Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Privacy-preserving data aggregation protocols in smart grids**
Ονοματεπώνυμο Φοιτητή	**Μαρία Κλάρα Αποστολάκου**
Πατρώνυμο	**Ηλίας**
Αριθμός Μητρώου	**ΜΠΠΛ/ 12006**
Επιβλέπων	**Κωνσταντίνος Πατσάκης, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Οκτώβριος 2018**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Πατσάκης Κωνσταντίνος Επίκουρος Καθηγητής	Αλέπης Ευθύμιος Επίκουρος Καθηγητής	Τασούλας Ιωάννης Επίκουρος Καθηγητής

ΠΕΡΙΛΗΨΗ

Ο όρος έξυπνα δίκτυα είναι σχετικά καινούργιος αφού μόλις το 2007 δόθηκε επίσημα ο ορισμός του στις ΗΠΑ. Πρόκειται για την εξέλιξη των δικτύων διανομής ηλεκτρικής ενέργειας με τεχνολογίες αιχμής που επιτρέπουν την αμφίδρομη επικοινωνία μεταξύ χρηστών και παρόχων με στόχο τη βελτιστοποίηση της παροχής και την ελαχιστοποίηση της παραγωγής. Ο κίνδυνος κακόβουλης χρήσης του έξυπνου δικτύου οδηγεί στην ανάγκη δημιουργίας μοντέλων προστασίας του δικτύου και των δεδομένων που συναθροίζονται σε αυτό. Η ιδιωτικότητα των χρηστών και η προστασία των παρόχων είναι πολύ σημαντική και για το λόγο αυτό έχουν γίνει πολλές μελέτες και έχουν αναπτυχθεί πρωτόκολλα για την προστασία των δεδομένων.

Στην παρούσα μεταπτυχιακή διατριβή εξετάζονται τα πρωτόκολλα συνάθροισης δεδομένων στα έξυπνα δίκτυα με διατήρηση της ιδιωτικότητάς τους. Γίνεται περιγραφή των έξυπνων δικτύων και των κινδύνων που απειλούν τη νέα τεχνολογία. Παρουσιάζονται μοντέλα και πρωτόκολλα συνάθροισης από τη διεθνή βιβλιογραφία.

Λέξεις κλειδιά: Smart grid, aggregation protocol, privacy-preserving aggregation

ABSTRACT

The term smart grids is relatively new since it was only 2007 when officially given its definition in the US. It is the evolution of power distribution networks with state-of-the-art technologies that allow two-way communication between users and providers to optimize supply and minimize production. The risk of malicious use of the smart grid leads to the need to create protection models for the network and the data aggregated in it. The privacy of users and the protection of providers is very important. Therefore, many studies have been conducted and data protection protocols have been developed.

In this dissertation, privacy-preserving data aggregation protocols in smart grids are examined. Smart grids and threats to new technology are described. Models and aggregation protocols from the international bibliography are presented.

Key words: Smart grid, aggregation protocol, privacy-preserving aggregation

Περιεχόμενα

Πίνακας σχημάτων

1. ΕΙΣΑΓΩΓΗ

Τα έξυπνα δίκτυα αποτελούν την εξέλιξη των σημερινών δικτύων διανομής ηλεκτρικής ενέργειας. Η Ευρωπαϊκή Ομάδα Ειδικών Καθηκόντων για τα Έξυπνα ηλεκτρικά Δίκτυα τα ορίζει ως τα δίκτυα ηλεκτρισμού στα οποία μπορούν να ενοποιηθούν αποτελεσματικά η συμπεριφορά και οι δράσεις του συνόλου των χρηστών που συνδέονται με αυτά, εταιρείες ηλεκτροπαραγωγής, καταναλωτές και όσοι έχουν και τις δύο ιδιότητες, ώστε να εξασφαλίζεται οικονομικά αποδοτικό, βιώσιμο και ασφαλές σύστημα ισχύος με χαμηλές απώλειες και υψηλή ποιότητα και ασφάλεια εφοδιασμού.
(http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group1.pdf).

Ενώ τα παραδοσιακά μοντέλα δικτύων διανομής ηλεκτρικής ενέργειας έχουν φτάσει στην αιχμή της αποτελεσματικότητας και της αξιοπιστίας τους, στις αρχές του 21^{ου} αιώνα αναπτυσσόμενες χώρες όπως η Κίνα, η Ινδία και η Βραζιλία παρουσιάστηκαν ως πρωτοπόρες στην ανάπτυξη έξυπνων δικτύων. Στην Ευρώπη και την Αμερική η συζήτηση γύρω από τα έξυπνα δίκτυα ξεκίνησε την τελευταία δεκαετία με την πρώτη επίσημη απόδοση του όρου έξυπνο δίκτυο (smart grid) να συναντάται το 2007 στις ΗΠΑ. Από τότε έχουν δρομολογηθεί μεγάλα προγράμματα γύρω από την νέα τεχνολογία.

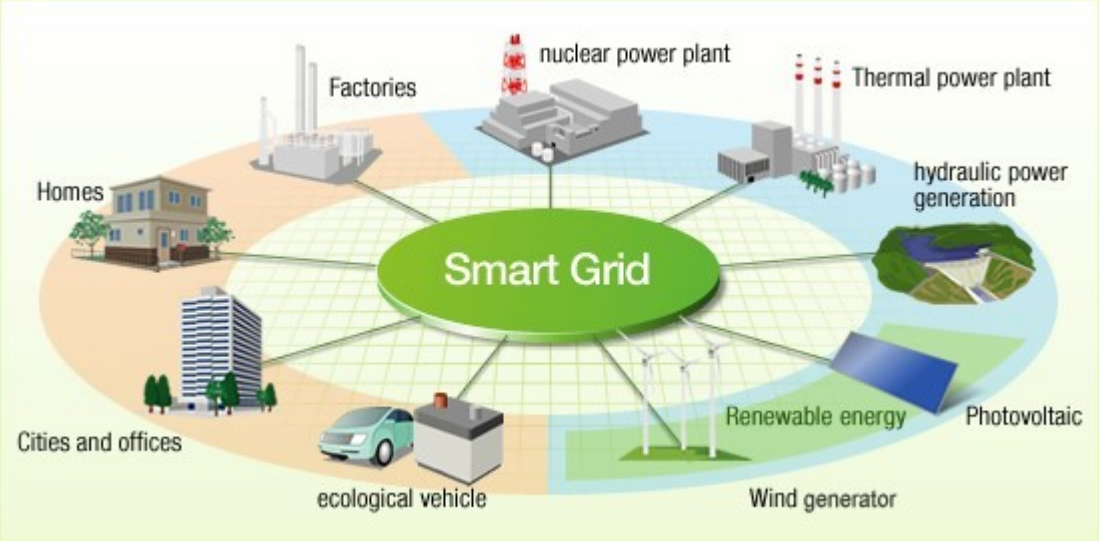
Η Ευρωπαϊκή Επιτροπή σε σχετική ανακοίνωσή της «Έξυπνα Δίκτυα – από την Καινοτομία στην Ανάπτυξη» (ανακοίνωση 52011DC0202 Απρίλιος 2011) ορίζει την πολιτική της όσον αφορά στα έξυπνα δίκτυα και θέτει ως στόχο την προώθηση της ταχύτερης και ευρύτερης αξιοποίησης των έξυπνων ηλεκτρικών δικτύων στην Ευρώπη. Η σταδιακή διείσδυση της νέας τεχνολογίας είναι πλέον γεγονός, με πολλές χώρες να επενδύουν στην ανάπτυξή της και να υιοθετούν την εφαρμογή της.

Ένα σημαντικό ζήτημα που τίθεται από το στάδιο του σχεδιασμού κιόλας των έξυπνων δικτύων είναι ο σεβασμός της ιδιωτικής ζωής των καταναλωτών και η προστασία των εταιρικών δεδομένων των διαχειριστών έξυπνων δικτύων και των υπολοίπων εμπλεκομένων παραγόντων. Τα δεδομένα στα έξυπνα δίκτυα θα πρέπει να μοιράζονται με ασφαλή τρόπο. Σχεδιασμένα να επιτρέπουν την επικοινωνία σε πραγματικό χρόνο μεταξύ των μονάδων και των μετρητών των καταναλωτών, έχουν το ρίσκο εγκληματικές ή και τρομοκρατικές ενέργειες να εκμεταλλευτούν τις δυνατότητες αυτές.

Κάποιες λύσεις σε αυτό το πρόβλημα έχουν αναπτυχθεί τα τελευταία χρόνια και περιλαμβάνουν μεταξύ άλλων τη κοινή χρήση δεδομένων βάσει πολιτικής.

Στην παρούσα διατριβή εξετάζεται το πρόβλημα του υπολογισμού του συναθροίσματος των δεδομένων με τρόπο που να προστατεύεται η ιδιωτική ζωή. Κατόπιν έρευνας στη διεθνή βιβλιογραφία παρουσιάζονται πρωτόκολλα που έχουν αναπτυχθεί για την κρυπτογράφηση της επικοινωνίας των δεδομένων αυτών.

2. ΕΞΥΠΝΑ ΔΙΚΤΥΑ (SMART GRIDS)



Η παραγωγή ηλεκτρικής ενέργειας από ανανεώσιμες πηγές ενέργειας θα πρέπει να αυξηθεί σημαντικά ώστε να επιτευχθεί ο στόχος της βιώσιμης ενέργειας για όλους (SE4ALL) και να διπλασιαστεί το μερίδιο της ανανεώσιμης ενέργειας (RE) στο παγκόσμιο ενεργειακό μείγμα μέχρι το 2030. Ευτυχώς, τα υψηλά επίπεδα διείσδυσης των ανανεώσιμων πηγών ενέργειας στο δίκτυο είναι εφικτά από τεχνική και οικονομική άποψη, καθώς οι ηλιακές και οι αιολικές τεχνολογίες έχουν εξελιχθεί σε μεγάλο βαθμό. Ωστόσο, η συνεχής και διευρυμένη αύξηση του μεριδίου των ανανεώσιμων πηγών ενέργειας σε κεντρικά και αποκεντρωμένα δίκτυα απαιτεί μια περισσότερο καινοτόμο και πιο αποτελεσματική προσέγγιση στη διαχείριση του δικτύου, αξιοποιώντας πλήρως τα «έξυπνα δίκτυα» και τις «τεχνολογίες έξυπνων δικτύων». Τα υφιστάμενα συστήματα πλέγματος (grids) ενσωματώνουν ήδη στοιχεία έξυπνης λειτουργικότητας, αλλά χρησιμοποιούνται κυρίως για να εξισορροπήσουν την προσφορά και τη ζήτηση.

Τα έξυπνα δίκτυα ενσωματώνουν την τεχνολογία πληροφοριών και επικοινωνιών σε όλες τις πτυχές της παραγωγής, της παράδοσης και της κατανάλωσης ηλεκτρικής ενέργειας, προκειμένου να ελαχιστοποιηθούν οι περιβαλλοντικές επιπτώσεις, να βελτιωθούν οι αγορές, να βελτιωθεί η αξιοπιστία και η εξυπηρέτηση, να μειωθεί το κόστος και να βελτιωθεί η αποτελεσματικότητα (EPRI 2013). Αυτές οι τεχνολογίες μπορούν να εφαρμοστούν σε όλα τα επίπεδα, από τις τεχνολογίες παραγωγής μέχρι τις καταναλωτικές συσκευές. Ως εκ τούτου, τα έξυπνα δίκτυα μπορούν να διαδραματίσουν καθοριστικό ρόλο στη μετάβαση σε ένα βιώσιμο ενεργειακό μέλλον με διάφορους τρόπους όπως: τη διευκόλυνση της ομαλής ενσωμάτωσης υψηλών μεριδίων μεταβλητών ανανεώσιμων πηγών ενέργειας, την υποστήριξη της αποκεντρωμένης παραγωγής ενέργειας, δημιουργώντας νέα επιχειρηματικά μοντέλα μέσω βελτιωμένων ροών πληροφόρησης, εμπλοκής των καταναλωτών και βελτιωμένου ελέγχου του συστήματος, παρέχοντας επίσης ευελιξία στην πλευρά της ζήτησης.

2.1. Περιγραφή έξυπνων δικτύων

Το Έξυπνο δίκτυο (Smart Grid) στην ουσία είναι η εξέλιξη του υπάρχοντος ηλεκτρικού δικτύου, όπου ενσωματώνονται καινοτόμες τεχνολογίες επικοινωνιών και δικτύων, και χρησιμοποιούνται συσκευές μέτρησης που λειτουργούν με αυτόματο τρόπο. Ο σκοπός της κατασκευής των έξυπνων δικτύων είναι η δημιουργία ενός ολοκληρωμένου συστήματος για την καλύτερη διαχείριση των ενεργειακών πόρων, την παρακολούθηση κατανάλωσης ενέργειας. Για να επιτευχθεί η δημιουργία ενός έξυπνου δικτύου χρησιμοποιούνται καινοτόμες υποδομές δικτύων και ειδικές συσκευές ελέγχου και μέτρησης, όπως οι έξυπνοι μετρητές (αναλύονται σε επόμενο κεφάλαιο). Σε όλα τα επίπεδα, όλες οι συσκευές είναι συνδεδεμένες με το κεντρικό σύστημα σε πραγματικό χρόνο (συστήματα AMR). Με τη χρήση έξυπνων συσκευών οι καταναλωτές έχουν τη δυνατότητα να ελέγχουν το φορτίο τους και να εξοικονομούν ενέργεια (πολιτικές DSM). (Kempener et al, 2013):

Οι δυνατότητες που παρέχει η επικοινωνία των έξυπνων δικτύων επιτρέπει την άμεση ενημέρωση που σχετίζεται με θέματα της ζήτησης, της τιμολόγησης ή τις διακοπές των φορτίων (πολιτικές DR). Λόγω του ότι η ζήτηση μεταβάλλεται, υπάρχουν κατάλληλα εφεδρικά συστήματα σε περίπτωση που η ζήτηση αυξηθεί. Ένα σημαντικό πλεονέκτημα του έξυπνου δικτύου είναι ότι προσφέρει αλληλεπίδραση μεταξύ φορτίου και παραγωγής σε πραγματικό χρόνο. Συνεπώς, τα σφάλματα ανιχνεύονται πολύ πιο εύκολα και εντοπίζονται γρήγορα οι εναλλακτικές διαδρομές για την ροή του ρεύματος.

Επίσης, τα έξυπνα δίκτυα προωθούν την "πράσινη ενέργεια" που μπορεί εύκολα να ενσωματωθεί σε ένα τέτοιο σύστημα καθώς κάθε καταναλωτής μπορεί να γίνει και ο ίδιος παραγωγός ενέργειας χρησιμοποιώντας φωτοβολταϊκά, ανεμογεννήτριες, μικρά υδροηλεκτρικά, κυψέλες υδρογόνου. Με αυτόν τον τρόπο η ενέργεια που δεν καταναλώνει ή δεν χρειάζεται ο ιδιοκτήτης, μπορεί να πωληθεί στους υπόλοιπους καταναλωτές. Με τους μετρητές κατανάλωσης ενέργειας ο χρήστης γνωρίζει σε πραγματικό χρόνο την ποσότητα ενέργειας που καταναλώνει (Smart metering) .

Ένα ευφυές δίκτυο δίνει δυνατότητες :

• “Ευφυούς” συνύπαρξης της κεντρικής και διεσπαρμένης παραγωγής με αποτέλεσμα την μείωση της χρήσης άνθρακα και αποδοτικού χειρισμού της ζήτησης.

• Εμπορίας ενέργειας και βελτιστοποίησης κόστους μέσω χρονομεταβλητών τιμολογίων και διαφόρων κινήτρων εξαρτώμενων από το μεταβαλλόμενο φορτίο.

• Ενεργού συμμετοχής του πελάτη με βάση την επικοινωνία σε δύο κατευθύνσεις και μεγάλη ροή πληροφορίας.

Ένα ευφυές δίκτυο προσφέρει :

• Αυξημένη αξιοπιστία.

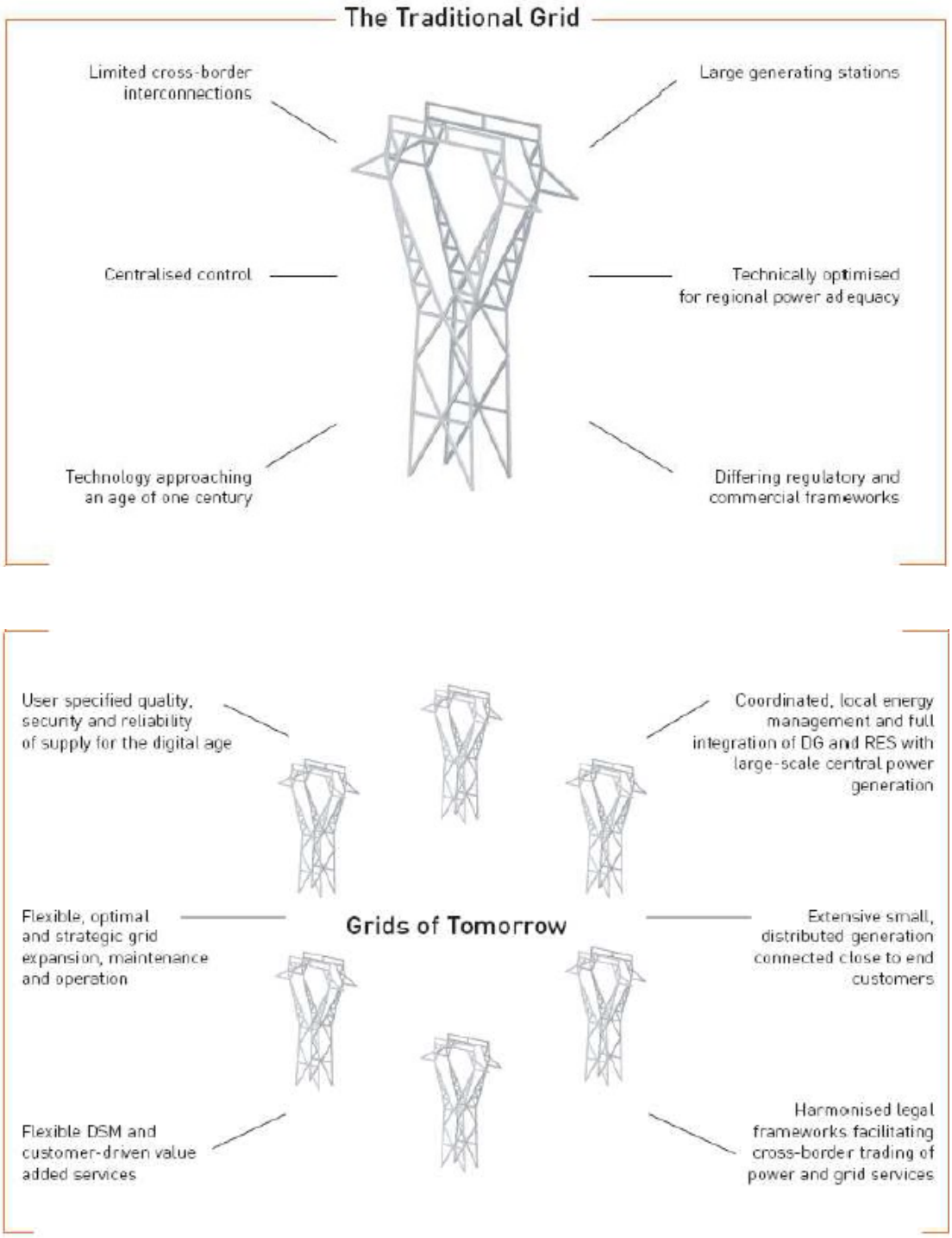
• Αποκεντρωμένη παραγωγή (οικιακοί καταναλωτές που μπορούν να γίνουν και παραγωγοί).

• Ελαστικότητα στη ζήτηση ενέργειας με τη χρήση ΑΠΕ.

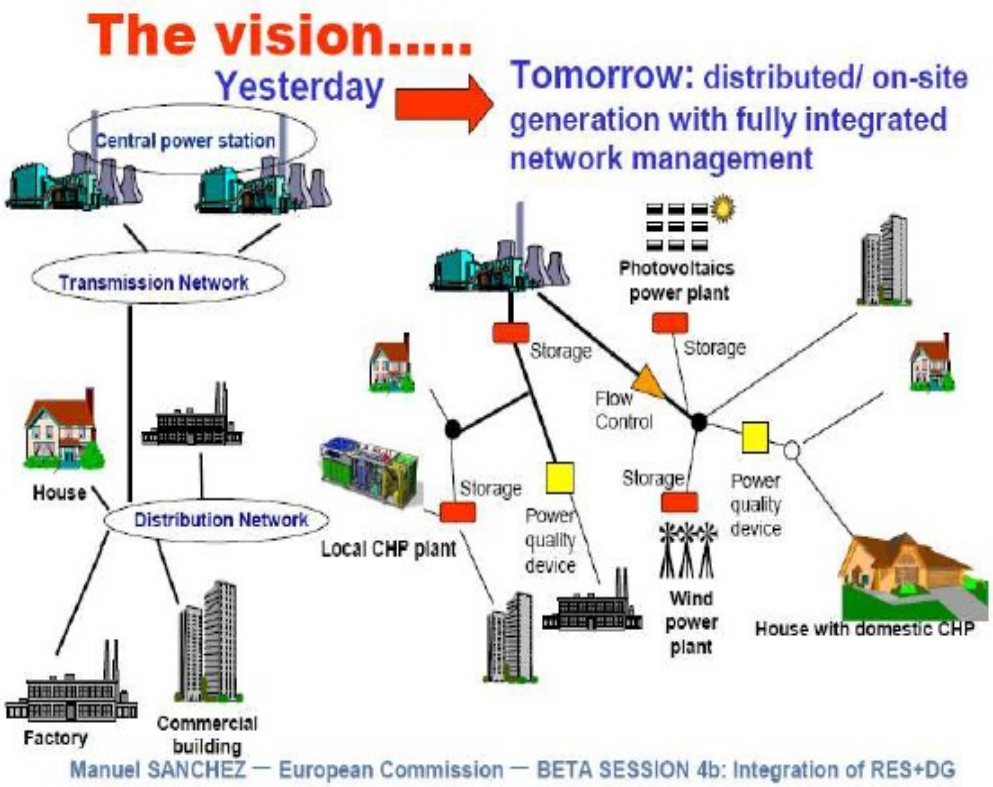
• Εξοικονόμηση Ενέργειας – Μείωση Απωλειών.

• Προστασία Περιβάλλοντος.

Η διαφορά της δομής ενός έξυπνου δικτύου σε σχέση με ένα παραδοσιακό παρουσιάζεται στις εικόνες 1 και 2:



Σχήμα 1- Δίκτυα Ενέργειας στο παρελθόν και στο μέλλον



Σχήμα 2- Δίκτυα Ενέργειας στο παρελθόν και στο μέλλον

Πηγή: Sanchez (2010)

Ένα έξυπνο δίκτυο μοιάζει με τον υπολογιστή. Οι τοποθετημένοι αισθητήρες σε διάφορες θέσεις στο δίκτυο συλλέγουν πληροφορίες σχετικά με τις συνθήκες λειτουργίας του δικτύου - συμπεριλαμβανομένων των όγκων ηλεκτρικής ενέργειας, των δυνάμεων και άλλων χαρακτηριστικών - και μεταδίδουν αυτές τις πληροφορίες (σε μερικές περιπτώσεις συνεχώς ή / και στιγμιαία) σε υπολογιστές κοινής ωφέλειας. Αυτοί οι υπολογιστές μπορούν να πραγματοποιούν αυτόματα αλλαγές στις ρυθμίσεις εξοπλισμού δικτύου χωρίς να είναι απαραίτητη η ανθρώπινη παρέμβαση. Σε πολλές περιπτώσεις, αυτές οι αλλαγές μπορούν να αντιμετωπίσουν προληπτικά ζητήματα προτού προκαλέσουν προβλήματα στους πελάτες. Οι πληροφορίες μπορούν επίσης να αποθηκευτούν για μελλοντική χρήση, ή ανάλυση και λήψη αποφάσεων από τους ανθρώπους.

Σε ένα παραδοσιακό δίκτυο, τα δεδομένα της λειτουργίας του δικτύου δεν διατίθενται σε πραγματικό χρόνο. Για την απόκτηση δεδομένων από το δίκτυο διανομής, είναι απαραίτητο ειδικές ομάδες έρευνας να χρησιμοποιήσουν και να τοποθετήσουν προσωρινές συσκευές καταγραφής δεδομένων σε επιλεγμένες τοποθεσίες και συνήθως αυτό γίνεται κατόπιν αιτήματος των παραπόνων από τους οικιακούς χρήστες. Στην περίπτωση του παραδοσιακού δικτύου διανομής ενέργειας, οι πληροφορίες είναι περιορισμένες λόγω της μη

έγκαιρης συλλογής τους, επειδή συλλέγονται και αναλύονται πολύ καιρό μετά την καταγραφή τους. Επιπλέον, ο εξοπλισμός των παραδοσιακών δικτύων ρυθμίζεται μόνο περιοδικά, με πολλές υπηρεσίες κοινής ωφέλειας να χρησιμοποιούν προεπιλεγμένες ρυθμίσεις που υποβλέπουν την απόδοση του δικτύου. Επίσης μια σημαντική διαφορά είναι ότι οι συσκευές που χρησιμοποιούνται στα συμβατικά δίκτυα δεν μπορούν να ελεγχθούν εξ αποστάσεως. Συνεπώς, οποιεσδήποτε προσαρμογές χρειάζονται, απαιτούν την αποστολή ειδικού συνεργείου εξυπηρέτησης πελατών και αυτό αυξάνει το κόστος.

2.2. Τεχνολογίες των έξυπνων δικτύων

Οι εφαρμογές τεχνολογιών των έξυπνων δικτύων (smart grids) ενσωματώνονται σε ολόκληρο τον κόσμο, από απομονωμένα νησιά έως πολύ μεγάλα ολοκληρωμένα συστήματα. Για τις ανεπτυγμένες χώρες, οι τεχνολογίες έξυπνων δικτύων μπορούν να χρησιμοποιηθούν για την αναβάθμιση, τον εκσυγχρονισμό ή την επέκταση των παλαιών συστημάτων πλέγματος, ενώ συγχρόνως παρέχουν ευκαιρίες για την εφαρμογή νέων καινοτόμων λύσεων. Για τις αναπτυσσόμενες και τις αναδυόμενες χώρες, οι τεχνολογίες έξυπνων δικτύων είναι απαραίτητες για την αποφυγή της δέσμευσης των παρωχημένων ενεργειακών υποδομών, την προσέλκυση νέων επενδυτικών ροών και τη δημιουργία αποδοτικών και ευέλικτων δικτύων που θα μπορούν να ικανοποιήσουν την αυξανόμενη ζήτηση ηλεκτρικής ενέργειας και μια σειρά διαφορετικών πηγών ενέργειας.

Οι τεχνολογίες έξυπνων δικτύων συμβάλλουν ήδη σημαντικά στη λειτουργία του δικτύου ηλεκτρισμού σε πολλές χώρες. Υπάρχουν αρκετές περιπτώσεις όπως αυτής Δανίας, της Τζαμάικα, των Κάτω Χώρων, της Σιγκαπούρης και των Ηνωμένων Πολιτειών (Νέο Μεξικό και Πουέρτο Ρίκο) όπου υπάρχουν επιτυχημένοι συνδυασμοί τεχνολογιών έξυπνων δικτύων με την ενσωμάτωση ανανεώσιμων πηγών ενέργειας. Ωστόσο, όπως δείχνουν περιπτωσιολογικές μελέτες, η επιτυχής εφαρμογή τεχνολογιών έξυπνων δικτύων για τις ανανεώσιμες πηγές ενέργειας απαιτεί αλλαγές στα πολιτικά και κανονιστικά πλαίσια για την αντιμετώπιση μη τεχνικών ζητημάτων, ιδίως όσον αφορά τη διανομή των οφελών και του κόστους μεταξύ των προμηθευτών, των καταναλωτών και των φορέων εκμετάλλευσης του δικτύου. Με την αύξηση των ανανεώσιμων πηγών ενέργειας, οι τεχνολογίες έξυπνων δικτύων σε συνδυασμό με τις κατάλληλες πολιτικές και κανονισμούς στήριξης θα είναι απαραίτητες για τη μετατροπή του συστήματος ηλεκτρικής ενέργειας και τη δημιουργία υποδομής δικτύου για την υποστήριξη ενός αειφόρου ενεργειακού μέλλοντος.

Οι τεχνολογίες των έξυπνων δικτύων μπορούν να βοηθήσουν στην υλοποίηση των ανανεώσιμων πηγών ενέργειας, αλλά η έλλειψη εμπειρίας και οι συναφείς αβεβαιότητες - όσον αφορά το κόστος και τις επιδόσεις των τεχνολογιών, το κόστος και τα οφέλη και τα μη τεχνικά ζητήματα όπως η ιδιωτική ζωή, καθιστούν δύσκολη την εφαρμογή τους. Οι μεγάλες διαφορές μεταξύ των συστημάτων ηλεκτρικής ενέργειας των χωρών έρχονται να δυσκολέψουν την εφαρμογή τους. Τα σημερινά επίπεδα των μεριδίων των ανανεώσιμων πηγών ενέργειας ποικίλλουν μεταξύ των χωρών, και κυμαίνονται από 67% στη Λατινική Αμερική έως λιγότερο από 2% στη Μέση Ανατολή. Ομοίως, οι εθνικοί στόχοι για τις ανανεώσιμες πηγές ενέργειας κυμαίνονται από μέτριους στόχους, από 5% έως 100% το 2020 στην περίπτωση αρκετών νησιωτικών κρατών.

Επίσης, το ίδιο το σύστημα ηλεκτρικής ενέργειας έχει εξελιχθεί διαφορετικά μεταξύ των χωρών, ανάλογα με τη γεωγραφική τους θέση, τη ζήτηση τους και το μείγμα των πηγών

ηλεκτρικής ενέργειας. Σε ορισμένες περιοχές, όπως η Ευρώπη, η ζήτηση ηλεκτρικής ενέργειας αναμένεται να σταθεροποιηθεί, ενώ σε περιοχές όπως η Ασία και η Αφρική η ζήτηση της ηλεκτρικής ενέργειας αναμένεται να διπλασιαστεί ή να τριπλασιαστεί τα επόμενα 20 χρόνια. Παρά τις αβεβαιότητες αυτές, τα αποτελέσματα του REMAP 2030 έδειξαν ότι θα υπάρξουν απαραίτητα υψηλότερα μερίδια ανανεώσιμων πηγών ενέργειας για την επίτευξη του στόχου για τον διπλασιασμό των ανανεώσιμων πηγών ενέργειας σε όλες τις περιφέρειες και χώρες. Μια από τις βασικές ερωτήσεις για τους υπεύθυνους για τη λήψη αποφάσεων είναι επομένως ο χρόνος και ο τρόπος εισαγωγής τεχνολογιών έξυπνων δικτύων. (REMAP, 2013)

2.3. Τεχνικά ζητήματα των έξυπνων δικτύων

Οι υψηλότερες συμμετοχές ανανεώσιμων πηγών ενέργειας στο σύστημα ηλεκτρικής ενέργειας δεν θα αλλάξουν μόνο την πηγή ενέργειας, αλλά θα μετατρέψουν την ίδια τη φύση του τρόπου λειτουργίας των δικτύων ηλεκτρικής ενέργειας. Τα ευφυή δίκτυα όχι μόνο είναι πιο αποτελεσματικά και διευκολύνουν το δρόμο προς ένα βιώσιμο μέλλον, αλλά μπορούν επίσης να αλλάξουν τις θεσμικές σχέσεις μεταξύ των παραγωγών, των καταναλωτών και των εταιρειών μεταφοράς και διανομής, τον τρόπο διαχείρισης και ρύθμισης των δικτύων. Αυτά τα μη τεχνικά ζητήματα θα πρέπει να αναγνωρίζονται όταν εξετάζεται η μετάβαση σε ένα ευφυέστερο δίκτυο και περιλαμβάνουν:

• την ιδιοκτησία δεδομένων και την πρόσβαση. Τα έξυπνα δίκτυα αυξάνουν την ποσότητα και τη διαθεσιμότητα των δεδομένων που έχουν αξία. Ποιος κατέχει αυτά τα δεδομένα; Ποιος μπορεί να έχει πρόσβαση στα δεδομένα;

• τον έλεγχο της ασφάλεια δικτύου. Πώς οι τεχνολογίες έξυπνων δικτύων επηρεάζουν την ευπάθεια του συστήματος ηλεκτρικής ενέργειας σε φυσικές καταστροφές ή κακόβουλες επιθέσεις;

• τον έλεγχο των κατανεμημένων πόρων. Ποιος πρέπει να ελέγχει μια κατανεμημένη γεννήτρια ανανεώσιμων πηγών ενέργειας - τον ιδιοκτήτη / φορέα εκμετάλλευσης ή τον φορέα εκμετάλλευσης του δικτύου / του συστήματος;

• τον ρόλο για νέους παράγοντες της αγοράς. Ποιες είναι οι συνέπειες του ανοίγματος του συστήματος ηλεκτρικής ενέργειας σε νέες εταιρείες και ιδιώτες; Πώς μπορεί αυτό το άνοιγμα να επηρεάσει την αξιοπιστία του συστήματος, την ποιότητα της ενέργειας, το κόστος και άλλες μεταβλητές;

• την ανάγκη για πρότυπα. Τα διάφορα συστατικά ενός ευφυέστερου δικτύου πρέπει να είναι σε θέση να επικοινωνούν μεταξύ τους. Ποια γλώσσα πρέπει να χρησιμοποιείται και ποιος λαμβάνει αυτή την απόφαση; Δεν υπάρχουν απλές απαντήσεις σε αυτές τις ερωτήσεις και είναι πολύ περιορισμένη η εμπειρία σε όλο τον κόσμο από την οποία μπορούμε να μάθουμε.

2.4. Έξυπνοι μετρητές (Smart Meters)

Δεν υπάρχει γενική συμφωνία για το τι χαρακτηρίζεται ως τεχνολογία έξυπνου δικτύου. Ωστόσο, γίνεται αντιληπτό ότι περιλαμβάνει ένα ευρύ φάσμα τεχνολογιών επικοινωνίας, διαχείρισης και ελέγχου πληροφοριών που συμβάλλουν στην

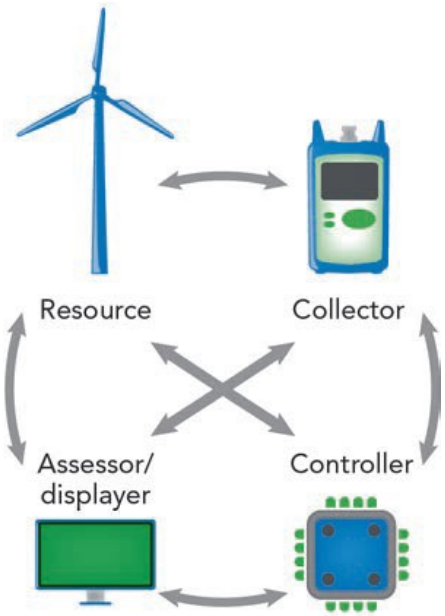
αποτελεσματικότητα και την ευελιξία της λειτουργίας του συστήματος ηλεκτρισμού. Αυτές οι τεχνολογίες μπορούν να τεθούν σε τέσσερις λειτουργικές κατηγορίες (Σχήμα 3).

● Συλλέκτες πληροφοριών: Τα έξυπνα δίκτυα βασίζονται σε δεδομένα που συλλέγονται από διάφορους τύπους αισθητήρων. Αυτοί οι αισθητήρες γενικά μετρούν τα χαρακτηριστικά που σχετίζονται με την απόδοση των στοιχείων του συστήματος ηλεκτρισμού. Παραδείγματα περιλαμβάνουν μετρητές που μετρούν συνεχώς την ισχύ και την απόδοση ηλεκτρικής ενέργειας ενός κατανεμημένου παραγωγού ανανεώσιμων πηγών ενέργειας, αισθητήρες που παρακολουθούν τη θερμοκρασία, τις δονήσεις και άλλα χαρακτηριστικά ενός μετασχηματιστή και μετρητές που μετρούν τα χαρακτηριστικά ηλεκτρικής ενέργειας (τάση, ρεύμα κ.λπ.) μιας γραμμής διανομής.

● Συναρμολογητές πληροφοριών, διαφημιστές και αξιολογητές: Αυτή η κατηγορία περιλαμβάνει συσκευές που δέχονται πληροφορίες και προβάλλουν ή / και αναλύουν.

● Ελεγκτές που βασίζονται σε πληροφορίες: Αυτές οι συσκευές λαμβάνουν πληροφορίες και τις χρησιμοποιούν για να ελέγχουν την λειτουργία άλλων συσκευών για να επιτύχουν ορισμένους στόχους, όπως τη μείωση της κατανάλωσης ηλεκτρικής ενέργειας ή την σταθεροποίηση τάσης.

● Ενεργειακά μέσα: Περιλαμβάνουν τεχνολογίες που μπορούν να δημιουργήσουν, να αποθηκεύσουν ή να μειώσουν τη ζήτηση ηλεκτρικής ενέργειας. Οι τεχνολογίες έξυπνου δικτύου διαφέρουν ευρέως όσον αφορά το κόστος, την εφαρμοσιμότητα και την ωριμότητα της αγοράς. Παρόλα αυτά, ένα προσεκτικά ενοποιημένο σύνολο τεχνολογιών έξυπνων δικτύων μπορεί να μειώσει το κόστος και τους κινδύνους της ενσωμάτωσης των κατανεμημένων ανανεώσιμων πηγών ενέργειας στα συστήματα ηλεκτρικής ενέργειας.



Σχήμα 3- Οι 4 βασικές λειτουργίες της τεχνολογίας των έξυπνων δικτύων

Πηγή: (Kempener et al, 2013)

3. ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΣΤΑ ΕΞΥΠΝΑ ΔΙΚΤΥΑ

Ένα θεμελιώδες πρόβλημα είναι αυτό της ανάλυσης ιδιωτικών δεδομένων, όπου ένα τρίτο μέρος πρέπει να υπολογίσει κάποια συγκεντρωτικά στατιστικά στοιχεία για ορισμένα ευαίσθητα δεδομένα. Αυτό το πρόβλημα εντοπίζεται σε συγκεκριμένες εφαρμογές αλλά σε πολλές περιπτώσεις. Όταν το τρίτο μέρος, που ονομάζεται συναθροιστής (aggregator), είναι αξιόπιστο, μια εύκολη λύση θα ήταν να ζητηθεί από τους χρήστες να κρυπτογραφήσουν τα δεδομένα τους, χρησιμοποιώντας το δημόσιο κλειδί του συναθροιστής. Με τη λήψη των κρυπτογραφημάτων, ο συναθροιστής χρησιμοποιεί το ιδιωτικό του κλειδί για να ανακτήσει τα δεδομένα και στη συνέχεια υπολογίζει τα στατιστικά στοιχεία. Το πρόβλημα γίνεται πολύ πιο δύσκολο στην περίπτωση ενός μη αξιόπιστου συναθροιστή. Σε αυτό το κεφάλαιο εξετάζεται το θέμα της κρυπτογράφησης των συναθροιστών (aggregators). (Libert & Joye, 2013)

3.1. Πρωτόκολλα κρυπτογράφησης ιδιωτικών δεδομένων

Η κρυπτογραφία εφαρμόστηκε αρχικά σε μια πρώτη μορφή από τους αρχαίους αιγυπτίους πριν από περίπου τέσσερις αιώνες με τη χρήση των ιερογλυφικών συμβόλων, τα οποία μπορούσαν να διαβάζουν μόνο επιλεγμένα πρόσωπα της βασιλικής αυλής. Στην νεότερη ιστορία, η κρυπτογραφία έπαιξε πολύ σπουδαίο ρόλο στον πρώτο παγκόσμιο πόλεμο. Μόλις στις αρχές του 1900, άρχισαν να δημοσιεύονται αποτελέσματα διάφορων συστημάτων κρυπτογραφίας που είχαν φυσικά υλοποιηθεί για τις ανάγκες του πολέμου. Μετά την λήξη του, στρατιωτικοί οργανισμοί των Ηνωμένων Πολιτειών άρχισαν να σχεδιάζουν τις βασικές αρχές της κρυπτογραφίας με απόλυτη μυστικότητα. Η μυστικότητα αυτή διατηρήθηκε και μέχρι τον δεύτερο παγκόσμιο πόλεμο, όπου όλα τα τηλεπικοινωνιακά ανεπτυγμένα κράτη (Ηνωμένες Πολιτείες, πρώην Σοβιετική Ένωση, Αγγλία, Γαλλία, Ισραήλ) διέθεταν υπέρογκα ποσά για την ασφάλεια των τηλεπικοινωνιών τους και την αποκωδικοποίηση των τηλεπικοινωνιών όλων των άλλων. Μετά το τέλος και αυτού του πολέμου, η κρυπτογραφία άρχισε να εξαπλώνεται στον κόσμο ενώ δημοσιεύτηκαν πολλές ερευνητικές και αναπτυξιακές εργασίες.

Οι επιστήμονες που εργάζονταν για κρατικούς οργανισμούς μεταπήδησαν σε ιδιωτικές εταιρείες και συστηματοποίησαν το σχεδιασμό κρυπτογραφικών αλγορίθμων και πρωτοκόλλων. Χρειάστηκαν 25 περίπου χρόνια, μέχρι τη δημοσίευση βασικών αλγόριθμων όπως ο RSA και ο DES, οι οποίοι βρίσκονται σε εφαρμογή ακόμη και σήμερα. Στις αρχές της δεκαετίας του ‘80 και ενώ το ενδιαφέρον των ακαδημαϊκών ινστιτούτων και των πανεπιστημίων αυξανόταν με εκθετικό ρυθμό λόγω της πίεσης της βιομηχανίας, η NSA (National Security Agency) με επιστολή της, προειδοποίησε την IEEE Publications (Institute of Electronic & Electrical Engineering), ότι πιθανή δημοσίευση τεχνικών άρθρων που έχουν σχέση με κρυπτογραφία δεν είναι θεμιτή από την κυβέρνηση.

Αυτό έφερε μάλλον το αντίθετο αποτέλεσμα, προσδίδοντας στον τομέα της κρυπτογραφίας τεράστια δημοσιότητα. Η NSA ωστόσο κατάφερε ως ένα σημείο να ελέγχει την εξαγωγή προϊόντων κρυπτογραφίας στο εξωτερικό. Η αυξανόμενη πίεση όμως λόγω του μεγάλου ενδιαφέροντος από διάφορα πανεπιστήμια ανά τον κόσμο σε συνδυασμό με τα μεγάλα οικονομικά συμφέροντα που είχαν εξαπλώσει πλέον τις επιχειρηματικές τους δραστηριότητες σε διάφορες χώρες, οδήγησαν στην πλήρη δημοσιοποίηση των αλγόριθμων κρυπτογράφησης δίνοντας έτσι νέα ώθηση στην έρευνα.

Στόχοι της κρυπτογραφίας

Βασικοί τεχνικοί όροι

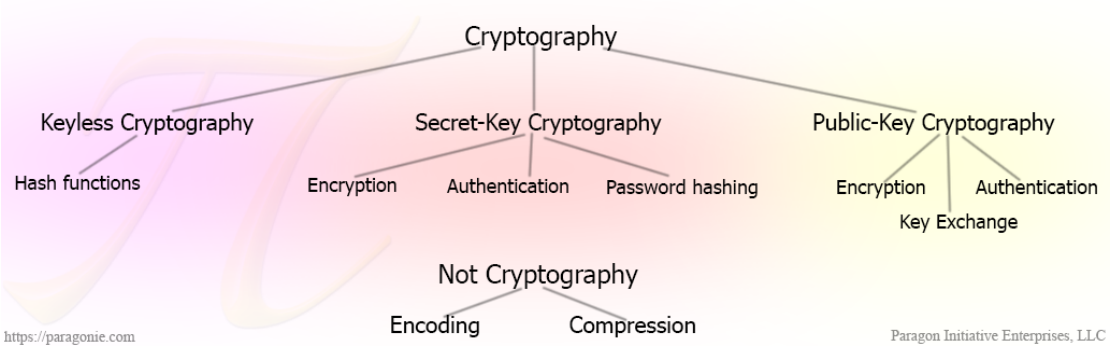
Η κρυπτογραφία βασίζεται σε έναν συνδυασμό μαθηματικών τεχνικών που αποσκοπούν στην επίτευξη της ασφάλειας δεδομένων. Οι βασικοί στόχοι της κρυπτογραφίας είναι οι εξής:

1. Εμπιστευτικότητα (Confidentiality). Πρόκειται για την κωδικοποίηση των δεδομένων επικοινωνίας μεταξύ δύο πλευρών, κατά τέτοιον τρόπο ώστε να είναι διαθέσιμα μόνο στις δυο αυτές πλευρές και σε κανέναν άλλον.

2. Ακεραιότητα Δεδομένων (Data Integrity). Είναι η διαδικασία σύμφωνα με την οποία ο παραλήπτης ενός μηνύματος θα πρέπει να είναι σίγουρος ότι το μήνυμα που έχει λάβει δεν έχει υποστεί αλλαγές κατά τη διάρκεια της μεταφοράς του.

3. Αυθεντικότητα (Authendication). Έχει σχέση με την πιστοποίηση της ταυτότητας. Η πιστοποίηση γίνεται σε δύο επίπεδα. Δύο πλευρές που επικοινωνούν με ένα ασφαλές κανάλι θα πρέπει να είναι σίγουρες η μία για την ταυτότητα της άλλης. Επίσης, η μία πλευρά θα πρέπει να είναι σίγουρη ότι το μήνυμα που έχει λάβει έχει αποσταλεί από την συγκεκριμένη πηγή και όχι από κάποιον τρίτο. Οι όροι που αντιστοιχούν στα δύο επίπεδα αυτά είναι entity authendication και data integrity authendication.

4. Μη-αποκήρυξη (Non-repudiation). Αποτρέπει μια οντότητα από την άρνηση κάποιας δέσμευσης ή πράξης. Για παράδειγμα, μια πλευρά επιτρέπει σε κάποια άλλη πλευρά την αγορά κάποιου προϊόντος μέσω ενός ασφαλούς καναλιού και αργότερα αρνείται ότι μια τέτοια πράξη έλαβε χώρα. Η κατηγοριοποίηση της κρυπτογραφίας φαίνεται στο Σχήμα 4



Σχήμα 4- Κατηγοριοποίηση της κρυπτογραφίας

Οι δύο μεγάλες κατηγορίες είναι η κατηγορία μοναδικού κλειδιού (Symmetric-Key ή αλλιώς Single-Key) και η κατηγορία Δημόσιου Κλειδιού (Public-Key). Η πρώτη κατηγορία περιλαμβάνει τους αλγόριθμους Single-key, τις hash-functions και τις ψηφιακές υπογραφές. Το χαρακτηριστικό των αλγορίθμων Single-key είναι η ύπαρξη ενός και μόνου κλειδιού για την κωδικοποίηση/αποκωδικοποίηση των δεδομένων.

Οι Hash-Functions είναι απεικονίσεις μιας κατεύθυνσης. Χρησιμοποιούνται τόσο για την επίτευξη της Ακεραιότητας Δεδομένων (Data Integrity), της Αυθεντικότητας

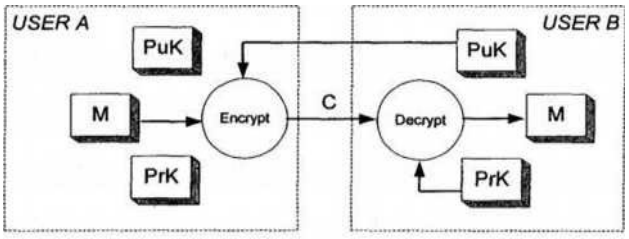
(Authentication) και της Μη-Αποκήρυξης (Non-repudiation). Οι υπογραφές με συμμετρικό κλειδί (symmetric-key) δεν είναι πολύ συνηθισμένες αλλά όπως όλες οι ψηφιακές υπογραφές αποσκοπούν στην Αυθεντικότητα (Authendication). Επίσης, οι αλγόριθμοι συμμετρικού κλειδιού (Single-key) διαχωρίζονται σε block και stream τύπους, ανάλογα με τον τρόπο επεξεργασίας των δεδομένων.

Οι block αλγόριθμοι επεξεργάζονται τα δεδομένα σε ομάδες (blocks) των 64 bits ή άλλου μεγέθους. Αντίστοιχα, οι stream αλγόριθμοι επεξεργάζονται τα δεδομένα σε επίπεδο bit ή το πολύ byte.

Η άλλη μεγάλη κατηγορία Δημοσίου Κλειδιού (Public-Key), περιλαμβάνει τους Public-Key αλγόριθμους και τις ψηφιακές υπογραφές.

3.2. Κρυπτογραφία δημοσίου κλειδιού

Η κρυπτογράφηση δεδομένων με τη χρήση δημοσίου κλειδιού είναι η πιο ασφαλής, όπως αναφέρεται στη διεθνή βιβλιογραφία. Η κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων ακολουθεί ένα σταθερό σχήμα αρχιτεκτονικής που περιλαμβάνει δύο κλειδιά: το δημόσιο κλειδί (Public Key) και το ιδιωτικό κλειδί (Private Key). Τα δύο κλειδιά έχουν την ιδιότητα της συμμετρικής αποκωδικοποίησης: δεδομένα που κωδικοποιούνται από το ένα μπορούν να αποκωδικοποιηθούν μόνο από το άλλο και αντίστροφα. Πρόκειται λοιπόν για ένα ζεύγος αριθμών που πληροί συγκεκριμένες ιδιότητες. Σχηματικά, η διαδικασία της κρυπτογράφησης δεδομένων με δημόσιο κλειδί φαίνεται στο Σχήμα 5

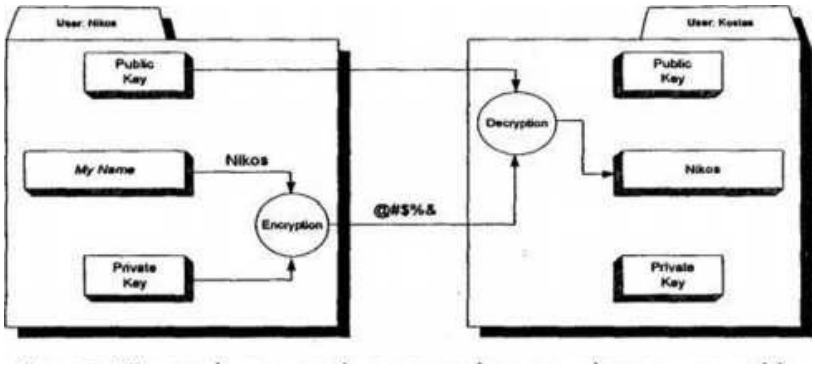


Σχήμα 5- Κρυπτογραφία Δημόσιου κλειδιού

Ο κάθε χρήστης έχει ένα ιδιωτικό κλειδί (PrK) και ένα δημόσιο κλειδί (PuK) όπως φαίνεται και στο παραπάνω σχήμα. Για να στείλει ο χρήστης Α ένα πακέτο δεδομένων Μ στον χρήστη Β, κωδικοποιεί το πακέτο αυτό με το δημόσιο κλειδί του Β (PuKB). Το αποτέλεσμα είναι το κρυπτογραφημένο μήνυμα C. Πρόσβαση σε αυτό το κρυπτογραφημένο μήνυμα μπορεί να έχουν πολλοί χρήστες εκτός του νόμιμου παραλήπτη Β. Κανένας άλλος όμως εκτός του χρήστη Β δεν μπορεί να αποκρυπτογραφήσει το μήνυμα C αφού για την επαναφορά του C στην αρχική κατάσταση Μ, απαιτείται το ιδιωτικό κλειδί του χρήστη Β (PrKB). Η διαδικασία που περιγράφεται παραπάνω χρησιμοποιείται τόσο για την κωδικοποίηση και αποκωδικοποίηση δεδομένων, όσο και για την παραγωγή της ψηφιακής υπογραφής (Digital Signature). Στη πρώτη περίπτωση, σκοπός είναι η κρυπτογράφηση των δεδομένων που μεταδίδονται στον παραλήπτη με το δημόσιο κλειδί του, μέσω ενός δικτύου που δεν είναι ασφαλές. Η αποκρυπτογράφηση των δεδομένων μπορεί να γίνει μόνο από τον ίδιο τον παραλήπτη, γιατί μόνο αυτός κατέχει το ιδιωτικό κλειδί του. Με αυτόν τον τρόπο, είναι

ασφαλής η μετάδοση των κρυπτογραφημένων δεδομένων στον συγκεκριμένο παραλήπτη. Στη δεύτερη περίπτωση, με την ηλεκτρονική υπογραφή, αποδεικνύεται η ταυτότητα του αποστολέα (sender authentication). Επίσης, με την ηλεκτρονική υπογραφή, μπορεί να πιστοποιηθεί ότι τα δεδομένα που απεστάλησαν δεν έχουν υποστεί αλλοίωση από τρίτο πρόσωπο μέχρι να φτάσουν στον προορισμό τους (document authentication).

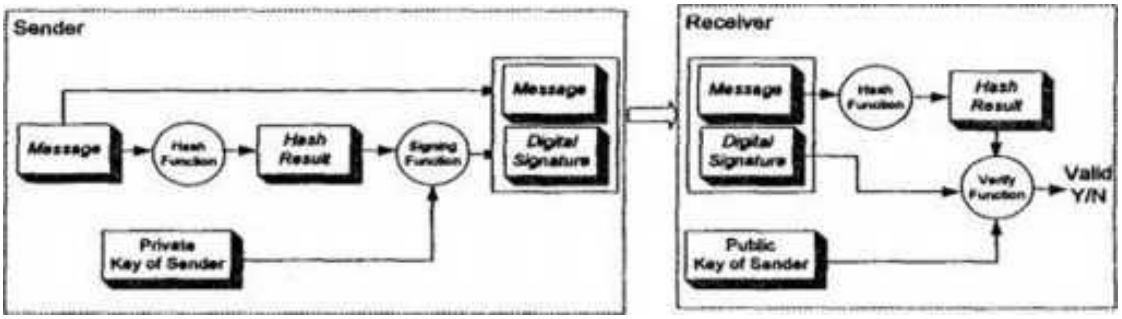
Στο Σχήμα 6 φαίνεται η χρήση της ηλεκτρονικής υπογραφής για την πιστοποίηση της ταυτότητας του αποστολέα.



Σχήμα 6- Χρήση της ηλεκτρονικής υπογραφής για την πιστοποίηση της ταυτότητας του αποστολέα.

Όπως φαίνεται στο σχήμα, ο αποστολέας κωδικοποιεί ένα πακέτο δεδομένων ή το όνομά του με το δικό του ιδιωτικό κλειδί. Το κρυπτογραφημένο κείμενο μπορούν να το αποκρυπτογραφήσουν όλοι όσοι βρίσκονται στο δίκτυο μετάδοσης, εφόσον γνωρίζουν το δημόσιο κλειδί του αποστολέα. Με τον τρόπο αυτό επιτυγχάνεται ο στόχος, ο οποίος είναι να πιστοποιηθεί σε κάθε ενδιαφερόμενο, ότι το πακέτο των δεδομένων προέρχεται από τον συγκεκριμένο αποστολέα και από κανέναν άλλο. Συνήθως, τέτοιες διαδικασίες δεν συναντάμε ποτέ μόνες τους στην εφαρμοσμένη κρυπτογραφία. Υπάρχει πάντα και η κρυπτογράφηση των δεδομένων σαν επιπλέον επίπεδο ασφάλειας. Επίσης, είναι δυνατόν να χρησιμοποιηθεί η ηλεκτρονική υπογραφή και για την πιστοποίηση της αυθεντικότητας ενός κειμένου, όπως αναφέρθηκε παραπάνω.

Στο Σχήμα 7 φαίνεται ο τρόπος που λειτουργεί αυτή η διαδικασία.



Σχήμα 7- Ψηφιακή υπογραφή - πιστοποίηση αυθεντικότητας μηνύματος

Στην πλευρά του αποστολέα εκτελούνται οι εξής διαδικασίες: το μήνυμα που πρόκειται να υπογράψει ψηφιακά περνάει μέσα από μια hash function. Η συνάρτηση αυτή είναι μιας κατεύθυνσης (δηλαδή μη-αντιστρέψιμη), η οποία απλώς απομονώνει ένα μέρος του κειμένου και το ανακατεύει με ψευδοτυχαίο τρόπο. Το αποτέλεσμα (Hash Result) περνάει από την διαδικασία της κρυπτογράφησης όπως περιγράφεται στο Σχήμα 6 και έχει ως αποτέλεσμα την ψηφιακή υπογραφή, η οποία είναι συνυφασμένη με το κείμενο (message).

Τόσο το κείμενο όσο και η ψηφιακή υπογραφή του αποστέλλονται στον παραλήπτη. Στην πλευρά του παραλήπτη, ακολουθείται η ίδια διαδικασία: Το κείμενο περνάει μέσα από την ίδια hash function και αποκωδικοποιείται με την βοήθεια του δημόσιου κλειδιού του αποστολέα. Το αποτέλεσμα συγκρίνεται με τη ψηφιακή υπογραφή που ακολουθεί το κείμενο. Σε περίπτωση που δεν είναι ίδια, τότε το κείμενο έχει υποστεί κάποια αλλαγή κατά την διάρκεια της μεταφοράς του στον παραλήπτη, οπότε και αγνοείται.

Τα πλεονεκτήματα της κρυπτογράφησης δημόσιου κλειδιού είναι τα εξής:

• Μόνο το ιδιωτικό κλειδί πρέπει να κρατηθεί μυστικό. Χρειάζεται μόνο ένας κεντρικός διαχειριστής που να είναι έμπιστος όλων των χρηστών, για τη διαχείριση και τη διανομή των δημοσίων κλειδιών.

• Τόσο το ιδιωτικό όσο και το δημόσιο κλειδί είναι δυνατόν να παραμείνουν ίδια για μεγάλες χρονικές περιόδους. Το γεγονός αυτό, αποκλείει την ανάγκη ύπαρξης μιας βάσης δεδομένων που να διατηρεί τα κλειδιά που παράγονται ανά σύνδεση ή ανά χρήστη.

• Πολλά συστήματα κρυπτογράφησης δημόσιου κλειδιού είναι πολύ αποδοτικά όταν χρησιμοποιούνται ως συστήματα ψηφιακής υπογραφής.

• Σε μεγάλα δίκτυα, ο αριθμός των απαραίτητων κλειδιών για την απρόσκοπτη επικοινωνία όλων των χρηστών μεταξύ τους είναι σχετικά μικρός.

Αντίστοιχα, τα μειονεκτήματα της κρυπτογράφησης δημόσιου κλειδιού είναι:

• Η υλοποίηση των αλγόριθμων τόσο σε software όσο και σε hardware δεν επιτυγχάνει μεγάλες ταχύτητες ή ρυθμούς λειτουργίας λόγω της έκτασης των υπολογισμών που απαιτούνται.

• Κανένα σύστημα κρυπτογραφίας δημόσιου κλειδιού δεν έχει αποδειχθεί ότι είναι εντελώς ασφαλές. Η ασφάλειά τους έγκειται στην υπολογιστική δυσκολία μικρότερων μαθηματικών συναρτήσεων.

Η σύλληψη της κρυπτογραφίας με δημόσιο κλειδί ανήκει στους Diffie και Heilman. Η ιδέα τους πρωτοπαρουσιάστηκε στο «National Computer Conference» το 1976, ενώ λίγους μήνες μετά δημοσίευσαν το ερευνητικό τους υλικό υπό τον τίτλο «New Directions in Cryptography». Από τότε μέχρι σήμερα έχουν αναπτυχθεί δεκάδες αλγόριθμοι κρυπτογράφησης δημοσίου κλειδιού, χωρίς όμως να είναι όλοι αποδοτικοί. Έτσι, πολλοί από αυτούς υστερούν όσον αφορά στην ασφάλεια, ενώ άλλοι χρησιμοποιούν υπερβολικά μεγάλο κλειδί κωδικοποίησης με αποτέλεσμα το παραγόμενο κρυπτογραφημένο μήνυμα να είναι πολύ μεγαλύτερο από το αρχικό μήνυμα.

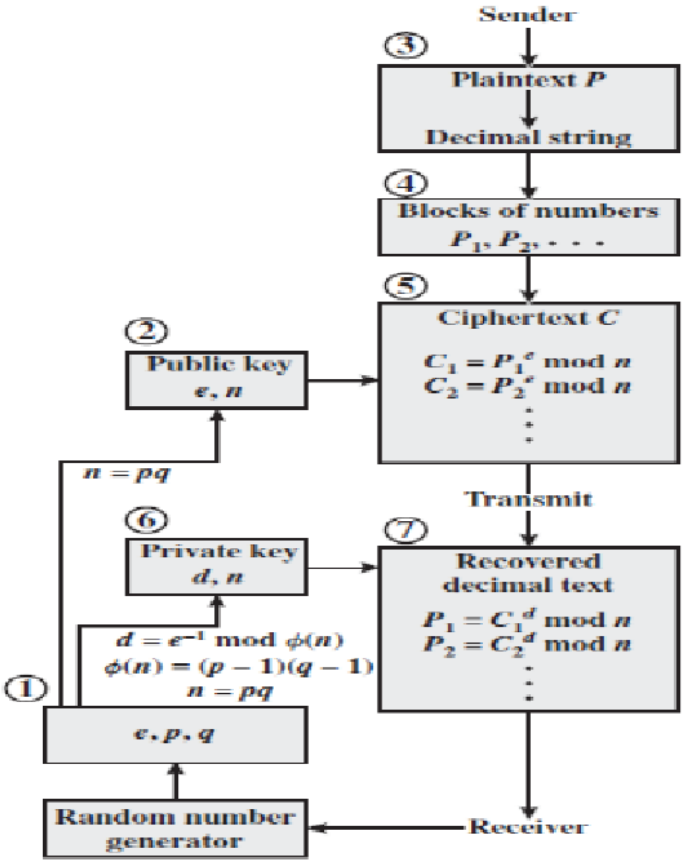
Είναι λοιπόν λίγοι τελικά οι αλγόριθμοι που μπορούν να χρησιμοποιηθούν στην πράξη ώστε και το απόρρητο του μηνύματος να εξασφαλίζεται και η υλοποίηση τους να είναι εύκολη και αποδοτική. Από αυτούς, μερικοί μπορούν να χρησιμοποιηθούν μόνο για την παραγωγή κλειδιών, άλλοι για κωδικοποίηση δεδομένων (άρα κατ' επέκταση και για την παραγωγή κλειδιών) και άλλοι μόνο για την παραγωγή ψηφιακής υπογραφής. Υπάρχουν συνολικά μόνο 3 αλγόριθμοι οι οποίοι μπορούν να χρησιμοποιηθούν και για τις τρεις παραπάνω διαδικασίες. Αυτοί είναι οι RSA, ElGamal και Rabin. Ο αλγόριθμος RSA που πήρε τα αρχικά του από τους Rivest, Shamir και Adelmann που τον σχεδίασαν, έχει γίνει πλέον de facto standard λόγω της τεράστιας αποδοχής που έχει από την βιομηχανία.

Ο Αλγόριθμος RSA

Ο Αλγόριθμος RSA προτάθηκε το 1977 από τους Rivest, Shamir και Adelmaim και βασίζεται στο γνωστό πρόβλημα της παραγοντοποίησης μεγάλων πρώτων αριθμών. Στον αλγόριθμο αυτό, υπάρχουν οι εξής πέντε παράμετροι που φαίνονται στον επόμενο πίνακα

Παράμετροι αλγόριθμου RSA

Παράμετρος	Τύπος	Περιγραφή
n	Ακέραιος αριθμός n-bits	Το γινόμενο p*q
q	Πρώτος αριθμός n-bits	
p	Πρώτος αριθμός n-bits	
e	Ακέραιος αριθμός n-bits	Παράγοντας κρυπτογράφησης
d	Ακέραιος αριθμός n-bits	Παράγοντας αποκρυπτογράφησης



Σχήμα 8- Αλγόριθμος RSA

Όπως φαίνεται από το σχήμα από το παραπάνω πίνακα, η παράμετρος n είναι το γινόμενο p*q, όπου p,q δύο μεγάλοι πρώτοι αριθμοί. Η διαδικασία της κρυπτογράφησης - αποκρυπτογράφησης με τον αλγόριθμο RSA έχει δύο στάδια. Την παραγωγή του δημόσιου κλειδιού και τον υπολογισμό του ιδιωτικού σε πρώτη φάση, και την διαδικασία της κωδικοποίησης – αποκωδικοποίησης δεδομένων σε δεύτερη.

Η μέθοδος Square and Multiply

Η μέθοδος αυτή βασίζεται στο γεγονός ότι μια πράξη ύψωσης ενός αριθμού σε μια δύναμη, μπορεί να αναλυθεί σε διαδοχικούς τετραγωνισμούς και πολλαπλασιασμούς των ενδιάμεσων αποτελεσμάτων με τον ίδιο τον αριθμό. Σε κάθε βήμα υπολογισμού, ο αριθμός τετραγωνίζεται. Σε κάθε βήμα επίσης, ανάλογα με την δυαδική τιμή του εκθέτη, ο αριθμός πολλαπλασιάζεται ή όχι με την προηγούμενη τιμή του τετραγώνου. Ο αλγόριθμος φαίνεται παρακάτω:

Η μέθοδος Square & Multiply

Είσοδος:	M: *Αρχικό Μήνυμα* E *Παράγοντας κρυπτογράφησης E-{ e„.,... , e„}*
Έξοδος:	C *Κρυπτογραφημενο Μήνυμα*
Αλγόριθμος:	1 *Z:* = M; 2 If e_0= o then 3 C := I; 4 Else 5 C := M; 6 End *{If}* 7 For i: = 1 to n-1 do *{n είναι* ο *αριθμός των bits}* 8 Z: = *7?* mod N; *{Τετραγωνισμός mod N }* 9 If ei = 1 then 10 C:=C ZmodN; 11 *{Πολλαπλασιασμός mod N}* 12 End *{If}* 13 End; *{For}* 14 Return C;

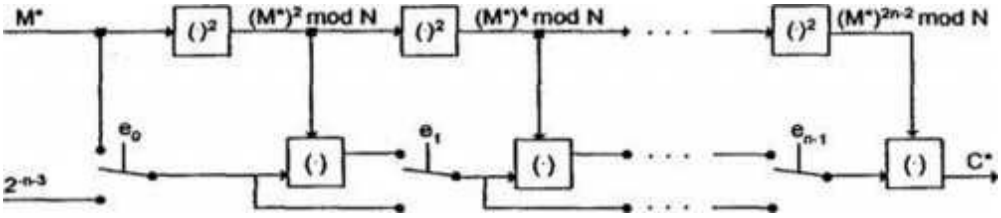
Ο αλγόριθμος μπορεί να γίνει πιο κατανοητός με την εφαρμογή του στο παρακάτω παράδειγμα. Έστω M=26 και $E=2_i$. Τα βήματα για τα οποία εκτελείται ο αλγόριθμος είναι ίσα με τον αριθμό των bits, στο παράδειγμά μας δηλαδή 5.

Στον παρακάτω πίνακα φαίνονται οι τιμές των μεταβλητών σε κάθε υπολογιστικό βήμα. Η μεταβλητή Z περιέχει το αποτέλεσμα των τετραγώνων, ενώ η μεταβλητή C το αποτέλεσμα των πολλαπλασιασμών.

Παράδειγμα υπολογισμού με τη μέθοδο Square and Multiply

Βήμα	e,	*ζ*	*C*
O	1	26	26
X	0	26*	26
2	1	26«	26<·26 = 20*
3	0	26»	26»
4	1	$20^{\cdot 6}$	$20^{16}\cdot$ 205 = 26'·“

Σε κάθε βήμα γίνεται επίσης και η πράξη modulo N οπότε δεν αυξάνει το μέγεθος των αποτελεσμάτων. Ο αριθμός των απαιτούμενων βημάτων για τον υπολογισμό του C δεν εξαρτάται από την τιμή του παράγοντα κρυπτογράφησης E αλλά από τον αριθμό των bits που χρησιμοποιούμε. Αυτή η ιδιότητα είναι πολύ σημαντική για την υλοποίηση του αλγόριθμου τόσο σε software αλλά πολύ περισσότερο σε hardware. Μια κυκλωματική προβολή του αλγόριθμου φαίνεται στο επόμενο σχήμα.



Σχήμα 9- Κυκλωματική προβολή του Square & Multiply σχήματος

Το κύκλωμα δέχεται στην είσοδο το αρχικό μήνυμα Μ. Τα κουτιά με τα χαρακτηριστικά $(.)^2$ και (.) αντιστοιχούν σε modulo δυνάμεις και πολλαπλασιαστές. Ο αριθμός των κυκλωμάτων για τον τετραγωνισμό και τον πολλαπλασιασμό είναι ίσος με τον αριθμό των ψηφίων των αριθμών που χρησιμοποιούνται. Σύμφωνα με τον αλγόριθμο, ο τετραγωνισμός γίνεται συνέχεια ενώ ανάλογα με την τιμή του αντίστοιχου ψηφίου του Ε, εκτελείται ή παρακάμπτεται ο πολλαπλασιασμός. Αν υποθέσουμε ότι έχουμε ένα κύκλωμα που εκτελεί τόσο τον τετραγωνισμό όσο και τον πολλαπλασιασμό, τότε η προβολή του Σχήματος 8 είναι ιδανική.

4. ΜΟΝΤΕΛΑ ΣΥΝΑΘΡΟΙΣΗΣ ΜΕ ΠΡΟΣΤΑΣΙΑ ΑΠΟΡΡΗΤΟΥ

4.1. Προστασία δεδομένων και ιδιωτικό απόρρητο

Όταν ένας έξυπνος μετρητής (smart meter) παρακολουθεί συνεχώς την τάση και το ρεύμα σε ένα οικιακό φωτοβολταϊκό σύστημα, ή την μέτρηση της κατανάλωσης του νερού, τότε συλλέγονται χρήσιμα δεδομένα για τα οποία όμως γεννιούνται ορισμένα ερωτήματα που σχετίζονται με την προστασία της ιδιωτικότητας των οικιακών χρηστών. Αυτά τα δεδομένα μπορεί να έχουν αξία για (Kempener et al, 2013):

• Τον ιδιοκτήτη σπιτιού

• Για το δίκτυο ηλεκτρικής ενέργειας.

• Τον εγκαταστάτη / κατασκευαστή, ώστε να αξιολογήσει την τεχνολογία των φωτοβολταϊκών συστημάτων.

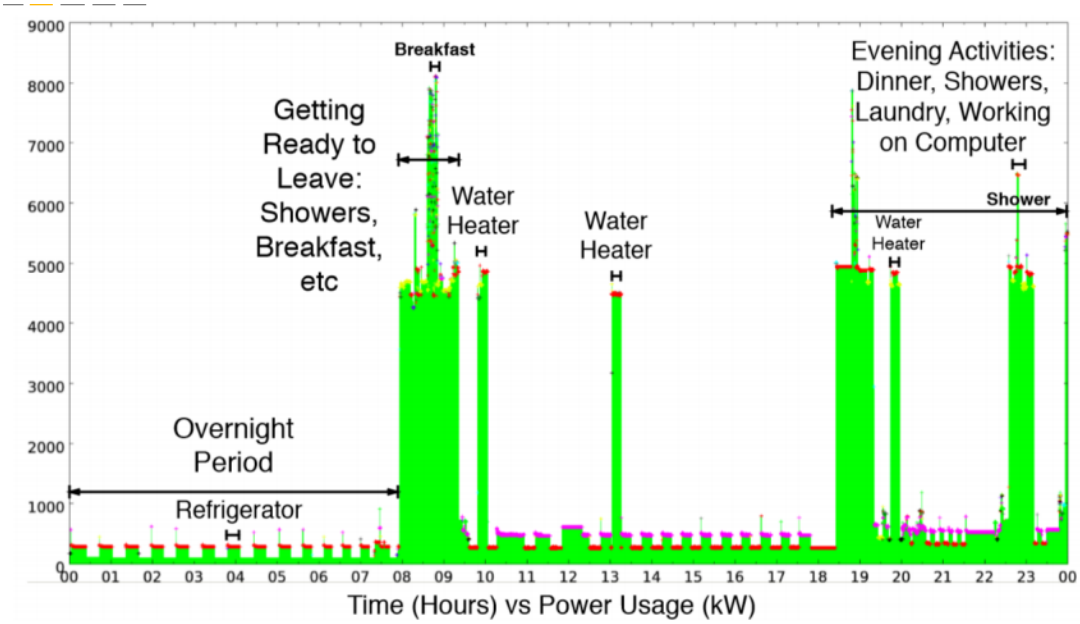
• Την πολιτική της σχεδίασης συστημάτων, για την καλύτερη κατανόηση του ρόλου των Φ/Β στα συστήματα ηλεκτρικής ενέργειας.

Ως ενδεικτικό παράδειγμα, θα εξετάσουμε την περίπτωση της έξυπνης μέτρησης ενέργειας (π.χ. αερίου, ηλεκτρισμού ή νερού). Οι συχνές μετρήσεις αθροίσματος της κατανάλωσης των χρηστών είναι πολύ χρήσιμες, για την ομαλή ρύθμιση της υπηρεσίας με την προσαρμογή του φορτίου ή την πρόβλεψη της προσφοράς, με αποτέλεσμα να υπάρξουν καλύτερες τιμές. Επίσης, η ανίχνευση των δυσλειτουργιών των δικτύων, εντοπίζεται πολύ πιο γρήγορα και σε περίπτωση διαρροής, η βλάβη εντοπίζεται άμεσα. Ενώ όμως ο υπολογισμός των συνολικών στατιστικών είναι χρήσιμος για τους καταναλωτές, δημιουργεί ανησυχίες για την προστασία της ιδιωτικής ζωής των χρηστών. Οι έξυπνοι μετρητές (smart meters) ηλεκτρικής ενέργειας τυπικά μετρούν τη χρήση της ηλεκτρικής ενέργειας κάθε 15 λεπτά. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν για την εξαγωγή πληροφοριών σχετικά με τις συμπεριφορές των χρηστών (π.χ. όταν είναι στο σπίτι και τι κάνουν). Άλλα παραδείγματα είναι η συλλογή ιατρικών δεδομένων για την παρακολούθηση των ασθενειών ή την ανάπτυξη νέων φαρμάκων, ή τη συλλογή προτιμήσεων των χρηστών για συστήματα συστάσεων κλπ. (Chan et al, 2012)

Τα παραπάνω παραδείγματα υπογραμμίζουν σαφώς την ανάγκη να επιτρέπεται στους χρήστες να μοιράζονται τα προσωπικά τους δεδομένα, επιτρέποντας ταυτόχρονα σε ένα όχι απαραίτητα έμπιστο συγκεντρωτή να διεξάγει μέτρηση των συνολικών στατιστικών στοιχείων. Διάφοροι τύποι στατιστικών στοιχείων μπορούν να υπολογιστούν σε ιδιωτικά δεδομένα. Τα ποσά και οι μέσοι όροι είναι ευρέως διαδεδομένα παραδείγματα.

Η συνεχής παρακολούθηση της κατανάλωσης ενέργειας από τους έξυπνους μετρητές μπορεί να αποκαλύψει δεδομένα τα οποία δεν είναι σωστό να αποκαλύπτονται, χωρίς την συγκατάθεση του ιδιοκτήτη του σπιτιού, όπου γίνεται η μέτρηση. Για παράδειγμα, από την παρακάτω εικόνα, η οποία δείχνει την κατανάλωση κατά τη διάρκεια κάποιας ημέρας σε ένα σπίτι όπου ζει μια οικογένεια, παρατηρούμε τις ώρες στις οποίες αυξάνεται η χρήση κατανάλωσης νερού ή ρεύματος. Επομένως, κάποιος θα μπορούσε να καταλάβει, ποιες ώρες

της ημέρας λείπουν τα μέλη της οικογένειας, η άλλες πληροφορίες οι οποίες θεωρούνται προσωπικά δεδομένα (Σχήμα 10).



Σχήμα 10- Κατανάλωση ενέργειας από οικία με την χρήση έξυπνου μετρητή

Τα θέματα που τίθενται ως προς την Ασφάλεια των Πληροφοριών και την Προστασία Προσωπικών των Δεδομένων είναι τα παρακάτω:

(1) Μέσω των έξυπνων δικτύων, μεταφέρονται δεδομένα σχετικά με την κατανάλωση ενέργειας των χρηστών και με αυτόν τον τρόπο κακόβουλοι χρήστες να έχουν την δυνατότητα να υποκλέψουν αυτά τα δεδομένα. Ο σκοπός τους είναι να αναλύσουν την κατανάλωση ενέργειας και τα προφίλ κατανάλωσης ενέργειας ώστε να αποκτήσουν κάποια γνώση σχετικά με τον τρόπο ζωής και τις συνήθειες των καταναλωτών ενέργειας.

(2) Κακόβουλοι χρήστες θα μπορούσαν να θέσουν σε κίνδυνο τους έξυπνους μετρητές των χρηστών, παρεμβαίνοντας στα συστήματα τους, και μπορούν να εισάγουν ψευδή δεδομένα ή εντολές ελέγχου στο δίκτυο (Khurana, 2010)

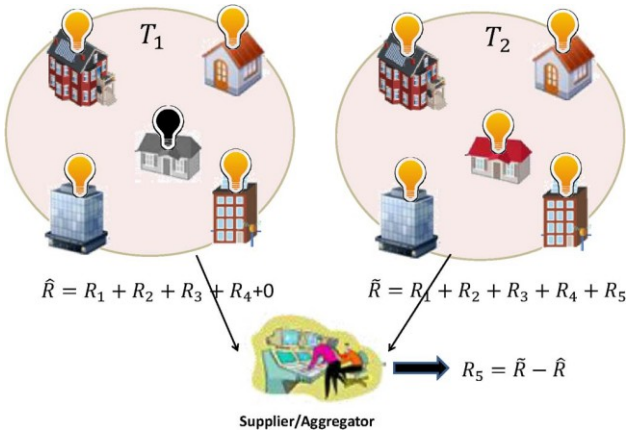
(3) Ορισμένες αρχές, όπως η χρησιμότητα, είναι επίσης περίεργες σχετικά με τα φορτία των χρηστών και τα προσωπικά δεδομένα. Είναι ζωτικής σημασίας να ελαχιστοποιούνται οι πληροφορίες απορρήτου κατά την εφαρμογή κανονικών λειτουργιών όπως η πληρωμή και ο έλεγχος.

Συνεπώς, γίνεται κατανοητό ότι η προστασία της ιδιωτικής ζωής στα έξυπνα δίκτυα αποτελεί κρίσιμο παράγοντα για την χρήση και αποδοχή των ιδιοκτητών. Στην ερευνητική κοινότητα, τα τελευταία χρόνια, έχει γίνει σοβαρή προσπάθεια στην αναζήτηση μεθόδων και πρωτοκόλλων τα οποία θα μπορούν να προστατέψουν στο μέγιστο την ιδιωτική ζωή και τα δεδομένα που συλλέγονται από τους έξυπνους μετρητές.

Για παράδειγμα, ο αλγόριθμος «NonIntrusive Load Monitoring» (NILM) που προτάθηκε από τον Hart (2002) είχε την ικανότητα να εξάγει πληροφορίες σχετικά με τις συσκευές από τα προφίλ φορτίου και έτσι μπορούσε κάποιος να αποκτήσει γνώση όσον αναφορά στις συνήθειες και τις συμπεριφορές κάποιου χρήστη που κατανάλωνε ενέργεια στην οικία του. Ο σκοπός του αλγορίθμου NILM ήταν να προβλέψει και να κατευθύνει τα ηλεκτρικά πρότυπα των χρηστών. Παρ' όλα αυτά, οι μη εξουσιοδοτημένοι χρήστες ή κακόβουλοι χρήστες θα μπορούσαν επίσης να εκμεταλλευτούν τον αλγόριθμο για να αναλύσουν τα πρότυπα και τις συνήθειες των χρηστών με σκοπό το κέρδος, πχ την υποκλοπή για διαφημιστικούς σκοπούς. Προκειμένου να επιτευχθεί αποτελεσματική προστασία της ιδιωτικής ζωής, προτάθηκαν διάφορες προσεγγίσεις που συνδυάζουν την τεχνολογία ασφάλειας πληροφοριών με τα νέα χαρακτηριστικά του έξυπνου δικτύου.

4.2. HDA επίθεση (Jia και Zhu, 2014)

Σε αυτό το μοντέλο επίθεσης, ο κακόβουλος χρήστης συνάγει τις στατιστικές πληροφορίες από το σύνολο των αποτελεσμάτων όπως φαίνεται στο σχήμα 2. Ο κακόβουλος χρήστης μπορεί να χρησιμοποιήσει ένα σύνολο από κατεστραμμένα μέτρα για να αποκαλύψει τις πραγματικές μετρήσεις. Οι τροποποιημένοι μετρητές μπορούν να αποκαλύψουν τους αναγνώσεις και μπορούν ακόμη να παρέχουν ψευδείς μετρήσεις στον συναθροιστή. Αυτή η επίθεση επινοήθηκε ως επίθεση διαφορικής συνάθροισης σε ανθρώπινο παράγοντα (HDA-**human-factor-aware differential aggregation**) και δεν μπορεί να αντιμετωπιστεί στα υπάρχοντα πρωτόκολλα συνάθροισης για την προστασία της ιδιωτικής ζωής που προτείνονται για έξυπνα δίκτυα.



Σχήμα 11- Επίθεση HAD σε ένα έξυπνο δίκτυο

Το πρωτόκολλό που προτείνουν οι Jia και Zhu (2014), διασφαλίζει ότι οι έξυπνοι μετρητές αποστέλλουν περιοδικά κρυπτογραφημένες μετρήσεις σε έναν προμηθευτή (ηλεκτρικής ενέργειας) έτσι ώστε να μπορούν να αντλούνται τα συγκεντρωτικά στατιστικά στοιχεία όλων των μετρήσεων, αλλά να μην μπορεί να μάθει κάποιος οποιαδήποτε πληροφορία σχετικά με τις ανθρώπινες δραστηριότητες. Επιπλέον, οι συγκεκριμένοι ερευνητές αξιολογούν την απόδοση του πρωτοκόλλου τους σε μια υλοποίηση που βασίζεται

στην γλώσσα Java θέτοντας διαφορετικές παραμέτρους. Η ανάλυση απόδοσης και χρησιμότητας δείχνει ότι το πρωτόκολλό των παραπάνω είναι απλό, αποτελεσματικό και πρακτικό.

Γενικό μοντέλο επίθεσης

Χρησιμοποιούνται τρεις τύποι προοδευτικής επίθεσης οι οποίες απεικονίζουν με απλό τρόπο τις πιθανές επιθέσεις στο έξυπνο δίκτυο.

1) Εξωτερική επίθεση (extrernal attack): ο εξωτερικός επιτιθέμενος προσπαθεί να θέσει σε κίνδυνο την ιδιωτικότητα δεδομένων των χρηστών παρακολουθώντας τα μεταδιδόμενα δεδομένα από την πλευρά του χρήστη στην πλευρά του συνόλου.

2) Εσωτερική Επίθεση (Inside Attack): Ο εισβολέας (π.χ. μη αξιόπιστος συναθροιστής) προσπαθεί να θέσει σε κίνδυνο την ιδιωτικότητα του μετρητή με μη εξουσιοδοτημένη πρόσβαση ή και εσφαλμένη χρήση των μετρητικών δεδομένων των χρηστών, γεγονός που μπορεί να προκαλέσει σοβαρές απειλές.

3) Κακόβουλη επίθεση εξόρυξης δεδομένων: ο εισβολέας αλλοιώνει τον συναθροιστή και χρησιμοποιεί άλλους τροποποιημένους μετρητές για να ανακαλύψει τις μετρήσεις των μετρητών των χρηστών, αλλοιώνοντας με αυτό τον τρόπο τα αποτελέσματα της συνάθροισης, π.χ. συγκρίνοντας τα συνολικά αποτελέσματα με την παρουσία και την απουσία συγκεκριμένου χρήστη.

Επίσημο πρότυπο επίθεσης και ορισμός απορρήτου

Για να γίνει κατανοητό το μοντέλο υιοθετείται ένα μοντέλο παιχνιδιού ώστε να εξηγηθεί η επίθεση HDA.

1) Παιχνίδι με μετρήσεις διαρροών μεμονωμένων μετρητών: Σε αυτό το παιχνίδι πραγματοποιούνται κάποια ερωτήματα και απαντήσεις μεταξύ του αντιπάλου και του χρήστη για να καθορίσουμε την ικανότητα του αντιπάλου. Η πιθανότητα επιτυχίας του αντιπάλου ορίζεται ως η πιθανότητα ο αντίπαλος να καταφέρει να ανακαλύψει με επιτυχία την αντιστοιχία μεταξύ ενός κρυπτογραφικού μηνύματος δεδομένων και των δεδομένων πραγματικών ενδείξεων.

Ρύθμιση: Ο χρήστης εκτελεί τον αλγόριθμο αρχικοποίησης του συστήματος για να δημοσιοποιήσει την προκύπτουσα κοινή παράμετρο στον αντίπαλο A. Ερωτήματα. Σε αυτή τη φάση, ο αντίπαλος όχι μόνο συλλαμβάνει τις κρυπτογραφημένες αναφορές των μετρητών αλλά επίσης εκκινεί αρχικά ερωτήματα συμβιβασμού και κρυπτογράφησης για μερικά μέτρα:

α) Κρυπτογράφηση. Ο αντίπαλος A επιλέγει έναν μετρητή i που δίνει τις αναγνώσεις R στην χρονική θυρίδα t και ζητάει τις μετρήσεις κρυπτογράφου. Χρησιμοποιούμε τα (i, t, R) για να μετρήσουμε τις μετρήσεις του μετρητή i στην χρονική θέση T. Ο αμφισβητίας επιστρέφει το encrypt Enc (sk_i, t, R) στον αντίπαλο εφαρμόζοντας το πρωτόκολλο. Επιπλέον, επιτρέπονται μόνο λιγότερα από ερωτήματα qc για ένα μέτρο i στη φάση Κρυπτογράφηση.

β) Συμβιβασμός. Ο αντίπαλος ορίζει ένα ακέραιο $i \in \{1,. . . , n\}$.

Αν i = 0, ο χρήστης επιστρέφει τη δυνατότητα συνάθροισης sk_0 στον αντίπαλο.

Εάν το i ισούται με 0, τότε ο αμφισβητίας επιστρέφει το sk_i, δηλαδή το μυστικό κλειδί για το i-μετρητή, στον αντίπαλο.

Πρόκληση. Ο Αντίπαλος εκδίδει δύο αναγνώσεις απλού κειμένου R_0 και R_1, μία ομάδα μετρητών $i_1, i_2, \ldots, i_l$, και μια χρονική θέση t*.

Ο αμφισβητίας παίρνει ένα κομμάτι πληροφορίας (bit) $b \in \{0, 1\}$ και επιστρέφει το αμφισβητούμενο κείμενο Enc (sk_i, t*, R_b). Οποιοδήποτε i δεν πρέπει να έχει συμβιβαστεί μέχρι το τέλος του παιχνιδιού.

Υπόθεση: Ο αντίπαλος εξάγει μια υπόθεση $b' \in \{0, 1\}$. Α κερδίζει εάν b = b'. Το πλεονέκτημα του Α κατά την επίθεση στο σχήμα ορίζεται ως εξής:

$$Adv_A = \left| \Pr[b = b'] - \frac{1}{2} \right|.$$

4.3. Επισκόπηση πρωτοκόλλων συνάθροισης

Οι Rastogi και Nath (2013) πρότειναν σε έρευνα τους κάθε χρήστης να κρυπτογραφεί τα προσωπικά του δεδομένα χρησιμοποιώντας ένα πρόσθετο ομοιόμορφο σύστημα κρυπτογράφησης (homomorphic encryption scheme). Ο συγκεντρωτής (aggregator) συγκεντρώνει όλα τα κρυπτογραφικά κείμενα, με σκοπό να δημιουργήσει την κρυπτογράφηση της συνολικής τιμής της μέτρησης και στη συνέχει στέλνει αυτή την τιμή στους χρήστες. Όλοι οι χρήστες, οι οποίοι διαθέτουν κάποιο μέρος του κλειδιού αποκρυπτογράφησης, συμβάλλουν στην αποκρυπτογράφηση της συνολικής τιμής αποστέλλοντας το κάθε μέρος της αποκρυπτογράφησης στον συναθροιστή.

Στη συνέχεια ο συναθροιστής συνδυάζει όλα τα μέρη της αποκρυπτογράφησης που λαμβάνονται από τους χρήστες για να εξαχθεί το άθροισμα των ιδιωτικών δεδομένων των χρηστών. Όπως και με άλλες προτάσεις (Gergely 2011, Cramer 2002), η προσέγγιση του (Rastogi , 2010) απαιτεί αμφίδρομη επικοινωνία μεταξύ των χρηστών και του συνόλου. Δυστυχώς δεν υπάρχει πάντοτε διαθέσιμο κανάλι επανάληψης. Για να λυθεί αυτό το ζήτημα, οι Garcia και Jacobs (2015) κατέληξαν σε ένα πρωτόκολλο συνάθροισης βασισμένο στην ομοιόμορφη κρυπτογράφηση και στην μοιραζόμενη μυστική προσθήκη. Η πρότασή τους εξαλείφει την ανάγκη επιπλέον καναλιού διόρθωσης. Από την άλλη πλευρά, η πολυπλοκότητα της επικοινωνίας είναι τετραγωνική όσο αναφορά τον αριθμό των χρηστών και κάθε χρήστης πρέπει να υπολογίσει έναν γραμμικό αριθμό ομοιόμορφων κρυπτογραφημάτων.

Οι Kursawe et al. (2011) περιγράφουν τέσσερα πρωτόκολλα που επιτρέπουν την συγκέντρωση των δεδομένων των χρηστών και συγκρίσεις μεταξύ των συναθροιστών των δεδομένων χωρίς τη χρήση αμφίδρομων καναλιών. Παρ' όλα αυτά, τα τρία πρώτα πρωτόκολλα χρειάζονται τις βασικές συμφωνίες του Diè-Hellman ή αξιολογήσεις bilinear map. Επομένως, απαιτούν την επικοινωνία μεταξύ των χρηστών και αυτό συνεπάγεται δαπανηρές αριθμητικές λειτουργίες. Το τέταρτο πρωτόκολλο των Kursawe et al [19] έχει χαμηλό γενικό κόστος αλλά, όπως και τα προηγούμενα, απαιτεί από κάθε χρήστη να αποθηκεύει το xed δημόσιο κλειδί όλων των άλλων χρηστών.

Οι Shi, Chan, Rie el, Chow και Song (2011) περιέγραψαν μια εντελώς αλληλεπιδραστική λύση. Το μοντέλο των Shi et al. παρουσιάζεται στο κεφάλαιο 6. Συνοπτικά αναφέρεται ότι διαχώρισαν την ικανότητα του συναθροιστή, που θεωρείται ως κλειδί, σε πρόσθετα μερίδια μεταξύ των χρηστών. Κάθε χρήστης χρησιμοποιεί το ιδιωτικό του κλειδί και κρυπτογραφεί τα ιδιωτικά του δεδομένα. Σε κάθε χρονική περίοδο, ο συναθροιστής συγκεντρώνει όλες τις κρυπτογραφημένες τιμές. Με τη χρήση του κλειδιού του ο συναθροιστής μπορεί να ανακτήσει εκ νέου το άθροισμα των ιδιωτικών δεδομένων των χρηστών. Οι Shi et al. (2011) προτείνουν μια λύση που γενικεύει μια οποιαδήποτε πρωταρχική ομάδα παραγγελιών όπου ισχύει η υπόθεση της απόφασης Diffie-Hellman (DDH). Παρείχαν επίσης μια απόδειξη ασφαλείας σε ένα τυπικό μοντέλο ιδιωτικότητας. Ωστόσο, υπάρχει μια σειρά ερευνητικών προκλήσεων, όπως η αποτυχία του χρήστη (ανοχή σφάλματος) και η αποτελεσματική υποστήριξη δυναμικών συνδέσεων και φύλλων. Λύσεις για αυτό το πρόβλημα πρότειναν οι Jawurek και Kerschbaum (2012).

Οι Joye και Libert (2013) σε εργασία τους επανεξετάζουν ένα πλήρως μη διαδραστικό μοντέλο των Shi et al. (2011) και δείχνουν πώς να εξαλείψουν μερικούς περιορισμούς τους. Μία σημαντική πρόκληση είναι αυτή της εκτίμησης των αθροισμάτων. Το μοντέλο των Joye και Libert (2013) υποστηρίζει τους μεγάλους χώρους και μεγάλο αριθμό χρηστών. Παράλληλα, ο αλγόριθμος αποκρυπτογράφησης λειτουργεί συνεχώς, ανεξάρτητα από τον αριθμό των χρηστών. Το μοντέλο των Joye and Libert παρουσιάζεται στο κεφάλαιο 7.

Ο σχεδιασμός μιας αρχιτεκτονικής συλλογής μετρήσεων φιλικής προς το ιδιωτικό απόρρητο και ενός συνδυασμού διαδικασιών περιλαμβάνει διάφορα επίπεδα, όπως την ασφαλή μεταφορά των δεδομένων μέσω του δικτύου επικοινωνίας, την ασφαλή αποθήκευση των μετρήσεων και τις κατάλληλες διαδικασίες για την πρόσβαση στα δεδομένα (NIST, 2010).

Όσον αφορά στην επικοινωνιακή υποδομή, οι Simo Fhom et al. (2010) και Berganza et al. (2011) προσδιορίζουν τις ακόλουθες βασικές απαιτήσεις:

1. Αναγνώριση των επιχειρηματικών οντοτήτων που έχουν πρόσβαση στα δεδομένα χρήστη.

2. Τα δεδομένα πρέπει να συλλέγονται με την ελάχιστη απαιτούμενη λεπτομέρεια για τις κατάλληλες λειτουργίες των έξυπνων δικτύων, ιδιαίτερα τα δεδομένα θα πρέπει να συλλέγονται ανώνυμα, εκτός εάν είναι απολύτως απαραίτητο και δεν γίνεται διαφορετικά.

3. Τα συλλεγμένα δεδομένα μπορούν να συσχετιστούν με την ταυτότητα του πελάτη μόνο όταν και όπου αυτό είναι απολύτως απαραίτητο.

4. Η υποδομή πρέπει να κλιμακωθεί σε μεγάλο αριθμό μετρητών (100.000 ή περισσότερο) με χρόνο ανάκτησης όχι περισσότερο των 5-10 λεπτών.

5. Τα δεδομένα πρέπει να παραδίδονται αξιόπιστα. Τουλάχιστον το 99,9% των μετρήσεων πρέπει να παραδοθεί στον καταναλωτή δεδομένων.

6. Οι μετρητές πρέπει να έχουν χαμηλό κόστος, δηλαδή όχι περισσότερο από 100 δολάρια.

Συνεπώς γίνεται κατανοητό ότι ορισμένα ειδικά θέματα των προηγμένων υπηρεσιών και εφαρμογών που επιτρέπονται από τα νέα συστήματα έξυπνης μέτρησης απαιτούν καινοτόμες αρχιτεκτονικές ασφάλειας για τη διαχείριση εύχρηστων και πολύπλοκων πολιτικών απορρήτου σε ένα σενάριο με πολλαπλούς παράγοντες.

Σύμφωνα με τα εννοιολογικά μοντέλα των έξυπνων μετρητών και των έξυπνων δικτύων που θεωρούνται σήμερα από τις αρχές κανονισμών και τυποποίησης (NIST, 2010), ένα βασικό στοιχείο της νέας αρχιτεκτονικής του συστήματος είναι η πλατφόρμα υπηρεσιών να μπορεί να είναι ανοικτή στις εφαρμογές που παρέχονται όχι μόνο από τις παραδοσιακές εταιρείες κοινής ωφέλειας αλλά και από τους ανεξάρτητους διαχειριστές συστημάτων (ISS), τους φορείς εκμετάλλευσης περιφερειακών μεταφορών (RTO), τους παρόχους υποδομών και τρίτους (π.χ. υπεύθυνους συλλογής) που μπορούν να διαδραματίσουν ρόλο σε μια ανοικτή αγορά υπηρεσίες προστιθέμενης αξίας.

Σε ένα σενάριο όπου διάφοροι παράγοντες μπορούν να παρέχουν υπηρεσίες με βάση τις πληροφορίες που συλλέγονται από το σύστημα έξυπνων μετρήσεων, είναι πρωταρχικής σημασίας η δημιουργία μιας υποδομής ασφάλειας ικανής να παρέχει πρόσβαση σε μετρητικά δεδομένα με διαφορετικά επίπεδα χωρικής και χρονικής συνάθροισης. Ωστόσο, δεδομένου του μεγάλου αριθμού εμπλεκόμενων φορέων, είναι εύλογο να ορισθεί μια ομάδα ανεξάρτητων τρίτων μερών, δηλαδή αρμόδιων για την συλλογή των στοιχείων και των μετρήσεων, με περιορισμένη γνώση των δεδομένων που πρέπει να συλλεχθούν, διότι αυτά τα στοιχεία αφορούν προσωπικά δεδομένα των καταναλωτών.

Μια προσέγγιση είναι ο έξυπνος μετρητής να κάνει υπολογισμούς και να παράσχει το σύστημα backend με τα αποτελέσματα. Για να αποφευχθεί η εξαπάτηση του μετρητή, χρησιμοποιούνται κρυπτογραφικές δεσμεύσεις και αποδεικτικά μηδενικής γνώσης (Zero Knowledge Proofs) για την επαλήθευση των αποτελεσμάτων. Αυτή η προσέγγιση χρησιμοποιείται αρκετούς ερευνητές (Molina et al, 2010) οι οποίοι προτείνουν λύσεις για τον υπολογισμό του λογαριασμού ενέργειας χωρίς να απελευθερώνονται οι πραγματικές μετρήσεις του κάθε καταναλωτή.

Όλες αυτές οι προτάσεις έχουν το πλεονέκτημα ότι μπορούν εύκολα να αναπτυχθούν με παραμετροποίηση του μετρητή και του βοηθητικού προγράμματος, αλλά έχουν ως στόχο τη χρονική συνάθροιση και δεν εκτελούν χωρική συνάθροιση. Επιπλέον, δεν εξετάζουν την περίπτωση πολλαπλών πληροφοριών καταναλωτών.

Η λύση που προτείνεται από τους Rottondi et al, 2013 είναι αρκετά ενδιαφέρουσα και έχει χαμηλότερη υπολογιστική πολυπλοκότητα αφού απαιτεί μόνο αρθρωτές προσθήκες. Επιπλέον, είναι ισχυρή για την απώλεια μηνυμάτων πρωτοκόλλου. Η λύση των Rottondi et al. παρουσιάζεται στο κεφάλαιο 8.

Μια άλλη προσέγγιση προτείνει την απόκρυψη της ταυτότητας των υποκειμένων χρησιμοποιώντας ψευδώνυμα. Με αυτόν τον τρόπο τα δεδομένα μπορούν να παραδοθούν στο βοηθητικό πρόγραμμα ή σε τρίτο μέρος όπου συγκεντρώνεται. Η χρήση τους στο πλαίσιο του έξυπνου δικτύου συζητείται, μεταξύ άλλων από τους Ευθυμίου και Καλογρίδη (2010) οι οποίοι προτείνουν τη διάσπαση των δεδομένων σε δεδομένα υψηλής συχνότητας και χαμηλής συχνότητας και την ανάθεση ενός ψευδώνυμου στο σύνολο των μετρήσεων υψηλής συχνότητας. Η συσχέτιση μεταξύ των δύο αναγνωριστικών στοιχείων γίνεται με τρόπο που να συσχετίζεται με την εισαγωγή πολύ μεγάλων τυχαίων διαστημάτων κατά τη διάρκεια της εγκατάστασης του συστήματος. Αυτή η λύση έχει το μειονέκτημα ότι απαιτεί μεγάλο χρόνο εγκατάστασης.

Η τρίτη προσέγγιση είναι να χρησιμοποιηθεί ο Υπολογισμός MultiParty (MPC) για να υπολογιστεί η συνάθροιση, γενικά ένα άθροισμα, πάνω στα δεδομένα χωρίς να τίθεται σε

κίνδυνο η ιδιωτικότητα των χρηστών. Με τη σειρά της, η προσέγγιση MPC μπορεί να διανεμηθεί σε όλους τους χρήστες ή να εκμεταλλευτεί έναν ή περισσότερους διακομιστές.

Στα πλαίσια των έξυπνων δικτύων, η κατανεμημένη λύση έχει προσελκύσει αρκετούς ερευνητές, ενώ ο πελάτης-εξυπηρετητής, που είναι και η προσέγγιση που χρησιμοποιείται σε αυτό το έγγραφο, χρησιμοποιείται για την αντιμετώπιση άλλων προβλημάτων σχετικών με την προστασία της ιδιωτικής ζωής όπως η ανώνυμη traction (Ahmad & Khokhar, 2007) και η συνεργατική συσσώρευση (Burkhart et al, 2010).

Οι Li, Luo και Liu (2010) προτείνουν ένα πρωτόκολλο συσσωμάτωσης χρησιμοποιώντας το κρυπτοσύστημα Homomorphic Pallier. Το πρωτόκολλό τους βασίζεται στη μυστική κατανομή του Shamir, η οποία έχει χαμηλότερη υπολογιστική πολυπλοκότητα και επίσης καθιστά δυνατή τη συγκέντρωση των ίδιων δεδομένων σύμφωνα με διάφορους κανόνες με περιορισμένη αύξηση του πρωτοκόλλου. Η πρόταση των Li et al. παρουσιάζεται στο κεφάλαιο 5.

5. ΠΡΩΤΟΚΟΛΛΟ ΤΩΝ LI ET AL. (2010)

Fengjun Li, Bo Luo, Peng Liu, Secure information aggregation for smart grids using homomorphic encryption. In: *Smart Grid Communications (SmartGridComm) 2010*, First IEEE International Conference on, pp. 327 –332, 2010.

Οι Li et al. παρουσίασαν μια προσέγγιση για κατανεμημένη σταδιακή συνάθροιση δεδομένων στην οποία η συνάθροιση πραγματοποιείται σε όλους τους έξυπνους μετρητές που εμπλέκονται στη δρομολόγηση των δεδομένων από τον πηγαίο μετρητή στη μονάδα συλλογής. Δηλαδή η συνάθροιση πραγματοποιείται εντός δικτύου (in-network), με κατανεμημένο τρόπο, αντί για να γίνεται κεντρικά στις συσκευές συλλογής. Μέσω ενός προσεκτικά κατασκευασμένου δένδρου συνάθροισης, η διαδρομή συνάθροισης καλύπτει οποιοδήποτε σύνολο από σχεδιασμένους κόμβους με την ελάχιστη επιβάρυνση.

Για την προστασία του προσωπικού απορρήτου χρησιμοποιείται ομομορφική κρυπτογράφηση (homomorphic encryption), ώστε να προστατευθούν τα δεδομένα στη διαδρομή. Ως εκ τούτου, όλοι οι μετρητές συμμετέχουν στη συνάθροιση χωρίς να βλέπουν κανένα ενδιάμεσο ή τελικό αποτέλεσμα, ενώ διατηρείται αποδοτική και αποτελεσματική η διεργασία συνάθροισης. Η προσέγγιση αυτή καθίσταται κατάλληλη για έξυπνα δίκτυα με επαναλαμβανόμενες ρουτίνες συνάθροισης δεδομένων.

Εφόσον είναι επιθυμητός ο ομομορφισμός με την ιδιότητα της πρόσθεσης, υιοθετείται το Paillier κρυπτοσύστημα στην προσέγγιση των Li *et al*.

Όλοι οι συμμετέχοντες θεωρείται ότι ακολουθούν το μοντέλο αντιπάλου έντιμος-αλλά-περίεργος (honest-but-curious). Δηλαδή όλα τα μέλη θεωρείται ότι ακολουθούν κατάλληλα το πρωτόκολλο (“έντιμοι”). Εν τω μεταξύ κρατάνε όλα τα δεδομένα εισόδου των άλλων μελών και όλα τα ενδιάμεσα υπολογιστικά αποτελέσματα, από τα οποία προσπαθούν να βρουν ή να συμπεράνουν γνώση για τους άλλους (“περίεργοι”). Έτσι, οι έντιμοι-αλλά-περίεργοι αντίπαλοι κρατάνε το σύστημα σε κανονική λειτουργία για να αποφύγουν να αναγνωριστούν, ενώ παράλληλα μεγιστοποιούν την πιθανότητα να αποκτήσουν τα προσωπικά δεδομένα. Οι έντιμοι-αλλά-περίεργοι αντίπαλοι θεωρείται ότι δεν αλλοιώνουν το πρωτόκολλο: δεν βγάζουν εκτός διεργασίας και δεν αλλοιώνουν κακεντρεχώς κάποια αρχική τιμή ή ενδιάμεσο αποτέλεσμα.

Αν και υπάρχουν άλλες προσεγγίσεις για την υποδομή επικοινωνίας στα έξυπνα δίκτυα, η πιο διαδεδομένη είναι η ασύρματη-ενσύρματη πολυεπίπεδη αρχιτεκτονική (wireless-wired multilayer architecture). Σε αυτή την αρχιτεκτονική οι έξυπνοι μετρητές στη γειτονιά επικοινωνούν με μια συσκευή συλλογής δεδομένων μέσω ενός ασύρματου πλεγματοειδούς δικτύου. Η συσκευή συλλογής επικοινωνεί στη συνέχεια με την εγκατάσταση κεντρικής διαχείρισης μέσω ενσύρματης επικοινωνίας.

Παραδοσιακά κάθε έξυπνος μετρητής δημιουργεί μια σύνδεση με το συλλέκτη και τη χρησιμοποιεί αποκλειστικά για να μεταδώσει τα δεδομένα του στο συλλέκτη. Ο συλλέκτης χειρίζεται όλες τις ταυτόχρονες συνδέσεις, υπολογίζει το αποτέλεσμα της συνάθροισης και το μεταδίδει στην κεντρική διαχείριση. Η παραδοσιακή προσέγγιση, αν και απλή και εύκολη να υιοθετηθεί, εισάγει υπερβολική κίνηση δικτύου και δυσβάστακτες απαιτήσεις από τους συλλέκτες.

5.1. Το κρυπτοσύστημα Paillier

Το κρυπτοσύστημα Pailler είναι ένας από τους συνήθως χρησιμοποιούμενους αλγορίθμους για λειτουργείες ομομορφικής κρυπτογράφησης με την ιδιότητα της πρόσθεσης. Το κρυπτοσύστημα Paillier λειτουργεί ως εξής:

Παραγωγή κλειδιών

1. Διάλεξε δύο μεγάλους πρώτους αριθμούς p και q.
2. $N = p \cdot q$ και $\lambda = \text{εκπ}(p-1, q-1)$.
3. Επέλεξε ένα τυχαίο αριθμό g τέτοιο που $g \in \mathbb{Z}^*_{n^2}$.
4. Όρισε μια συνάρτηση $L(u)$ ως $L(u) = (u-1)/N$.
5. Εξασφάλισε ότι το N διαίρει την τάξη του g: έλεγξε αν το $L(g^\lambda \bmod N^2)$ και το n είναι πρώτοι μεταξύ τους, δηλαδή $\text{μκδ}\big(L(g^\lambda \bmod N^2), N\big) = 1$.
6. Το (N, g) είναι το δημόσιο κλειδί.
7. Το (p, q) είναι το ιδιωτικό κλειδί.

Κρυπτογράφηση

1. Θέλουμε να κρυπτογραφήσουμε το μήνυμα $m \in \mathbb{Z}_N$.
2. Επέλεξε ένα τυχαίο αριθμό $r \in \mathbb{Z}^*_N$.
3. Κρυπτογράφησε το m χρησιμοποιώντας τη $c = \mathrm{E}(m) = g^m \cdot r^N \bmod N^2$.

Αποκρυπτογράφηση

1. Θέλουμε να αποκρυπτογραφήσουμε το κρυπτογραφημένο μήνυμα $c \in \mathbb{Z}^*_{N^2}$.
2. Αποκρυπτογράφησε με $m = \mathrm{D}(c) = \left(\frac{L(c^\lambda \bmod N^2)}{L(g^\lambda \bmod N^2)}\right) \bmod N$.

Δεδομένου ότι $c_1 = \mathrm{E}(m_1)$ και $c_2 = \mathrm{E}(m_2)$, για κάθε $m_1, m_2 \in \mathbb{Z}_N$, έχουμε $\mathrm{D}(c_1 \cdot c_2 \bmod N^2) = m_1 + m_2 \bmod N$. Δηλαδή το άθροισμα των αρχικών μηνυμάτων υπολογίζεται από τον πολλαπλασιασμό των κρυπτογραφημένων μηνυμάτων τους. Επίσης, το κρυπτοσύστημα Paillier είναι απροσδιόριστο (indeterministic), δηλαδή το ίδιο αρχικό μήνυμα θα κρυπτογραφηθεί σε διαφορετικά κρυπτογραφημένα μηνύματα χρησιμοποιώντας διαφορετικές τυχαίες παραμέτρους r, θέτοντας έτσι το κρυπτοσύστημα ανθεκτικό σε επιθέσεις λεξικού.

5.2. Επισκόπηση του πρωτοκόλλου

Οι Li et al. προτείνουν μια εντός δικτύου σταδιακή συνάθροιση, όπου αντί να απαιτείται από κάθε μετρητή να δημιουργεί ανεξάρτητη σύνδεση με τον συλλέκτη, ζητείται από μετρητές ίδιας διαδρομής (enroute) να μοιραστούν το κανάλι.

Πρώτο βήμα είναι η κατασκευή ενός εικονικού δένδρου συνάθροισης βασισμένου στην δικτυακή τοπολογία και στο ασύρματο πλέγμα. Σε μια από κάτω προς τα πάνω συνάθροιση, κάθε κόμβος στο δέντρο συγκεντρώνει τα δεδομένα από τα παιδιά του, υπολογίζει και συναθροίζει όλα αυτά τα δεδομένα και τα δικά του και περνάει το αποτέλεσμα στο γονέα του. Ο συλλέκτης, ως κόμβος ρίζα, λαμβάνει τελικά την συνάθροιση από όλο το δέντρο.

5.3. Το δένδρο συνάθροισης

Το δίκτυο έξυπνων μετρητών θεωρείται ως ένας γράφος $G(V, E)$ όπου V είναι το σύνολο των έξυπνων μετρητών (ως κόμβοι) και E είναι το σύνολο των διαθέσιμων ασύρματων συνδέσεων (ως ακμές) μεταξύ δύο οποιονδήποτε μετρητών. Το δένδρο

συνάρτησης είναι ένα γεννητικό δένδρο του γράφου, αποτελούμενο από ένα (ελάχιστο) υποσύνολο των E που συνδέει όλους τους κόμβους στο δένδρο. Κάθε μετρητής θα πρέπει να έχει τουλάχιστον μια διαδρομή επικοινωνίας με τον συλλέκτη. Το δέντρο έχει ρίζα το συλλέκτη, ο οποίος αρχικοποιεί όλες τις εργασίες συνάθροισης και συλλέγει τα τελικά αποτελέσματα. Η συνάθροιση υπολογίζεται αναδρομικά από κάτω προς τα πάνω: κάθε κόμβος παίρνει δεδομένα εισόδου από τον εαυτό του και από τους κόμβους παιδιά του, συναθροίζει τα δεδομένα και στέλνει το αποτέλεσμα στο γονέα κόμβο.

Το ύψος του δένδρου θα πρέπει να είναι μικρό, ώστε να μειωθούν οι μέγιστες προσπελάσεις της μακρύτερης διαδρομής συνάθροισης. Ένας εσωτερικός κόμβος δε θα πρέπει να έχει πολλά παιδιά για να αποφευχθεί η υπολογιστική και επικοινωνιακή φόρτωση στον κόμβο. Ο συλλέκτης μπορεί να επαν-εξισορροπήσει το δένδρο ώστε να βελτιώσει την απόδοσή του.

Η δρομολόγηση δικτύου στο δίκτυο έξυπνων μετρητών είναι σχετικά στατική. Στις περισσότερες περιπτώσεις η συσκευή συλλογής έχει το γράφο του δικτύου για όλη τη γειτονιά. Επομένως το δένδρο συνάθροισης κατασκευάζεται τοπικά στο συλλέκτη, χωρίς να εξεταστούν όλοι οι έξυπνοι μετρητές. Επιπλέον ένας γράφος συνάθροισης παραμένει σταθερός για μεγάλο χρονικό διάστημα.

5.4. Δικτυακή συνάθροιση με ομομορφική κρυπτογράφηση (in-network aggregation using homomorphic encryption)

Με το δένδρο συνάθροισης κατασκευάζονται σχέδια λειτουργίας για τους συμμετέχοντες κόμβους και διανέμονται στους έξυπνους μετρητές από πάνω προς τα κάτω. Το σχέδιο λειτουργίας ενός έξυπνου μετρητή είναι η 7-πλάδα: $\{T_{ID}, Trigger, Data, Collect, Operation, Destination, Key\}$. T_{ID} είναι ένα μοναδικό αναγνωριστικό που χρησιμοποιείται για να αναγνωριστούν μηνύματα. Η $Trigger$ ορίζει το πότε η συνάθροιση θα διεξαχθεί: περιοδικά σε κάποια συχνότητα, κατόπιν αιτήσεως του παρόχου ή σε μια συγκεκριμένη χρονική στιγμή. Σημειώνεται ότι η $Trigger$ ορίζει το χρόνο της ανάγνωσης των τοπικών δεδομένων, όχι το χρόνο της συνάθροισης. Έτσι εξασφαλίζεται ότι καμία απώλεια συγχρονισμού δε θα προκληθεί εξαιτίας λανθάνοντος χρόνου στον υπολογισμό ή τη δικτυακή επικοινωνία. Η $Data$ ορίζει ποια πληροφορία θα συλλεχθεί στη συνάθροιση από το τοπικό έξυπνο δίκτυο πχ η τρέχουσα χρήση ενέργειας. Η $Collect$ λέει στο μετρητή να περιμένει τα δεδομένα εισόδου από ένα σύνολο κόμβων, δηλαδή τα παιδιά του στο δένδρο συνάθροισης. Η $Operation$ λέει σε ένα μετρητή ποια λειτουργία να εκτελέσει, συμπεριλαμβανομένης της προεπεξεργασίας, της κρυπτογράφησης και της λειτουργίας συνάθροισης. $Destination$ είναι ο κόμβος γονιός, δηλαδή εκείνος στον οποίον το δεδομένο εξόδου της $Operation$ θα υποβληθεί. Key είναι το σύνολο των κλειδιών που θα χρησιμοποιηθούν για την κρυπτογράφηση. Στο Paillier κρυπτοσύστημα Key είναι ένα δημόσιο κλειδί από τον συλλέκτη που θα χρησιμοποιηθεί για την κρυπτογράφηση των τοπικών δεδομένων.

Η ομομορφική κρυπτογράφηση χρησιμοποιείται σε κάθε συμμετέχοντα έξυπνο μετρητή. Ο συλλέκτης μεταφράζει μια πράξη στο αρχικό μήνυμα σε κάποια πράξη στο κρυπτογραφημένο μήνυμα. Για παράδειγμα, οι αθροίσεις στο πηγαίο κείμενο μετατρέπονται σε πολλαπλασιασμούς στο Paillier κρυπτοσύστημα.

Ο κάθε έξυπνος μετρητής λαμβάνει το πλάνο λειτουργίας του και ακολουθεί το παρακάτω πρωτόκολλο:

1. Ο μετρητής προσδιορίζει αν θα πρέπει να ξεκινήσει τη συνάθροιση ή να περιμένει την ενεργοποίηση (trigger).
2. Όταν θα πρέπει να εκτελεστεί η συνάθροιση, ο έξυπνος μετρητής ανακτά τα τοπικά δεδομένα όπως ορίζονται στο πεδίο $Data$ του πλάνου και τα κρυπτογραφεί με το Key ως τοπικά δεδομένα εισόδου.
3. Τότε ο μετρητής περιμένει τα δεδομένα εισόδου από τους κόμβους παιδιά, όπως αυτά ορίζονται στο $Collect$. Μόλις λάβει όλα τα δεδομένα εισόδου ακολουθεί την $Operation$ για να εκτελέσει τη συνάθροιση επί όλων των κρυπτογραφημένων μηνυμάτων εισόδου.
4. Τελικά ο έξυπνος μετρητής στέλνει το δεδομένο εξόδου από το προηγούμενο βήμα στον κόμβο $Destination$, δηλαδή στον κόμβο γονέα του στο δένδρο συνάθροισης. Το μήνυμα εξόδου δομείται ως $\{T_{ID}, TS, Data\}$ όπου TS είναι η χρονοσφραγίδα των τοπικών δεδομένων. Η χρονοσφραγίδα χρησιμοποιείται για το συγχρονισμό διαφορετικών συμβάντων επαναλαμβανόμενων εργασιών.

Ο συλλέκτης λαμβάνει τα κρυπτογραφημένα δεδομένα εισόδου από τους κόμβους παιδιά του. Υπολογίζει το γινόμενο των κρυπτογραφημάτων. Τελικά ο συλλέκτης αποκρυπτογραφεί το γινόμενο για να βρει το αθροιστικό αποτέλεσμα.

5.5. Ανάλυση

Παρακάτω παρουσιάζεται η σύγκριση της πολυπλοκότητας της προσέγγισης των Li *et al*. Σε σχέση με την παραδοσιακή προσέγγιση συνάθροισης στην οποία συλλέγονται τα δεδομένα από κάθε μετρητή και η συνάθροιση εκτελείται στη συσκευή συλλογής.

Δίκτυο: Στην παραδοσιακή προσέγγιση τα μηνύματα από όλους τους έξυπνους μετρητές δρομολογούνται στη συσκευή συλλογής ταυτόχρονα. Ο μέσος όρος $\bar{h}$ των προσπελάσεων (hops) για τη μετάδοση του κάθε μηνύματος στο συλλέκτη καθορίζεται από το μέγεθος της γειτονιάς που καλύπτει ο συλλέκτης, το εύρος ασύρματης επικοινωνίας κάθε έξυπνου μετρητή και το σχέδιο δρομολόγησης. Έστω N το πλήθος των κόμβων του γραφήματος. Προκειμένου να μεταδοθούν τα δεδομένα από όλους τους συμμετέχοντες μετρητές, ο συνολικός φόρτος στο δίκτυο θα είναι $\bar{h} * N$ προσπελάσεις. Ωστόσο, στην προτεινόμενη προσέγγιση, ο συνολικός φόρτος θα είναι N προσπελάσεις. Δεδομένου ότι στην πράξη η συσκευή συγκέντρωσης καλύπτει μια μεγάλη γειτονιά, δηλαδή ένα μεγάλο $\bar{h}$, η διαφορά στο φόρτο του δικτύου είναι σημαντική.

Επεκτασιμότητα: Η επεκτασιμότητα του συστήματος εξαρτάται σε μεγάλο βαθμό από την τοπολογία του δικτύου έξυπνων μετρητών. Σε ένα καλοσχεδιασμένο δίκτυο, το δένδρο συνάθροισης είναι συνήθως πλατύ και αβαθές, κάτι που κάνει την προτεινόμενη προσέγγιση ιδιαιτέρως επεκτάσιμη.

Συμφόρηση: Δεδομένου ότι οι περισσότεροι υπολογισμοί κατανέμονται στους έξυπνους μετρητές, με μοντέλο που επαν-εξισορροπείται, δεν υπάρχει σχεδόν καμία μη αναπόφευκτη συμφόρηση στην προτεινόμενη προσέγγιση. Αντιθέτως, οι περισσότεροι υπολογισμοί στην παραδοσιακή προσέγγιση είναι συγκεντρωμένοι στη συσκευή συλλογής. Ο συλλέκτης αναλαμβάνει την κύρια συμφόρηση, ειδικά όταν το πλήθος N των μετρητών είναι μεγάλο.

Ευρωστία: Στην προτεινόμενη συνάθροιση εντός δικτύου, όταν ένας έξυπνος μετρητής αποτύχει, ανιχνεύεται άμεσα από το γονέα του στο δένδρο συνάθροισης και αναφέρεται στο συλλέκτη. Ο συλλέκτης ενημερώνει το δένδρο συνάθροισης και επανεκδίδει το ερώτημα. Η διαδικασία ανάκτησης θα αποτύχει μόνο όταν ο γράφος γίνει μη συνεκτικός, κάτι που συνήθως προκαλείται από την αποτυχία μεγάλου αριθμού κόμβων. Σε τέτοιες περιπτώσεις οι περισσότερες προσεγγίσεις θα αποτύγχαναν.

Ανάλυση ασφάλειας και ιδιωτικότητας: Το κρυπτοσύστημα Paillier είναι σημασιολογικά ασφαλές (IND-CPA, Indistinguishability under chosen-plaintext attack): αντίπαλος πολυωνυμικού χρόνου δεν μπορεί να αντλήσει σημαντικές πληροφορίες για το αρχικό μήνυμα μέσω του κρυπτογραφημένου μηνύματος και του δημοσίου κλειδιού. Εν τω μεταξύ, δεδομένου ότι το κρυπτοσύστημα Paillier περιλαμβάνει μια τυχαία παράμετρο r, τα ίδια δεδομένα κρυπτογραφούνται σε διαφορετικά κρυπτογραφημένα μηνύματα με διαφορετική r, κάτι που καθιστά την προσέγγιση ανθεκτική σε επιθέσεις λεξικού.

Όλα τα συστήματα ομομορφικής κρυπτογράφησης είναι ευάλωτα απέναντι σε κακόβουλα λογισμικά. Έχοντας το κρυπτογραφημένο μήνυμα και το δημόσιο κλειδί, ένας αντίπαλος μπορεί να παράγει ένα άλλο κρυπτογραφημένο μήνυμα το οποίο αποκρυπτογραφείται σε ένα άλλο αρχικό μήνυμα με νόημα στο ίδιο πεδίο ορισμού με το πρωτότυπο αρχικό μήνυμα. Κατά συνέπεια, ένας ανέντιμος ή ψεύτικος έξυπνος μετρητής μπορεί να νοθεύσει τα δεδομένα και να προκαλέσει ανακρίβεια στο αποτέλεσμα της συνάθροισης. Κάτι τέτοιο θα μπορούσε να συμβεί σε οποιαδήποτε προσέγγιση και δεν είναι πρόβλημα που εισάγεται από την προτεινόμενη προσέγγιση. Η ανίχνευση χειραγώγησης της συνάθροισης από αντιπάλους δεν καλύπτεται από το παρόν πρωτόκολλο και μπορεί να αφορά αντικείμενο μελλοντικής εργασίας.

Υπολογισμοί: Η ασύμμετρη κρυπτογράφηση είναι περισσότερο υπολογιστικά δαπανηρή από τη συμμετρική κρυπτογράφηση. Στην παραδοσιακή προσέγγιση κάθε έξυπνος μετρητής κρυπτογραφεί το μήνυμά του άπαξ με το δημόσιο κλειδί, ενώ ο συλλέκτης χρειάζεται να αποκρυπτογραφήσει N μηνύματα. Στην προτεινόμενη προσέγγιση κάθε μετρητής χρειάζεται να κρυπτογραφήσει το μήνυμα μία φορά με ομομορφική (ασύμμετρη ακόμη) κρυπτογράφηση, αλλά ο συλλέκτης χρειάζεται να κάνει μόνο μια ασύμμετρη αποκρυπτογράφηση, στο τελικό συναθροιστικό αποτέλεσμα. Επιπλέον, η εντός δικτύου προσέγγιση συνάθροισης κατανέμει τον υπολογισμό της συνάθροισης από το συλλέκτη στους ενδιάμεσους έξυπνους μετρητές και εισάγει επιπλέον επιβάρυνση (τον πολλαπλασιασμό στο κρυπτογραφημένο μήνυμα). Ωστόσο η επιβάρυνση θεωρείται μικρή και αποδεκτή ανά έξυπνο μετρητή.

6. ΠΡΩΤΟΚΟΛΛΟ ΤΩΝ SHI ET AL. (2011)

Elaine Shi, T.-H. Hubert Chan, Eleanor G. Rieffel, Richard Chow, and Dawn Song. Privacy-preserving aggregation of time-series data. In *Network and Distributed System Security Symposium (NDSS 2011)*. The Internet Society, 2011.

Η εργασία των Shi *et al*. πραγματεύεται τον υπολογισμό απλών στατιστικών αποτελεσμάτων –εν προκειμένω του αθροίσματος– από τα περιοδικά δεδομένα πολλαπλών συμμετεχόντων σε έναν μη αξιέμπιστο συγκεντρωτή δεδομένων, χωρίς να θίγεται το απόρρητο των συμμετεχόντων. Συνοπτικά ορίζονται τα εξής:

- Ο συγκεντρωτής και οι συμμετέχοντες θεωρούνται μη αξιέμπιστοι.
- Οι συμμετέχοντες δεν ανταλλάσσουν δεδομένα μεταξύ τους.
- Οι συμμετέχοντες αποστέλλουν στο συγκεντρωτή τα δεδομένα τους κρυπτογραφημένα και με θόρυβο.
- Ο συγκεντρωτής μπορεί και βρίσκει το σύνολο των δεδομένων σε κάθε χρονική περίοδο και τίποτε άλλο.
- Το υπολογιζόμενο σύνολο περιλαμβάνει το θόρυβο που έχουν προσθέσει οι συμμετέχοντες.

Το απόρρητο διασφαλίζεται με δύο βασικές τεχνικές:

- Ο συγκεντρωτής αποκρυπτογραφεί το σύνολο πολλαπλών κρυπτογραφημένων μηνυμάτων (ciphertexts) κωδικοποιημένων υπό διαφορετικά κλειδιά χρηστών.
- Η διαδικασία τυχαιοποίησης κατανεμημένων δεδομένων (distributed data randomization procedure) εξασφαλίζει το απόρρητο (distributed differential privacy) των εξαγόμενων στατιστικών, ακόμα και εάν ένα υποσύνολο των συμμετεχόντων τεθεί σε κίνδυνο.

6.1. Επισκόπηση του πρωτοκόλλου

Έστω ένας συγκεντρωτής δεδομένων και n συμμετέχοντες. Ο συγκεντρωτής αριθμείται με το 0 και οι συμμετέχοντες με $1, 2, \dots, n$. Έστω $[n] := \{1, 2, \dots, n\}$. Σε κάθε χρονική περίοδο $t \in \mathbb{N}$ κάθε συμμετέχοντας $i \in [\mathrm{n}]$ έχει δεδομένα $x_{i,t} \in \mathrm{D}$ από ένα πεδίο ορισμού D. Τίθεται $\mathrm{x} = (x_1, \dots, x_n) \in \mathrm{D}^{\mathrm{n}}$ το διάνυσμα των δεδομένων όλων των συμμετεχόντων σε κάποια χρονική περίοδο. Ο συγκεντρωτής θέλει να υπολογίσει κάποια συγκεντρωτικά στατιστικά που αναπαρίστανται από τη συνάρτηση $f : D^n \to O$. Η συνάρτηση $f(\mathrm{x})$ παράγει αποτέλεσμα από κάποιο πεδίο τιμών O, που αντιπροσωπεύει τα επιθυμητά στατιστικά.

Προκειμένου να εξασφαλιστεί το απόρρητο των δεδομένων των συμμετεχόντων, κάθε συμμετέχοντας δημιουργεί ανεξάρτητα τυχαίο θόρυβο από κάποιο χώρο Ω, που αναπαρίσταται από $\mathrm{r} := (\mathrm{r}_1, \dots, \mathrm{r}_\mathrm{n}) \in \Omega^{\mathrm{n}}$. Έστω ότι η $\chi : D \times \Omega \to D$ ορίζει κάποια συνάρτηση τυχαιοποίησης (randomization) που επιτρέπει σε κάθε συμμετέχοντα να υπολογίζει μια έκδοση των δεδομένων του με θόρυβο $\widehat{x_i} := \chi(x_i, r_i)$ πριν την κρυπτογράφηση και τη μεταφορά στο συγκεντρωτή. Από τα κρυπτογραφημένα δεδομένα $\hat{\mathrm{x}} := (\widehat{x_1}, \widehat{x_2}, \dots, \widehat{x_n})$, ο συγκεντρωτής υπολογίζει ένα στατιστικό με θόρυβο $f(\hat{\mathrm{x}})$, που πρέπει να είναι κοντά στο επιθυμητό στατιστικό $f(\mathrm{x})$.

Στόχος είναι ο σχεδιασμός ενός μηχανισμού απορρήτου τέτοιου ώστε σε κάθε χρονική περίοδο ο συγκεντρωτής να μπορεί να μάθει κάποια συγκεντρωτικά στατιστικά $f(\hat{\mathrm{x}})$, αλλά όχι τα δεδομένα κάθε συμμετέχοντα, ακόμα και αν έχει αυθαίρετες βοηθητικές πληροφορίες. Ένα μοντέλο που καλύπτει αυτές τις απαιτήσεις καλείται ως Private Stream Aggregation (PSA) mechanism και αποτελείται από τους ακόλουθους αλγόριθμους.

$Setup\ (1^{\lambda})$: λαμβάνει μια παράμετρο ασφαλείας λ και εξάγει τις δημόσιες παραμέτρους param, ένα ιδιωτικό κλειδί sk_i για κάθε συμμετέχοντα, καθώς και μια ικανότητα συγκεντρωτή sk_0 για την αποκρυπτογράφηση των συγκεντρωτικών στατιστικών κάθε χρονική περίοδο. Κάθε συμμετέχοντας i λαμβάνει το ιδιωτικό κλειδί του sk_i και ο συγκεντρωτής λαμβάνει την ικανότητα sk_0.

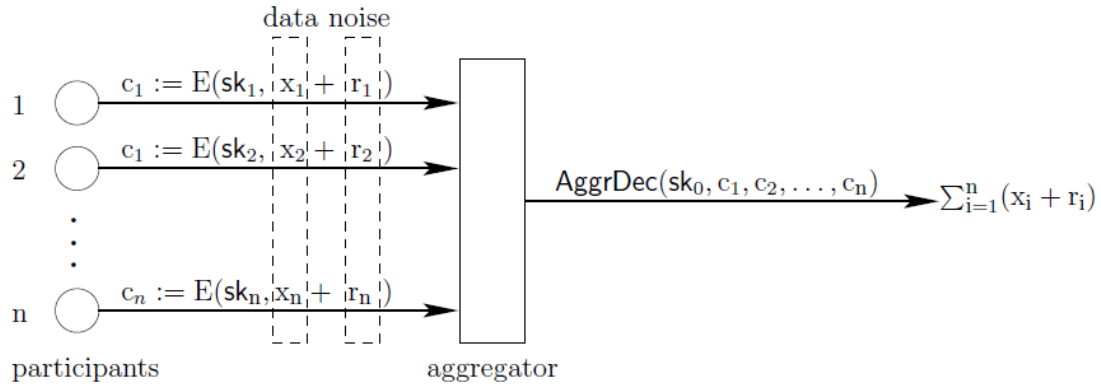
$NoisyEnc(param, sk_i, t, x, r)$: Κατά το χρονικό βήμα t, κάθε συμμετέχοντας καλεί τον αλγόριθμο $NoisyEnc$ για να κωδικοποιήσει τα δεδομένα του x με θόρυβο r. Το αποτέλεσμα είναι μια κρυπτογράφηση των δεδομένων x τυχαιοποιημένα με θόρυβο r. Σαφώς μπορεί να γραφτεί $NoisyEnc(param, sk_i, t, \hat{x})$, όπου $\hat{x} := \chi(x, r)$ η εκδοχή με θόρυβο των δεδομένων του χρήστη και χ κάποια υποβόσκουσα συνάρτηση τυχαιοποίησης.

$AggrDec(param, sk_0, t, c_1, c_2, \dots, c_n)$: Ο αλγόριθμος αποκρυπτογράφησης λαμβάνει τις δημόσιες παραμέτρους $param$, την ικανότητα sk_0 και τα κρυπτογραφημένα μηνύματα (ciphertexts) $c_1, c_2, \dots, c_n$ για την ίδια χρονική περίοδο t. Για κάθε $i \in [\mathrm{n}]$ τίθεται $c_i = NoisyEnc(sk_i, t, \widehat{x_i})$, όπου $\widehat{x_i} := \chi(x_i, r_i)$. Τίθεται $\mathrm{x} = (x_1, \dots, x_n)$ και $\hat{\mathrm{x}} := (\widehat{x_1}, \dots, \widehat{x_n})$. Ο αλγόριθμος αποκρυπτογράφησης εξάγει $f(\hat{\mathrm{x}})$ που είναι μια εκδοχή με θόρυβο των στοχοθετημένων στατιστικών $f(\mathrm{x})$.

Η περίπτωση της άθροισης

Οι Shi *et al*. εξετάζουν κυρίως την περίπτωση της άθροισης. Κάθε συμμετέχοντα τα δεδομένα x_i ανήκουν στο $\mathbb{Z}_p$ για κάποιον πρώτο p. Ορίζεται η αθροιστική συνάρτηση $sum(\mathrm{x}) := \sum_{i=1}^{n} x_i$. Επιπλέον, κάθε συμμετέχοντας παράγει θόρυβο r_i από τη σειρά των ακεραίων και εφαρμόζει την συνάρτηση τυχαιοποίησης $\chi(x_i, r_i) := x_i + r_i \ mod\ p$ δηλαδή ο συμμετέχοντας προσθέτει θόρυβο πριν την κρυπτογράφηση των δεδομένων του.

Η επόμενη εικόνα παρουσιάζει μια υψηλού επιπέδου επισκόπηση του μοντέλου.



Σχήμα 12: Επισκόπηση του μοντέλου των Shi et al.

6.2. Τυπικές έννοιες απορρήτου

Λαμβάνεται υπόψη ένας μη-αξιέμπιστος συγκεντρωτής που μπορεί να έχει αυθαίρετες βοηθητικές πληροφορίες. Για παράδειγμα, ο συγκεντρωτής μπορεί να συνωμοτήσει με κάποιους συμμετέχοντες οι οποίοι να του αποκαλύψουν τα δεδομένα τους και το θόρυβό τους, που μπορούμε τα θεωρήσουμε βοηθητικές πληροφορίες. Βοηθητικές πληροφορίες μπορούν να αντληθούν και με άλλους τρόπους, πχ από προσωπική γνώση συγκεκριμένων συμμετεχόντων.

Ο στόχος είναι να διασφαλιστεί το απόρρητο κάθε των προσωπικών δεδομένων απέναντι στον μη-αξιέμπιστο συγκεντρωτή, ακόμα και όταν ο συγκεντρωτής έχει αυθαίρετες βοηθητικές πληροφορίες. Σε υψηλό επίπεδο, η τυπική έννοια απορρήτου αποτελείται από δύο ιδιότητες:

Λήθη του συγκεντρωτή (aggregator oblivious). Έστω ότι ο συγκεντρωτής έχει βοηθητικές πληροφορίες aux. Με την κατάλληλη ικανότητα, ο συγκεντρωτής μαθαίνει τα συγκεντρωτικά στατιστικά με θόρυβο $f(\hat{x})$ στο τέλος της χρονικής περιόδου. Πρέπει να διασφαλιστεί ότι ο συγκεντρωτής μαθαίνει τίποτα άλλο από ότι μπορεί να συμπεράνει από τις aux και τα $f(\hat{x})$. Επιπλέον είναι απαιτούμενο ένα μέλος χωρίς την κατάλληλη ικανότητα συγκεντρωτή να μην μπορεί να μάθει οτιδήποτε.

Κατανεμημένο διαφορικό απόρρητο (Distributed differential privacy ή DD-Privacy). Είναι απαιτούμενο η συμμετοχή του χρήστη στο σύστημα να διαρρέει μόνο αμελητέες πληροφορίες για τον ίδιο. Με άλλα λόγια, το συγκεντρωτικό στατιστικό $f(\hat{x})$ που προκύπτει να είναι χονδρικά το ίδιο είτε ένας συγκεκριμένος χρήστης συμμετέχει στο σύστημα είτε όχι. Για να επιτευχθεί αυτός ο στόχος, στο πρωτόκολλο οι συμμετέχοντες δεν εμπιστεύονται τα δεδομένα τους στο συγκεντρωτή ή σε άλλους συμμετέχοντες αλλά προσθέτουν ο κάθε ένας θόρυβο στα δεδομένα τους και ο θόρυβος στο τελικό αποτέλεσμα συγκεντρώνεται από αυτούς.

Αν και κακόβουλοι συμμετέχοντες μπορούν να μολύνουν με τα δεδομένα τους το σύστημα προκειμένου να επηρεάσουν το τελικό αποτέλεσμα, η επιρροή μπορεί να οριοθετηθεί περιορίζοντας τα δεδομένα που μπορεί να εξάγει κάθε συμμετέχοντας εντός έγκυρου εύρους.

Οι Shi *et al*. προσδιόρισαν και απέδειξαν την λήθη του συγκεντρωτή για την περίπτωση (μόνο) του αθροίσματος, εκτελώντας ένα παιχνίδι ασφαλείας με όλες τις παραπάνω προϋποθέσεις. Επίσης απέδειξαν την επίτευξη διαφορικού απορρήτου καθώς η δομή τους είναι ασφαλής εναντίον αντιπάλων πολυωνυμικού χρόνου. Αναφέρονται στην (ε, δ)-DD-Privacy, όπου $\varepsilon > 0$ και $0 \leq \delta < 1$.

6.3. Επίτευξη ασφάλειας λήθης συγκεντρωτή (Aggregator oblivious security)

Στην παρούσα λύση, μετά την έμπιστη φάση ρύθμισης μεταξύ όλων των συμμετεχόντων και στου συγκεντρωτή, καμία άλλη αλληλεπίδραση δεν απαιτείται εκτός από την μεταφορά των κρυπτογραφημάτων με θόρυβο στο συγκεντρωτή σε κάθε χρονική περίοδο.

Η έμπιστη ρύθμιση μπορεί να εκτελεστεί από ένα έμπιστο τρίτο μέρος ή μέσω ενός καθιερωμένου ασφαλούς πρωτοκόλλου πολλών μερών (Secure Multi-Party protocol).

Βασική δομή

Έστω ότι το $\mathbb{G}$ δηλώνει ένα κυκλικό σύνολο πρώτου πληθικού αριθμού (prime order cyclic group) p για το οποίο η Decisional Diffie–Hellman assumption (DDH assumption) είναι ισχυρή. Έστω ότι η $H : \mathbb{Z} \to \mathbb{G}$ δηλώνει μια συνάρτηση κατακερματισμού (hash function) μοντελοποιημένη ως random oracle. Οι Shi *et al*. απέδειξαν ότι η παρακάτω δομή ικανοποιεί τη συνθήκη λήθης του συγκεντρωτή στο μοντέλο της εφάπαξ κρυπτογράφησης ("encrypt-once").

$Setup\left(1^{\lambda}\right)$: ένας αξιέμπιστος διαμοιραστής (dealer) επιλέγει μια τυχαία γεννήτρια $g \in \mathbb{G}$ και $n+1$ τυχαία μυστικά $s_0, s_1, \ldots, s_n \in \mathbb{Z}_p$ τέτοια που $s_0 + s_1 + s_2 + \cdots + s_n = 0$. Επίσης $param := g$ η δημόσια παράμετρος. Ο συγκεντρωτής λαμβάνει την ικανότητα $sk_0 := s_0$ και ο συμμετέχοντας i λαμβάνει το ιδιωτικό κλειδί $sk_i := s_i$.

$NoisyEnc(param, sk_i, t, \hat{x})$: Ο συμμετέχοντας i για να κρυπτογραφήσει μια τιμή $\hat{x} \in \mathbb{Z}_p$ για το χρονικό βήμα t υπολογίζει το ακόλουθο κρυπτογραφημένο μήνυμα (ciphertext):

$$c \leftarrow g^{\hat{x}} \cdot H(t)^{sk_i}$$

Εφόσον θεωρούμε ότι κάθε συμμετέχοντας προσθέτει θόρυβο στα δεδομένα του πριν την κρυπτογράφηση, χρησιμοποιούμε τον όρο $\hat{x} := x + r \bmod p$ για να δηλώσουμε ένα τυχαιοποιημένο αρχικό μήνυμα.

$AggrDec(param, sk_0, t, c_1, c_2, \ldots, c_n)$: Υπολογίζεται

$$V \leftarrow H(t)^{sk_0} \prod_{i=1}^{n} c_i \,.$$

Έστω $c_i = NoisyEnc(param, sk_i, t, \hat{x}_i)$ για $i \in [\mathrm{n}]$. Δεν είναι δύσκολο να δούμε ότι η V είναι της μορφής

$$V = g \sum_{i=1}^{n} \hat{x}_i \,.$$

Για να αποκρυπτογραφηθεί το σύνολο αρκεί να υπολογιστεί ο διακριτός λογάριθμος (discrete log) του V με βάση g. Όταν το μέγεθος του αρχικού μηνύματος είναι μικρό, η αποκρυπτογράφηση μπορεί να επιτευχθεί μέσω μιας brute-force αναζήτησης. Μια καλύτερη προσέγγιση είναι η χρήση της Pollard's λάμδα μεθόδου η οποία απαιτεί χρόνο αποκρυπτογράφησης χονδρικά την τετραγωνική ρίζα του μεγέθους του αρχικού μηνύματος πχ $\sqrt{n\Delta}$ όπου n ο αριθμός των συμμετεχόντων και υποθέτοντας ότι η τιμή εισόδου κάθε συμμετέχοντα είναι εντός του πεδίου τιμών $\{0, 1, \ldots, \Delta\}$.

Απόδοση της δομής

Στην παραπάνω κρυπτογραφική δομή, η κρυπτογράφηση αποτελείται από μια λειτουργία κατακερματισμού, δύο πράξεις εκθετοποίησης υπολοίπων (modular exponentiations) και έναν πολλαπλασιασμό σε ένα Diffie-Hellman σύνολο. Ο χρόνος εκτέλεσης κυριαρχείται από τις modular exponentiations καθώς ο χρόνος υπολογισμού τους είναι πολύ μεγαλύτερος των υπολοίπων. Οι Shi *et al*. υπολογίζουν χονδρικά τον χρόνο κρυπτογράφησης σε 0.6ms. Η αποκρυπτογράφηση περιλαμβάνει ένα διακριτό λογάριθμο, όπου, αν χρησιμοποιηθεί η brute-force μέθοδος, περιλαμβάνει μία modular exponentiation, δηλαδή χρειάζεται 0.3ms για να δοκιμάσει κάθε πιθανό μήνυμα. Κατά συνέπεια το μοντέλο είναι πρακτικό σε καταστάσεις όπου το αρχικό μήνυμα είναι μικρό.

6.4. Επίτευξη κατανεμημένου διαφορικού απορρήτου (distributed differential privacy – DD-privacy)

Το πρωτόκολλο παρέχει μια εγγύηση διαφορικού απορρήτου των δεδομένων κάθε συμμετέχοντα στην κρυπτογραφική δομή. Οι συμμετέχοντες είναι υπεύθυνοι για την διασφάλιση του διαφορικού απορρήτου των δεδομένων τους. Κάθε συμμετέχοντας προσθέτει θόρυβο στα δεδομένα του πριν την κρυπτογράφηση. Υπάρχουν δύο προκλήσεις στον μηχανισμό διαφορικού απορρήτου:

Διακυβευμένοι συμμετέχοντες. Ένα υποσύνολο των συμμετεχόντων μπορεί να έχει διακυβευτεί και να συνωμοτήσει με το συγκεντρωτή δεδομένων. Εάν ένα κλάσμα γ των συμμετεχόντων είναι έμπιστο και μη διακυβευμένο, τότε μπορεί να κατανεμηθεί η εργασία παραγωγής θορύβου μεταξύ αυτών των συμμετεχόντων. Το παρόν μοντέλο θεωρεί ότι οι συμμετέχοντες έχουν εκ των προτέρων μια εκτίμηση του χαμηλότερου ορίου των έμπιστων, μη-διακυβευμένων συμμετεχόντων. Κάθε συμμετέχοντας δημιουργεί θόρυβο από μια κατανομή που εξαρτάται από το γ. Η δομή εγγυάται ότι, με μεγάλη πιθανότητα, το στατιστικό αποτέλεσμα που θα προκύψει θα συσσωρεύσει επαρκή θόρυβο από τους έμπιστους συμμετέχοντες, κρατώντας χαμηλό το σφάλμα του τελικού στατιστικού.

Αλγεβρικοί περιορισμοί. Τα περισσότερα κρυπτογραφικά συστήματα απαιτούν το αρχικό μήνυμα να έχει ληφθεί από ένα σύνολο αποτελούμενο από διακριτά στοιχεία. Κατά συνέπεια θα πρέπει τα δεδομένα και ο θόρυβος να κωδικοποιηθούν σε διακριτό σύνολο. Επιλέχθηκε λοιπόν η χρήση συμμετρικής γεωμετρικής κατανομής, διασφαλίζοντας παράλληλα ότι ο συγκεντρωτής θα μπορεί με μεγάλη πιθανότητα να αποκρυπτογραφήσει επιτυχώς τα στατιστικά με θόρυβο.

DD-privacy στην άθροιση

Έστω $\mathrm{x} = (x_1, \dots, x_n) \in D^n$ και $\mathrm{r} = (r_1, \dots, r_n) \in \Omega^n$ οι τιμές των δεδομένων και του θορύβου αντίστοιχα από όλους τους συμμετέχοντες μια συγκεκριμένη χρονική περίοδο. Έχουμε εδώ $D = O = \mathbb{Z}_p$ το κυκλικό σύνολο εφοδιασμένο με προσθήκη modulo p και $\Omega = \mathbb{Z}$. Θεωρούμε την αθροιστική συνάρτηση $\mathrm{sum} : D^n \to O$, όπου $\mathrm{sum}(\mathrm{x}) = \sum_{i=1}^{n} x_i \bmod p$. Κάθε συμμετέχοντας χρησιμοποιεί την ίδια συνάρτηση τυχαιοποίησης $\chi(x_i, r_i) \coloneqq x_i + r_i \bmod p$.

Το πρωτόκολλο διασφαλίζει ότι εάν τουλάχιστον γn συμμετέχοντες είναι έμπιστοι και μη διακυβευμένοι, θα συσσωρευτεί θόρυβος όμοιου μεγέθους. Έτσι δεν διασφαλίζεται μόνο το διαφορικό απόρρητο αλλά εξασφαλίζεται και ότι ο συσσωρευμένος θόρυβος είναι οριοθετημένος στο τελικό αποτέλεσμα ώστε το σφάλμα να είναι μικρό. Μάλιστα το σφάλμα θα

είναι το ελάχιστο που απαιτείται για να επιτευχθεί το ε-differential privacy Επιπλέον, το σφάλμα είναι ανεξάρτητο από το πλήθος n των χρηστών, κάτι που επιβεβαιώθηκε και εμπειρικά μέσω προσομοίωσης. Στην πραγματικότητα το αποτέλεσμα είναι σχεδόν το βέλτιστο. Ο παρακάτω αλγόριθμος περιγράφει μια διαδικασία που εγγυάται το DD-privacy με μικρό σφάλμα.

Algorithm 1: DD-Private Data Randomization Procedure

Let $\alpha \coloneqq \exp\left(\frac{\varepsilon}{\Delta}\right)$ and $\beta \coloneqq \frac{1}{\gamma n}\log\frac{1}{\delta}$.

Let $\mathrm{x} = (x_1, \ldots, x_n)$ denote all participants' data in a certain time period.

foreach participant $i \in [n]$ **do**

Sample noise r_i according to the following distribution.

$$r_i \leftarrow \begin{cases} \mathrm{Geom}(\alpha) & \text{with probability } \beta \\ 0 & \text{with probability } 1-\beta \end{cases}$$

Randomize data by computing $\hat{x}_i \leftarrow x_i + r_i \bmod p$.

6.5. Επεκτάσεις και ανοικτές ερευνητικές προκλήσεις

Δυνατότητες επέκτασης του πρωτοκόλλου

- Το μοντέλο μπορεί να επεκταθεί ώστε να εκτιμάται περιοδικά η κατανομή δεδομένων.
- Με μια μικρή παραλλαγή το άθροισμα μπορεί να γίνει δημόσιο.
- Μπορεί να δημιουργηθεί δομή με πολλαπλού επιπέδου ιεράρχηση που να εμφωλεύει το πρωτόκολλο στους κόμβους της.
- Η βασική δομή μπορεί εύκολα να τροποποιηθεί για τον υπολογισμό του γινομένου αντί του αθροίσματος. Μάλιστα σε αυτή την περίπτωση δεν θα υπάρχει πια περιορισμός στο μέγεθος του αρχικού μηνύματος.

Περιορισμοί του πρωτοκόλλου

- Το μοντέλο είναι πρακτικό για μικρού μεγέθους αρχικά μηνύματα.
- Το μοντέλο αφορά σε απλές στατιστικές συναρτήσεις όπως το άθροισμα, επεκτείνεται και σε άλλες δυνατότητες αλλά δεν υποστηρίζει πιο περίπλοκες συναρτήσεις.
- Δεν υποστηρίζεται η δυναμική είσοδος / έξοδος συμμετεχόντων. Η αλλαγή των συμμετεχόντων απαιτεί νέα αρχικοποίηση.
- Ο συγκεντρωτής δεν μπορεί να εξάγει αποτελέσματα εάν δεν λάβει στοιχεία από όλους τους συμμετέχοντες. Αυτό μπορεί να συμβεί είτε γιατί κάποιος συμμετέχοντας δεν μπόρεσε να μεταφέρει τα δεδομένα του, είτε γιατί αποκλείστηκε ως κακοήθης.

7. ΠΡΩΤΟΚΟΛΛΟ ΤΩΝ M. JOYE ΚΑΙ B. LIBERT (2013)

Marc Joye and Benoît Libert, A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data. In A.-R. Sadeghi, Ed., *Financial Cryptography and Data Security* (FC 2013), vol. 7879 of Lecture Notes in Computer Science, pp. 111-125, Springer, 2013.

Το πρωτόκολλο των Shi *et al*. δίνει μια καλή απάντηση στο πρόβλημα του μη-αξιέμπιστου συγκεντρωτή, αφήνει όμως και θέματα ανοικτά προς βελτίωση. Πολλές εργασίες έχουν γίνει με αφορμή αυτό το πρωτόκολλο. Παρακάτω παρουσιάζεται μια ενδιαφέρουσα προσέγγιση που καθιστά το πρωτόκολλο πιο κατάλληλο για χρήση σε smart grid.

Οι M. Joye και B. Libert, παίρνοντας τη σκυτάλη από τους Shi *et al*., εξετάζουν τους περιορισμούς του πρωτοκόλλου και προτείνουν ένα μοντέλο που να λύνει έναν από αυτούς.

Η γενική ιδέα είναι ίδια: μια σειρά πολλαπλών χρηστών μεταφέρει σε κάθε χρονική περίοδο κρυπτογραφημένες τιμές κάποιων δεδομένων σε έναν μη-αξιέμπιστο συγκεντρωτή δεδομένων, ο οποίος θα πρέπει να υπολογίζει το σύνολο των τιμών όλων των χρηστών και τίποτε άλλο.

Το πρωτόκολλο των Shi *et al*. περιορίζεται σε αρχικά μηνύματα μικρού μεγέθους. Οι Marc Joye and Benoit Libert δημιουργούν ένα πρωτόκολλο που υποστηρίζει μεγάλου μήκους αρχικά μηνύματα, πολυπληθή αριθμό χρηστών, συνεχή λειτουργία ανεξάρτητα του αριθμού των χρηστών και ικανότητα λειτουργίας on και off line ακόμα και από συσκευές περιορισμένων πόρων.

Περιορισμοί του πρωτοκόλλου

Το πρωτόκολλο κληρονομεί κάποιες από τις αδυναμίες του πρωτοκόλλου των Shi *et al*..

- Δεν επιτρέπει τη μερική συνάθροιση σε περίπτωση απουσίας συμμετεχόντων.
- Δεν μπορεί να επεκταθεί για τον υπολογισμό σταθμισμένων αθροισμάτων.
- Απαιτεί συγχρονισμό μεταξύ των συμμετεχόντων.

Πλεονεκτήματα του πρωτοκόλλου

Από την άλλη κληρονομεί κάποια ουσιώδη οφέλη.

- Ο συγκεντρωτής δεδομένων μπορεί να επεξεργαστεί τα δεδομένα χρηστών από μόνος του χωρίς να χρειάζεται να αλληλεπιδράσει με υπηρεσία διαχείρισης κατάνεμημένων κλειδιών (distributed key-managing authority) σε κάθε συνάθροιση. Το αξιέμπιστο μέρος που παράγει το δημόσιο κλειδί δεν εμπλέκεται σε καμία συνάθροιση και μπορεί να μείνει off line μετά τη φάση ρύθμισης.
- Το μοντέλο απαιτεί οι χρήστες να αποθηκεύουν μόνο $O(1)$ τιμές και δεν απαιτεί αμφίδρομο κανάλι επικοινωνίας.
- Όλες οι επεκτάσεις του πρωτοκόλλου των Shi *et al*. είναι δυνατές από αυτό το πρωτόκολλο.

7.1. Επισκόπηση του πρωτοκόλλου

Όπως παρουσιάστηκε και στο πρωτόκολλο των Shi *et al*., το μοντέλο κρυπτογράφησης υπό τη λήθη του συγκεντρωτή (aggregator-oblivious encryption scheme) αποτελείται από ένα σύνολο αλγορίθμων, που ορίζονται ως εξής:

$Setup\ (1^{\kappa})$: Λαμβάνοντας ως είσοδο μια παράμετρο ασφαλείας κ, ένας αξιέμπιστος διαμοιραστής (dealer) παράγει τις παραμέτρους συστήματος param, το ιδιωτικό κλειδί του συγκεντρωτή sk_0 και το ιδιωτικό κλειδί sk_i για κάθε χρήστη $i\ (1 \le i \le n)$.

$Enc(param, sk_i, x_{i,t})$: Τη χρονική περίοδο t, ο χρήστης i κρυπτογραφεί μια τιμή $x_{i,t}$ χρησιμοποιώντας το ιδιωτικό κλειδί του sk_i για να παράγει $c_{i,t} = Enc(param, sk_i, x_{i,t})$.

$AggrDec(param, sk_0, c_{1,t}, \dots, c_{n,t})$: Τη χρονική περίοδο t, ο συγκεντρωτής χρησιμοποιώντας το κλειδί του sk_0 βρίσκει $X_t = \sum_{i=1}^{n} x_{i,t}$ ως $X_t = AggrDec(param, sk_0, c_{1,t}, \dots, c_{n,t})$.

7.2. Κρυπτογράφηση υπό τη λήθη του συγκεντρωτή (Aggregatior-oblivious encryption)

Η έννοια ασφαλείας της λήθης του συγκεντρωτή (aggregator obliviousness – AO) προϋποθέτει ότι ο συγκεντρωτής δεν μπορεί να μάθει, για κάθε χρονική περίοδο, τίποτα περισσότερο από την αθροιστική τιμή X_t, από τα κρυπτογραφημένα δεδομένα των n (αδιάβλητων) χρηστών. Εάν υπάρχουν διεφθαρμένοι χρήστες (δηλαδή χρήστες που μοιράζονται τα ιδιωτικά δεδομένα τους με το συγκεντρωτή), η έννοια απαιτεί μόνο ότι ο συγκεντρωτής δεν θα πάρει επιπλέον πληροφορίες για τις τιμές των αδιάβλητων χρηστών πέρα από την αθροιστική τιμή. Επιπλέον θεωρείται ότι κάθε χρήστης κρυπτογραφεί μόνο μια τιμή ανά χρονική περίοδο.

Οι Shi *et al*. απέδειξαν ότι το μοντέλο τους πληροί την έννοια ασφαλείας AO υπό την Decisional Diffie–Hellman assumption (DDH assumption), σε random oracle model. Για σύνολα που ικανοποιούν τη σύνθεση των Shi *et al*. (δηλαδή prime-order DDH σύνολα), η πιο κατάλληλη μέθοδος είναι χρήση του Pollard's λ αλγορίθμου, ή παραλλαγών αυτού, όπου απαιτείται το εύρος των X_t να είναι μικρό. Το μοντέλο τους περιλαμβάνει τον υπολογισμό διακριτών λογαρίθμων (discrete logarithms) σε σύνολα πρώτου πληθικού αριθμού (prime-order groups), για τα οποία η DDH assumption είναι ισχυρή.

Παρακάτω παρουσιάζεται ένα μοντέλο όπου ο υπολογισμός διακριτών λογαρίθμων μπορεί να γίνει αποτελεσματικά χωρίς αυτόν τον περιορισμό του εύρους και παράλληλα να ικανοποιείται η έννοια της AO ασφάλειας.

7.3. Νέο μοντέλο

Θεωρούνται σύνολα $\mathbb{G}$ σύνθετου πληθικού αριθμού (groups of composite order) για τα οποία υπάρχει ένα υποσύνολο $\mathbb{G}_1$ [αγνώστου πληθικού αριθμού] όπου ισχύει κάποια παραδοχή δυσεπιλυσιμότητας (intractability assumption) και ένα άλλο υποσύνολο $\mathbb{G}_2$ όπου διακριτοί λογάριθμοι είναι εύκολα υπολογίσιμοι. Είναι κρίσιμο μόνο ο αξιέμπιστος διαμοιραστής να γνωρίζει τη πληθικότητα $\#\mathbb{G}_1$ του $\mathbb{G}_1$. Για οποιονδήποτε άλλο, περιλαμβανομένου και του συναθροιστή, η $\#\mathbb{G}_1$ πρέπει να παραμείνει άγνωστη. Απλώς ένα άνω όριο του μπορεί να εξαχθεί.

$Setup\ (1^\kappa)$: Λαμβάνοντας ως είσοδο μια παράμετρο ασφαλείας κ, ο αξιέμπιστος διαμοιραστής (dealer) τυχαία παράγει ένα modulus $N = pq$, το οποίο είναι το γινόμενο δύο πρώτων αριθμών p, q ίσου μεγέθους. Σημειώνεται ότι η προϋπόθεση μεγέθους των p και q συνεπάγεται ότι $gcd(\varphi(N), N) = 1$. Επίσης ορίζει μια συνάρτηση κατακερματισμού (hash function) $H : \mathbb{Z} \to (\mathbb{Z}/N^2\mathbb{Z})^*$ που θα θεωρείται random oracle στην ανάλυση ασφαλείας. Θέτοντας l το bit-μήκος του N, από n τυχαία επιλεγμένα στοιχεία στο $\pm\{0,1\}^{2l}, s_1, \dots, s_n$, θέτει τελικά $s_0 = -\sum_{i=1}^{n} s_i$ και προσδιορίζει $param = \{N, H\}$ καθώς και $sk_i = s_i\ (για\ 0 \le i \le 1)$.

$Enc(param, sk_i, x_{i,t})$: Τη χρονική περίοδο t, για μια ιδιωτική είσοδο $x_{i,t} \in \mathbb{Z}/N\mathbb{Z}$, ο χρήστης i παράγει

$$c_{i,t} = \left(1 + x_{i,t}N\right) \cdot H(t)^{s_i} \bmod N^2.$$

$AggrDec(param, sk_0, c_{1,t}, \dots, c_{n,t})$: Ο συγκεντρωτής βρίσκει το άθροισμα X_t για τη χρονική περίοδο t υπολογίζοντας πρώτα το $V_t := H(t)^{s_0} \prod_{i=1}^{n} c_{i,t} \bmod N^2$ και έπειτα το X_t ως

$$X_t = \frac{V_t - 1}{N}.$$

Η ορθότητα έπεται από την παρατήρηση ότι

$$H(t)^{s_0} \prod_{i=1}^{n} c_{i,t} \equiv \prod_{i=1}^{n} \left(1 + x_{i,t}N\right) \equiv 1 + \left(\sum_{i=1}^{n} x_{i,t} \bmod N\right) N \ (\mathrm{mod}\ N^2)\,.$$

Και πάλι παρατηρούμε ότι η τιμή X_t ορίζεται ως modulo N. Συνεπώς, εάν $\sum_{i=1}^{n} x_{i,t} < N$, τότε $X_t = \frac{V_t - 1}{N} = \sum_{i=1}^{n} x_{i,t}$ επί των ακεραίων. Η κυρίως διαφορά από το μοντέλο των Shi *et al*. βρίσκεται στο ότι δεν υπάρχει διακριτός λογάριθμος που να μπορεί να υπολογιστεί σε ένα σύνολο στο οποίο η DDH assumption είναι ισχυρή. Αντιθέτως, η ανάκτηση του X_t από το συσσωρευμένο γινόμενο (accumulated product) V_t είναι πλέον εύκολη. Ως αποτέλεσμα δεν υπάρχει πια ο περιορισμός του μέγεθος του $x_{i,t}$, ούτε στο πλήθος n των χρηστών, εφόσον $\sum_{i=1}^{n} x_{i,t} < N$. Συνήθως το N είναι μια 2048-bit τιμή. Πρακτικά λοιπόν δεν υπάρχει περιορισμός.

7.4. Απόδοση μοντέλου

Σε αντίθεση με προηγούμενες λύσεις, το μοντέλο δεν περιορίζεται στο μέγεθος του μηνύματος ή το πλήθος των χρηστών. Αυτό οδηγεί σε γρηγορότερη κρυπτογράφηση και συνάθροιση, ακόμα και στην περίπτωση μεγάλων μηνυμάτων ή/και πλήθος χρηστών.

Ένα ακόμα ενδιαφέρον πλεονέκτημα του μοντέλου σε σχέση με το μοντέλο των Shi *et al*. είναι ότι επιτρέπει αποτελεσματική κρυπτογράφηση on the fly. Συγκεκριμένα, οι εκθετικοί υπολογισμοί $H(t)^{s_i} \bmod N^2$ μπορούν να προ-υπολογιστούν με τέτοιο τρόπο που, όταν το αρχικό μήνυμα $x_{i,t}$ είναι γνωστό, ο αποστολέας να πρέπει μόνο να υπολογίσει ένα modular πολλαπλασιασμό για να βρει το $c_{i,t}$. Σε εφαρμογές για έξυπνα συστήματα μέτρησης, αυτό το πλεονέκτημα μπορεί να είναι κρίσιμο καθώς οι υπολογισμοί συνήθως γίνονται σε συσκευές περιορισμένων πόρων. Επιπλέον το μοντέλο είναι εξαιρετικά απλό χωρίς να διακυβεύεται η ασφάλειά του.

Αν και το μοντέλο είναι παρόμοιο με το μοντέλο των Shi *et al*., η ανάλυση ασφαλείας του είναι τελείως διαφορετική και στην πραγματικότητα απλούστερη. Οι M. Joye και B. Libert

στην απόδειξη της ασφάλειας του μοντέλου λαμβάνουν πολύ καλύτερη συμπαγή ασφάλεια στο random oracle model καθώς το όριο ασφαλείας προκύπτει εντελώς ανεξάρτητο από τον αριθμό των χρηστών. Συγκριτικά, η ανάλυση ασφαλείας των Shi *et al*. συνεπάγεται ένα πολλαπλασιαστικό χάσμα ανάλογο του n^3 στη μείωση από την DDH assumption. Λαμβάνοντας υπόψη ότι μεγάλες τιμές του n όπως $n \approx 2^{20}$ αναμένονται σε πρακτικές εφαρμογές, φαίνεται σκόπιμο να μεγαλώσει το μέγεθος του κλειδιού ανάλογα. Στους M. Joye και B. Libert η μείωση ελαττώνει την απώλεια ασφαλείας σε μόλις 30 bits αν επιτρέψουμε τον αριθμό των queries κρυπτογράφησης $q_{enc} = 2^{30}$, όπου και αυτή η τιμή θα πρέπει να ληφθεί ως θεωρητική αφού κανείς μπορεί να περιορίσει το q_{enc} σε μικρές τιμές όπως $q_{enc} \leq 3$.

8. ΠΡΩΤΟΚΟΛΛΟ ΤΩΝ ROTTONDI ET AL. (2013)

Cristina Rottondi, Giacomo Verticale and Antonio Capone, Privacy-preserving smart metering with multiple data consumers. In *Computer Networks 57.7*, pp. 1699-1713, 2013.

Οι Rottondi *et al*. προτείνουν μια αρχιτεκτονική και ένα πρωτόκολλο επικοινωνίας σε ένα έξυπνο δίκτυο που να επιτρέπει σε οργανισμούς κοινής ωφέλειας (ΟΚΩ) και τρίτα μέρη (αναφέρονται ως Καταναλωτές δεδομένων) να συλλέγουν δεδομένα μέτρησης με διαφορετικά επίπεδα χωρικής και χρονικής συνάθροισης από έξυπνους μετρητές χωρίς να αποκαλύπτονται οι επιμέρους μετρήσεις σε κανένα κόμβο της αρχιτεκτονικής.

Στην προτεινόμενη αρχιτεκτονική εισάγεται ένα σύνολο λειτουργικών κόμβων στο έξυπνο δίκτυο, οι κόμβοι διατήρησης απορρήτου (Privacy Preserving Nodes – PPNs), οι οποίοι συλλέγουν κρυπτογραφημένα δεδομένα πελατών (Παραγωγών δεδομένων) και θεωρείται ότι ελέγχονται από ανεξάρτητα μέρη. Η κρυπτογράφηση των δεδομένων γίνεται μέσω του Shamir's Secret Sharing Scheme (SSS). Αξιοποιώντας τις ομομορφικές ιδιότητες του μοντέλου κρυπτογράφησης, τα δεδομένα μπορούν να συναθροιστούν απευθείας από το κρυπτογραφημένο πεδίο ορισμού. Επομένως, ένας έντιμος-αλλά-περίεργος (honest-but-curious) επιτιθέμενος δεν μπορεί να αποκτήσει συναθροισμένα ή και μη συναθροισμένα δεδομένα. Ο PPN εκτελεί διαφορετικές χωρικές και χρονικές συναθροίσεις για κάθε Καταναλωτή ανάλογα με τις ανάγκες του και τα δικαιώματα προσπέλασής του. Οι Καταναλωτές δεδομένων ανακτούν τα συναθροισμένα δεδομένα συλλέγοντας πολλαπλά μερίδια από τους PPNs.

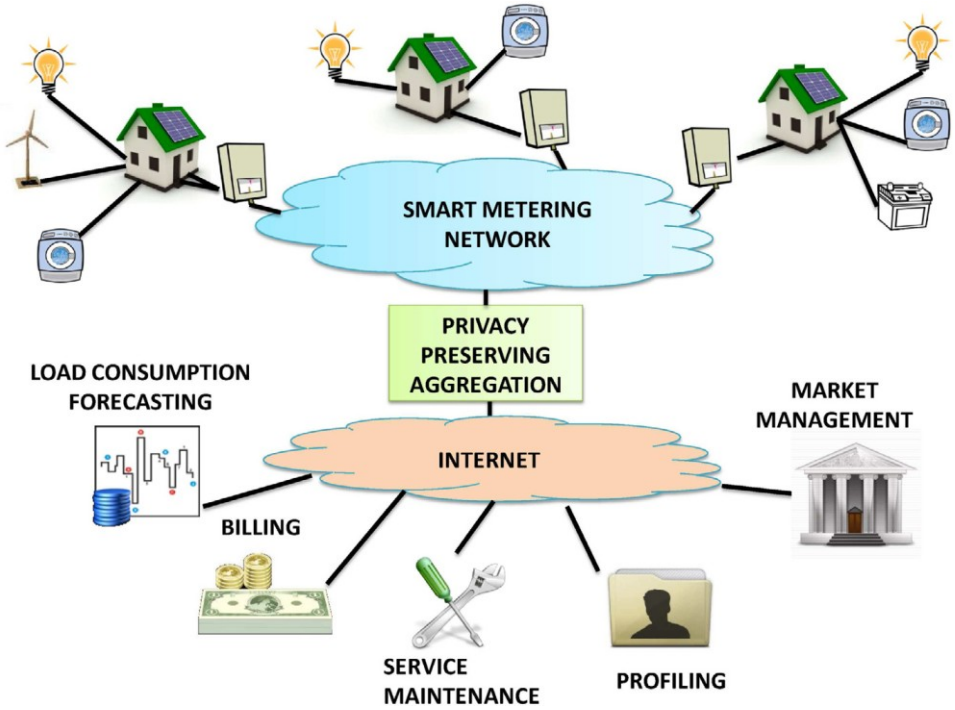
Η εργασία τους επίσης εξετάζει το πρόβλημα της ροής πληροφοριών από τους Παραγωγούς στους PPN's και από εκεί στους Καταναλωτές πληροφοριών σε ένα περιβάλλον περιορισμένων πόρων. Το πρωτόκολλο είναι σε θέση να λειτουργεί ακόμα και εάν υπάρχουν απώλειες στα δεδομένα είτε λόγω σφαλμάτων στη δικτυακή επικοινωνία λόγω καθυστερήσεων στη μετάδοση. Τέλος αξιολογούν το βαθμό της ανωνυμίας της σχέσης μεταξύ των Παραγωγών πληροφορίας και των Καταναλωτών πληροφορίας που επιτυγχάνεται από την υποδομή.

8.1. Γενικά

Το ενδιαφέρον για την ασφάλεια στα δίκτυα δεδομένων γενικά επικεντρώνεται στο απόρρητο των δεδομένων, το οποίο είναι διαφορετική έννοια από απόρρητο του χρήστη: το μεν πρώτο ασχολείται με την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, το δε δεύτερο σχετίζεται με την προστασία των ατόμων και μπορεί να επεκταθεί σε διάφορες διαστάσεις. Ο πιο σχετικός στόχος είναι η προστασία των δεδομένων που θα μπορούσαν να αποκαλύψουν πληροφορίες σχετικά με την ταυτότητα ενός ατόμου μαζί με τα φυσικά, οικονομικά, κοινωνικά χαρακτηριστικά του ή της προσωπικές του συμπεριφορές. Ως εκ τούτου, η φιλικότητα προς την ιδιωτικότητα (privacy-friendliness) στην αυτόματη υποδομή μέτρησης (Automatic Metering Infrastructure – AMI) είναι ιδιαίτερα σημαντική στην περίπτωση οικιακών πελατών και κάπως λιγότερο κρίσιμη στην περίπτωση των επιχειρηματικών οντοτήτων, αν και ωφέλιμη παρόλα αυτά.

Οι Rottondi *et al*. θεωρούν ότι στοιχείο κλειδί για μια νέα αρχιτεκτονική συστήματος είναι μια πλατφόρμα υπηρεσιών που να μπορεί να είναι ανοικτή σε εφαρμογές που

παρέχονται όχι μόνο από τις παραδοσιακές εταιρείες ΟΚΩ, αλλά και από ανεξάρτητους διαχειριστές συστήματος (Independent System Operators – ISOs), διαχειριστές περιφερειακής μετάδοσης (Regional Transmission Operators – RTOs), προμηθευτές υποδομής και τρίτα μέρη (πχ. μεσίτες ενέργειας και συναθροιστές), που μπορούν να παίξουν ρόλο σε μια ανοικτή αγορά υπηρεσιών προστιθέμενης αξίας. Η ιδέα τους παρουσιάζεται εποπτικά στην επόμενη εικόνα.



Σχήμα 13: Το σενάριο έξυπνου δικτύου με πολλαπλούς Καταναλωτές δεδομένων σύμφωνα με τους Rottondi *et al*.

Επομένως, σε ένα σενάριο στο οποίο διάφοροι παράγοντες μπορούν να παρέχουν υπηρεσίες βασισμένες στις πληροφορίες που συλλέγονται στο σύστημα έξυπνης μέτρησης, είναι υψίστης σημασίας ο ορισμός της υποδομής ασφαλείας που μπορεί να παρέχει πρόσβαση σε δεδομένα μετρήσεων με διαφορετικά επίπεδα χωρικής και χρονικής συνάθροισης. Εν τούτοις, δεδομένου του μεγάλου αριθμού των εμπλεκομένων ενδιαφερόμενων μελών, είναι εύλογο να ορισθεί μια δεξαμενή ανεξάρτητων συναθροιστών τρίτου μέρους με μερική ή περιορισμένη γνώση των δεδομένων που συλλέγονται. Οι Rottondi *et al*. προτείνουν μια υποδομή που επιτρέπει στους Καταναλωτές να συγκεντρώνουν δεδομένα που έχουν συναθροιστεί σε χωρική και χρονική βάση σύμφωνα με τη συγκεκριμένη υπηρεσία που τα χρησιμοποιεί.

8.2. Συνεισφορές του πρωτοκόλλου

Η εργασία των Rottondi *et al*. παρέχει τις παρακάτω βασικές εισφορές:

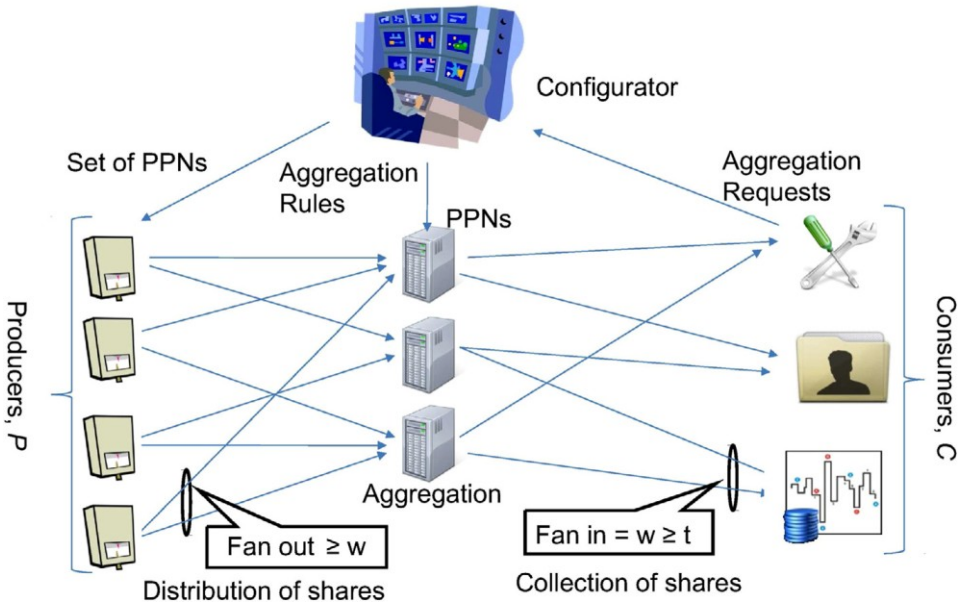
Το σχεδιασμό μιας υποδομής απορρήτου που περιλαμβάνει ένα σύνολο λειτουργικών κόμβων (PPNs), τους οποίους μπορούν να χειριστούν ανεξάρτητα μέρη ή

ρυθμιστικές αρχές. Το σύστημα είναι σχεδιασμένο να συμπεριφέρεται σωστά ακόμα και στην περίπτωση συνομωσίας ή εσφαλμένης συμπεριφοράς από περιορισμένο αριθμό των κόμβων. Οι κόμβοι συλλέγουν μερίδια από τα δεδομένα των πελατών που λαμβάνονται με τη χρήση του SSS. Οι PPNs εκτελούν πολλαπλές συναθροίσεις με διαφορετική διακριτότητα, σύμφωνα με τις ανάγκες και τα δικαιώματα πρόσβασης κάθε Καταναλωτή.

Την τυποποίηση ενός πρωτοκόλλου επικοινωνίας που διαχειρίζεται τις ροές πληροφοριών μεταξύ των Παραγωγών δεδομένων, των Καταναλωτών και των PPNs.

8.3. Η αρχιτεκτονική μιας AMI φιλικής προς την ιδιωτικότητα

Συναθροιστική αρχιτεκτονική και επισκόπηση του πρωτοκόλλου



Σχήμα 14: Αρχιτεκτονική φιλική προς την ιδιωτικότητα σύμφωνα με τους Rottondi *et al*.

Όπως παρουσιάζεται και στην παραπάνω εικόνα, η αρχιτεκτονική περιλαμβάνει τρία σύνολα κόμβων:

- Το σύνολο των Παραγωγών πληροφοριών, P, που εκπροσωπούν τους έξυπνους μετρητές.
- Το σύνολο των PPNs, N, που εκτελούν ομομορφική συνάθροιση στα κρυπτογραφημένα δεδομένα.
- Το σύνολο των Καταναλωτών πληροφοριών, C, που λαμβάνουν χρονικά ή και χωρικά συναθροισμένες πληροφορίες και εκπροσωπούν τα ΟΚΩ ή άλλες υπηρεσίες τρίτων μερών όπως εταιρείες τιμολόγησης ή μεσίτες ενέργειας.

Υποθέτουμε ότι το πλέγμα έχει κάποιες πολιτικές απορρήτου που όλα τα αιτήματα συνάθροισης θα πρέπει να ικανοποιούν. Οι πολιτικές μπορεί να διαφέρουν ανάλογα με τον κάθε Καταναλωτή.

Ένας κόμβος Διαμορφωτής περιλαμβάνεται επίσης στην αρχιτεκτονική. Αυτός είναι υπεύθυνος για τον έλεγχο της συμμόρφωσης των αιτημάτων συνάθροισης που λαμβάνονται από τους Καταναλωτές με τις πολιτικές απορρήτου του πλέγματος. Επίσης είναι υπεύθυνος για τη διαμόρφωση των PPNs με τους σωστούς κανόνες συνάθροισης. Δεν αναμειγνύεται στη διαδικασία συνάθροισης δεδομένων και δεν έχει πρόσβαση στις μετρήσεις. Ο Διαμορφωτής μπορεί να παρέχεται για παράδειγμα από μια ρυθμιστική αρχή ή από μια εταιρεία πλέγματος.

Κατά την αρχική διαμόρφωση ο Διαμορφωτής μπορεί να ανιχνεύει και να εμποδίζει προσπάθειες συνεννοημένων περίεργων Καταναλωτών να εξορύξουν λεπτομερέστερα από τα προβλεπόμενα δεδομένα ή να εξορύξουν δεδομένα από πολύ μικρό σύνολο συνάθροισης.

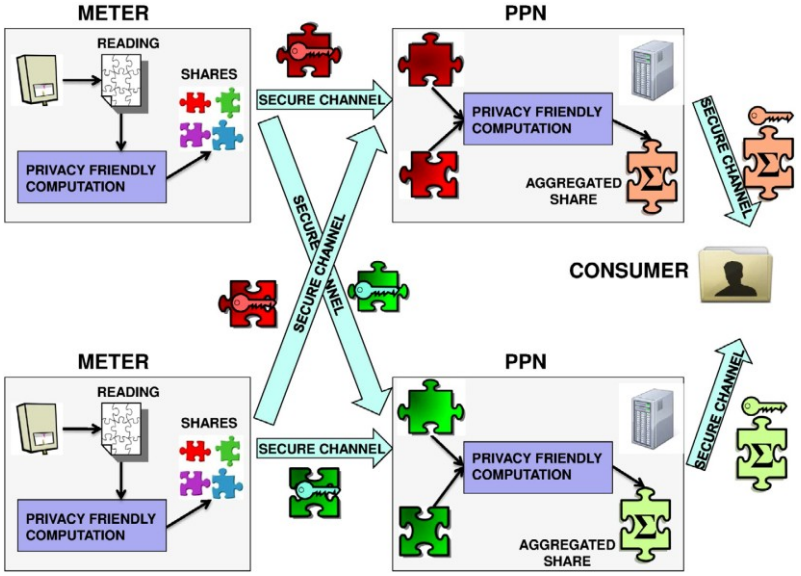
Θεωρείται ότι οι Καταναλωτές καθορίζουν τα αιτήματα συνάθροισής τους με βάση αποκλειστικά το αναγνωριστικό των Παραγωγών και δεν μπορούν να συμπεριλάβουν κανέναν υπολογισμό επί των ατομικών δεδομένων των Παραγωγών, που τα γνωρίζουν μόνο οι ίδιο οι Παραγωγοί.

Οι μετρήσεις κάθε Παραγωγού χωρίζονται σε μερίδια βάσει του (w, t) Shamir's Secret Sharing Scheme όπου w το πλήθος των μεριδίων και t ο ελάχιστος αριθμός των μεριδίων που απαιτούνται για την ανάκτηση της μυστικής πληροφορίας. Η επιλογή των κατάλληλων παραμέτρων σχεδιασμού του συστήματος w και t είναι κρίσιμη. Όπως παρουσιάζεται και στην προηγούμενη εικόνα, οι Παραγωγοί στέλνουν κάθε μερίδιο σε διαφορετικό PPN, συνεπώς ατομικές μετρήσεις μπορούν να ληφθούν μόνο από τουλάχιστον t συνεννοημένους PPNs.

Οι PPNs αθροίζουν ανεξάρτητα τα μερίδια που έχουν λάβει από διαφορετικούς Παραγωγούς ή και από τον ίδιο Παραγωγό σε διαφορετική χρονική στιγμή κα στέλνουν τα αθροισμένα μερίδια στον Καταναλωτή. Ο Καταναλωτής μπορεί να ανακτήσει τη συναθροισμένη μέτρηση μόνο εάν λάβει t τέτοια μερίδια.

Χάρη στις ομομορφικές ιδιότητες του μοντέλου Shamir σε σχέση με την άθροιση, τα συναθροισμένα μερίδια που λαμβάνονται με την παραπάνω διαδικασία είναι ισοδύναμα με τα μερίδια που προκύπτουν εάν πρώτα συναθροιστούν οι επιμέρους μετρήσεις και έπειτα κρυπτογραφηθούν τα συναθροισμένα δεδομένα. Συνεπώς ο Καταναλωτής μπορεί να ανακτήσει τα συναθροισμένα δεδομένα αλλά δεν αποκτά τις επιμέρους μετρήσεις.

Επίσης, τα κανάλια επικοινωνίας μεταξύ Παραγωγών και PPNs και μεταξύ PPNs και Καταναλωτών θεωρούνται εμπιστευτικά και πιστοποιημένα.



Σχήμα 15: Πρωτόκολλο φιλικό προς την ιδιωτικότητα σύμφωνα με τους Rottondi *et al.*

Ορισμός του προβλήματος

Θεωρείται ότι ο χρόνος διαιρείται σε γύρους σταθερής διάρκειας και ότι όλοι οι κόμβοι έχουν κοινή χρονική αναφορά. Κάθε Παραγωγός, PPN και καταναλωτής προσδιορίζεται από μια μοναδική ετικέτα.

Σε κάθε γύρο i, ο p-οστός Παραγωγός παράγει μια μέτρηση μ_i^p, η οποία μπορεί να αναπαρίσταται από έναν ακέραιο. Κατά τη φάση ρύθμισης, ο c-οστός Καταναλωτής ορίζει ένα σύνολο Παραγωγών Π_c και έναν χρονικό παράγοντα συνάθροισης k_c. Σε κάθε χρονικό διάστημα i πού είναι ένας ακέραιος πολλαπλάσιος του k_c, ο Καταναλωτής αναμένει να μάθει το σύνολο:

$$\sigma_i^c = \sum_{p \in \Pi_c} \sum_{\alpha=i-k_c+1}^{i} \mu_\alpha^p \qquad (1)$$

Το μοντέλο επίθεσης

Το πρωτόκολλο λαμβάνει υπόψη τις παρακάτω υποθέσεις επίθεσης:

Οι Παραγωγοί θεωρούνται πλήρως αξιόπιστοι.

Οι PPNs ακολουθούν το έντιμος-αλλά-περίεργος (honest-but-curious) μοντέλο.

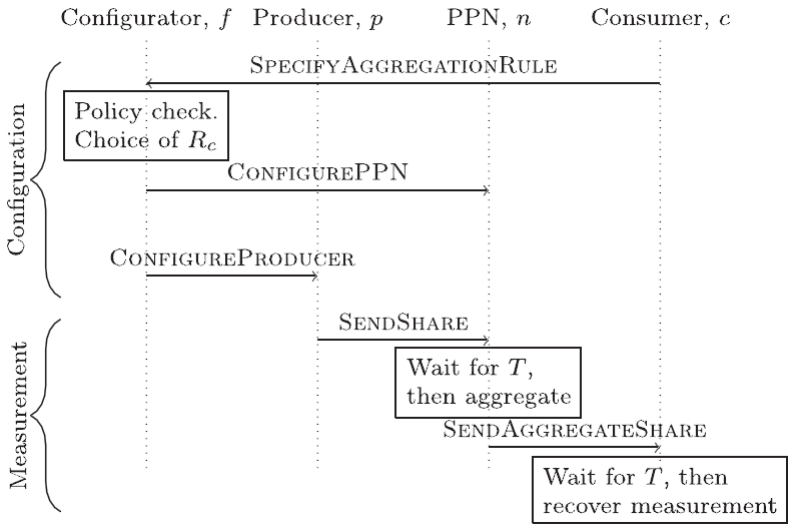
Οι Καταναλωτές θεωρούνται έντιμοι-αλλά-περίεργοι (honest-but-curious).

Υποτίθεται η παρουσία ενός παντογνώστη παθητικού εξωτερικού επιτιθέμενου.

Εφόσον τα κανάλια επικοινωνίας θεωρούνται ασφαλή, δεν λαμβάνεται υπόψη εξωτερική επίθεση από υποκλοπή των μετρήσεων ή από παραποίηση των μηνυμάτων.

8.4. Το πρωτόκολλο επικοινωνίας

Το πρωτόκολλο επικοινωνίας αποτελείται από δύο φάσεις. Η πρώτη εκτελείται άπαξ ανά Καταναλωτή ώστε να εγκατασταθεί η αρχική ρύθμιση και περιλαμβάνει έναν Καταναλωτή, το Διαμορφωτή και τους PPNs. Η δεύτερη φάση εκτελείται σε κάθε γύρο και περιλαμβάνει τους Παραγωγούς, τους PPNs και τους Καταναλωτές. Αυτή η φάση διευθύνει τη χωρική και χρονική συνάθροιση καθώς και την ανάκτηση των απωλειών μετάδοσης. Η επόμενη εικόνα παρουσιάζει τα μηνύματα του πρωτοκόλλου. Οι μεταβλητές f, p, n και c αντιπροσωπεύουν αντίστοιχα το Διαμορφωτή, τον Παραγωγό, τον PPN και τον Καταναλωτή που περιλαμβάνονται στην επικοινωνία.



Σχήμα 16: Το πρωτόκολλο συνάθροισης των Rottondi et. al.

Κατά τη φάση διαμόρφωσης τα ακόλουθα μηνύματα ανταλλάσσονται:

1. SPECIFY AGGREGATION RULE

$$c \rightarrow f : \Pi_c \parallel k_c$$

Ο Καταναλωτής ορίζει έναν κανόνα συνάθροισης όσον αφορά: (1) στο σύνολο Π_c των Παραγωγών που ο Καταναλωτής θέλει να παρακολουθήσει και (2) στον αριθμό k_c των χρονικών διαστημάτων κατά τα οποία τα δεδομένα πρέπει να συναθροίζονται. Ο κανόνας συνάθροισης (Π_c, k_c) αποστέλλεται στον Διαμορφωτή.

2. CONFIGURE PPN

$$f \rightarrow n : \Pi_c \parallel k_c \parallel R_c$$

Ο Διαμορφωτής ελέγχει τη συμμόρφωση του κανόνα με τις πολιτικές του πλέγματος και επιβεβαιώνει ότι ο συνδυασμός πολλαπλών κανόνων συνάθροισης από διαφορετικούς Καταναλωτές δεν οδηγεί στην ανάκτηση μεγάλης διακριτότητας στα αποτελέσματα ή σε υπολογισμό επί πολύ περιορισμένου συνόλου συνάθροισης. Εφόσον το αίτημα συνάθροισης

γίνει αποδεκτό, ο Διαμορφωτής επιλέγει ένα σύνολο Ω_c από $w \geq t$ PPNs και μεταβιβάζει σε κάθε PPN τους αντίστοιχους κανόνες χωροχρονικής συνάθροισης. Ο Διαμορφωτής στέλνει επίσης έναν τυχαία επιλεγμένο μοναδικό αναγνωριστικό, που είναι γνωστό μόνο στον ίδιο το Διαμορφωτή και τους PPNs.

3. CONFIGURE PRODUCER

$$f \rightarrow p : \Omega_c$$

Για κάθε Καταναλωτή c, ο Διαμορφωτής μεταβιβάζει σε κάθε Παραγωγό στο Π_c το σύνολο Ω_c των PPNs στους οποίους πρέπει να στείλει ένα μερίδιο των μετρήσεών του.

Εφόσον η αρχική φάση διαμόρφωσης ολοκληρωθεί, εκτελούνται τα επόμενα βήματα στο τέλος κάθε γύρου i.

4. SEND SHARE

$$p \rightarrow n : i \parallel \mu_i^p(n)$$

Κάθε Παραγωγός p παράγει μια μέτρηση μ_i^p. Εάν ο Παραγωγός λαμβάνει μέρος σε περισσότερους κανόνες συνάθροισης, μπορεί να χρειαστεί να αποστείλει τα μερίδιά του σε περισσότερους από w PPNs.Έστω w_p ο αριθμός των απαιτούμενων μεριδίων, ο οποίος γενικά μπορεί να διαφέρει από κόμβο σε κόμβο. Κάνοντας χρήση του μοντέλου του Shamir ο Παραγωγός χωρίζει τη μέτρησή του σε w_p μερίδια και τα αποστέλλει στους w_p PPNs. Το $\mu_i^p(n)$ συμβολίζει το μερίδιο του μυστικού μ_i^p που ο Παραγωγός p στέλνει στον n-οστό PPN κατά τον i γύρο. Τα μερίδια υπολογίζονται από τον Παραγωγό με το παρακάτω πολυώνυμο:

$$\mu_i^p(n) = \mu_i^p + \sum_{v=1}^{t-1} r_v n^v \bmod q \ \ \forall n \in \Omega_c \qquad (2)$$

Οι ακέραιοι r_v είναι ένα σύνολο τυχαίων ακέραιων αριθμών ομοιόμορφα κατανεμημένων στο διάστημα $[0,q)$ και αλλάζουν σε κάθε γύρο. Ο πρώτος αριθμός q είναι μια παράμετρος συστήματος μεγαλύτερη από οποιαδήποτε πιθανή συναθροισμένη μέτρηση και από τον μεγαλύτερο αναγνωριστικό αριθμό PPN. Οι δυνάμεις του n μπορούν να υπολογιστούν προκαταβολικά ώστε να μην έχουν υπολογιστικό κόστος κατά τη φάση των μετρήσεων.

5. SEND AGGREGATE SHARE

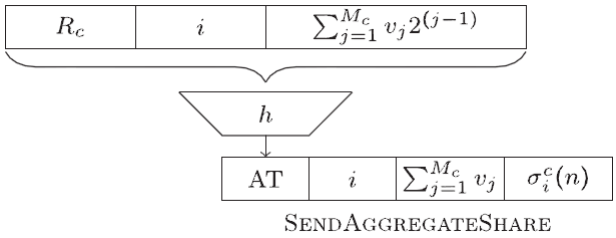
$$n \rightarrow c : AT \parallel i \parallel \sum_{j=1}^{M_c} v_j \parallel \sigma_i^c(n)$$

όπου $M_c = |\Pi_c|$ και v_j ισούται με 1 εάν όλα τα k_c μερίδια από τον j-οστό Παραγωγό στο Π_c έχουν παραληφθεί από τον PPN, αλλιώς είναι ίσο με 0. Για κάθε κανόνα συνάθροισης που έχει μεταβιβαστεί από το Διαμορφωτή, κάθε PPN περιμένει τα εισερχόμενα μερίδια για έναν ορισμένο χρόνο T. Έπειτα, ανεξάρτητα από τους άλλους PPNs, εκτελεί συνάθροιση επί

των κρυπτογραφημένων δεδομένων σύμφωνα με τον κανόνα, υπολογίζοντας την συναθροισμένη μέτρηση $\sigma_c^c(n)$ ως:

$$\sigma_c^c(n) = \sum_{p \in \Pi_c} \sum_{\alpha=i-k_c+1}^{i} \mu_a^p(n) \bmod q \qquad (3)$$

Οι PPNs χρησιμοποιούν το SEND AGGREGATE SHARE μήνυμα, όπως παρουσιάζεται στην επόμενη εικόνα, για να στείλουν τις συναθροισμένες μετρήσεις στους Καταναλωτές.



Εικόνα 1: Το SEND AGGREGATE SHARE μήνυμα του πρωτοκόλλου των Rottondi *et al.*

Στην περίπτωση λαθών στην επικοινωνία, καθυστερήσεων ή αποτυχίας κόμβου, κάποια από τα μερίδια μπορεί να μην φτάσουν εγκαίρως σε κάποιους ή σε οποιονδήποτε από τους PPNs. Εάν έστω και ένα μερίδιο από έναν Παραγωγό λείψει, τότε όλες οι μετρήσεις από αυτόν τον Παραγωγό θεωρούνται μηδενικές για όλο το παράθυρο συνάθροισης. Εφόσον ο Καταναλωτής μπορεί να ανακτήσει συναθροισμένες μετρήσεις που έχουν υπολογιστεί από των ίδιων δεδομένων εισόδου, το SEND AGGREGATE SHARE μήνυμα περιλαμβάνει και ένα Aggregation Tag (AT), που υπολογίζεται ως:

$$AT = h\left(R_c \parallel i \parallel \sum_{j=1}^{M_c} v_j \, 2^{(j-1)}\right)$$

όπου h μια κρυπτογραφικά ασφαλής συνάρτηση κατακερματισμού. Το AT είναι ίσο σε όλους τους PPNs εάν τα υποκείμενα δεδομένα εισόδου είναι τα ίδια, ενώ είνα διαφορετικό, με μεγάλη πιθανότητα, εάν τα δεδομένα εισόδου είναι διαφορετικά. Το μήνυμα περιλαμβάνει επίσης τον αριθμό του γύρου και την πληθικότητα του συνόλου των Παραγωγών που χρησιμοποιήθηκαν πραγματικά στον υπολογισμό. Η συνάθροιση εκτελείται μόνο σε γύρους που είναι ακέραια πολλαπλάσια του χρονικού παράγοντα συνάθροισης k_c.

Κατά την υποδοχή των συναθροισμένων μεριδίων ο Καταναλωτής ανακτά τις μετρήσεις λαμβάνοντας υπόψη μόνο τα μεγαλύτερα σύνολα μεριδίων που έχουν το ίδιο AT. Περιλαμβάνοντας το μοναδικό αναγνωριστικό στο AT γίνεται δύσκολο για τον Καταναλωτή να ελέγξει το κατά πόσον ο PPN έχει χρησιμοποιήσει ένα συγκεκριμένο υποσύνολο του P. Έτσι ο Καταναλωτής δεν μπορεί να μάθει ποιός Παραγωγός είχε μια αποτυχία, αλλά μόνο τον αριθμό τους. Περιλαμβάνοντας τον αριθμό του τρέχοντα γύρου στη συνάρτηση

κατακερματισμού καθιστά δύσκολο για τον Καταναλωτή να μάθει το κατά πόσον ένα σύνολο από συναθροισμένους Παραγωγούς έχει αλλάξει από γύρο σε γύρο. Άπαξ και ο Καταναλωτής ανακτήσει τη συναθροισμένη μέτρηση μπορεί να κλιμακώσει κατά το κλάσμα των σωστά συναθροισμένων μετρήσεων προκειμένου να εκτιμήσει το σύνολο, ακόμα και εάν κάποια δεδομένα Παραγωγών απουσιάζουν.

8.5. Απόδοση του πρωτοκόλλου

Πολυπλοκότητα πρωτοκόλλου

Όσον αφορά στην υπολογιστική πολυπλοκότητα και λαμβάνοντας υπόψη μόνο τη φάση υπολογισμών, το πρωτόκολλο έχει το παρακάτω κόστος πολυπλοκότητας.

Στον Παραγωγό, ο υπολογισμός των μεριδίων απαιτεί την παραγωγή t – 1 κρυπτογραφικά ασφαλών τυχαίων αριθμών και t – 1 σύνολα για κάθε από τα w_p μερίδια. Οι t – 1 πολλαπλασιασμοί στη (2) έχουν αμελητέο κόστος καθώς το n είναι μικρό. Υποθέτοντας ότι το w_p είναι ανάλογο του $|N|$, η μέση πολυπλοκότητα είναι $O(t|N|)$.

Στον PPN, η συνάθροιση εκτελείται μέσω της (3). Για τον c-οστό κανόνα απαιτούνται $M_c k_c$ αθροίσεις, συνεπώς η μέση ασυμπτωτική πολυπλοκότητα είναι $O(|C||P|\tilde{k})$, όπου $\tilde{k}$ το μέσο διάστημα συνάθροισης.

Στον Καταναλωτή η πολυπλοκότητα κυριαρχείται από την ανάκτηση των συναθροισμένων μετρήσεων. Ο Berlekamp-Welch αλγόριθμος έχει πολυπλοκότητα $O(w^3)$ και επιτρέπει την αναδόμηση του σωστού συναθροίσματος στην περίπτωση που $w \geq t + 2e + l$, όπου e είναι ο αριθμός των μεριδίων με εσφαλμένες τιμές και l είναι το πλήθος των χαμένων μεριδίων.

Αξιολόγηση απορρήτου

Παρακάτω ορίζονται ιδιότητες προστασίας του απορρήτου και γίνεται ανασκόπηση των ιδιοτήτων αυτών στην προτεινόμενη αρχιτεκτονική.

- Ορίζεται ότι η αρχιτεκτονική εξασφαλίζει τη **συναθροιστική λήθη** (is aggregator oblivious) εάν:

1. Ο Καταναλωτής δεν μπορεί να διακρίνει μεταξύ δύο διαφορετικών συνόλων μετρήσεων μ_i^p εφόσον το άθροισμά τους είναι το ίδιο. Προπαντός, δεν μπορεί να μάθει τίποτα για οποιονδήποτε Παραγωγό δεν περιλαμβάνεται στο παρακολουθούμενο σύνολο.
2. Εφόσον ένα σύνολο Καταναλωτών $\hat{C}$ συνωμοτήσει με ένα σύνολο Παραγωγών $\hat{P}$, δεν μπορούν να μάθουν τίποτα περισσότερο από ότι συνεπάγεται από τη γνώση του σ_i^c για όλους τους $c \in \hat{C}$ και του μ_i^p για όλους τους $p \in \hat{P}$.

Η προτεινόμενη αρχιτεκτονική παραδίδει στον Καταναλωτή μόνο τα μερίδια $\sigma_i^c(n)$ για $n \in \Omega_c$, έτσι ο Καταναλωτής έχει πρόσβαση μόνο στο άθροισμα των παρακολουθούμενων Παραγωγών. Μια συμπαιγνία με ένα σύνολο Παραγωγών $\hat{P}$ συνεισφέρει όλα τα μερίδια $\mu_i^p(n)$ για των Παραγωγών στο $\hat{P}$, κάτι το οποίο δεν δίνει πληροφορίες πέραν της γνώσης του μ_i^p. Συνεπώς η αρχιτεκτονική εξασφαλίζει τη συναθροιστική λήθη.

- Ορίζεται ότι η αρχιτεκτονική είναι ***t*-τυφλή** (t-blind) εάν μια συνομωσία λιγότερων από t PPNs δεν μπορούν να μάθουν τίποτα για οποιαδήποτε μ_i^p.

- Επίσης ορίζεται ότι η αρχιτεκτονική είναι **εύρωστη** (robust) εάν μια συνομωσία λιγότερων από t PPNs και ένα σύνολο Παραγωγών ή Καταναλωτών δεν μπορούν να μάθουν τίποτα για τη μ_i^p από όσο μπορεί να μαθευτεί από το σύνολο Παραγωγών και Καταναλωτών χωρίς τους PPNs.

Η χρήση του SSS μοντέλου εξασφαλίζει ότι κανένα σύνολο συνεννοημένων PPNs με πληθικότητα μικρότερη από t δεν μπορεί να ανακτήσει τις ατομικές μετρήσεις ούτε τις συναθροισμένες μετρήσεις. Συνεπώς η προτεινόμενη αρχιτεκτονική είναι t-τυφλή. Λιγότερα από t μερίδια είναι επίσης άχρηστα σε μια συνομωσία που περιλαμβάνει Καταναλωτές ή Παραγωγούς, συνεπώς η προτεινόμενη αρχιτεκτονική είναι εύρωστη απέναντι σε συνομωσίες.

- Ορίζεται ότι η αρχιτεκτονική είναι **(l,e)-ελαστική** ((l,e)-resilient) εφόσον:
  1. Παραδίδει το σωστό αποτέλεσμα ακόμα και εάν το πολύ l PPNs δεν έχουν πρόσβαση σε όλες τις μετρήσεις,
  2. Παραδίδει το σωστό αποτέλεσμα ακόμα και εάν το πολύ e PPNs δεν εκτελούν σωστά την άθροιση, είτε επίτηδες είτε εσφαλμένα,
  3. Στην περίπτωση που κάποιοι Παραγωγοί δεν μεταδίδουν τις μετρήσεις τους ή οι μετρήσεις αποτυγχάνουν να φτάσουν στους PPNs, η αρχιτεκτονική παρέχει το σωστό άθροισμα των υπολοίπων μετρήσεων και παρέχει το πλήθος των μετρήσεων που λείπουν.
     Η ιδιότητα της ελαστικότητας σχετίζεται κυρίως με την ανοχή σφάλματος της αρχιτεκτονικής αλλά έχει να κάνει και με την περίπτωση κακόβουλων PPNs που μολύνουν τα δεδομένα.

Δυνάμει του Berlekamp-Welch αλγορίθμου, το προτεινόμενο σύστημα είναι $(w-t-2e,e)$-ελαστικό. Μπορεί να διορθώσει τα εσφαλμένα μερίδια που αποστέλλονται από e εσφαλμένους ή εκτεθειμένους PPNs εάν τουλάχιστον $t+2e$ μερίδια είναι διαθέσιμα στον Καταναλωτή.

- Η αρχιτεκτονική παρέχει **(ζ_c,ξ_c)-ανωνυμία σχέσεων** ((ζ_c,ξ_c)-relationship anonymity) όσον αφορά στον Καταναλωτή c, εάν ένας επιτεθείς μπορεί να βρει το κατά πόσον ένας Παραγωγός παρακολουθείται από έναν Καταναλωτή c με ευαισθησία (sensitivity) ζ_c και εξειδίκευση (specificity) ξ_c. Η ευαισθησία ορίζεται ως το ποσοστό των Παραγωγών παρακολουθούμενων από τον c που μπορούν πράγματι να προσδιορισθούν ως τέτοιοι (παρακολουθούμενων από τον c). Η εξειδίκευση ορίζεται ως το ποσοστό των Παραγωγών που δεν παρακολουθούνται από τον c και που μπορούν πράγματι να προσδιορισθούν ως τέτοιοι (μη παρακολουθούμενων από τον c).

Οι Rottondi *et al.* αποδεικνύουν ότι το σύστημά τους παρέχει $(1,\xi_c)$-ανωνυμία σχέσεων με το ξ_c να προσεγγίζει το μηδέν όσο οι υπολογιστική ικανότητα των PPNs μεγαλώνει.

Επεκτασιμότητα αρχιτεκτονικής

Η αρχιτεκτονική των Rottondi *et al.* αποδεικνύεται επεκτάσιμη σε εκατομμύρια μετρητών. Όμως ο συνολικός αριθμός των απαραίτητων μεριδίων μεγαλώνει όταν ο αριθμός των Παραγωγών και η πιθανότητα σφαλμάτων επικοινωνίας αυξάνεται, δείχνοντας έτσι ότι τα

σφάλματα επικοινωνίας περιορίζουν την επεκτασιμότητα του συστήματος. Ένα πρωτόκολλο για ανάκτηση χαμένων δεδομένων είναι απαραίτητο σε εκτενή σενάρια.

Επιπλέον, για μια ορισμένη πιθανότητα σφαλμάτων επικοινωνίας, η παρουσία χρονικής συνάθροισης αυξάνει περαιτέρω τον απαραίτητο αριθμό μεριδίων, κάτι το οποίο οδηγεί σε αύξηση του αριθμού των PPNs.

Η μόλυνση με αλλοιωμένα συναθροισμένα μερίδια έχει ηπιότερη επίπτωση στην επεκτασιμότητα του συστήματος.

9. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα διατριβή έγινε επισκόπηση πρωτοκόλλων διατήρησης της ιδιωτικότητας των δεδομένων των έξυπνων μετρητών που συναθροίζονται σε ένα έξυπνο δίκτυο.

Τέτοια πρωτόκολλα έχουν ιδιαίτερη σημασία στη σύγχρονη εποχή όπου οι πάροχοι και διαχειριστές των δικτύων διανομής μπορούν να συγκεντρώσουν τεράστια ποσότητα δεδομένων. Αυτό θέτει σοβαρό πρόβλημα διατήρησης της ιδιωτικής ζωής, καθώς τα δεδομένα γίνονται στόχος κακόβουλων χρηστών κατά τη μεταφορά τους. Το ιδανικό είναι να αξιοποιηθούν τα δεδομένα για την καλύτερη λειτουργία του δικτύου χωρίς να θυσιαστεί η ιδιωτικότητα των δεδομένων. Δηλαδή να επιτραπεί η επεξεργασία των δεδομένων χωρίς να δίνεται πρόσβαση σε μη εξουσιοδοτημένους τρίτους. Κάτι τέτοιο φαίνεται πως είναι πλέον δυνατόν με πρωτόκολλα κρυπτογράφησης όπως αυτά που παρουσιάστηκαν.

Τέλος, είναι εμφανές στη βιβλιογραφία ότι υπάρχει δουλειά για το μέλλον όπως όσον αφορά στην επέκταση των πρωτοκόλλων σε διαφορετικά μοντέλα, στη βελτίωση της αποδοτικότητας, στον περιορισμό των δεδομένων που διακινούνται, στην ορθή αξιολόγηση των πληροφοριών που μεταφέρονται αλλά και σε άλλους τομείς.

10. ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Elaine Shi, T.-H. Hubert Chan, Eleanor G. Rieffel, Richard Chow, and Dawn Song. Privacy-preserving aggregation of time-series data. In *Network and Distributed System Security Symposium (NDSS 2011)*. The Internet Society, 2011.

2. EPRI (Electric Power Research Institute). Estimating the Costs and Benefits of the Smart Grid, March 2011.

3. Flavio D. Garcia and Bart Jacobs. Privacy-friendly energy-metering via homomorphic encryption. In *Proceedings of the 6th International Workshop on Security and Trust Management*, 2010.

4. Hubert Chan, Elaine Shi, and Dawn Song. Privacy-preserving stream aggregation with fault tolerance. In *Proceedings of the 16th International Conference on Financial Cryptography and Data Security*, FC '12, 2012.

5. Marek Jawurek, Florian Kerschbaum and George Danezis. SoK: Privacy technologies for smart grids – A survey of options. Technical Report MSR-TR-2012-119, Microsoft Research, 2012.

6. Marek Jawurek and Florian Kerschbaum. Fault-tolerant privacy-preserving statistics. In S. Fischer-Hübner and M. Wright, editors, *PETS*, volume 7384 of *Lecture Notes in Computer Science*, pp. 221-238. Springer, 2012.

7. Smart grids and renewables. A Guide for Effective Deployment. International Renewable Energy Agency, IRENA, 2013.

8. Marc Joye and Benoît Libert, A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data. In A.-R. Sadeghi, Ed., *Financial Cryptography and Data Security* (FC 2013), vol. 7879 of Lecture Notes in Computer Science, pp. 111-125, Springer, 2013.

9. A Renewable Energy Roadmap, Remap 2030, IRENA, 2013.

10. Cristina Rottondi, Giacomo Verticale and Antonio Capone, Privacy-preserving smart metering with multiple data consumers. In *Computer Networks 57.7*, pp. 1699-1713, 2013.

11. National Institute of Standards and Technology (NIST), Guidelines for smart grid cyber security, NIST Interagency Report 7628, 2010.

12. H. Simo Fhom, N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, A. Monti. A user-centric privacy manager for future energy systems. In *Power System Technology (POWERCON, 2010 International Conference on*, 2010.

13. I. Berganza, E. Lambert, A. Paice, R. Napolitano, A. Sendin. Communications requirements for smart grids. In *21st International Conference on Energy Distribution* (CIRED), Frankfurt, Germany, 2011.

14. H. Khurana, M. Hadley, N. Lu, D. A. Frincke. Smart-grid security issues. IEEE Security & Privacy, pp. 81-85, 2010.

15. G. Hart. Nonintrusive appliance load monitoring. Proceedings of the IEEE, volume 80 issue 12, pp. 1870 –1891, 1992.

16. A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, D. Irwin. Private memoirs of a smart meter. In *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, BuildSys '10, ACM, New York, NY, USA, pp. 61-66, 2010.

17. M. Jawurek, M. Johns, F. Kerschbaum. Plug-in privacy for smart metering billing. In S. Fischer-Hübner and N. Hopper, editors, *PETS*, volume 6794 of *Lecture Notes in Computer Science*, pp. 192–210. Springer, 2011.

18. A. Rial, G. Danezis. Privacy-preserving smart metering. In *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, WPES '11, ACM, New York, NY, USA, pp. 49-60, 2011.

19. Klaus Kursawe, George Danezis, and Markulf Kohlweiss. Privacy-friendly aggregation for the smart-grid. In S. Fischer-Hübner and N. Hopper, editors, *PETS*, volume 6794 of *Lecture Notes in Computer Science*, pp. 175-191, Springer, 2011.

20. Gergely Acs and Claude Castelluccia. I have a dream! (DiffeRentially privatE smArt Metering). In T. Filler et al., editors, *Information Hiding (IH 2011), volume 6958 of Lecture Notes in Computer Science*, pp. 118-132. Springer, 2011.

21. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In L. R. Knudsen, editor, *Advances in Cryptology, EUROCRYPT 2002, volume 2332 of Lecture Notes in Computer Science*, pp. 45-64, Springer, 2002.

22. Vibhor Rastogi and Suman Nath. Differentially private aggregation of distributed time-series with transformation and encryption. In *Proceedings of the 2010 international conference on Management of data*, SIGMOD ’10, pp 735–746, New York, NY, USA, ACM 2010.

23. Weiwei Jia, Haojin Zhu, *Member, IEEE*, Zhenfu Cao, *Senior Member, IEEE*, Xiaolei Dong, and Chengxin Xiao. Human-Factor-Aware Privacy-Preserving Aggregation in Smart Grid. In *IEEE systems journal*, volume 8, no 2, 2014.

24. C. Efthymiou and G. Kalogridis. Smart grid privacy via anonymization of smart metering data. In *Smart Grid Communications (Smart-GridComm),2010 First IEEE International Conference on*, pages 238–243, 2010.

25. M. Burkhart, M. Strasser, D. Many, X. Dimitropoulos, SEPIA: Privacy-preserving aggregation of multi-domain network events and statistics, in: Usenix security symposium, Usenix, 2010.

26. H. Simo Phom, N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, A. Monti. A user-centric privacy manager for future energy systems. In *Power System Technology (POWERCON), 2010 International Conference on*, pp. 1-7, 2010.

27. I. Berganza, E. Lambert, A. Paice, R. Napolitano, A. Sendin, Communications requirements for smart grids. In *21st International Conference on Energy Distribution (CIRED)*, Frankfurt, Germany, 2011.

28. W. Ahmad, A. Khokhar. An architecture for privacy preserving collaborative filtering on web portals. In *Information Assurance and Security, IAS 2007. Third International Symposium on*, pp. 273 –278, 2007.

29. Fengjun Li, Bo Luo, Peng Liu, Secure information aggregation for smart grids using homomorphic encryption. In: *Smart Grid Communications (SmartGridComm) 2010*, First IEEE International Conference on, pp. 327 –332, 2010.