεφάλαιο, αφορούσε στα Replay Attacks. Τις επιθέσεις δηλαδή κατά τις οποίες μηνύματα που αποστέλλονται, καταγράφονται από κακόβουλους χρήστες με στόχο την αναμετάδοσή τους σε μετέπειτα χρονικές στιγμές. Τέτοιου τύπου επιθέσεις μπορούν να αντιμετωπιστούν με διάφορους τρόπους στα πλαίσια του Smart Grid. Συγκεκριμένα όπως προτείνεται από τους Aravithan., Namboodiri, Sunku και Jewell στο [43], οι επιθέσεις αυτές, θα μπορούσαν να αποφευχθούν με τη χρήση timestamps, sequence numbers ή ακόμα και χρησιμοποιώντας session keys. Η χρήση timestamps στα πακέτα μας επιτρέπει να εντοπίσουμε πότε ο χρόνος αποστολής που αναγράφεται πάνω σε ένα συγκεκριμένο πακέτο, διαφέρει ουσιαστικά από την τρέχουσα ώρα για να το αγνοήσουμε. Την ίδια στιγμή, τα sequence numbers, μας εξυπηρετούν στο να εντοπίζουμε διπλότυπα πακέτα ή πακέτα τα οποία προκύπτουν εκτός σειράς ενώ, η χρήση session keys μπορεί, αν και πιο πολύπλοκη από τις δύο πιο πάνω μεθόδους, να συμβάλει και αυτή, στον εντοπισμό πακέτων τα οποία είναι προϊόντα Replay-Attack. Εναλλακτικά, οι Xiao et al. [128] προτείνουν για την αντιμετώπιση των Replay Attacks να αξιοποιούνται ψευδοτυχαίοι αριθμοί (nonce) στα διάφορα μηνύματα, με κάθε αριθμό να χρησιμοποιείται μόνο μια φορά, κάνοντας έτσι τα πακέτα μοναδικά. Έναν διαφορετικό τρόπο αντιμετώπισης των Replay Attacks ο οποίος στηρίζεται, στην έννοια της αυθεντικοποίησης στο φυσικό επίπεδο, ανεξάρτητα από τη μέθοδο που χρησιμοποιείται για να λάβει ο κακόβουλος χρήστης πρόσβαση στο σύστημα ελέγχου, προτείνουν οι Mo et.al στο [24].

5.3.2 Εξασφαλίζοντας Αυθεντικότητα και Μη αποποίηση ευθύνης.

Εξίσου μεγάλης σημασίας με την εξασφάλιση της ακεραιότητας των μηνυμάτων που αποστέλλονται στο Smart Grid, είναι και η εξασφάλιση της αυθεντικότητας των οντοτήτων του και των μηνυμάτων που αυτές αποστέλλουν, αλλά και η δυνατότητα εξασφάλισης μη αποποίησης ευθύνης. Η επιβεβαίωση ότι μια οντότητα είναι πράγματι αυτή που ισχυρίζεται πως είναι καθώς επίσης και η διαβεβαίωση ότι ανά πάσα στιγμή μπορούμε να αποδείξουμε

την αλήθεια οποιουδήποτε ισχυρισμού έχει να κάνει με την αποστολή/παραλαβή ή μη μηνυμάτων στο Smart Grid, αποτελούν επίσης θέμα μελετών της σύγχρονης βιβλιογραφίας για θέματα ασφάλειας στο Smart Grid.

Ανάμεσα στους τρόπους εξασφάλισης αυθεντικοποιήσης, ακεραιότητας και μη αποποίησης ευθύνης προτείνονται τόσο οι συνηθισμένοι τρόποι που αξιοποιούνται σήμερα στα δίκτυα όσο και πολλοί νέοι. Συγκεκριμένα, σε ότι αφορά στις ήδη υφιστάμενες τεχνικές[92], προτείνονται οι αλγόριθμοι κατακερματισμού που κάνουν χρήση κλειδιού αλλά και οι ψηφιακές υπογραφές. Ένα παράδειγμα αλγόριθμου κατακερματισμού με κλειδί είναι ο HMAC ο οποίος σχεδιάστηκε για να μπορεί να χρησιμοποιηθεί με οποιαδήποτε συνάρτηση κατακερματισμού από αυτές που είδαμε στον πίνακα 5.2. Σε ότι αφορά τώρα στις ψηφιακές υπογραφές, το Digital Signature Standard (DSS) ορίζει ένα μηχανισμό για την εξασφάλιση αυθεντικότητας των μηνυμάτων με την βοήθεια ασύμμετρης κρυπτογράφησης. Ο μηχανισμός αυτός λειτουργεί ως εξής : πριν την αποστολή του μηνύματος, ο αποστολέας δημιουργεί ένα hash του μηνύματος το οποίο κρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί. Όταν ο παραλήπτης λάβει το μήνυμα, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφηση του hash ενώ υπολογίζει μόνος του το hash του μηνύματος που έχει λάβει. Εάν το αποκρυπτογραφημένο hash ταιριάζει με την υπολογιζόμενη τιμή από το μήνυμα που δέχτηκε, ο παραλήπτης μπορεί να είναι σίγουρος πως το μήνυμα στάλθηκε όντως από τον αποστολέα που ισχυρίζεται πως το έστειλε και έφτασε σε αυτόν άθικτο. Κατά συνέπεια, η ψηφιακή υπογραφή διασφαλίζει την αυθεντικότητα και ακεραιότητα του μηνύματος. Επιπλέον, ο αποστολέας μπορεί να απαιτήσει παραλαβή υπογεγραμμένης επιβεβαίωσης γεγονός που θα μπορούσε να αποτελέσει απόδειξη για τον αποστολέα πως ο παραλήπτης όντως δέχτηκε το μήνυμα του (καλύπτοντας έτσι το στόχο της μη αποποίησης ευθύνης).
Το DSS πρότυπο αναγνωρίζει τρεις διαφορετικούς αλγορίθμους παραγωγής υπογραφών. Και οι τρεις αλγόριθμοι είναι αποδεκτοί από την NIST για χρήση στα Smart Grids και φαίνονται στον πίνακα 5.3 [73]. Παρατηρούμε, πως όπως και σε άλλα πρότυπα κρυπτογράφησης, μεγαλύτερα κλειδιά χρησιμοποιούνται για την σχεδίαση εφαρμογών μετά το 2030.

Εναλλακτικοί τρόποι προστασίας κατά των επιθέσεων αυθεντικότητας και των περιστατικών αποποίησης ευθύνης, προτάθηκαν επίσης και μέσα από τη σύγχρονη βιβλιογραφία. Πιο κάτω, παρουσιάζουμε ορισμένες ιδέες που θεωρήσαμε ενδιαφέρουσες.

Algorithm	Algorithms/Key Lengths for use between 2011-2029	Algorithms/Key Lengths for use now and beyond 2030
Digital Signature Standard (DSS): Digital Signature Algorithm (DSA) RSA digital signature algorithm (RSA) Elliptic Curve Digital Signature Algorithm (ECDSA)	DSA with (L=2048,N=224) or (L=2048, N=256) RSA with (|n|=2048) ECDSA2 with curves P-224,K-233, or B-233	DSA with (L=3072, N=256)** RSA with (|n|=3072)** ECDSA2 with curves P-256,P-384,P-521,K-283,K-409,K-571,B-283,B-283,B-409,B-571 **For CAs only

Πίνακας 5.3 Εγκεκριμένοι Ασύμμετροι Αλγόριθμοι.

Οι Nabeel, Kerr, Ding και Bertino προτείνουν στο [129] τη δική τους προσέγγιση για εξασφάλιση αυθεντικοποιήσης των μετρητών που επικοινωνούν μεταξύ τους στα πλαίσια του Smart Grid, κάνοντας χρήση Physically Unclonable Functions – PUFs, μιας τεχνολογίας η οποία παρέχει αυθεντικοποίηση σε επίπεδο hardware. Οι μετρητές στην προσέγγιση αυτή, διατηρούν ένα συμμετρικό κλειδί το οποίο χρησιμοποιούν για σκοπούς κρυπτογράφησης, δημιουργούν ένα Message Authentication Code (MAC), και διατηρούν παράλληλα και συνθηματικά πρόσβασης μέσω των οποίων εξασφαλίζουν έλεγχο πρόσβασης στα δεδομένα τους. Κάπως έτσι η μέθοδος αυτή μπορεί να εξασφαλίσει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων, αλλά και την εξουσιοδότηση πρόσβασης σε αυτά. Η αυθεντικοποίηση που υπόσχεται η μέθοδος, προκύπτει από τη χρήση PUFs, μονόδρομων συναρτήσεων οι οποίες «ενσωματώνονται» σε μια φυσική δομή. Στην ουσία μια PUF λαμβάνει ως είσοδο μια πρόκληση (challenge) και επιστρέφει μια απάντηση (response). Οι συναρτήσεις αυτού του τύπου βασίζονται πάνω στην τυχαιότητα που υπάρχει αναπόφευκτα σε ολοκληρωμένα κυκλώματα, με αποτέλεσμα ακόμα και δύο φαινομενικά ίδια PUFs παράγουν εντελώς ξεχωριστές συναρτήσεις, οδηγώντας στην αυθεντικοποίηση των μετρητών μας.

Οι Fouda et al. [130] από την άλλη προτείνουν τη δική τους lightweight μέθοδο δύο βημάτων για αμοιβαία αυθεντικοποίηση. Συγκεκριμένα οι συγγραφείς, παρουσιάζουν ένα πλαίσιο το οποίο αποτελείται από τρία ξεχωριστά επίπεδα. Στο πρώτο επίπεδο, τοποθετούν την αυθεντικοποίηση η οποία θεωρούν ότι θα βασίζεται είτε σε πρωτόκολλα της μορφής Diffie-Helman, είτε σε πρωτόκολλα της μορφής SIGn-and-Mac(SIGMA), είτε σε πρωτόκολλα όπως το IKEv2. Στο επόμενο επίπεδο, συναντάμε θέματα που αφορούν στη διαχείριση της

επικοινωνίας, όπου οι συγγραφείς τοποθετούν τόσο θέματα κρυπτογράφησης (για την οποία προτείνουν τους αλγόριθμους DES, AES, RSA) όσο και θέματα προστασίας από άκρο σε άκρο της επικοινωνίας (όπου προτείνονται τα IPSec και Virtual Tunnel). Στο τρίτο επίπεδο το οποίο αφορά σε παρακολούθηση της κατάστασης του δικτύου και προστασία του, οι συγγραφείς τοποθετούν συστήματα Intrusion Detection, συστήματα επιβεβαίωσης της ασφάλειας ενημερώσεων και συστήματα ανταπόκρισης σε επιθέσεις. Ακολούθως, οι συγγραφείς επικεντρώνονται στο πρώτο επίπεδο και προτείνουν τη δική τους μέθοδο για εξασφάλιση αυθεντικοποιήσης. Η μέθοδος τους, εγγυάται την αμοιβαία αυθεντικοποίηση και επιτυγχάνει τη δημιουργία ενός session key μεταξύ των έξυπνων μετρητών που επικοινωνούν. Μια απλουστευμένη περιγραφή του τρόπου λειτουργίας της συγκεκριμένης μεθόδου θα μπορούσε να ήταν η εξής: Έστω ότι έχουμε δύο συσκευές ένα HAN Gateway (X) και ένα BAN Gateway(Y) οι οποίες θέλουν να επικοινωνήσουν μεταξύ τους. Στο πρώτο βήμα της συγκεκριμένης επικοινωνίας ο X επιλέγει ένα τυχαίο αριθμό α ο οποίος ανήκει στο group Z_q* και υψώνει το g του στη δύναμη αυτή, στη συνέχεια κρυπτογραφεί την ταυτότητα του, την ταυτότητα του Y και το g^{α} με το δημόσιο κλειδί του Y στον οποίο αποστέλλει το μήνυμα. Ο Y με το που λαμβάνει το μήνυμα το αποκρυπτογραφεί και στέλνει τη δική του απάντηση στην οποία περιλαμβάνεται όλο το μήνυμα που έλαβε από τον X συν το δικό του g^b κρυπτογραφημένο με το δημόσιο κλειδί του X. Λαμβάνοντας αυτό το μήνυμα ο X λαμβάνει τα g^{α} και g^b (αποκρυπτογραφώντας με το ιδιωτικό του κλειδί). Αν το g^{α} είναι ορθό τότε ο X επιβεβαιώνει την αυθεντικότητα του Y, κι έπειτα χρησιμοποιώντας το g^b και το α υπολογίζει το session key (το οποίο αποτελεί το Hash των X,Y και $(g^b)^a$) στη συνέχεια ο X στέλνει στον Y το g^b. Ο Y επαναλαμβάνει τη διαδικασία που ολοκλήρωσε προηγουμένως ο X, αυθεντικοποιώντας τον και υπολογίζοντας επίσης το session key ως το hash των X,Y και $(g^a)^b$. Από τη στιγμή αυτή, οι δύο οντότητες έχουν πιστοποιήσει την αυθεντικότητα η μια της άλλης έχοντας εξασφαλίσει παράλληλα και ένα κοινό κλειδί για την επικοινωνία τους.

Πιο πρόσφατα οι Lu,Wang και Ma στο [131] , ασχολήθηκαν με την αυθεντικοποίηση και τη διαφύλαξη της ακεραιότητας σε συστήματα αυτοματοποίησης εντός υποσταθμών, αξιοποιώντας ένα μικρής κλίμακας πρότυπο στο οποίο τα μηνύματα προωθούνται χρησιμοποιώντας τυπικά συστήματα αυθεντικοποίησης όπως RSA, MAC και One-Time Signatures. Για σκοπούς επιλογής του πιο κατάλληλου συστήματος αυθεντικοποίησης οι συγγραφείς μελέτησαν την επίδοση και των τριών πιο πάνω κατηγοριών τεχνολογιών αυθεντικοποιήσης για να καταλήξουν τελικά στα εξής συμπεράσματα:

Ο RSA αλγόριθμος για σκοπούς αυθεντικοποίησης, θα ήταν καλύτερο να περιοριστεί σε εφαρμογές οι οποίες δεν έχουν αυστηρά χρονικά περιθώρια σε ότι αφορά την επιτρεπόμενη καθυστέρηση.

Οι λύσεις που βασίζονται σε MAC για σκοπούς αυθεντικοποίησης ενώ φαίνεται να μπορούν να εξυπηρετήσουν τον σκοπό αυτό και στα Smart Grids χρειάζονται ρυθμίσεις οι οποίες θα ενισχύουν την αποδοτικότητα τους.

Οι One-Time Signature μέθοδοι (HORS), παρά την καλύτερη επίδοσή τους (στα διάφορα πειράματα που διενεργήθηκαν από τους συγγραφείς), αφήνουν ανοικτό το περιθώριο για δύο νέους τύπους επιθέσεων.

Οι συγγραφείς δεν προτείνουν μια αποκλειστική λύση η οποία να εξασφαλίζει την αυθεντικοποίηση, αντίθετα συγκρίνουν μεταξύ τους τις διαφορετικές προσεγγίσεις σχολιάζοντας διάφορες παραμέτρους τους και περιγράφοντας συγκεκριμένους περιορισμούς που εντοπίζουν σε αυτές. Σε γενικές γραμμές, η επίδοση των MAC και HORS based τεχνικών φαίνεται αρκετά ικανοποιητική τόσο σε ενσύρματες (Ethernet) όσο και σε ασύρματες επικοινωνίες (WiFi).

Κλείνοντας την ενότητα αυτή, στρέφουμε το ενδιαφέρον μας στους τρόπους με τους οποίους μπορούμε να εξασφαλίσουμε τη μη αποποίηση ευθύνης. Η μη αποποίηση ευθύνης, είναι περισσότερο ένα νομικό θέμα το οποίο μπορούμε να επιλύσουμε με τη βοήθεια της τεχνολογίας σε αντίθεση με την αυθεντικοποίηση η οποία είναι καθαρά ένα τεχνικό θέμα. Παρόλα αυτά, εξακολουθεί να μας απασχολεί στο Smart Grid, για όλους τους λόγους που αναφέραμε στο προηγούμενο κεφάλαιο.

Οι Xiao et al. στο[128] ασχολήθηκαν με τρόπους εγγύησης της μη αποποίησης ευθύνης, παρουσιάζοντας μια στρατηγική αμοιβαίας παρακολούθησης μεταξύ μετρητών, στόχος της οποίας, είναι ο εντοπισμός προβληματικών μετρητών ή/και ανακριβών μετρήσεων. Η στρατηγική που προτείνεται για το σκοπό αυτό, έχει να κάνει με την εγκατάσταση μετρητών στα δύο άκρα του καναλιού που συνδέει ένα πελάτη με την υπηρεσία. Ο μετρητής που βρίσκεται στο άκρο του πελάτη λαμβάνει τη μέτρηση που αντιπροσωπεύει την κατανάλωσή του, ενώ ο μετρητής που βρίσκεται στο άκρο της εταιρείας παροχής αντιπροσωπεύει την ένδειξη που έφτασε στην εταιρεία παροχής. Τυπικά, οι δύο ενδείξεις θα διαφέρουν έως ένα βαθμό λόγω της απώλειας ισχύος κατά τη μεταφορά ενέργειας, λόγω σφαλμάτων που εισάγουν ο κακός συγχρονισμός και οι καθυστερήσεις που επηρεάζουν την επικοινωνία, αλλά και λόγω απρόβλεπτων παραγόντων όπως π.χ. η θερμοκρασία κτλ.. Διαφορά στις δύο ενδείξεις εντούτοις, μπορεί να προκαλέσει και μια οποιαδήποτε προσπάθεια επηρεασμού της

ένδειξης του μετρητή ως αποτέλεσμα κακόβουλης ενέργειας. Στόχος της πρότασης των Xiao et al. είναι ο εντοπισμός τέτοιων περιπτώσεων και η εγγύηση ότι οποιαδήποτε προσπάθεια αποποίησης ευθύνης κάτω από τέτοιες περιπτώσεις δε θα μπορούσε να ευσταθεί. Για τον σκοπό αυτό τα δύο άκρα έχουν την ευκαιρία να ανταλλάξουν τις ενδείξεις τους και να επιλύσουν τη διαφωνία, ελέγχοντας αν η διαφορά των δύο μετρήσεων ξεπερνά ένα συγκεκριμένο όριο το οποίο έχει τεθεί. Η μέθοδος αυτή, εγγυάται την εγκυρότητα των δεδομένων μέσα από κρυπτογράφηση δημόσιου κλειδιού, την ακεραιότητα μέσα από τη χρήση MAC σε κάθε μήνυμα, την προστασία κατά των spoofing attacks λόγω της σύνδεσης της πραγματικής ταυτότητας της οντότητας με το certificate το οποίο κατέχει, την προστασία κατά των Replay attacks μέσω nonces, την προστασία κατά των Man-In-The-Middle attacks και την εξασφάλιση υπευθυνότητας (accountability) από πλευράς των εμπλεκόμενων στην επικοινωνία μερών.

Εναλλακτικά οι Aravithan, Namboodiri, Sunku και Jewell στο [43] προτείνουν για την εξασφάλιση μη αποποίησης ευθύνης στα πλαίσια του AMI, τη χρήση μοναδικών κλειδιών για σκοπούς κρυπτογράφησης (αφότου οι οντότητες περάσουν από μια αρχική φάση αυθεντικοποίησης χρησιμοποιώντας τα δικά τους ζεύγη δημόσιου-ιδιωτικού κλειδιού) και τη διατήρηση από πλευράς του AMI ενός αρχείου που περιλαμβάνει όλες τις επικοινωνίες που είχε για ένα συγκεκριμένο χρονικό διάστημα. Εάν οποιοδήποτε εμπλεκόμενο στην επικοινωνία μέλος αμφισβητήσει την οποιαδήποτε συναλλαγή τότε το αρχείο αυτό θα μπορεί να χρησιμοποιηθεί για να επιλυθεί η όποια διαφορά και να μπορεί να εφαρμοστεί σωστά η οποιαδήποτε διαδικασία διερεύνησης από νομικές οντότητες.

5.4 Εξασφαλίζοντας Διαθεσιμότητα

Έχοντας ήδη μελετήσει τρόπους με τους οποίους μπορούμε να διασφαλίσουμε τους στόχους της εμπιστευτικότητας και της ακεραιότητας των δεδομένων στα πλαίσια του Smart Home/Smart Grid περιβάλλοντος, έφθασε πια η στιγμή να επικεντρώσουμε την προσοχή μας σε τρόπους με τους οποίους μπορούμε να διαφυλάξουμε τη διαθεσιμότητα του Smart Grid. Το κεφάλαιο αυτό, ασχολήθηκε με την εξασφάλιση των στόχων της εμπιστευτικότητας, της ακεραιότητας και τώρα της διαθεσιμότητας ακολουθώντας τη σειρά με την οποία παρουσιάζονται οι στόχοι στο γνωστό τρίπτυχο CIA – Confidentiality , Integrity, Availability το οποίο δεν θέτει κάποιον από τους τρεις στόχους πάνω από τους άλλους δύο. Πολλοί μελετητές του Smart Grid ωστόσο, εισηγούνται ότι σε ότι αφορά υποδομές κρίσιμης σημασίας όπως το Smart Grid το τρίπτυχο αυτό θα πρέπει να παρουσιάζεται ως AIC – Availability, Integrity, Confidentiality με τη σειρά να υποδηλώνει τη σημασία κάθε ενός από

τους τρεις θεμελιώδεις στόχους ασφάλειας[132]. Κάτι τέτοιο προφανώς, θέτει το στόχο της διαθεσιμότητας πάνω από τους άλλους δύο. Ο λόγος είναι μάλλον προφανής αν σκεφτούμε την κρισιμότητα του Smart Grid ως υποδομή, για την κοινωνία, την οικονομία και την ανάπτυξη.

Στο προηγούμενο κεφάλαιο εντοπίσαμε διάφορες απειλές κατά της διαθεσιμότητας του Smart Grid. Κοινός στόχος των απειλών αυτών, ήταν η υπερφόρτωση/κατάρρευση του δικτύου ή των επί μέρους τμημάτων του ώστε αυτό να μη μπορεί να ανταποκριθεί στις απαιτήσεις των χρηστών του. Παρά τη μεγάλη σημασία της διαθεσιμότητας, η βιβλιογραφία για τρόπους διασφάλισής της δεν είναι ιδιαίτερα πλούσια ακόμα. Το γεγονός αυτό όμως δε μας εμποδίζει να εντοπίσουμε ορισμένες ιδιαίτερα ενδιαφέρουσες προσεγγίσεις.

Αρχή κάνουμε με επιθέσεις κατά της διαθεσιμότητας στο φυσικό επίπεδο. Τέτοιου τύπου επιθέσεις θεωρούνται για παράδειγμα τα False Data Injection Attacks για τα οποία μιλήσαμε στην ενότητα που αφορούσε στην εξασφάλιση ακεραιότητας. Επιθέσεις τέτοιας μορφής μπορούν να πλήξουν τη διαθεσιμότητα, (παίρνοντας τη μορφή ενός SYN flooding attack για παράδειγμα). Στην ουσία, τέτοιες επιθέσεις καταφέρνουν να επιβαρύνουν σημαντικά τον παραλήπτη με μεγάλο φόρτο ψευδών αιτήσεων τις οποίες καλείται να επεξεργαστεί με αποτέλεσμα να μη μπορεί να ανταποκριθεί σε πραγματικές αιτήσεις. Οι τρόποι αντιμετώπισης που παρουσιάσαμε για τα False Data Injection Attacks στην προηγούμενη ενότητα μπορούν να μας βοηθήσουν να ξεπεράσουμε και στην προκειμένη περίπτωση τον κίνδυνο[133].

Άλλος ένας τύπος επίθεσης στο φυσικό επίπεδο έχει να κάνει με την προσπάθεια παρεμποδισμού των διάφορων κόμβων να αποκτήσουν πρόσβαση στο μέσο (ακόμα και όταν επιτελούν νόμιμες Medium Access Control λειτουργίες) ή την εσκεμμένη πρόκληση συγκρούσεων πακέτων στο μέσο. Σε τέτοιους τύπους επίθεσης, ο επιτιθέμενος, θέτει τον δικό του back-off timer για πολύ μικρό χρονικό διάστημα με αποτέλεσμα να καταλαμβάνει πάντοτε εκείνος πρώτα το μέσο αφήνοντας τους άλλους κόμβους πάντα σε αναμονή για να λάβουν τον έλεγχο του μέσου. Αυτός ο τύπος επίθεσης μας θυμίζει ιδιαίτερα reactive jamming, έναν τύπο επίθεσης με τον οποίο θα ασχοληθούμε εκτενέστερα πιο κάτω.

Η πιο συνηθισμένη επίθεση κατά της διαθεσιμότητας στο φυσικό επίπεδο, είναι το jamming attack. Σε τέτοιες επιθέσεις τυπικά, ένας κακόβουλος χρήστης ξεκινά τη μετάδοση σημάτων στο ασύρματο μέσο αυξάνοντας το θόρυβο σε αυτό[133]. Το γεγονός αυτό επηρεάζει τους

υπόλοιπους κόμβους στο δίκτυο αφού όποτε κάνουν carrier sensing το μέσο φαίνεται να είναι κατειλημμένο, ενώ παράλληλα μπορεί να τους εμποδίσει και από το να ανακτήσουν την μεταφερόμενη πληροφορία λόγω του ιδιαίτερα μικρού SNR. Βάσει της βιβλιογραφίας υπάρχουν δύο κατηγορίες jamming, το proactive και το reactive[134]. Με τον όρο proactive jamming αναφερόμαστε στις επιθέσεις οι οποίες έχουν ως στόχο τους το μπλοκάρισμα ενός καναλιού ανεξάρτητα από το αν χρησιμοποιείται για επικοινωνίες ή όχι. Το proactive jamming, μπορεί να γίνεται περιοδικά, συνεχώς και με τυχαίο τρόπο. Σαν επίθεση, είναι ιδιαίτερα εύκολη να υλοποιηθεί, εντούτοις θεωρείται ιδιαίτερα ενεργειακά δαπανηρή και ο επιτιθέμενος μπορεί εύκολα να αποκαλυφθεί λόγω ασυνήθιστης συμπεριφοράς. Για το λόγο αυτό, δεν παρατηρείται συχνά ως φαινόμενο. Από την άλλη, με τον όρο reactive jamming, καλούμε τις επιθέσεις οι οποίες στοχεύουν συγκεκριμένα στα κανάλια όπου υπάρχει επικοινωνία με τυπικά είδη επιθέσεων σε αυτή την κατηγορία το scan-and-jam (για δίκτυα πολλαπλών καναλιών) και το listen-and-jam.(για δίκτυα ενός καναλιού) .Τέτοιες επιθέσεις θεωρούνται δύσκολο να εντοπιστούν και να αντιμετωπιστούν καθότι ο επιτιθέμενος σε αυτές μπορεί να λειτουργεί υπό κάλυψη (stealth mode) κάνοντας ζημιά και έπειτα συνεχίζοντας με μια καθόλα νόμιμη συμπεριφορά για αρκετό διάστημα ώστε να περάσει απαρατήρητος.

Για την αντιμετώπιση τέτοιων τύπων επιθέσεων οι Aravithan., Namboodiri, Sunku και Jewell στο [43], εισηγούνται την εναλλασσόμενη χρήση πολλαπλών καναλιών διαφορετικών συχνοτήτων όταν το τρέχον κανάλι που χρησιμοποιείται για τη μετάδοση της πληροφορίας παρουσιάζει παρεμβολές οι οποίες οδηγούν σε απώλειες πακέτων που ξεπερνούν ένα ανώτατο επιτρεπόμενο όριο. Για την επίτευξη της μετάβασης από μια συχνότητα σε άλλη, οι συγγραφείς εισηγούνται μια τυχαία ακολουθία συχνοτήτων να εισάγεται εξ' ορισμού σε κάθε κόμβο του AMI δικτύου, και να αξιοποιείται στις περιπτώσεις που περιγράψαμε πιο πάνω. Στον αλγόριθμό τους, κάθε κόμβος στο AMI δίκτυο διαθέτει μια προκαθορισμένη ακολουθία από κανάλια διαφορετικών συχνοτήτων στα οποία μεταπηδά συναρτήσει του χρόνου. Αυτή η ακολουθία αποστέλλεται κρυπτογραφημένη με το δημόσιο κλειδί κάθε κόμβου, στον κόμβο αυτό, κατά την εισαγωγή του στο AMI δίκτυο. Χάρη στην ύπαρξη της ψευδοτυχαίας συνάρτησης παραγωγής των ακολουθιών, οι συγγραφείς θεωρούν, πως ένας επιτιθέμενος πολύ δύσκολα θα καταφέρει να προβλέψει το επόμενο κανάλι, ακόμα και αν διαθέτει ολόκληρο το ιστορικό των διαδοχών από κανάλι σε κανάλι, γεγονός που μας ασφαλίζει έναντι σε jamming attacks.

Παρόμοια άποψη φαίνεται να έχουν και οι Lee, Gerla και Oh οι οποίοι στο [135], παρουσιάζουν το δικό τους τυχαίο μοντέλο επικοινωνίας βασισμένο όπως και το πιο πάνω σε

spread spectrum τεχνικές, για την αντιμετώπιση επιθέσεων κατά της διαθεσιμότητας στο φυσικό επίπεδο. Το μοντέλο τους καλείται Frequency Quorum Rendezvous και εισάγει την καινοτομία του συγχρονισμού δύο τυχαίων ακολουθιών μετάβασης (hopping sequences) αξιοποιώντας ένα quorum σύστημα, γεγονός που εγγυάται ότι αποστολέας και παραλήπτης αναμφίβολα θα συναντηθούν εντός ενός χρονικού πλαισίου. Ο αλγόριθμος αυτός, είναι κατανεμημένος και δεν προϋποθέτει οποιαδήποτε προϋπάρχουσα γνώση από πλευράς των εμπλεκόμενων στην επικοινωνία μερών. Για να κατανοήσουμε καλύτερα τον τρόπο με τον οποίο λειτουργεί ο συγκεκριμένος αλγόριθμος όμως, χρειάζεται πρώτα να εξηγήσουμε τι είναι ένα Quorum σύστημα. Ένα Quorum σύστημα είναι μια συλλογή από υποσύνολα (ή αλλιώς quorums) ενός παγκόσμιου συνόλου, στο οποίο κάθε ζεύγος δύο υποσυνόλων που μπορούμε να επιλέξουμε έχει τουλάχιστον ένα κοινό στοιχείο. Το μοντέλο που προτείνεται λειτουργεί για την ακρίβεια αξιοποιώντας ένα κυκλικό σύστημα Quorum για να κατασκευάσει ένα σύνολο από συχνότητες μετάβασης. Οι συχνότητες αυτές, συνδέονται με ένα συγκεκριμένο time slot με τη χρήση ενός αλγορίθμου τον οποίο θα παρουσιάσουμε ακολούθως, αξιοποιώντας ένα παράδειγμα το οποίο μας δίνουν οι ίδιοι οι δημιουργοί του.

Έστω ότι έχουμε στη διάθεσή μας ένα σύνολο Z που αποτελείται από επτά quorums (N=7) {0,……,6} κάθε ένα από τα οποία έχει πληθικό αριθμό 3 (κ=3) με το ζεύγος αριθμών (N,κ) γνωστό ως difference set. Χρησιμοποιώντας αυτό το difference set μπορούμε να κατασκευάσουμε ένα κυκλικό quorum σύστημα, από το οποίο ο αποστολέας επιλέγει έναν τυχαίο αριθμό που θα αναπαριστά ένα από τα quorums. Έστω ότι ο αποστολέας στην προκειμένη περίπτωση επέλεξε το quorum με αριθμό 5. Αυτό σημαίνει πως το quorum αυτό πρέπει να ανατεθεί σε μια συγκεκριμένη χρονική στιγμή j χρησιμοποιώντας την εξής μέθοδο $x_j = (j,g_m)$ και $yj=(j,g_n)$ όπου $m = j \bmod k$ και $n=j-(j \bmod k)/k$. Το βήμα αυτό επαναλαμβάνεται από τον αποστολέα για κ^2 time slots. Γεγονός το οποίο κατασκευάζει την ακολουθία αποστολής X = {(0,5),(1,6),(2,1),(3,5),(4,6),(5,1),(6,5),(7,6),(8,1)} και την ακολουθία παραλαβής Y = {(0,5),(1,5),(2,5),(3,6),(4,6),(5,6),(6,1),(7,1),(8,1)}. Τα ίδια βήματα επαναλαμβάνονται και από τον παραλήπτη ο οποίος επιλέγει ένα διαφορετικό quorum και κατασκευάζει τα δικά του X’ και Y’. Όταν ένας κόμβος έχει κάτι να στείλει χρησιμοποιεί την ακολουθία αποστολής για να μπορεί να μεταβαίνει από τη μια συχνότητα στην άλλη. Αλλιώς ακολουθεί την ακολουθία παραλαβής. Μετά από κάποιο χρονικό διάστημα, εγγυημένα ο αποστολέας θα βρεθεί με τον παραλήπτη για την επικοινωνία τους. Προφανώς ένας επιτιθέμενος δε μπορεί εύκολα να προβλέψει ούτε το πού – ούτε το πότε αυτό θα γίνει κάτω από αυτό το σενάριο.

Πέρα από τις επιθέσεις στο φυσικό επίπεδο βέβαια, υπάρχουν και άλλες (όπως SYN flood attacks και buffer overflows) σε ανώτερα επίπεδα οι οποίες μπορούν να προκαλέσουν άρνηση υπηρεσίας και να πλήξουν τη διαθεσιμότητα του συστήματός μας. Ενάντια σε τέτοιες επιθέσεις, συνήθως προτείνεται η αξιοποίηση συστημάτων για Intrusion Detection.

Ένα Intrusion Detection System (IDS), μπορεί να είναι signature-based, specification-based ή anomaly-based. Στην κατηγορία των signature-based IDS, εντάσσουμε τα συστήματα ανίχνευσης εισβολής τα οποία στηρίζουν τη λειτουργία τους σε μια λίστα επιθέσεων την οποία διατηρούν και ενημερώνουν. Βάσει των όσων εισηγούνται οι συγγραφείς του [136], ο τύπος αυτός δε θα μπορούσε να θεωρηθεί κατάλληλος για την εξασφάλιση διαθεσιμότητας στο πλαίσιο του Smart Grid, λόγω της δυναμικότητας με την οποία μεταβάλλεται το Smart Home/Smart Grid περιβάλλον και οι επιθέσεις ενάντια σε αυτό. Από την άλλη η κατηγορία των specification-based IDSs, φαίνεται πολλά υποσχόμενη για τους σκοπούς του Smart Grid. Πιο κάτω, παρουσιάζουμε ένα παράδειγμα IDS που ανήκει σε αυτή την κατηγορία. Παρόμοια, ενδιαφέρουσα φαίνεται να είναι και η προσέγγιση που αξιοποιεί anomaly-based IDS, ένα παράδειγμα της οποίας παρουσιάζουμε επίσης πιο κάτω.

Αρχή κάνουμε με τη δουλειά των Faisal,Aung,Williams και Sanchez στο [136]. Στο άρθρο τους, οι συγγραφείς προτείνουν την αξιοποίηση μιας αρχιτεκτονικής (anomaly-based) IDS για το AMI δίκτυο η οποία θα λειτουργεί συμπληρωματικά με άλλες τεχνικές ασφάλειας (όπως η κρυπτογράφηση, η εξουσιοδότηση κτλ.). Η αρχιτεκτονική αυτή αποτελείται στην πραγματικότητα από τρία IDS τα οποία συστήνεται να τοποθετηθούν σε τρία ξεχωριστά σημεία στο δίκτυο. Σε Smart Meters, Concentrators και στο κεντρικό σύστημα. Για τον εντοπισμό οποιασδήποτε ασυνήθιστης κατάστασης στο δίκτυο, οι συγγραφείς προτείνουν την αξιοποίηση της λογικής του Stream Mining, μιας τεχνικής εξόρυξης δεδομένων η οποία θεωρούν ότι αποδίδει πιο ρεαλιστικά την κατάσταση ενός δικτύου. Πιο συγκεκριμένα, για κάθε μια από τις οντότητες του AMI δικτύου οι συγγραφείς θεωρούν ότι υπάρχει μια συνεχής ροή δεδομένων η οποία υπερβαίνει σε μέγεθος τη μνήμη της οντότητας αυτής, ενώ την ίδια στιγμή ο ίδιος αλγόριθμος εξόρυξης δε μπορεί να τρέξει λόγω της περιορισμένης επεξεργαστικής ισχύος της οντότητας. Για την επίλυση του συγκεκριμένου προβλήματος οι Faisal et. al, προτείνουν την αξιοποίηση μιας ασφαλούς οντότητας την οποία αποκαλούν security box, η οποία θα μπορούσε να είναι ενσωματωμένη εξωτερικά σε έναν μετρητή, για να λειτουργεί ως ένα τοπικό IDS για τους σκοπούς της έρευνάς τους, αλλά γιατί όχι και ως ένα firewall, ή ως η οντότητα που αναλαμβάνει το encryption/authentication κτλ. γενικότερα στο AMI περιβάλλον. Το μοντέλο των Faisal et al. λειτουργεί σειριακά. Τα δεδομένα

επικοινωνίας που λαμβάνονται από διάφορες πηγές προωθούνται στο Acceptor Module, το οποίο με τη σειρά του τα περνά μέσα από ένα Pre-processing unit που αναλαμβάνει να παράγει δεδομένα σύμφωνα με κάποια προκαθορισμένα χαρακτηριστικά. Τα δεδομένα αυτά, θα χρησιμοποιηθούν μετέπειτα ως είσοδος στο Stream Mining Module. Το Module αυτό θα τρέξει τον αλγόριθμο εξόρυξης πάνω από το παραγόμενο set δεδομένων και θα προωθήσει τα αποτελέσματα στο Decision maker unit, στο οποίο κρατούνται και οι πληροφορίες για τις διάφορες επιθέσεις, για να λάβει την απόφαση για το κατά πόσο παρατηρείται οτιδήποτε ύποπτο στα δεδομένα, το οποίο να απαιτεί την ενημέρωση του διαχειριστή του συστήματος. Τα τρία επίπεδα IDS που εντοπίσαμε πιο πάνω θα επικοινωνούν μεταξύ τους μέσω ενός ασφαλούς δικτύου το οποίο είναι ξεχωριστό από το AMI δίκτυο.

Την εναλλακτική λύση του specification based IDS, υιοθετούν από την άλλη οι Berthier και Sanders στο [137]. Οι συγγραφείς αυτοί συνεχίζουν στην πραγματικότητα προηγούμενη δουλειά τους, στην οποία πρότειναν μια κατανεμημένη αρχιτεκτονική, που επιτρέπει την παρακολούθηση της κατάστασης του δικτύου μέσα από αισθητήρες που βρίσκονται σε διάφορα μέρη-κλειδιά του δικτύου και επικοινωνούν με μια κεντρική οντότητα που συγκεντρώνει τα στοιχεία τους. Κάθε ένας από αυτούς τους αισθητήρες λειτουργεί στην πραγματικότητα ως ένα specification-based IDS. Κατά την άποψη των συγγραφέων, η μέθοδος αυτή θεωρείται η καλύτερη προσέγγιση για την εξασφάλιση διαθεσιμότητας στο AMI δίκτυο γεγονός το οποίο υποστηρίζεται μεταξύ άλλων από το ότι η μέθοδος αυτή με μικρότερο κόστος και μεγαλύτερη επεκτασιμότητα, παρέχει μεγαλύτερη ακρίβεια από τις signature based τεχνικές αφού μπορεί να ανιχνεύσει ακόμα και επιθέσεις οι οποίες είναι άγνωστες. Οι αισθητήρες στο δίκτυο των Berthier et. al, έχουν τη δυνατότητα εντοπισμού επιθέσεων σε επίπεδο εφαρμογών, μεταφοράς και δικτύου. Οι συγγραφείς, εντοπίζουν την αναμενόμενη συμπεριφορά των μετρητών σε επίπεδο δικτύου βασισμένοι στα διάφορα specifications των πρωτοκόλλων που αξιοποιούν και μοντελοποιούν τη συμπεριφορά αυτή με ένα απλό διάγραμμα καταστάσεων το οποίο αναπαριστά όλες τις πιθανές καταστάσεις στις οποίες μπορεί να βρεθεί ένας μετρητής στο δίκτυο (το διάγραμμα αυτό συνοδεύεται από ένα ακόμα που αφορά στο application level το οποίο αποτελεί μια προέκταση αυτού που περιγράφει το πρότυπο ANSI που μελετούν οι συγγραφείς). Κάθε μια από τις τρεις καταστάσεις του απλού μοντέλου καθορίζει διαφορετικά ήδη λειτουργικότητας και διαφορετικά επίπεδα δικαιωμάτων πρόσβασης. Ένας μετρητής σε κατάσταση in use διαθέτει όλες τις λειτουργικότητες που θα μπορούσε να διαθέτει, από την άλλη ένας μετρητής σε κατάσταση to configure μπορεί να λάβει μόνο πληροφορίες για τη ρύθμισή του και δε μπορεί σε καμία περίπτωση να αλληλεπιδράσει με άλλες οντότητες. Από την άλλη ένας μετρητής σε

κατάσταση offline δεν πρέπει για κανένα λόγω να παρουσιάζει οποιαδήποτε δραστηριότητα στο δίκτυο. Ο διαχωρισμός αυτός αν και απλός βοηθά να εντοπίσουν μετρητές οι οποίοι δε συμπεριφέρονται με τον ορθό τρόπο ώστε να μπορέσουμε να λάβουμε έγκαιρα μέτρα. Η ορθότητα της λύσης που προτείνεται επικυρώνεται ακολούθως μέσα από ένα τυπικό πλαίσιο (formal framework) και μια πρότυπη υλοποίηση των συγκεκριμένων αισθητήρων, η οποία αξιολογήθηκε κάτω από ρεαλιστικά μοτίβα κίνησης στο AMI δίκτυο.

5.5 Εξασφαλίζοντας Εξουσιοδότηση

Ο τελευταίος στόχος με τον οποίο θα ασχοληθούμε στο κεφάλαιο αυτό, είναι η εξουσιοδότηση. Ως εξουσιοδότηση είχαμε ορίσει τη διαβεβαίωση πως καμία οντότητα στο Smart Home/Smart Grid περιβάλλον δε μπορεί να έχει πρόσβαση σε πληροφορίες ή υπηρεσίες οι οποίες δεν εμπίπτουν στη δικαιοδοσία της.

Η βιβλιογραφία για θέματα εξουσιοδότησης στο Smart Home/Smart Grid περιβάλλον, είναι αρκετά περιορισμένη παρά τη μεγάλη σημασία της, εντούτοις πρόσφατα παρουσιάστηκαν ενδιαφέρουσες ιδέες σε ότι αφορά την εξασφάλισή της. Πιο κάτω παρουσιάζουμε ορισμένες από αυτές.

Αρχή κάνουμε με τη μελέτη των Ruj et al. [116] την οποία παρουσιάσαμε και πιο πάνω, επικεντρώνοντας την προσοχή μας, αυτή τη φορά, στο μοντέλο που προτείνουν οι συγγραφείς για σκοπούς ελέγχου πρόσβασης. Στο μοντέλο αυτό ένα RTU συλλέγει πληροφορίες από διαφορετικά NANs με τον τρόπο που είχαμε περιγράψει προηγουμένως (με επιμέρους aggregation της πληροφορίας σε κάθε ένα από τα HAN,BAN και NAN και κρυπτογράφησή της με τη μέθοδο Paillier), τα κρυπτογραφεί περεταίρω κάτω από ένα σύνολο χαρακτηριστικών (attributes) και τα αποστέλλει σε μια βάση δεδομένων. Τα χαρακτηριστικά στα οποία αναφερόμαστε, θα μπορούσαν να αφορούν για παράδειγμα στην πηγή από την οποία προήλθε η ενέργεια (ορυκτά καύσιμα, ήλιος, άνεμος κλπ.), τον τύπο του καταναλωτή (άτομο, εταιρεία, όχημα), ή ακόμα και τον τύπο των συσκευών που χρησιμοποιήθηκαν (υψηλής / χαμηλής κατανάλωσης). Το RTU βέβαια μπορεί να προσθέσει και έμμεσα χαρακτηριστικά στα πιο πάνω, τα οποία θα μπορούσαν να αφορούν στην ώρα κατανάλωσης (ώρα αιχμής/ ή μη), των τύπο των χρηστών που δικαιούνται πρόσβαση σε αυτά (τεχνικοί της εταιρείας παροχής, ερευνητές, νομικοί, οικολόγοι κτλ.), την τοποθεσία στην οποία βρίσκονται οι καταναλωτές κλπ.. Η βάση δεδομένων που αναφέραμε πιο πάνω,

είναι υπεύθυνη τόσο για την αποθήκευση όσο και για την επεξεργασία της πληροφορίας που φτάνει σε αυτήν από τα RTU. Οι χρήστες που θέλουν να αποκτήσουν πρόσβαση σε αυτήν, αποκτούν μυστικά κλειδιά και χαρακτηριστικά. Κάθε αίτηση τους για δεδομένα από τη βάση αυτή, τους δίνει τη δυνατότητα να αποκρυπτογραφήσουν μόνο τα δεδομένα των οποίων τα χαρακτηριστικά ταιριάζουν με τα δικά τους, γεγονός που εξασφαλίζει τον έλεγχο πρόσβασης στα δεδομένα. Η τεχνική που μόλις περιγράψαμε ονομάζεται Attribute Based Encryption και στηρίζεται στην απλή ιδέα της απόδοσης ορισμένων χαρακτηριστικών τόσο στον αποστολέα όσο και στον παραλήπτη της πληροφορίας, ώστε η αποκρυπτογράφησή να είναι εφικτή μόνο από τους κατόχους χαρακτηριστικών που ταιριάζουν με αυτά της πληροφορίας. Τα attribute based keys βάσει των οποίων κρυπτογραφούνται τα δεδομένα διανέμονται από Key Distribution Centres. Οι Ruj et al. στην ουσία αξιοποιούν μια μικρή παραλλαγή αυτής όπως προτάθηκε από τους Lewko και Waters, την οποία αναπροσάρμοσαν για τα Smart Grids. Η μέθοδος αυτή κρυπτογραφεί τη πληροφορία ακολουθώντας δύο απλά βήματα. Για να κατανοήσουμε το πρώτο εξ' αυτών είναι σημαντικό να γνωρίζουμε πως οποιαδήποτε πολιτική πρόσβασης μπορεί να εκφραστεί ως Boolean συνάρτηση, (δηλαδή μια ακολουθία χαρακτηριστικών συνδυασμένα με κατάλληλους τελεστές AND και OR) και μπορεί να αναπαρασταθεί από ένα δέντρο (τα φύλλα του οποίου περιλαμβάνουν τα χαρακτηριστικά και οι ενδιάμεσοι κόμβοι με τη ρίζα περιλαμβάνουν τους τελεστές). Στο πρώτο βήμα της κρυπτογράφησης, το Boolean δέντρο που μόλις περιγράψαμε, μετατρέπεται σε έναν LSSS πίνακα (Linear Secret Sharing Scheme), οι γραμμές του οποίου γίνονται labelled από χαρακτηριστικά. Στο δεύτερο βήμα, το μήνυμα κρυπτογραφείται και αποστέλλεται στη βάση δεδομένων μαζί με τον LSSS πίνακα μέσω ενός ασφαλούς καναλιού μετάδοσης (π.χ. SSH). Όταν ο χρήστης ζητήσει μια πληροφορία, τότε αυτή μεταφέρεται κρυπτογραφημένη σε αυτόν μέσω SSH και αν τα χαρακτηριστικά του είναι συμβατά τότε μπορεί να την αποκρυπτογραφήσει.

Σε παρόμοιο ύφος κινούνται και οι Vaidya, Makrakis και Mouftah στο [138] προτείνοντας τη δική τους προσέγγιση για αυθεντικοποίηση και Attribute Based εξουσιοδότηση για συστήματα αυτοματοποίησης υποσταθμών (SAS), αξιοποιώντας πιστοποιητικά δημόσιου κλειδιού και συστήματα μηδενικής γνώσης για αυθεντικοποίηση και πιστοποιητικά χαρακτηριστικών (attribute certificates) για εξουσιοδότηση. Ένα πιστοποιητικό χαρακτηριστικών θεωρείται το συμπλήρωμα ενός πιστοποιητικού δημόσιου κλειδιού. Τα πιστοποιητικά δημόσιου κλειδιού όπως ήδη έχουμε αναφέρει εκδίδονται από μια αρχή πιστοποίησης (Certification Authority – CA) και χρησιμοποιούνται για να πιστοποιήσουν την ταυτότητα του κατόχου τους όπως ένα διαβατήριο. Από την άλλη τα πιστοποιητικά

χαρακτηριστικών εκδίδονται από μια αρχή χαρακτηριστικών (Attribute Authority) και χαρακτηρίζουν τον κάτοχό τους όπως μια άδεια παραμονής (Visa) η οποία όπως γνωρίζουμε δίνει στον κάτοχό της δικαίωμα παραμονής σε μια περιοχή, για ένα συγκεκριμένο διάστημα, με συγκεκριμένα δικαιώματα για τη διάρκεια παραμονής κλπ. [139]. Η διάρκεια ισχύος των πιστοποιητικών χαρακτηριστικών είναι συνήθως μικρή. Η αναλογία που δώσαμε προηγουμένως με το διαβατήριο και την άδεια παραμονής μπορεί να μας βοηθήσει να κατανοήσουμε το γιατί. Τα χαρακτηριστικά που καθορίζουν το ποιοι είμαστε, στο διαβατήριο μας, σπάνια αλλάζουν· από την άλλη, άδειες παραμονής σε μια χώρα για συγκεκριμένους σκοπούς (που μπορεί να διαφέρουν κάθε φορά), εκδίδουμε συχνά. Σε ορισμένες περιπτώσεις ένα Attribute Certificate μπορεί να περιέχει αναφορές σ' ένα πιστοποιητικό δημόσιου κλειδιού για σκοπούς πιστοποίησης της ταυτότητας του ιδιοκτήτη. Συνήθως τέτοια Attribute Certificates περιλαμβάνουν στοιχεία τα οποία έχουν να κάνουν τον κάτοχο, τον εκδότη, τον αλγόριθμο με τον οποίο υπογράφηκε το πιστοποιητικό, ένα μοναδικό αριθμό πιστοποιητικού, την περίοδο για την οποία θεωρείται έγκυρο, τα χαρακτηριστικά που αποδίδει στον κάτοχο του πιστοποιητικού κλπ.. Στην πρόταση των Vaidya et. al, οποτεδήποτε ένας χρήστης ζητήσει πρόσβαση σε οποιοδήποτε IED ενός υποσταθμού, τόσο ο χρήστης όσο και η ίδια η συσκευή αυθεντικοποιούνται. Μόλις αυθεντικοποιηθεί ο χρήστης, ο controller του υποσταθμού παρέχει στον χρήστη το πιστοποιητικό χαρακτηριστικών του. Το πιστοποιητικό αυτό, μεταφέρεται στον χρήστη υπογεγραμμένο από τον controller με τη χρήση ενός αλγόριθμου ελλειπτικών καμπύλων. Όταν ο χρήστης επιθυμήσει πρόσβαση σ' ένα IED λοιπόν αρκεί να αποστείλει υπογεγραμμένο το μήνυμά του, το πιστοποιητικό δημόσιου κλειδιού του και το πιστοποιητικό χαρακτηριστικών του, το πρώτο πιστοποιητικό θα χρησιμοποιηθεί για την αυθεντικοποίησή του, ενώ το δεύτερο θα χρησιμοποιηθεί για την πιστοποίηση των υπογραφών των μηνυμάτων και του πιστοποιητικού χαρακτηριστικών χρησιμοποιώντας τα δημόσια κλειδιά του αποστολέα και του controller.

Σε μια εναλλακτική προσέγγιση, αξιοποιώντας ένα Service Oriented Approach βασισμένο σε Web Services οι Jung et al στο [58] προτείνουν το δικό τους μοντέλο για εξασφάλιση ελέγχου πρόσβασης στο πλαίσιο του Smart Grid. Το δικό τους μοντέλο αξιοποιεί XACML (eXtensible Access Control Markup Language) και SAML (Security Assertion Markup Language). Το πρότυπο XACML ορίζει μια δηλωτική γλώσσα για την περιγραφή πολιτικών πρόσβασης η οποία υλοποιείται σε XML, καθορίζοντας παράλληλα και τον τρόπο με τον οποίο μια αίτηση εξουσιοδότησης θα αποτιμάται αναλόγως των κανόνων που καθορίζουν οι πολιτικές που ορίζονται. Η XACML μπορεί να χαρακτηριστεί ως ένα σύστημα Attribute

Based Access Control, όπου τα διάφορα χαρακτηριστικά που σχετίζονται με έναν χρήστη αξιοποιούνται ως είσοδος στη συνάρτηση που καθορίζει κατά πόσο ένας χρήστης μπορεί να έχει πρόσβαση σε ένα συγκεκριμένο πόρο με ένα συγκεκριμένο τρόπο. Οι πολιτικές του XACML, καθορίζονται από μια συλλογή από κανόνες. Οι κανόνες αυτοί, όπως επίσης και οι αιτήσεις εξουσιοδότησης, χρησιμοποιούν subjects (τις οντότητες οι οποίες αιτούνται εξουσιοδότησης – οι οποίες χαρακτηρίζονται από ένα σύνολο από χαρακτηριστικά), resources (δεδομένα/υπηρεσίες ή πόροι του συστήματος στους οποίους η οντότητα ζητά να έχει πρόσβαση) και actions(τα οποία καθορίζουν τον τύπο πρόσβασης που μπορεί να έχει το subject στα resources). Η λογική πάνω στην οποία στηρίζεται η εξουσιοδότηση όταν χρησιμοποιείται η XACML θα μπορούσε να περιγραφεί ως εξής : Αρχικά ένας χρήστης (ο οποίος καλείται subject με την ορολογία της XACML) αιτείται δεδομένα/υπηρεσίες από κάποια συγκεκριμένη οντότητα του Smart Grid. Η αίτησή του δρομολογείται σε μια οντότητα γνωστή ως Policy Enforcement Point (PEP) η οποία χρησιμοποιεί την XACML γλώσσα για να δημιουργήσει μια αίτηση βασισμένη πάνω στα χαρακτηριστικά του subject, τους πόρους στους οποίους θέλει να έχει πρόσβαση και άλλες σχετικές πληροφορίες. Η αίτηση που δημιουργείται, προωθείται ακολούθως σε ένα Policy Decision Point (PDP), το οποίο επικοινωνεί με ένα Policy Store για να λάβει τις πολιτικές που θα μπορούσαν να εφαρμοστούν βάσει της αίτησης. Λαμβάνοντάς τις το PDP συγκρίνει την αίτηση που έλαβε και τις πολιτικές που του στάλθηκαν και καθορίζει κατά πόσο θα έπρεπε να δοθεί δικαίωμα πρόσβασης ή όχι στην αιτούμενη οντότητα. Για την αυθεντικοποίηση των οντοτήτων στο συγκεκριμένο σενάριο αξιοποιείται ένας Identity Provider (IDP).

Κεφάλαιο 6

Further Challenges and Future Directions

6.1 Σύγχρονες και μελλοντικές προκλήσεις

Η βιομηχανία παραγωγής ηλεκτρικής ενέργειας βρίσκεται πλέον στο κατώφλι μιας νέας εποχής. Μιας εποχής, που υπόσχεται μέσα από τη μετεξέλιξη των υφιστάμενων δικτύων ηλεκτροδότησης σε Smart Grids, πολλά πλεονεκτήματα για την κοινωνία, την οικονομία και το περιβάλλον. Το Smart Grid, αποτελεί το μέλλον μιας από τις πιο κρίσιμες υποδομές κάθε χώρας, της υποδομής ηλεκτροδότησης. Μπορούμε λοιπόν να συνειδητοποιήσουμε τους λόγους για τους οποίους η ανάγκη για διασφάλιση της ορθής και απρόσκοπτης λειτουργίας του είναι τόσο μεγάλη. Στα προηγούμενα κεφάλαια, εντοπίσαμε κινδύνους που μπορούν να προκύψουν κατά την αλληλεπίδραση των οντοτήτων του Smart Home/Smart Grid περιβάλλοντος και παρουσιάσαμε τρόπους αντιμετώπισης για πολλούς από αυτούς, όπως προκύπτουν μέσα από τη σύγχρονη βιβλιογραφία. Στο κεφάλαιο αυτό, συζητάμε για ανοικτά ζητήματα και προκλήσεις στον τομέα της ασφάλειας του Smart Home/Smart Grid περιβάλλοντος, τα οποία θα μπορούσαν να αποτελέσουν έμπνευση για μελλοντική έρευνα.

Αρχή κάνουμε με μια από τις μεγαλύτερες προκλήσεις που καλούμαστε να αντιμετωπίσουμε η οποία έχει να κάνει με την απουσία προτύπων επικοινωνίας στο πλαίσιο του Smart Grid. Οι μεγάλες αλλαγές που αναμένεται να γίνουν κατά την αναδιαμόρφωση των υφιστάμενων δικτύων ηλεκτροδότησης σε Smart Grids οφείλουν να εξασφαλίζουν τη διαλειτουργικότητα, την ασφάλεια και την αποδοτικότητα του συστήματος. Το Smart Grid είναι ένα σύνθετο ετερογενές δίκτυο, που αποτελείται από μια πληθώρα υποδικτύων κάθε ένα με το δικό του εξοπλισμό, τις δικές του απαιτήσεις και τις δικές του δυνατότητες[77] . Η εξασφάλιση επικοινωνίας μεταξύ αυτών των δικτύων είναι που δίνει στο Smart Grid όλες του τις δυνατότητες. Χωρίς αυτήν τίποτα από όσα έχουμε περιγράψει πιο πάνω δε μπορεί να υπάρξει. Χρειαζόμαστε λοιπόν πρωτόκολλα επικοινωνίας τα οποία θα είναι συμβατά το ένα ως προς το άλλο, ικανοποιώντας τις ίδιες απαιτήσεις και εξυπηρετώντας τους ίδιους στόχους.

Για να επιτύχουμε κάτι τέτοιο όμως πρέπει πρώτα να ορίσουμε με σαφήνεια τους στόχους αυτούς και τις απαιτήσεις, σε ένα πρότυπο. Ένα τέτοιο πρότυπο το οποίο φαίνεται να απολαμβάνει ευρείας αποδοχής στον τομέα της ανταλλαγής πληροφοριών στο πλαίσιο του Smart Grid είναι το πρότυπο αυτοματοποίησης υποσταθμών IEC 61850. Το πρότυπο αυτό καθορίζει αρχές πάνω στις οποίες μπορεί να βασιστεί η μεταφορά μηνυμάτων στο πλαίσιο των υποσταθμών και εμπλουτίζεται διαρκώς με καινούρια πρότυπα [140]. Ένα σύστημα το οποίο κτίζεται ακολουθώντας τέτοια πρότυπα εξασφαλίζει τόσο την επικοινωνία μεταξύ των οντοτήτων του, όσο και τη δυνατότητα αυτοματοποιημένης διαχείρισής τους. Μια μεγάλη πρόκληση κρύβεται λοιπόν πίσω από την επιλογή ενός συνόλου από τέτοια πρότυπα για τα διάφορα υποδίκτυα με τα οποία έχουμε να κάνουμε, τα οποία να μπορούν να συνεργάζονται μεταξύ τους για να επιτύχουμε το στόχο του interoperability στο Smart Grid. Πέρα από αυτό ωστόσο, πρόκληση αποτελεί και η πιστοποίηση ότι ένα δίκτυο ηλεκτροδότησης χρησιμοποιεί πρωτόκολλα τα οποία συμμορφώνονται με το πρότυπο που επέλεξε να ακολουθήσει[141]. Η δημιουργία αρχών πιστοποίησης και πιστοποιητικών συμμόρφωσης είναι λοιπόν το επόμενο βήμα. Όλες οι συσκευές στο πλαίσιο του Smart Grid οφείλουν να διαθέτουν τέτοια πιστοποιητικά, ενώ συχνοί έλεγχοι σε ολόκληρο το δίκτυο πρέπει να επιβεβαιώνουν ότι η λειτουργία του συνάδει με τα πρότυπα τα οποία ακολουθεί.

Μια εξίσου σημαντική πρόκληση, έχει να κάνει με την έλλειψη μετρικών για την αξιολόγηση των μηχανισμών ασφάλειας που προτείνονται για το Smart Grid. Η απουσία τέτοιων μετρικών δε μας επιτρέπει να αξιολογούμε τα πρωτόκολλα που προτείνονται κατά καιρούς σε μια κοινή βάση, με συγκρίσιμο τρόπο. Γεγονός, το οποίο καθιστά πιο δύσκολο το έργο της υιοθέτησης υφιστάμενων πρωτοκόλλων και της δημιουργίας νέων. Τέτοιες μετρικές χρειάζονται μεταξύ άλλων και για την αξιολόγηση των συνεπειών των διαφόρων επιθέσεων στην επίδοση του συστήματος [141].

Ανοικτό πεδίο έρευνας υπάρχει επίσης και σε ότι αφορά στη σχεδίαση και υλοποίηση νέων πρωτόκολλων επικοινωνίας, δρομολόγησης και συνάθροισης δεδομένων εξειδικευμένα για τις απαιτήσεις του Smart Grid. Το Smart Grid χρειάζεται πρωτόκολλα τα οποία να ανταποκρίνονται σε ιδιαίτερες απαιτήσεις και κυρίως σε αυστηρούς χρονικούς περιορισμούς. Το IEC 61850, το οποίο αναφέραμε και προηγουμένως, για παράδειγμα καθορίζει μια σειρά από διαφορετικές στοίβες πρωτοκόλλων μεταξύ των οποίων οι TCP/IP, UDP/IP και Application to MAC. Οι διαφορετικές αυτές στοίβες πρωτοκόλλων προτείνονται για να βοηθήσουν το πρότυπο να εξασφαλίσει ότι τα πιο κρίσιμα μηνύματα για ένα υποσταθμό, τα οποία έχουν να κάνουν με απομόνωση προβληματικών περιοχών (fault isolation) και

προστασία των συστημάτων του, θα φθάνουν σε αυτόν με καθυστέρηση η οποία δε ξεπερνά τα 3ms, σε αντίθεση με τυπικά μηνύματα τα οποία μπορούν να καθυστερήσουν από 20ms μέχρι και 500ms[95]. Τέτοιοι περιορισμοί δε μπορούν να αγνοηθούν τόσο εύκολα κυρίως λόγω του κινδύνου στον οποίο μπορούν να θέσουν το Smart Grid, αφού η καθυστέρηση στην παράδοση κρίσιμων μηνυμάτων σε αυτό, μπορεί να στοιχίσει τη διαθεσιμότητά του.

Μια ακόμα μεγάλη πρόκληση στο πλαίσιο του Smart Grid έχει να κάνει με την εισαγωγή συστημάτων κατανεμημένης παραγωγής ενέργειας όπως ανεμογεννήτριες, φωτοβολταϊκά κ.α. σε αυτό [142]. Η εμπειρία μας σε θέματα ασφάλειας σύνθετων δικτύων μας επιτρέπει να κατανοήσουμε πως η ενσωμάτωση των συστημάτων αυτών στο Smart Grid, δε μπορεί παρά να δημιουργήσει νέες αδυναμίες στο δίκτυο. Εξ' όσων γνωρίζουμε, μέχρι σήμερα καμία μελέτη δεν έχει ασχοληθεί σε βάθος με τους κινδύνους που ενέχονται στην εισαγωγή κατανεμημένων συστημάτων παραγωγής ενέργειας στο Smart Grid, και στους τρόπους με τους οποίους θα μπορούσαμε να τους ανιχνεύσουμε. Θεωρούμε πως το θέμα αυτό, αξίζει να τύχει περισσότερης μελέτης, η οποία πέρα από τον εντοπισμό των ενδεχόμενων κινδύνων που μπορούν να προκύψουν από τα συστήματα αυτά, καλό θα ήταν να ασχοληθεί και με τρόπους με τους οποίους τα συστήματα αυτά θα καταφέρνουν να ανταποκρίνονται όσο το δυνατό πιο αποτελεσματικά σε καταστάσεις κινδύνου ώστε να εξασφαλίζουν την απρόσκοπτη παροχή ενέργειας. Για να επιτύχουμε την ανίχνευση τέτοιων περιστατικών κατά τα οποία τα συστήματα κατανεμημένης παραγωγής αρχίζουν να συμπεριφέρονται με τρόπους που θέτουν το Smart Grid σε κίνδυνο μια λύση όπως προτείνεται στο [11] θα μπορούσε να ήταν η αξιοποίηση της λογικής του Trust Management ώστε να αποφεύγουμε τη χρήση συστημάτων που αξιολογούνται ως χαμηλής εμπιστοσύνης. Σε τέτοια συστήματα επιτρέπονται μόνο οι ενέργειες που προέρχονται από οντότητες που έχουν να καταδείξουν επαρκή διαπιστευτήρια ανεξάρτητα από την ταυτότητά τους. Συχνά τέτοια συστήματα περιγράφονται με την αναλογία ενός εισιτηρίου το οποίο αγοράζει κάποιος, για να παρακολουθήσει για παράδειγμα ένα ποδοσφαιρικό αγώνα. Το εισιτήριο αυτό αποτελεί τη διαβεβαίωση πως ο κάτοχός του έχει πληρώσει και άρα δικαιούται να λάβει μια θέση μέσα στο γήπεδο. Αν ο αρχικός αγοραστής του εισιτηρίου αποφασίσει στη συνέχεια να το δώσει σε κάποιον άλλο, τότε η εμπιστοσύνη μεταβιβάζεται ταυτόχρονα σε αυτόν, μαζί με το δικαίωμα εισόδου στο γήπεδο. Με τον τρόπο αυτό η διαδικασία είναι ανεξάρτητη από την ταυτότητα του κατόχου [143].

Παράλληλα, ανοικτές προκλήσεις υπάρχουν και στον τομέα ανάπτυξης μηχανισμών ασφάλειας οι οποίοι θα κληθούν να λάβουν το ρόλο των TLS/SSL , SSH και IPsec, χωρίς να

επιβαρύνουν τους ήδη περιορισμένους πόρους του Smart Grid. Για την ανάπτυξη μηχανισμών που θα μπορούν να εξασφαλίσουν την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητά της μεταφερόμενης πληροφορίας, απαραίτητη προϋπόθεση είναι ο εντοπισμός των περιορισμών και των απαιτήσεων των δικτύων αυτών, αλλά και των ευκαιριών που μας παρέχουν για να υλοποιήσουμε λύσεις οι οποίες να ανταποκρίνονται σε συγκεκριμένους στόχους και περιορισμούς. Χρειαζόμαστε πρωτόκολλα και μηχανισμούς τα οποία θα λειτουργούν εισάγοντας το μικρότερο δυνατό κόστος (overhead) στην επικοινωνία, σχεδόν για κάθε στόχο που έχει να κάνει με υποδίκτυα του Smart Grid στα οποία η υπολογιστική ισχύς των πόρων είναι περιορισμένη (HANs και τα δίκτυα από PMUs και sensors).

Μια ακόμα ανοικτή περιοχή έρευνας, βρίσκεται στον τομέα της συλλογής πληροφορίας εσωτερικού ελέγχου (audit logs) από το σύστημα σε όλη τη διάρκεια της λειτουργίας του [77]. Χρειαζόμαστε έναν τρόπο με τον οποίο το Smart Grid θα μπορεί να εξασφαλίζει για όλα τα συστήματά του accountability, διατηρώντας στοιχεία και αναφορές οι οποίες μπορούν να βοηθήσουν στην εγκληματολογική ανάλυση που διενεργείται στο σύστημα μετά από επιθέσεις σε αυτό, ώστε να μπορούν να αποδοθούν ευθύνες. Η παραμικρή αλλαγή σ' ένα τοπικό σύστημα, είτε αυτή έγινε από μια νόμιμη οντότητα με το σωστό τρόπο, είτε όχι, οφείλει να καταγράφεται. Με αυτό τον τρόπο κάθε οντότητα στο Smart Grid θα μπορεί να θεωρείται υπόλογη για τις πράξεις της και κανένας να δε μπορεί να αποποιηθεί την ευθύνη για οποιαδήποτε αλληλεπίδρασή του με το σύστημα.

Σε ότι αφορά τώρα σε τρόπους διαφύλαξης της ιδιωτικότητάς στο πλαίσιο του Smart Grid, μια πληθώρα προκλήσεων αφήνουν ανοικτό το πεδίο για περισσότερη έρευνα. Η πρώτη μεγάλη πρόκληση σε αυτόν τον τομέα βρίσκεται στην απουσία νομικού πλαισίου εξειδικευμένου για το Smart Grid. Το Smart Grid χρειάζεται απαραίτητα ένα πλαίσιο που να καθορίζει με ακρίβεια και σαφήνεια τον τρόπο συλλογής ευαίσθητης πληροφορίας, τον τρόπο μεταφοράς της μέσα στο δίκτυο, το κατά πόσο πρέπει πρώτα να υπάρξει έγκριση από τον ιδιοκτήτη, το σε ποιόν μπορεί η πληροφορία αυτή να εκτίθεται χωρίς να θεωρείται ότι θέτουμε την ασφάλεια του ιδιοκτήτη σε κίνδυνο, τις συνέπειες που μπορούν να υπάρξουν αν η πληροφορία παραπέσει αλλά και πώς τις διαχειριζόμαστε [144].

Πέραν του νομικού πλαισίου βέβαια χρειαζόμαστε και ένα γερό τεχνικό πλαίσιο για την εξασφάλιση της ιδιωτικότητας. Όπως έχουμε ήδη δει και στο προηγούμενο κεφάλαιο, πολλές από τις τεχνικές που προτείνονται για την εξασφάλιση ιδιωτικότητας, στηρίζονται στην ιδέα

της συλλογής και συνάθροισης της πληροφορίας σε συγκεκριμένα σημεία του δικτύου σχεδόν πάντα κάτω από την προϋπόθεση ότι η οντότητα στην οποία γίνεται το aggregation είναι μια αξιόπιστη οντότητα. Πρόκληση αποτελεί το να βρούμε τρόπους να δώσουμε στην οντότητα αυτή τη δυνατότητα να μας παράγει την «περίληψη» του μεγάλου όγκου της πληροφορίας που λαμβάνει, χωρίς να γνωρίζει την ίδια την πληροφορία, και χωρίς να εισάγει στο δίκτυο επιπρόσθετες καθυστερήσεις που θα μπορούσαν να μας στοιχίσουν [77]. Κάποια θετικά βήματα προς αυτή την κατεύθυνση έχουν ήδη αρχίσει να γίνονται, εντούτοις ο τομέας αυτός είναι ακόμα ανεξερεύνητος στο μεγαλύτερο κομμάτι του [145].

Ανοικτά ζητήματα, βέβαια, παραμένουν και σε τομείς όπως η προστασία του Smart Grid από DoS και DDoS επιθέσεις. Τέτοιες επιθέσεις θέτουν σε κίνδυνο τον σπουδαιότερο ίσως από όλους τους στόχους ασφάλειας του Smart Grid, αυτόν της διαθεσιμότητας του συστήματος. Για το λόγο αυτό, πρέπει να μπορούν να εντοπιστούν και να περιοριστούν έγκαιρα για να προλάβουμε ανεπανόρθωτες ζημιές στο σύστημα[Secure Service Provision]. Κάτι τέτοιο φυσικά, δεν είναι εύκολο να γίνει. Το Smart Grid είναι ένα σύνθετο cyber-physical σύστημα που περιλαμβάνει πέρα από δίκτυα επικοινωνίας και δίκτυα ηλεκτροδότησης. Αν θέλουμε να επιτύχουμε την αντιμετώπιση τέτοιων επιθέσεων λοιπόν, πρέπει να αρχίσουμε να αξιολογούμε τις συνέπειες οι οποίες θα μπορούσαν να προκύψουν από αυτές τόσο στο δίκτυο επικοινωνίας του Smart Grid όσο και στις εγκαταστάσεις του δικτύου ηλεκτροδότησης. Μέθοδοι αξιολόγησης ρίσκου υπάρχουν πολλές σήμερα[95]. Τέτοιες μέθοδοι μπορούν να είναι είτε πιθανοτικές (probabilistic) όπου το επίπεδο ασφάλειας ενός συστήματος υπολογίζεται μέσω της πιθανότητας να προκύψει ένα οποιοδήποτε περιστατικό κατά της ασφάλειας του συστήματος και της πιθανότητας οι συνέπειες αυτού να οδηγήσουν σε άλλα γεγονότα τα οποία μπορούν να προκαλέσουν μέχρι και διακοπή στην παροχή ενέργειας. Είτε βασισμένες σε γράφους οι οποίοι μπορούν να μας βοηθήσουν να μοντελοποιήσουμε τις συνέπειες ενδεχόμενων επιθέσεων και να λάβουμε αποφάσεις οι οποίες αξιολογούν την κρισιμότητα αυτών και την πιθανότητα εμφάνισης τους. Είτε βασισμένες σε μετρικές ασφάλειας όπου μια συνολική βαθμολογία δίδεται σε κάθε IED στο σύστημα βάσει της επιτυχημένης αναγνώρισης προηγούμενων επιθέσεων και της γνώσης περισσότερων τεχνικών αντιμετώπισης, με αποτέλεσμα πιο ασφαλείς οντότητες να έχουν μεγαλύτερη βαθμολογία. Το μειονέκτημα στην πρώτη τεχνική είναι ότι στηρίζει την επιτυχία της σε προϋπάρχουσα γνώση σε αντίθεση με τις άλλες δύο μεθόδους οι οποίες εντούτοις δε χαρακτηρίζονται από μεγάλη επεκτασιμότητα (scalability). Επιπλέον, καμία από τις τρεις τεχνικές δε μπορεί να υπολογίσει το βαθμό στον οποίο μια DoS επίθεση θα μπορούσε να επηρεάσει το Smart Grid ως προς την αποστολή και παραλαβή χρονικά κρίσιμων (time-

critical) μηνυμάτων όπως π.χ.. τα μηνύματα fault detection & diagnosis. Κατά συνέπεια, οι τεχνικές αυτές κρίνονται ανεπαρκείς. Για το Smart Grid χρειαζόμαστε νέα τέτοια συστήματα, τα οποία θα αξιολογούν το ρίσκο και θα μοντελοποιούν με ακρίβεια τις συνέπειες τέτοιων επιθέσεων σε ολόκληρο το δίκτυο.

Την ίδια στιγμή ανοικτή πρόκληση υπάρχει και σε ότι αφορά στις spread - spectrum τεχνικές οι οποίες αξιοποιούνται σήμερα για την αντιμετώπιση επιθέσεων τύπου jamming attacks [95]. Οι τεχνικές αυτές εισάγουν επιπλέον overhead στο δίκτυο, γεγονός το οποίο δεν είναι ξεκάθαρο ακόμα σε ποιο βαθμό επηρεάζει τα time-critical μηνύματα που πρέπει να μεταφέρει το Smart Grid για την απρόσκοπτη λειτουργία του. Χρειαζόμαστε, συνεπώς, νέα συστήματα τα οποία να επικεντρώνονται τόσο στην αντιμετώπιση του jamming όσο και στη διασφάλιση της έγκαιρης παράδοσης των κρίσιμων μηνυμάτων στο δίκτυο.

Ο συμβιβασμός αυτός μεταξύ των απαιτήσεων που έχουμε για ασφάλεια και των απαιτήσεων που έχουμε για έγκαιρη παράδοση χρονικά κρίσιμων μηνυμάτων, προκύπτει βέβαια και κάτω από άλλα σενάρια στο πλαίσιο του Smart Grid δημιουργώντας έτσι, ακόμα περισσότερες προκλήσεις. Ας θυμηθούμε για παράδειγμα τα συστήματα ανταλλαγής δημόσιου κλειδιού στα οποία μεγαλύτερο κλειδί σημαίνει μεγαλύτερη ασφάλεια αλλά συνεπάγεται μεγαλύτερης καθυστέρησης στο σύστημα. Σε τέτοιες περιπτώσεις είναι καίριας σημασίας να αξιολογήσουμε τις δύο αυτές αντικρουόμενες απαιτήσεις και να βρούμε τη λύση η οποία διατηρεί τις ισορροπίες επιτρέποντας στο Smart Grid να επιτελεί τις λειτουργίες του σωστά και με ασφάλεια.

Η τελευταία πρόκληση με την οποία επιλέγουμε να ασχοληθούμε, έχει να κάνει με τη διαχείριση κλειδιών. Όπως έχουμε ήδη αναφέρει και στο προηγούμενο κεφάλαιο, η συμμετρική κρυπτογράφηση θεωρείται πιο κατάλληλη για τη μεταφορά μηνυμάτων στο πλαίσιο του Smart Grid, λόγω του ότι δεν εισάγει το ίδιο υπολογιστικό κόστος με την ασύμμετρη στα περιορισμένης υπολογιστικής ισχύος συστήματα του Smart Grid. Τα συμμετρικά κλειδιά όμως που αξιοποιεί αυτό το είδος κρυπτογράφησης δε χαρακτηρίζονται από μεγάλη διάρκεια ζωής, εξαιτίας του γεγονότος ότι πολλά δεδομένα κρυπτογραφούνται με αυτά. Είναι προφανές, πως όσο πιο συχνά αλλάζουμε το συμμετρικό κλειδί κρυπτογράφησης, τόσο πιο ασφαλές είναι το σύστημα, αφού μειώνεται το ρίσκο έκθεσης του κλειδιού [95]. Παρόλα αυτά, κάτι τέτοιο συνεπάγεται επιπλέον κόστος από τη διαρκή παραγωγή και διανομή νέων συμμετρικών κλειδιών από το σύστημα διαχείρισης και δημιουργεί ανάγκη για ύπαρξη εμπιστοσύνης μεταξύ του παραγωγού του κλειδιού και του

καταναλωτή αλλά και επιπρόσθετο ρίσκο για το σύστημα λόγω της διανομής κλειδιών. Το θέμα αυτό της σχεδίασης ενός συστήματος ανταλλαγής συμμετρικών κλειδιών θα μπορούσε να ήταν ιδιαίτερα ενδιαφέρον.

Παράλληλα, σε ότι αφορά στη διαχείριση κλειδιών στο πλαίσιο του AMI και των Wide Area Measurement δικτύων, η έρευνα είναι επίσης πολύ περιορισμένη. Χρειαζόμαστε καινούριες εισηγήσεις στον τομέα της παραγωγής, διαχείρισης και διανομής κλειδιού οι οποίες οφείλουν (συμμετρικές, ασύμμετρες, attribute based κλπ..) να χαρακτηρίζονται από μικρή πολυπλοκότητα, χαμηλό κόστος (overhead) και μεγάλη επεκτασιμότητα (scalability).

«Η ασφάλεια στο Smart Grid είναι κάτι περισσότερο από το να περιορίζουμε την πρόσβαση στα δεδομένα και να κρύβουμε τα συστήματά μας πίσω από ένα firewall» δηλώνει ο διευθύνων σύμβουλος της IBM για θέματα ενέργειας, Jeffrey Katz , «είναι σημαντικό να αντιληφθούμε την πολυπλοκότητα των συστημάτων που εμπλέκονται και να κτίσουμε την ασφάλεια από την αρχή μέσα στο σύστημα. Το γεγονός ότι το Smart Grid είναι πιο έξυπνο, μας δίνει ακριβώς την ευκαιρία να έχουμε πιο καλή ορατότητα των κινδύνων που εμφανίζονται. Πλέον, μπορούμε να εντοπίσουμε διακοπές στην παροχή ηλεκτρικής ενέργειας και να αντιδράσουμε γρηγορότερα, ανακατευθύνοντας την ενέργεια μέσα από εναλλακτικά μονοπάτια, ή αποσυνδέοντας ορισμένους υποσταθμούς προσωρινά από το δίκτυο. Μπορούμε επίσης πιο εύκολα να αντιληφθούμε ύποπτες συμπεριφορές και να αντιδράσουμε πρωτού μικρής σημασίας προβλήματα προσλάβουν μεγάλες διαστάσεις. Η καλύτερη ορατότητα του Grid, μας οδηγεί από μόνη της τελικά σε μεγαλύτερη ασφάλεια.» [146] .

Βιβλιογραφία

[1] C. Wickham-Hills, “Smart Metering Projects Map - Google Maps.” [Online]. Available: https://maps.google.com/maps/ms?ie=UTF8&oe=UTF8&msa=0&msid=115519311058367534348.0000011362ac6d7d21187. [Accessed: 11-May-2013].

[2] Wikipedia, “Electric power transmission,” 2011.

[3] Wikipedia, “History of electrification.”

[4] N. I. of Technology-Calicut, “An Advanced Metering Infrastructure for Future Electricity Networks,” pp. 1–16.

[5] Χρήστος Ε. Τσιράκης, “Θέματα Ασφάλειας και Συνεργατικών Υπηρεσιών σε Δίκτυα Smart Grid ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ,” 2012.

[6] ENISA, “Smart Grid Security - Annex I - General Concepts and Dependencies with ICT,” 2012.

[7] ΔΣΜ, “TSO - Σύστημα Ηλεκτρικής Ενέργειας.” .

[8] ΔΣΜ, “Διαχειριστής Συστηματος Μεταφοράς Κύπρος.” pp. Http://www.dsm.org.cy/nqcontent.cfm?a_id=918&tt=gr.

[9] D. Telecom, “SCADA Tutorial - YouTube.” .

[10] ΔΣΜ, “TSO - Σύστημα Τηλελέγχου και Διαχείρισης Ενέργειας.” .

[11] X. Li and I. Lille, “Securing Smart Grid : Cyber Attacks , Countermeasures , and Challenges,” no. August, pp. 38–45, 2012.

[12] T. Flick, *Securing the Smart Grid Securing the Smart Grid Next Generation Power Grid Security*. ELSEVIER, 2011.

[13] Minnesota Power, “About Electricity.” 2012.

[14] J. R. Luoma, “The Challenge for Green Energy How to Store Excess Electricity.” 2009.

[15] D. Y. Xi Yang, Satyajayant Misra, Guoliang Xue, “Smart Grid – The New and Improved Power Grid : A Survey,” 2011.

[16] E. Commision and Brussels, “Smart Grids: from innovation to deployment,” *COM(2011) 202 final*, 2011.

[17] EU Commission Task Force for Smart Grids, “Functionalities of smart grids and smart meters Final Deliverable,” no. December, pp. 1–69, 2010.

[18] NIST and Smart Grid Co-ordination Group, “White paper on standardization of Smart Grids.”

[19] C. Boutin, “U.S., Europe Collaborating on Smart Grid Standards Development.” p. NIST Tech Beat, 2011.

[20] CEN CENELEC ETSI, “Final report Standards for Smart Grids,” no. May, 2011.

[21] U.S. Department of Commerce, “NIST Special Publication 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards , NIST Special Publication 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards ,Release 1.0,” 2010.

[22] C. Lima, “Enabling a Smarter Grid,” no. September, 2010.

[23] D. He, C. Chen, and J. Bu, “Secure Service Provision in Smart Grid Communications,” no. August, pp. 53–61, 2012.

[24] B. Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, “Cyber – Physical Security of a Smart Grid Infrastructure,” pp. 1–15, 2011.

[25] IEEE Standards Coordinating Committee 21, *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications , and Loads*, no. September. 2011.

[26] Y. Kim, M. Thottan, V. Kolesnikov, and W. Lee, “E NERGY E FFICIENCY IN C OMMUNICATIONS A Secure Decentralized Data-Centric Information Infrastructure for Smart Grid,” no. November, pp. 58–65, 2010.

[27] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, “Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[28] I. Ghansah, “Smard Grid Cyber Security Potential Threats, Vulnerabilities and Risks.”

[29] G. Wynn, “Privacy concerns challenge smart grid rollout.” REUTERS, 2010.

[30] The Smart Grid Interoperability Panel – Cyber Security Working Group, “NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid,” vol. 2, no. August, 2010.

[31] T. GJELTEN, “Cyberworm’s Origins Unclear, But Potential Is Not.” npr, 2012.

[32] K. J. Higgins, “Stuxnet, Duqu, Flame Targeted Illegal Windows Systems In Iran.” 2012.

[33] eChannelNEWS and ecnTV, “Don’t Be Left in the Dark The Impact of Blackouts to Your Bottom Line.” .

[34] S. GORMAN, “Electricity Grid in U.S. Penetrated By Spies.” The Wall Street Journal, 2009.

[35] European Commission, “Challenges ahead - Research & Innovation - Industrial technologies.” .

[36] U.S Department of Energy, “Buildings Energy Data Book,” *2012*. [Online]. Available: http://buildingsdatabook.eren.doe.gov/ChapterIntro1.aspx.

[37] S. Bin and L. Jun, “Building Energy Efficiency Policies in China - Status Report.” 2012.

[38] J. K. W. Wong, H. Lia, and S. W. Wangb, “Intelligent building research: a review,” *Automation in Construction*, vol. 14, no. 1, pp. 143–159, Mar. 2005.

[39] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, “A Review of Smart Homes—Past, Present, and Future,” *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 6, pp. 1190–1203, Nov. 2012.

[40] T. A. Nguyen and M. Aiello, “Energy Intelligent Buildings based on User Activity: A Survey,” *Energy and Buildings*, vol. 56, pp. 244–257, Sep. 2012.

[41] OpenHAN Task Force UtilityAMI Working Group, “UtilityAMI 2008 Home Area Network System Requirements Specification.” pp. 1–102, 2008.

[42] G. Mantas, D. Lymberopoulos, and N. Komninos, “Security in Smart Home Environment,” in *Wireless Technologies for Ambient Assisted Living and Healthcare:Systems and Applications*, 2011, pp. 170–191.

[43] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, “Wireless AMI application and security for controlled home area networks,” *2011 IEEE Power and Energy Society General Meeting*, pp. 1–8, Jul. 2011.

[44] W. Su, W. Zeng, and M.-Y. Chow, “A digital testbed for a PHEV PEV enabled parking lot in a Smart Grid environment,” in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, 2012, pp. 1–7.

[45] E. 7th F. P. Commision, “Technology Trends for SmartHouse / SmartGrid,” *Smart Houses Interacting with Smart Grids to achieve next-generation energy efficiency and sustainability*, pp. 1–50, 2010.

[46] “Home - HomePlug Powerline Alliance.” [Online]. Available: https://www.homeplug.org/home/.

[47] A. Hardy, F. Bouhafs, and M. Merabti, “A Survey of Communication and Sensing for Energy Management of Appliances,” *International Journal of Advanced Engineering Sciences and Technologies*, vol. 3, no. 2, pp. 61–77, 2009.

[48] “KNX Association [Official website].” [Online]. Available: http://www.knx.org/.

[49] “Echelon tops 90 million LonWorks chips globally,” 2010. [Online]. Available: http://www.eetimes.com/electronics-news/4182670/Echelon-tops-90-million-LonWorks-chips-globally.

[50] C. Gomez and J. Paradells, “Wireless Home Automation Networks : A Survey of Architectures and Technologies,” no. June, pp. 92–101, 2010.

[51] L. Goldberg, “ZigBee’s Smart Energy 2.0,” 2012. [Online]. Available: http://www.digikey.com/us/en/techzone/energy-harvesting/resources/articles/zigbees-smart-energy-20-profile.html.

[52] K. D. Craemer and G. Deconinck, “Analysis of State-of-the-art Smart Metering Communication Standards,” in *Proceedings of the 5th Young Researchers Symposium*, 2010, pp. 1–6.

[53] Z.-W. Alliance, “Z-Wave.” [Online]. Available: http://www.z-wave.com/.

[54] “INSTEON - Wireless Home Control Solutions for Lighting, Security, HVAC, and A V Systems.” [Online]. Available: http://www.insteon.net/about-home.html.

[55] S. Feuerhahn, M. Zillgith, C. Wittwer, and C. Wietfeld, “Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications,” *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 410–415, Oct. 2011.

[56] “IEC 62056-21 Official Standard.” [Online]. Available: http://webstore.iec.ch/webstore/webstore.nsf/artnum/031526.

[57] “M-Bus.” [Online]. Available: http://www.m-bus.com/.

[58] A. Weidlich and S. Karnouskos, “Integrating Smart Houses with the Smart Grid Through Web Services for Increasing Energy Efficiency,” 2007.

[59] A. Kamilaris, Y. Tofis, C. Bekara, A. Pitsillides, and E. Kyriakides, “Integrating Web-Enabled Energy-Aware Smart Homes to the Smart Grid,” *International Journal On Advances in Intelligent Systems*, vol. 5, pp. 15–31, 2012.

[60] C. Warmer, K. Kok, S. Karnouskos, A. Weidlich, and D. Nestle, “Web services for integration of smart houses in the smart grid,” *Grid-Interop Forum 2009*, pp. 1–5, 2009.

[61] “Java Web Services Architecture,” 2003. [Online]. Available: http://www.w3.org/TR/ws-arch/#relwwwrest.

[62] C. Pautasso and F. Leymann, “RESTful Web Services vs . ‘ Big ’ Web Services : Making the Right Architectural Decision Categories and Subject Descriptors,” pp. 805–814, 2008.

[63] G. Moritz, E. Zeeb, S. Prüter, F. Golatowski, D. Timmermann, and R. Stoll, “Devices Profile for Web Services and the REST,” in *Industrial Informatics (INDIN), 2010 8th IEEE International Conference on*, 2010, pp. 584– 591.

[64] E Source Companies LLC, “Demand Response 101 : The Basics How Customers Benefit from.” 2003.

[65] P. Palensky, S. Member, and D. Dietrich, “Demand Side Management : Demand Response , Intelligent Energy Systems , and Smart Loads,” vol. 7, no. 3, pp. 381–388, 2011.

[66] K. Kok, S. Karnouskos, D. Nestle, A. Dimeas, A. Weidlich, and C. Warmer, “Smart Houses for a Smart Grid,” in *20 th International Conference on Electricity Distribution - 20th International Conference on Electricity Distribution Aggregation of Houses*, 2009, no. 0751, pp. 8–11.

[67] CitiPower and Powercor Australia, “Load Shedding.” .

[68] S. Darby, “The effectiveness of feedback on energy consumption,” *Environmental Change Institude University of Oxford*, no. April, 2006.

[69] K. Willett and L. Layne, “The consumer’s energy analysis environment,” *Energy Policy*, vol. 22, no. 10, pp. 857–866, 1994.

[70] A. Kamilaris and A. Pitsillides, “Exploiting Demand Response in Web-based Energy-aware Smart Homes,” in *the First International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies (Energy 2011)*, 2011.

[71] BSOL Batterie Systeme, “Smart Grid Systems - Peak Shaving.” .

[72] Computer Security Division Information Technology Laboratory - NIST, “Standards for Security Categorization of Federal Information and Information Systems,” no. February, 2004.

[73] The Smart Grid Interoperability Panel – Cyber Security Working Group, *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security - All Volumes*, no. September. 2010.

[74] F. . Cleveland, “Cyber security issues for Advanced Metering Infrasttructure (AMI),” in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 2008, pp. 1– 5.

[75] S. Saponara and T. Bacchillone, “Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid,” *Journal of Computer Networks and Communications*, vol. 2012, pp. 1–19, 2012.

[76] Xanthus Consulting International, “White Paper for NIST CSWG : Cyber Security Requirements for Business Processes Involving Home Area Networks (HAN).”

[77] J. Liu, Y. Xiao, S. Member, S. Li, W. Liang, and C. L. P. Chen, “Cyber Security and Privacy Issues in Smart Grids,” vol. 14, no. 4, pp. 981–997, 2012.

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

[79] L. Blumenfield, “Dissertation Could Be Security Threat,” *Washington Post*, p. A01, 2003.

[80] M. Govindarasu, “Cyber-Physical Systems Security for Smart Grid.”

[81] T. Report, “A complex malware for targeted attacks,” vol. 05, 2012.

[82] “Duqu Trojan Questions and Answers Dell SecureWorks.” [Online]. Available: http://www.secureworks.com/cyber-threat-intelligence/threats/duqu/.

[83] “Ralph Langner Cracking Stuxnet, a 21st-century cyber weapon Video on TED.” [Online]. Available: http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html.

[84] S. a. Shaikh, H. Chivers, P. Nobles, J. a. Clark, and H. Chen, “Network reconnaissance,” *Network Security*, no. 11, pp. 12–16, Nov. 2008.

[85] H. Mohsenian-rad, “False Data Injection Attacks with Incomplete Information Against Smart Power Grids.”

[86] Y. Liu, M. K. Reiter, and P. Ning, “False data injection attacks against state estimation in electric power grids,” *Proceedings of the 16th ACM conference on Computer and communications security - CCS ’09*, p. 21, 2009.

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

[88] F. Skopik, Z. Ma, T. Bleier, and H. Grüneis, “A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures,” 2012.

[89] F. Alsiherov and T. Kim, “Secure SCADA Network Technology and Methods,” pp. 434–438.

[90] European Commission, “Smart Grids: from innovation to deployment COM (2011) 202,” 2011. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:EN:PDF. [Accessed: 11-May-2013].

[91] F. Aloul, A. R. Al-ali, R. Al-dalky, and M. Al-mardini, “Smart Grid Security : Threats , Vulnerabilities and Solutions,” no. 971, 2012.

[92] J. Benoit, “An Introduction to Cryptography as Applied to the Smart Grid Jacques Benoit Senior Analyst Information Security Cooper Power Systems,” pp. 1–17.

[93] “Cryptographic Key Management for the Advanced Metering Infrastructure.” [Online]. Available: file:///C:/Users/Dell/Desktop/THESIS BIBLIOGRAPHY/CHAPTER4_BIBLIOGRAPHY/Chapter5_5.htm. [Accessed: 11-May-2013].

[94] T. Smart, G. Interoperability, C. Security, and W. Group, *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*, no. September. 2010.

[95] W. Wang and Z. Lu, “Cyber Security in the Smart Grid : Survey and Challenges,” 2012.

[96] W. Stallings, *Cryptography and Network Security Principles and Practice*, 5th ed. Prentice Hall, 2011.

[97] A. R. Metke and R. L. Ekl, “Security Technology for Smart Grid Networks,” *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[98] H. Nicanfar and P. Jokar, “Efficient Authentication and Key Management Mechanisms for Smart Grid Communications,” pp. 1–13.

[99] C. L. Beaver, D. R. Gallup, W. D. Neumann, and M. D. Torgerson, “Key Management for SCADA,” no. March, 2002.

[100] R. Dawson, C. Boyd, E. Dawson, and J. Nieto, “SKMA: a key management architecture for SCADA systems,” *ACSW Frontiers ’06 Proceedings of the 2006 Australasian workshops on Grid computing and e-research*, vol. 54, pp. 183–192, 2006.

[101] D. Choi, H. Kim, D. Won, and S. Kim, “Advanced Key-Management Architecture for Secure SCADA Communications,” *Power Delivery, IEEE Transactions*, pp. 1154 – 1163, 2009.

[102] S. Choi, Donghyun ; Lee, Sungjin ; Won, Dongho ; Kim, “Efficient Secure Group Communications for SCADA,” *Power Delivery, IEEE Transactions*, vol. 25, no. 2, pp. 714 – 722, 2010.

[103] A. Saxena, O. Pal, S. Saiwan, and Z. Saquib, “TOKEN BASED KEY MANAGEMENT SCHEME FOR SCADA COMMUNICATION,” vol. 2, no. 4, pp. 69–86, 2011.

[104] J. Kamto, L. Qian, J. Fuller, and J. Attia, “Light-weight key distribution and management for Advanced Metering Infrastructure,” in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, 2011, pp. 1216 – 1220.

[105] S. Das, Y. Ohba, M. Kanda, and D. Famolari, “A key management framework for AMI networks in smart grid,” *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 30 – 37, 2012.

[106] F. Zhao, Y. Hanatani, Y. Komano, M. Ieee, B. Smyth, S. Ito, and T. Kambayashi, “Secure Authenticated Key Exchange with Revocation for Smart Grid,” 2011.

[107] Y. Law, M. Palaniswami, G. Kounga, and A. Lo, “WAKE Key management scheme for wide-area measurement systems in smart grid,” *Communications Magazine, IEEE*, vol. 51, no. 1, pp. 34 – 41, 2013.

[108] U. Greveler, B. Justus, and D. Loehr, “Multimedia Content Identification Through Smart Meter Power Usage Profiles.”

[109] F. Skopik, “Security Is Not Enough ! On Privacy Challenges in Smart Grids,” 2012.

[110] M. Jawurek, F. Kerschbaum, and G. Danezis, “SoK : Privacy Technologies for Smart Grids – A Survey of Options .”

[111] J.-J. Quisquater, M. Quisquater, M. Quisquater, M. Quisquater, L. Guillou, M. A. Guillou, G. Guillou, A. Guillou, G. Guillou, and S. Guillou, “How to explain Zero-

Knowledge Protocols to Your Children," in *Advances in Cryptology — CRYPTO' 89 Proceedings*, 1990, pp. 628–631.

[112] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 238 – 243.

[113] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building - BuildSys '10*, p. 61, 2010.

[114] T. Jeske, "PRIVACY-PRESERVING SMART METERING WITHOUT A TRUSTED-THIRD-PARTY," 2011.

[115] A. Rial, K. U. Leuven, E. Cosic, and G. Danezis, "Privacy-Preserving Smart Metering," pp. 49–60, 2011.

[116] S. Ruj, A. Nayak, and I. Stojmenovic, "A Security Architecture for Data Aggregation and Access Control in Smart Grids," no. Dlc, pp. 1–12.

[117] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," *Advances in Cryptology — CRYPTO' 99 Proceedings*, vol. 1592, pp. 223–238, 1999.

[118] B. Hayers, "Alice and Bob in Cipherspace," *American Scientist*, vol. 100, pp. 362–367, 2012.

[119] F. Li, B. Luo, and P. Liu, "Secure and privacy-preserving information aggregation for smart grids," *International Journal of Security and Networks*, vol. 6, no. 1, p. 28, 2011.

[120] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Privacy-preserving advance power reservation," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 18–23, 2012.

[121] E. Shi, T. H. Han, E. Rieffel, D. Song, and R. Chow, "Privacy-Preserving Aggregation of Time-Series Data."

[122] G. Acs and C. Castelluccia, "DREAM : DiffeRentially privatE smArt Metering Technical report," pp. 1–29.

[123] D. Varodayan and A. Khisti, "SMART METER PRIVACY USING A RECHARGEABLE BATTERY : MINIMIZING THE RATE OF INFORMATION LEAKAGE," pp. 8–11.

[124] S. Bhattarai, G. Linqiang, and Y. Wei, "A novel architecture against false data injection attacks in smart grid," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 907 – 911.

[125] Y. Huang, H. Li, K. A. Campbell, and H. Z, "Defending false data injection attack on smart grid network using adaptive CUSUM test," *2011 45th Annual Conference on Information Sciences and Systems*. Ieee, pp. 1–6, Mar-2011.

[126] E. . Page, “Continuous Inspection Schemes,” *Biometrika*, vol. 41, no. 1/2, pp. 100–115, 1954.

[127] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, “Smart Grid Data Integrity Attacks : Characterizations and Countermeasures Smart Grid Data Integrity Attacks :,” 2011.

[128] Z. Xiao, Y. Xiao, and D. H.-C. Du, “Non-repudiation in neighborhood area networks for smart grid,” *Communications Magazine, IEEE*, vol. 51, no. 1, pp. 18 – 26, 2013.

[129] M. Nabeel, S. Kerr, and E. Bertino, “Authentication and key management for Advanced Metering Infrastructures utilizing physically unclonable functions,” *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, pp. 324–329, Nov. 2012.

[130] M. M. Fouda, S. Member, Z. Fadlullah, N. Kato, S. Member, R. Lu, X. S. Shen, A. Smart, and G. Sg, “A Light-weight Message Authentication Scheme for Smart Grid Communications,” pp. 1–11.

[131] X. Lu, W. Wang, and J. Ma, “Authentication and Integrity in the Smart Grid: An Empirical Study in Substation Automation Systems,” *International Journal of Distributed Sensor Networks*, vol. 2012, pp. 1–13, 2012.

[132] CEN-CENELEC-ETSI Smart Grid Coordination Group, “Smart Grid Information Security,” no. November, pp. 1–46, 2012.

[133] S. Y. Eun-Kyu Lee ; Gerla, M. ; Oh, “Physical layer security in wireless smart grid,” *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 46 – 52, 2012.

[134] H. Nguyen, K. Nahrstedt, and T. Pongthawornkamol, “Alibi Framework for Identifying Reactive Jamming Nodes in Wireless LAN,” *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, pp. 1–6, Dec. 2011.

[135] E.-K. Lee, S. Y. Oh, and M. Gerla, “Frequency quorum rendezvous for fast and resilient key establishment under jamming attack,” *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 14, no. 4, p. 1, Feb. 2011.

[136] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, “Using Intrusion Detection System with Data Stream Mining,” pp. 96–111, 2012.

[137] R. Berthier and W. H. Sanders, “Specification-Based Intrusion Detection for Advanced Metering Infrastructures,” *2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing*, pp. 184–193, Dec. 2011.

[138] B. Vaidya, D. Makrakis, and H. T. Mouftah, “Device authentication mechanism for Smart Energy Home Area Networks,” *2011 IEEE International Conference on Consumer Electronics (ICCE)*, no. 1, pp. 787–788, Jan. 2011.

[139] “Authorization certificate.” [Online]. Available: http://en.wikipedia.org/wiki/Authorization_certificate. [Accessed: 01-Jun-2013].

[140] “Standardisation is key to Smart Grid success - Power Engineering International.” [Online]. Available: http://www.powerengineeringint.com/articles/print/volume-20/issue-5/features/standardisation-is-key-to-smart-grid-success.html. [Accessed: 11-May-2013].

[141] G. C. Wilshusen, “Challenges in Securing the Electricity Grid,” *United States Government Accountability Office*, 2012.

[142] M. Kim, “A survey on guaranteeing availability in smart grid communications,” in *Advanced Communication Technology (ICACT), 2012 14th International Conference on*, 2012, pp. 314 – 317.

[143] “Trust management (information system).” [Online]. Available: http://en.wikipedia.org/wiki/Trust_management_(information_system). [Accessed: 11-May-2013].

[144] H. Daojing, C. Chun, B. Jiajun, S. ; Chan, Z. ; Yan, and M. Guizani, “Secure service provision in smart grid communications,” *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 53 – 61, 2012.

[145] X. Li, L. Xiaohui, L. Rongxing, S. Xuemin, L. Xiaodong, and Z. Haojin, “Securing smart grid cyber attacks, countermeasures, and challenges,” *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 38 – 45, 2012.

[146] “IBM - Cyber Security - United States.” [Online]. Available: http://www.ibm.com/smarterplanet/us/en/smart_grid/article/cyber_security.html. [Accessed: 17-May-2013].