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

Θέματα Ασφάλειας και Συνεργατικών Υπηρεσιών σε Δίκτυα Smart Grid

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χρήστος Ε. Τσιράκης

Επιβλέπων : Αθανάσιος Δ. Παναγόπουλος
Λέκτορας Ε.Μ.Π

Αθήνα, Ιούλιος 2012

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

Θέματα Ασφάλειας και Συνεργατικών Υπηρεσιών σε Δίκτυα Smart Grid

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χρήστος Ε. Τσιράκης

Επιβλέπων : Αθανάσιος Δ. Παναγόπουλος
Λέκτορας Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 19η Ιουλίου 2012.

.....	.....	.....
Αθανάσιος Δ. Παναγόπουλος Λέκτορας Ε.Μ.Π.	Φίλιππος Κωνσταντίνου Καθηγητής Ε.Μ.Π.	Ιωάννης Κανελλόπουλος Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2012

.....

Χρήστος Ε. Τσιράκης

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

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία αποτελεί το τελευταίο αλλά και σημαντικότερο σημείο του κύκλου της φοιτήσεώς μου στο ίδρυμα. Ήταν ευκαιρία κατά τη διάρκεια της εργασίας να αξιοποιήσω τις γνώσεις μου και να τις συνδυάσω με το δημιουργικό και ερευνητικό μου πνεύμα.

Αρχικά θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Αθανάσιο Δ. Παναγόπουλο, Λέκτορα Ε.Μ.Π., για την ανάθεση της διπλωματικής εργασίας αλλά για την πολύτιμη στήριξη και συμβουλές που μου προσέφερε σε οποιαδήποτε ζητήματα με απασχόλησαν.

Επιπλέον θα ήθελα να ευχαριστήσω τον κ. Χαράλαμπο Πήτα, Διδάκτορα Μηχανικό Ε.Μ.Π., για την καθοδήγηση, τη βοήθεια καθώς και την άμεση ανταπόκρισή του σε οποιοδήποτε πρόβλημα ή απορία είχα στη διαδικασία εκπόνησης της διπλωματικής εργασίας.

Τέλος θα ήθελα να ευχαριστήσω ιδιαίτερα την οικογένειά μου και τους φίλους μου για την υποστήριξη που μου προσέφεραν και την κατανόηση που έδειξαν καθ' όλη τη διάρκεια των σπουδών μου.

Χρήστος Ε. Τσιράκης

Μοσχάτο, 18 Ιουλίου 2012

ΠΕΡΙΛΗΨΗ

Το έξυπνο δίκτυο επιχειρεί να εκσυγχρονίσει το υπάρχον απαρχαιωμένο σύστημα δικτύου ηλεκτρικής ενέργειας. Τα ευεργετικά χαρακτηριστικά του έξυπνου δικτύου, κύριος εκφραστής των οποίων αποτελεί ο έξυπνος μετρητής, συμβάλλουν στη βέλτιστη αξιοποίηση ηλεκτρικής ενέργειας τόσο στην πλευρά της παραγωγής όσο και στην πλευρά της κατανάλωσης. Εισάγοντας τις νέες τεχνολογίες επικοινωνιών και πληροφορικής σε καίρια σημεία του δικτύου, επιτυγχάνεται η ενσωμάτωση ανανεώσιμων πηγών ενέργειας καθώς και η ενεργητικότητα των καταναλωτών στο σενάριο λειτουργίας του έξυπνου δικτύου.

Ωστόσο, η ενσωμάτωση των νέων τεχνολογιών, ειδικά αυτών που σχετίζονται με το Διαδίκτυο, ίσως εισάγουν νέες απειλές για την ασφάλεια του έξυπνου δικτύου. Ορισμένοι κακοπροαίρετοι επιτιθέμενοι μπορούν να εκμεταλλευτούν τα ευάλωτα σημεία του δικτύου επικοινωνιών και να καταλάβουν ηλεκτρονικές συσκευές, να υποκλέψουν απόρρητες ή προσωπικές πληροφορίες, να απαγορεύσουν τη διαθεσιμότητα απαραίτητων υπηρεσιών, να προκαλέσουν μια εκτεταμένη διακοπή ρεύματος, με συνέπεια ένα δυσμενές οικονομικό κόστος.

Για αυτό το λόγο, η αντιμετώπιση των ζητημάτων ασφάλειας στο έξυπνο δίκτυο παίζει πρωταρχικό ρόλο. Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των διακινούμενων πληροφοριών είναι ανάγκη να προστατευθούν, έτσι ώστε να αυξηθεί η αξιοπιστία του συστήματος. Η κρυπτογράφηση των δεδομένων μέτρησης συνιστά μια αποδοτική λύση, όπως και η προστασία των προσωπικών καταναλωτικών πληροφοριών με το καινοτόμο σύστημα διαχείρισης ηλεκτρικού φορτίου “ElecPrivacy”.

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

Τέλος, η λειτουργία του έξυπνου δικτύου προσομοιώνεται με τη βοήθεια του περιβάλλοντος προσομοίωσης OMNET++. Το βασικό σενάριο λειτουργίας περιλαμβάνει τη χρήση ενός κοινού δικτύου επικοινωνιών για την ανταλλαγή πληροφοριών μεταξύ έξυπνων μετρητών και υπεύθυνων του κέντρου ελέγχου, την εξαπόλυση επίθεσης Άρνησης Υπηρεσιών (DoS) από επιτιθέμενους προς ανυποψίαστους έξυπνους μετρητές, την εξυπηρέτηση κινούμενων χρηστών από απομακρυσμένους εξυπηρετητές του Διαδικτύου (Http, VideoStream) αλλά και από άλλους συνεργατικούς χρήστες (VideoStream).

Λέξεις Κλειδιά

Έξυπνο δίκτυο, έξυπνοι μετρητές, κίνδυνοι, επιθέσεις, ασφάλεια, προστασία προσωπικών δεδομένων, κρυπτογραφία, ασύρματες συνεργατικές επικοινωνίες.

ABSTRACT

The smart grid is attempting to modernize the existing antiquated electricity grid system. The beneficial features of the smart grid, whose main representative is the smart meter, contribute to the optimal use of electricity in both the production side and consumption side. Introducing the new communications and information technologies at key points in the network achieved the integration of renewable energy and the energy consumer in the scenario of operation of the smart grid.

However, integration of new technologies, especially those related to the Internet, may introduce new security threats to the smart grid. Some malicious attackers can exploit the vulnerabilities of network communications and seize electronic devices, steal confidential personal information or to prohibit the availability of essential services, causing a widespread power outage, resulting in adverse economic costs.

For this reason, addressing safety issues in smart grid plays a key role. The confidentiality, integrity and availability of mobile information need to be protected so as to increase system reliability. Data encryption is an effective measurement solution, and the protection of personal consumer information with the innovative load management system "ElecPrivacy".

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

Finally, the operation of the smart grid is simulated using the simulation environment OMNET++. The baseline operation involves the use of a common communications network for exchanging information between smart meters and responsive control center, launching denial of service attack (DoS) from attackers to unsuspecting smart meters, serving mobile users by remote Internet servers (Http, VideoStream) and other collaborative users (VideoStream).

Key Words

Smart grid, smart meters, risks, attacks, security, privacy, cryptography, wireless cooperative communications.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ-ΓΡΑΦΗΜΑΤΩΝ

ΠΙΝΑΚΕΣ

ΓΡΑΦΗΜΑΤΑ

1. Το έξυπνο δίκτυο (smart grid) και οι υπηρεσίες του (services)

1.1. Ορισμός ηλεκτρικού δικτύου (electric power grid) και η λειτουργία του

Το σύστημα δικτύου ηλεκτρικής ισχύος συνδέει την παραγωγή ηλεκτρικής ισχύος, όπως εργοστάσια παραγωγής ισχύος από ορυκτά καύσιμα, και τους καταναλωτές ηλεκτρικής ισχύος. Η βασική λειτουργία του ηλεκτρικού δικτύου ισχύος είναι να διανέμει το ηλεκτρικό ρεύμα με οικονομικό τρόπο ανταποκρινόμενο στους περιορισμούς χωρητικότητας και αξιοπιστίας του εξοπλισμού ηλεκτρικής ισχύος και των γραμμών ηλεκτρικής ισχύος. Το σύστημα δικτύου ηλεκτρικής ισχύος περιλαμβάνει δύο μέρη- μετάδοση και διανομή. Η μετάδοση είναι το μεγαλύτερο μέρος μεταφοράς ηλεκτρικού ρεύματος, που λειτουργεί σε υψηλή τάση(100 kV ή και παραπάνω) και διανέμει την ηλεκτρική ισχύ από τα εργοστάσια παραγωγής ισχύος προς τους υποσταθμούς που βρίσκονται κοντά σε κατοικημένες περιοχές. Η διανομή διανέμει το ηλεκτρικό ρεύμα από τους υποσταθμούς προς τους τελικούς καταναλωτές, όπως εμπορικούς, βιομηχανικούς και αστικούς καταναλωτές, λειτουργώντας σε μεσαία και χαμηλά επίπεδα τάσης(λιγότερα από 100 kV).

1.2. Το ξεπερασμένο ηλεκτρικό δίκτυο και η εξέλιξη της τεχνολογίας

Η βαθμιαία αύξηση της κατανάλωσης οδήγησε σε αύξηση της ζήτησης και σαν αποτέλεσμα και της παραγωγής. Το σύστημα αναγκάστηκε να λειτουργεί πιο κοντά στα όριά του λόγω οικονομικών και περιβαλλοντικών περιορισμών και οι γραμμές μεταφοράς ηλεκτρικού ρεύματος στη μέγιστη χωρητικότητά τους. Συνέπεια αυτού του γεγονότος ήταν να συμβαίνουν αρκετές και πολύωρες διακοπές της τάσης λόγω υπερφόρτωσης των γραμμών.

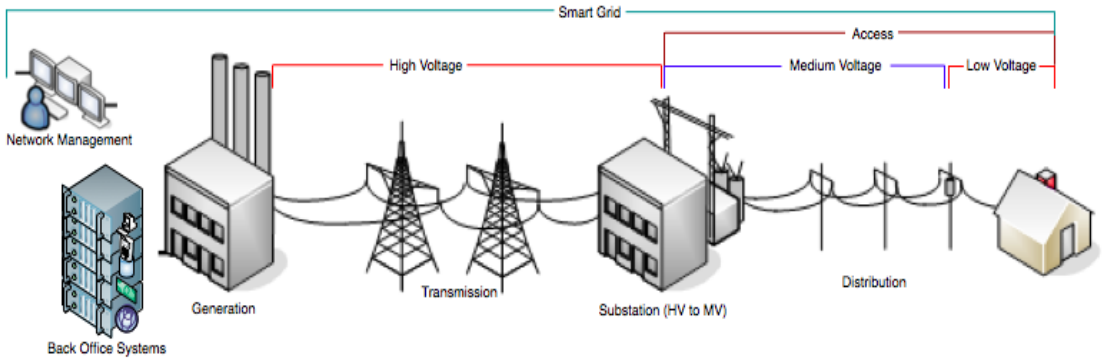
Επίσης, η δομή των επικοινωνιών που υπάρχει αυτή τη στιγμή σχεδιάστηκε για να ανταποκριθεί στις ανάγκες της βιομηχανίας που χρονολογείται αρκετές δεκαετίες πριν. Τα δίκτυα επικοινωνιών στα ηλεκτρικά δίκτυα σχεδιάστηκαν για να υποστηρίξουν λειτουργίες ελέγχου και επικοινωνίες δεδομένων μεταξύ των κέντρων ελέγχου και των υποσταθμών μόνο. Τα συστήματα SCADA είχαν τη δυνατότητα να μετρούν τάση, θερμοκρασία καλωδίων, κατάσταση ασφαλειών και να εκτελούν εντολές να ανοίξουν ή να κλείσουν ασφάλειες.

Η αξιοπιστία του συστήματος προς τους πελάτες μειωνόταν συνεχώς, το ίδιο και η απόδοσή του. Το σύστημα έπρεπε να έχει τη δυνατότητα να ανταποκρίνεται άμεσα στις συνεχώς αυξανόμενες επιθυμίες, στην ανεπάρκεια αποθεμάτων ή στις σοβαρές έκτακτες ανάγκες. Ήταν πασιφανές πως το υπάρχον ηλεκτρικό δίκτυο ισχύος έπρεπε να εκσυγχρονιστεί και να μεταβληθεί ο τρόπος διαχείρισής του για να προσφέρει την καλύτερη δυνατή εξυπηρέτηση.

Παράλληλα, η ραγδαία εξέλιξη της τεχνολογίας ερχόταν σε αντιδιαστολή με το πεπαλαιωμένο ηλεκτρικό δίκτυο. Οι τεράστιες δυνατότητες των προσωπικών υπολογιστών, τα Microsoft Windows, τα πρωτόκολλα επικοινωνίας TCP/IP/Ethernet, η εξάλειψη της καθυστέρησης μετάδοσης και η αύξηση του εύρους ζώνης, η ψηφιακή τεχνολογία, οι οπτικές ίνες, η ασύρματη τεχνολογία, τα πρότυπα ZigBee, Wi-Fi, WiMAX, δημιούργησαν σκέψεις για αποτελεσματική εκμετάλλευσή τους στον τομέα της ηλεκτρικής ισχύος. Επίσης, οι γραμμές ηλεκτρικού ρεύματος, με τις πανταχού

παρούσες πρίζες, έχει γίνει ένα πολύ επιθυμητό μονοπάτι ενσύρματων επικοινωνιών στο σπίτι, προσφέροντας υψηλή ταχύτητα και ποιότητα επικοινωνιών (PLC—Power Line Communications).

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



Εικόνα 1-1 Δίκτυο ηλεκτρικής ισχύος

1.3. Συστήματα SCADA

Τα συστήματα Ελέγχου Επιτήρησης και Απόκτησης Δεδομένων (SCADA) χρησιμοποιούνται για έλεγχο και παρακολούθηση λειτουργιών βιομηχανικής και κρίσιμης υποδομής, όπως ηλεκτρικό ρεύμα, φυσικό αέριο, νερό, απορρίμματα και απόβλητα, σιδηροδρόμους και κυκλοφοριακής κίνησης.

Τα πρώτα πρωτόκολλα επικοινωνιών αυτών των συστημάτων δημιουργήθηκαν πάνω στην τεχνολογία των τηλεφωνικών γραμμών και είχαν ως στόχο να διασφαλίσουν την ασφάλεια των εντολών ελέγχου. Σήμερα, αυτά τα συστήματα μετακινήθηκαν προς τις ψηφιακές επικοινωνίες και τη χρήση μεθόδων με χρήση bits για τον έλεγχο λαθών

Σε κάθε σπίτι, ο έξυπνος μετρητής συλλέγει τα δεδομένα κατανάλωσης ηλεκτρικής ενέργειας από όλες τις οικιακές συσκευές του σπιτιού και τα στέλνει στο τοπικό γραφείο διεύθυνσης της εταιρίας παρόχου. Αυτά τα δεδομένα συναθροίζονται και προωθούνται στο διαχειριστή παροχής του συστήματος SCADA. Με αυτή την πληροφορία, ο διαχειριστής παροχής του συστήματος SCADA μπορεί να παρακολουθήσει ολόκληρο το έξυπνο δίκτυο και να ελέγξει την κατάστασή του. Έπειτα, έχει τη δυνατότητα να προσαρμόσει την παραγωγή, τη μεταφορά και τη διανομή ισχύος για βέλτιστη ποιότητα ισχύος, να εξομαλύνει τη μέγιστη ζήτηση και να αποφύγει πιθανές διακοπές ρεύματος στην πλευρά του παρόχου.

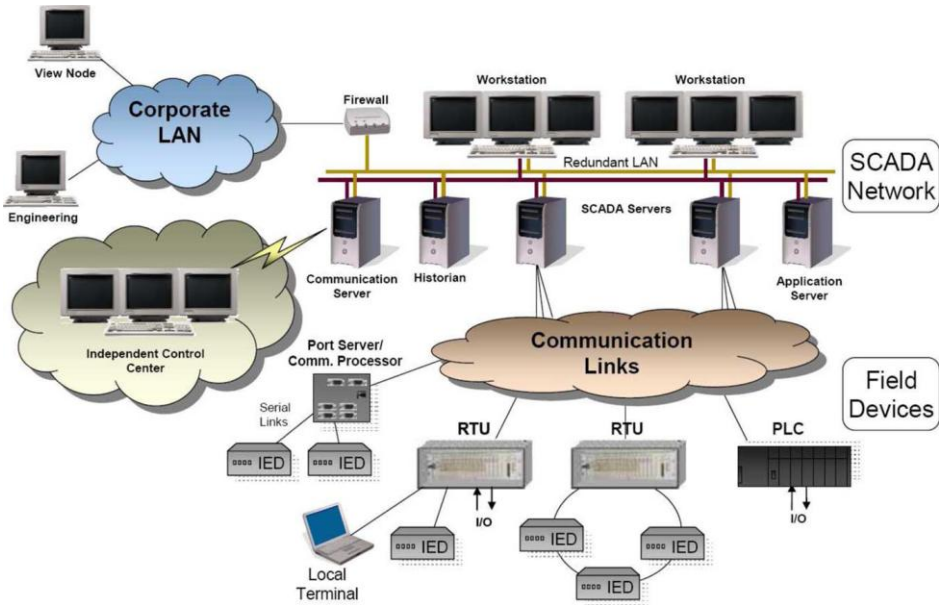
Αυτά τα μηνύματα διαχείρισης πραγματικού χρόνου θα διανεμηθούν στους καταναλωτές και πάλι μέσω των έξυπνων μετρητών. Με αυτό τον τρόπο, οι έξυπνες οικιακές συσκευές αναπρογραμματίζουν τις εργασίες τους και τις περιόδους λειτουργίας τους σύμφωνα με τις οδηγίες των συστημάτων SCADA.

Το ηλεκτρικό δίκτυο βασίζεται σε μεγάλο βαθμό σε αυτά τα συστήματα. Στην κορυφή της υποδομής ισχύος, τοποθετούνται τα στρώματα της τεχνολογίας

πληροφορικής και επικοινωνιών, τα οποία διασυνδέονται με τα ηλεκτρικά δίκτυα. Αυτές οι τεχνολογίες έχουν εξελίξει τα ηλεκτρικά δίκτυα από απομονωμένες δομές σε ανοιχτά και δικτυωμένα περιβάλλοντα βασισμένα σε Ethernet και TCP/IP.

Οι υψηλές ταχύτητες, οι μετρήσεις και η ανάλυση δεδομένων σε πραγματικό χρόνο είναι ουσιαστικά ζητήματα για την επιτυχία μιας καλής ορατότητας του τεράστιου δικτύου ηλεκτρικής ισχύος και παροχή καθ όλη τη διάρκεια διασυνδέσεις. Συγχρονισμένες μετρήσεις από γεωγραφικά διασκορπισμένες τοποθεσίες μέσα σε μια τεράστια περιοχή δίνουν τη δυνατότητα για καλύτερη λειτουργική ενημερότητα της κατάστασης πραγματικού χρόνου του δικτύου και επιτρέπει στους διαχειριστές να λαμβάνουν σωστότερες αποφάσεις.

Οι μονάδες μέτρησης φασιθέτη (PMU), που αναπτύχθηκαν στις αρχές του 1990, ήταν ανάμεσα στις πρώτες συσκευές που μπορούσαν να παρακολουθήσουν το δίκτυο με συγχρονισμένο τρόπο και να παράγουν συντονισμένες μετρήσεις φασιθετών. Ένα ρολόι GPS ήταν η χρονική στιγμή αναφοράς για τις συγχρονισμένες μετρήσεις. Ο ρυθμός δειγματοληψίας αυτών των μονάδων κυμαίνεται από 30 δείγματα το δευτερόλεπτο έως 120 δείγματα το δευτερόλεπτο. Ακόμη και το κατώτατο όριο ρυθμού δειγματοληψίας, 30 δείγματα το δευτερόλεπτο, είναι μια τάξη μεγέθους μεγαλύτερο από το ρυθμό δειγματοληψίας των συστημάτων SCADA. Αυτό το γεγονός καθιστά τις μονάδες μέτρησης φασιθετών την ιδανική συσκευή παρακολούθησης WAMS.



Εικόνα 1-2 Σύστημα SCADA

1.4. Τα χαρακτηριστικά του έξυπνου δικτύου (smart grid)

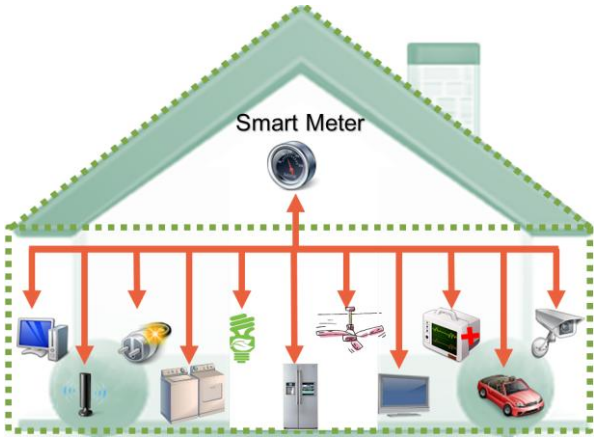
Το έξυπνο ηλεκτρικό δίκτυο θεωρείται ως ο εκσυγχρονισμός του υπάρχοντος ηλικιωμένου συστήματος ηλεκτρικής ισχύος. Αποτελεί το σημείο σύγκλισης της πληροφορικής, των επικοινωνιών και των συστημάτων ισχύος με σκοπό να δημιουργήσει ένα πιο στιβαρό, αποτελεσματικό και ευέλικτο δίκτυο ηλεκτρικής ισχύος.

Η ιδέα του έξυπνου δικτύου υπόσχεται στον κόσμο μια αποτελεσματική και ευφυή προσέγγιση διαχείρισης της προμήθειας και κατανάλωσης ηλεκτρικής ενέργειας. Το έξυπνο δίκτυο μπορεί να πάρει έξυπνες αποφάσεις για να διατηρήσει την ισορροπία στο ηλεκτρικό δίκτυο. Οι καταναλωτές και οι προμηθευτές ενέργειας μπορούν να επωφεληθούν από την πρακτικότητα, την ευκολία, τη φιλικότητα προς το περιβάλλον, την αξιοπιστία, την ασφάλεια και την εξοικονόμηση ενέργειας που θα παρέχεται μέσω της διαχείρισης ενέργειας σε πραγματικό χρόνο.

Ένα από τα πλεονεκτήματα του έξυπνου δικτύου είναι η εγκατάσταση ενός εντελώς καινούριου, αμφίδρομου δικτύου επικοινωνιών μεταξύ των προμηθευτών ενέργειας και των πελατών τους. Αυτό το γεγονός του επιτρέπει να συγκεντρώνει και να αναλύει τα δεδομένα σε κάθε επίπεδο σε πραγματικό χρόνο και να βοηθάει στην ισορροπία παραγωγής και ζήτησης. Επίσης, η ικανότητα επικοινωνίας σε πραγματικό χρόνο θα δώσει τη δυνατότητα στους παρόχους να βελτιστοποιήσουν και να εκσυγχρονίσουν το δίκτυο ηλεκτρικής ισχύος και να κατανοήσουν τις πλήρεις δυνατότητές του. Αυτό το δίκτυο επικοινωνιών θα παρέχει:

- αυτόνομη ανάρρωση δικτύου
- τιμολόγηση πραγματικού χρόνου
- διαχείριση κατανάλωσης και προγραμμάτων απόκρισης ζήτησης
- απομακρυσμένος έλεγχος έξυπνων οικιακών συσκευών μέσω έξυπνων μετρητών
- εξοικονόμηση κόστους από τη μείωση του φορτίου αιχμής
- αύξηση ενεργειακής απόδοσης και ποιότητας ισχύος
- ενσωμάτωση plug-in υβριδικών ηλεκτρικών οχημάτων για αποθήκευση ενέργειας
- ενσωμάτωση εναλλακτικών κατανεμημένων πηγών παραγωγής, όπως ανεμογεννήτριες και φωτοβολταϊκά συστήματα.

Ωστόσο, αυτές οι εφαρμογές και υπηρεσίες έχουν συγκεκριμένες επικοινωνιακές απαιτήσεις που δεν μπορούν να εκπληρωθούν από την υπάρχουσα υποδομή επικοινωνιών.



Εικόνα 1-3 Έξυπνο σπίτι

1.4.1. Αυτόνομη ανάρρωση δικτύου (self-healing)

Αυτόνομη ανάρρωση σημαίνει ότι το δίκτυο μπορεί να ανακατευθύνει και να αναπροσαρμόσει τη ροή του ηλεκτρικού ρεύματος στην περίπτωση που ένα μονοπάτι

μετάδοσης διακοπεί. Αυτό επιτυγχάνεται με συνεχή αυτοεκτίμηση της κατάστασης του συνολικού δικτύου. Σαν αποτέλεσμα μπορεί να μειωθεί η συχνότητα και η διάρκεια διακοπών ρεύματος.

1.4.2. Κατανεμημένη παραγωγή ενέργειας (distributed power generation)

Ένα από τα σημαντικά οφέλη του έξυπνου δικτύου είναι η εισαγωγή κατανεμημένων πηγών ενέργειας σε μεγάλη κλίμακα μες στο ηλεκτρικό δίκτυο. Αυτές οι κατανεμημένες πηγές ενέργειας θα έχουν τη δυνατότητα να προμηθεύουν συγκεκριμένες περιοχές με ηλεκτρικό ρεύμα όταν αυτές απομονώνονται από το κύριο δίκτυο χάρη σε αποτυχίες του συστήματος.

Αυτή τη στιγμή, το να παρέχεις ηλεκτρικό ρεύμα σε απομονωμένες περιοχές είναι εξαιρετικά δαπανηρό για το δίκτυο διανομής, αφού η πλειονότητα της ενέργειας που προορίζεται για τους πελάτες σπαταλείται σε θερμότητα πριν χρήσιμη ενέργεια φθάσει στον καταναλωτή. Σε αυτή την περίπτωση, οι κατανεμημένες πηγές ενέργειας αντιπροσωπεύουν μια φθηνότερη και αποτελεσματικότερη λύση που μπορεί να μεταδώσει ενέργεια από σημεία πιο κοντά στον καταναλωτή σε σχέση με το υπάρχον συγκεντρωμένο δίκτυο διανομής.

Επίσης, ενώ στο παραδοσιακό ηλεκτρικό δίκτυο, το ηλεκτρικό ρεύμα ρέει από τους κεντρικούς σταθμούς παραγωγής προς τους καταναλωτές, στο έξυπνο δίκτυο με την ενσωμάτωση των κατανεμημένων πηγών ενέργειας, το ηλεκτρικό ρεύμα ρέει προς δυο κατευθύνσεις. Έτσι, τα δίκτυα διανομής θα βρίσκονται πια σε συνεχή αλλαγή ροής ανάλογα με την κατεύθυνση και τις αλλαγές στην ποσότητα ροής ισχύος.

Για τη δημιουργία ενός τέτοιου ενεργού συστήματος ελέγχου, πρέπει να ελέγχεται συνεχώς η κατάσταση του δικτύου διανομής. Αισθητήρες θα πρέπει να αναπτυχθούν για να παρακολουθούν αποτελεσματικά την κατάσταση του δικτύου, όπως ελαττώματα στους μετασχηματιστές, κατάσταση των ασφαλειών, μέγεθος ροής ισχύος, κατευθύνσεις ροής ισχύος στις γραμμές διανομής.

Όλες αυτές οι αλλαγές θα οδηγήσουν στην αλλαγή της φιλοσοφίας ελέγχου, από το συγκεντρωμένο έλεγχο σε ένα πιο κατανεμημένο έλεγχο του ηλεκτρικού δικτύου.

1.4.3. Από συγκεντρωμένες σε κατανεμημένες επικοινωνίες (centralized to distributed communications)

Τα κληρονομημένα συστήματα ελέγχου του ηλεκτρικού δικτύου αποτελούνται από συσκευές ελέγχου που ονομάζονται απομακρυσμένες τερματικές μονάδες(RTUs: Remote Terminal Units). Αυτά τα συστήματα βασίζονται στην ιδέα του αφέντη RTU και των ενσύρματα συνδεδεμένων σε αυτόν σκλάβων του RTUs, αναφέροντας τις μετρήσεις τους περιοδικά.

Η κύρια διαδικασία επικοινωνίας αυτής της συγκεντρωμένης ιεραρχικής οργάνωσης είναι η αποστολή των μετρήσεων των σκλάβων RTUs στον αφέντη τους RTU και η δυνατότητα του αφέντη RTU να στέλνει εντολές στους σκλάβους του. Αυτή η κάθετη επικοινωνία δεν ταιριάζει με τις απαιτήσεις του κατανεμημένου ελέγχου του έξυπνου δικτύου.

Χρειάζεται μια πιο ευέλικτη και οριζόντια ανταλλαγή δεδομένων ανάμεσα στους ελεγκτές και τα RTUs μαζί με την κάθετη επικοινωνία—χωρίς να είναι απαραίτητα ενσύρματη. Νέα πρωτόκολλα επικοινωνίας θα πρέπει να δώσουν τη δυνατότητα ομαδικών ελέγχων των RTUs και όχι ατομικά, να παρέχουν λειτουργικότητες όπως

δρομολόγηση δεδομένων, μονοεκπομπή(unicasting), ευρυεκπομπή(broadcasting), πολυεκπομπή(multicasting) και άλλα.

1.4.4. Plug-in ηλεκτρικά υβριδικά οχήματα

Τα οχήματα αποτελούν μέρος της καθημερινής μας ζωής και αντιπροσωπεύουν ένα σημαντικό παράγοντα της παγκόσμιας ενεργειακής κατανάλωσης και περιβαλλοντικής μόλυνσης. Αντίθετα, τα plug-in ηλεκτρικά υβριδικά ηλεκτρικά οχήματα περιορίζουν τις εκπομπές CO2 και μειώνουν το κόστος μεταφοράς.

Αν και αυτού του τύπου τα οχήματα δεν έχουν υιοθετηθεί σε μεγάλη κλίμακα, η μελέτη φόρτισης αυτών των οχημάτων είναι σε προχωρημένο στάδιο. Για παράδειγμα, όταν ένα plug-in ηλεκτρικό υβριδικό ηλεκτρικό όχημα προσπαθεί να φορτίσει τη μπαταρία του, ένα σύστημα οικιακής ενεργειακής διαχείρισης θα μπορούσε να καθυστερήσει ή ακόμα και να αρνηθεί τη διαδικασία φόρτισης εάν υπάρχει μεγάλη ζήτηση στο δίκτυο.

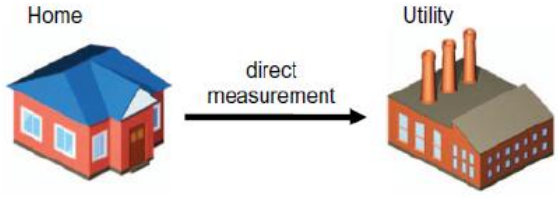
1.4.5. Έξυπνοι μετρητές (smart meters)

Το έξυπνο δίκτυο αποτελείται από συστήματα αισθητήρων, επικοινωνιών, ελέγχου και ενεργοποίησης που δίνουν τη δυνατότητα διεισδυτικής παρακολούθησης και ελέγχου του δικτύου ηλεκτρικής ισχύος. Εκατομμύρια έξυπνες συσκευές μέτρησης, αναπτυσσόμενες σε μια περιοχή, μπορούν να δώσουν τη δυνατότητα στους παρόχους να αλληλεπιδρούν με τους καταναλωτές. Αυτοί οι έξυπνοι μετρητές εγκαθίστανται στη μεριά του καταναλωτή και αποτελούν την ψηφιακή-ηλεκτρονική έκδοση των υπαρχόντων μετρητών κατανάλωσης ισχύος. Παίζουν ζωτικό ρόλο στην υποδομή του έξυπνου δικτύου και μετατρέπουν το δίκτυο ηλεκτρικού ρεύματος σε αξιόπιστο και αποτελεσματικό, αφού μπορούν να:

- παρακολουθούν τη λεπτομερή κατανάλωση ενέργειας σε πραγματικό χρόνο και επεμβαίνουν σε έκτακτες περιπτώσεις απόκρισης ζήτησης
- παρακολουθούν την ποιότητα ηλεκτρικής ισχύος
- υποστηρίζουν τα δίκτυα ιδιοκτητών HANs, κατεβάζοντας αυτόματα ενημερώσεις λογισμικού από το Διαδίκτυο
- παρέχουν στους πελάτες πληροφορίες πραγματικού χρόνου τιμολόγησης ενέργειας
- εκτελούν αυτόματο έλεγχο στις έξυπνες οικιακές συσκευές για να εξοικονομήσουν ενέργεια.

Με αυτό τον τρόπο, αποφεύγεται το χειροκίνητο διάβασμα του μετρητή, δρομολόγια υπηρετικού προσωπικού για συνδέσεις ή αποσυνδέσεις υπηρεσιών, διακοπής ρεύματος και αποκατάστασης και άλλες λειτουργίες.

Επιπλέον, η χρήση των αμφίδρομων επικοινωνιών επιτρέπει στους παρόχους να στέλνουν σήματα τιμολόγησης για να ενημερώσουν τους πελάτες για κρίσιμες περιόδους αύξησης της τιμολόγησης της ενέργειας. Τα σήματα τιμολόγησης πραγματικού χρόνου θα δώσουν τη δυνατότητα στους πελάτες να διαχειριστούν την χρησιμοποίηση ενέργειας πιο αποτελεσματικά και θα ενθαρρύνουν τους πελάτες να κάνουν συντήρηση και εξοικονόμηση ενέργειας, εξοικονομώντας παράλληλα και χρήματα από το λογαριασμό που θα πληρώσουν.



Εικόνα 1-4 Άμεση δρομολόγηση μετρήσεων

Το δίκτυο επικοινωνιών που αναπτύσσεται για να διευκολύνει την ανταλλαγή των πληροφοριών ανάμεσα στους παρόχους και τους καταναλωτές είναι το εξής:

Οι έξυπνοι μετρητές των νοικοκυριών (δίκτυο HAN) που βρίσκονται στην ίδια γειτονιά, εξοπλισμένοι με διεπιφάνειες επικοινωνίας, συνδέονται με ένα συλλέκτη δεδομένων, δημιουργώντας το δίκτυο NAN. Ο συλλέκτης δεδομένων συνδέεται σε ένα μεγαλύτερο δίκτυο WAN, ώστε να μεταφέρει τα δεδομένα στην εφαρμογή διαχείρισης δεδομένων του κέντρου ελέγχου.

Ακόμη, τα δίκτυα επικοινωνιών που είναι χτισμένα σε παλιές τεχνολογίες, όπως τηλεφωνικές γραμμές, έχουν στενό εύρος ζώνης. Αντίθετα, απαιτείται μεγάλο εύρος ζώνης που θα μπορεί να αντιμετωπίσει τον τεράστιο όγκο δεδομένων που συνεχώς θα ανταλλάσσεται.

1.5. Αρχιτεκτονική δικτύου και ασύρματη τεχνολογία

1.5.1. Πρότυπα ασύρματης τεχνολογίας (wireless technology standards)

Τα πρότυπα που είναι κατάλληλα για την ασύρματη τεχνολογία είναι τα εξής:

- Το πρότυπο IEEE 802.15.4 ZigBee, χαμηλού κόστους και χαμηλής ισχύος, μπορεί ευρέως να αναπτυχθεί και να χρησιμοποιηθεί. Έχει τρεις ζώνες συχνοτήτων: 868-868.6 MHz με 1 κανάλι για Ευρωπαϊκές παροχές, 902-928 MHz με 10 κανάλια για παροχές Β.Αμερικής, και 2.4 GHz με 16 μη επικαλυπτόμενα κανάλια για παγκόσμιες παροχές. Η ακτίνα κάλυψής του φτάνει τα 150 m.
- Το πρότυπο IEEE 802.11n Wi-Fi μπορεί να προσφέρει γρηγορότερες ταχύτητες μετάδοσης δεδομένων και δεν είναι πια απαγορευτικό λόγω κόστους. Μοιράζεται την ίδια ζώνη συχνοτήτων με το πρότυπο 802.15.4 ZigBee στο φυσικό στρώμα. Ο αριθμός των μη επικαλυπτόμενων καναλιών είναι 23. Η ακτίνα κάλυψής του φτάνει τα 250 m.
- Το πρότυπο IEEE 802.16 WiMAX μπορεί να παρέχει χαμηλό κόστος και απομακρυσμένες επικοινωνίες μες στο ασύρματο δίκτυο. Η ακτίνα κάλυψής του φτάνει τα 3 km.

1.5.2. Αρχιτεκτονική δικτύου (network architecture)

Η αρχιτεκτονική δικτύου αποτελείται από 3 στρώματα:

- Home Area Network (HAN), το οποίο αποτελείται από τον έξυπνο μετρητή που καταγράφει την κατανάλωση ενέργειας της οικίας και ένα

εξάρτημα που παρέχει κόστος ενέργειας πραγματικού χρόνου και δεδομένα κατανάλωσης προς τους καταναλωτές.

- Neighborhood Area Network (NAN), το οποίο είναι ένα μεγαλύτερο δίκτυο μετρήσεων και ελέγχου που συλλέγει τις μετρήσεις και τις πληροφορίες εξυπηρέτησης από τα πολλαπλά HANs που είναι γεωγραφικά κοντά μεταξύ τους. Επίσης αποτελείται από ελεγκτή κεντρικής πρόσβασης και το συλλέκτη δεδομένων από έξυπνους μετρητές. Ο ελεγκτής κεντρικής πρόσβασης μπορεί να θεωρηθεί ως η διεπαφή που διαχειρίζεται την επικοινωνία ανάμεσα στα HANs και τον προμηθευτή ενέργειας. Τέλος, ο συλλέκτης δεδομένων από έξυπνους μετρητές είναι ο ασύρματος κόμβος που έχει την ευθύνη της καταγραφής των μετρήσεων ολόκληρης της κοινότητας που συνθέτουν τα γειτονικά HANs.
- Wide Area Network (WAN), το οποίο παρέχει ευρυζωνικές ενσύρματες ή ασύρματες επικοινωνίες ανάμεσα στο NAN, τους υποσταθμούς και τον προμηθευτή. Επίσης αποτελείται από το σύστημα κατανομής ενέργειας και τον ελεγκτή SCADA. Το σύστημα κατανομής ενέργειας είναι υπεύθυνο για την κατανομή της ηλεκτρικής ενέργειας και των μετρήσεων. Ο ελεγκτής SCADA παρέχει στον προμηθευτή έλεγχο κατανομής για να διαχειρίζεται τα διάφορα στοιχεία του έξυπνου δικτύου.

1.5.3. Απαιτήσεις αρχιτεκτονικής και επιλογή προτύπων (standards)

Για να θεωρηθεί το έξυπνο δίκτυο επιτυχημένο, απαιτείται συνεργασία, ενοποίηση και διαλειτουργικότητα (interoperability) ανάμεσα στα διάφορα είδη τεχνολογίας.

Έτσι, για την επιλογή των βέλτιστων προτύπων δικτύου του δικτύου επικοινωνιών του έξυπνου δικτύου, θα πρέπει να προσδιοριστούν οι απαιτήσεις των διαφορετικών στρωμάτων της δεδομένης αρχιτεκτονικής δικτύου.

Στα δύο χαμηλότερα στρώματα HAN και NAN, οι απαιτήσεις περιλαμβάνουν υψηλή χωρητικότητα δικτύου και υψηλό ρυθμό μετάδοσης δεδομένων. Στο τρίτο στρώμα WAN, η κύρια απαίτηση είναι η σταθερότητα και η αξιοπιστία του δικτύου επικοινωνιών.

- Στο HAN, το πρότυπο δικτύου που επιλέγεται είναι το 802.15.4 ZigBee, που παρέχει ραδιοεπικοινωνίες ειδικά κατάλληλες για δίκτυα προσωπικής και οικιακής περιοχής. Η ζώνη συχνοτήτων των 2.4 GHz επιλέγεται επειδή υποστηρίζει εναέριο ρυθμό μετάδοσης δεδομένων 250 kbps που είναι υψηλότερος των ρυθμών μετάδοσης των δυο άλλων ζωνών συχνοτήτων. Αυτή η ζώνη συχνοτήτων έχει επίσης 16 κανάλια. Η μέγιστη ασύρματη χωρητικότητα μιας ζεύξης δεδομένων υπό το πρότυπο 802.15.4 ZigBee προκύπτει 4 Mbps.
- Στο NAN, το πρότυπο δικτύου που επιλέγεται είναι το 802.11n Wi-Fi, το οποίο συγκρινόμενο με άλλα πρότυπα Wi-Fi, προσφέρει το μεγαλύτερο εναέριο ρυθμό μετάδοσης δεδομένων 300 Mbps στη ζώνη συχνοτήτων των 2.4 GHz. Παρέχοντας 23 μη επικαλυπτόμενα κανάλια, η μέγιστη ασύρματη χωρητικότητα μιας ζεύξης δεδομένων υπό το πρότυπο 802.11n Wi-Fi προκύπτει 6900 Mbps.
- Στο WAN, το πρότυπο δικτύου που επιλέγεται είναι το 802.16 WiMAX. Ο σημαντικότερος λόγος είναι ότι παρέχει επικοινωνίες σε απόσταση έως και 3 km. Επίσης υποστηρίζει εναέριο ρυθμό μετάδοσης δεδομένων 70 Mbps.

1.6. Μηχανισμοί επικοινωνίας M2M

Το έξυπνο δίκτυο αποτελείται από πολλά εξελιγμένα αυτοματοποιημένα με κρίσιμες στιγμιαίες αποφάσεις και αυτόνομου ελέγχου χαρακτηριστικά. Σημαντικά συστατικά για τέτοιου τύπου αυτοματισμούς αποτελούν οι μηχανισμοί επικοινωνίας M2M(machine-to-machine), οι οποίοι συνδέουν αδιάκοπα σημεία μετρήσεων και ελέγχου με κάποια έξυπνη μηχανή απόφασης. Μια τυπική εφαρμογή είναι η χρήση μετρητών σαν σημεία μέτρησης, διακοπτών σαν σημεία ελέγχου και το κέντρο ελέγχου του παρόχου σαν σημείο αποφάσεων.

Τα πλεονεκτήματα που προσφέρει η παραπάνω εφαρμογή είναι η παρακολούθηση του δικτύου και του φορτίου του σε πραγματικό χρόνο. Με αυτό τον τρόπο, διακοπές και λάθη μπορούν να εντοπιστούν και να αντιμετωπιστούν με την ελάχιστη καθυστέρηση. Επίσης, ο τελικός καταναλωτής έχει τη δυνατότητα να προγραμματίζει τη λειτουργία των ηλεκτρικών συσκευών του όταν το κόστος ενέργειας, για το οποίο ενημερώνεται συνεχώς, είναι φθηνότερο.

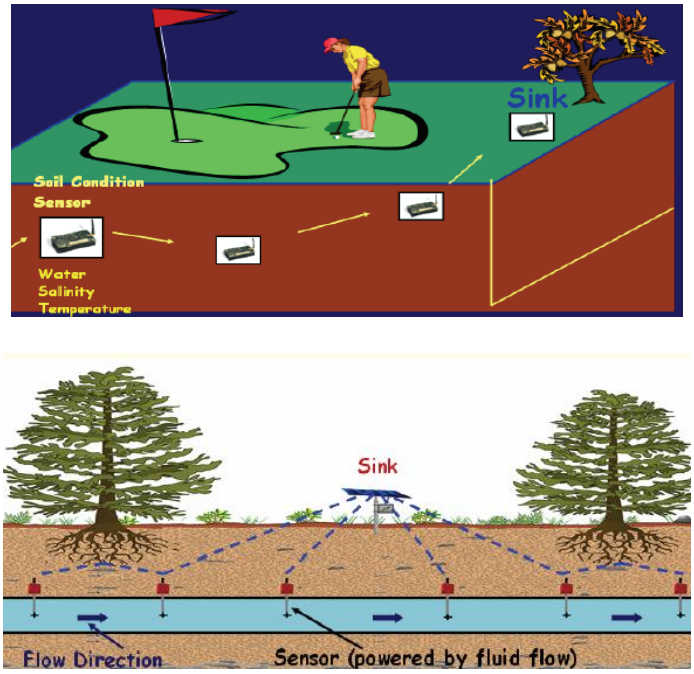
Τα ασύρματα συστήματα επικοινωνίας παίζουν σημαντικό ρόλο στην πραγματοποίηση αυτής της εφαρμογής. Ενσωματωμένες κεραίες εγκαθίστανται σε κάθε σημείο ελέγχου ή μέτρησης, τα οποία σημεία επικοινωνούν ασύρματα μεταξύ τους. Επίσης όλα αυτά τα σημεία περιέχουν μια ενσωματωμένη κάρτα SIM που τους επιτρέπει συνδεσιμότητα με σταθμό βάσης κινητής τηλεφωνίας.

Ωστόσο, αυτοί οι κόμβοι έχουν περιορισμένους πόρους, όπως ισχύ τροφοδοσίας, μνήμη και ισχύ επεξεργασίας. Το φάσμα που χρησιμοποιούν για να επικοινωνήσουν τείνει να γίνει σπάνιο. Το ασύρματο κανάλι επικοινωνίας αποτελεί μια πηγή αβεβαιότητας που οδηγεί σε λάθη πακέτων και επαναμεταδόσεις (retransmissions). Το ασύρματο κανάλι είναι broadcast εκ φύσεως και συνεπώς επιρρεπές σε ζητήματα ασφάλειας. Έτσι, το σύστημα χρειάζεται να γίνει περισσότερο ενεργειακά αποδοτικό και ασφαλές.

Για αύξηση της ενεργειακής αποτελεσματικότητας, ένα πρώτο βήμα είναι η χρήση συνάθροισης δεδομένων σε κάθε κόμβο, που συναθροίζει τα λαμβανόμενα πακέτα από τους κόμβους φύλλα του πριν προωθήσει το αθροισμένο πακέτο στον κόμβο πατέρα του.

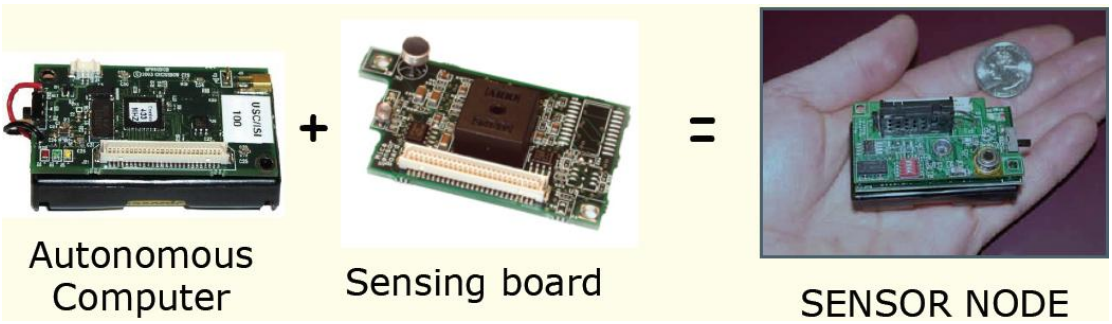
1.7. Ασύρματα δίκτυα αισθητήρων WSN (Wireless Sensor Networks)

Τα ασύρματα δίκτυα αισθητήρων αναπτύσσονται με τρομακτικό ρυθμό και προσελκύουν όλο και μεγαλύτερες περιοχές εφαρμογών, όπως γεωργία (παρακολούθηση αγροκτημάτων, συνθήκες καλλιέργειας (π.χ. θερμοκρασία, υγρασία), προμήθεια νερού και ηλεκτρικού ρεύματος), επιχειρήσεις, κρίσιμες υποδομές προστασίας, περιβάλλον (περιβαλλοντικές συνθήκες), ιατρική φροντίδα (παρακολούθηση τηλε-υγείας (tele-health monitoring), χορήγηση/ανίχνευση φαρμάκων), ασφάλεια οικίας, βιομηχανία (συλλογή επιπέδων μόλυνσης), στρατός (επιτήρηση συνόρων, εντοπισμός βιολογικών ή χημικών όπλων), έξυπνη μετακίνηση (intelligent transportation), παρακολούθηση βιομηχανίας, αυτοματισμούς στο σπίτι και άλλες. Η κυριότερη κοινή αδυναμία όλων των ασύρματων εφαρμογών και τεχνολογιών είναι τα ευάλωτα σημεία που παρουσιάζουν στις επιθέσεις/απειλές ασφάλειας, επηρεάζοντας την απόδοση και τη συμπεριφορά τους.



Εικόνα 1-5 Εφαρμογές WSN

Ένα ασύρματο δίκτυο αισθητήρων αποτελείται από έναν αριθμό μικρών κόμβων, εξοπλισμένων με αισθητήρες, οι οποίοι σε συνεργασία δημιουργούν ένα δίκτυο που μπορεί να εκτελέσει διάφορες εργασίες επικοινωνώντας ασύρματα ο ένας με τον άλλον. Επειδή μεταφέρουν ευαίσθητες πληροφορίες για την εξυπηρέτηση ποικίλων εφαρμογών, είναι αναγκαίο να προστατεύονται από διάφορες ηλεκτρονικές επιθέσεις.



Εικόνα 1-6 Η σύνθεση ενός κόμβου αισθητήρα

Οι κόμβοι αισθητήρων είναι συσκευές που λειτουργούν με μπαταρία(battery-powered) και έχουν περιορισμένες ικανότητες:

- Παρακολουθούν το περιβάλλον και μεταφέρουν αυτά τα δεδομένα σε γειτονικούς κόμβους
- Λειτουργούν και συνεργάζονται με ασύρματο τρόπο
- Επικοινωνούν άμεσα μόνο με γειτονικούς κόμβους
- Υποστηρίζουν πολλαπλά μονοπάτια επικοινωνίας
- Παρέχουν ικανότητες δρομολόγησης

Συγκρινόμενη με την παραδοσιακή ασφάλεια δικτύου, η ασφάλεια στα WSN είναι πιο περίπλοκη λόγω των υπολογιστικών περιορισμών των κόμβων και του αντικειμενικού στόχου τους να εξοικονομήσουν ενέργεια για να μεγιστοποιήσουν το χρόνο ζωής των ίδιων αλλά και του δικτύου. Το απρόβλεπτο και ανάξιο εμπιστοσύνης κανάλι επικοινωνίας καθώς και η ελλιπής παρακολούθηση λειτουργίας του καθιστούν την ασφάλεια στο WSN ακόμη δυσκολότερη.

2. Ζητήματα ασφάλειας στο έξυπνο δίκτυο

2.1. Κίνδυνοι που δημιουργούνται

Το έξυπνο δίκτυο πρόκειται να προσθέσει νέες λειτουργικότητες στο υπάρχον ηλεκτρικό δίκτυο. Ωστόσο, θα εισάγει και νέους κινδύνους στο σύστημα. Η καθημερινότητά μας βασίζεται στο ηλεκτρικό ρεύμα και η εξάρτησή μας αυτή κάνει το ηλεκτρικό δίκτυο ένα κρίσιμο ζήτημα. Η διακοπή του ηλεκτρικού ρεύματος θα έχει μεγάλες κοινωνικές συνέπειες. Το έξυπνο δίκτυο θα εισάγει νέους κινδύνους που σχετίζονται με τις απαιτούμενες επικοινωνίες, τα συστήματα αυτοματισμού και συλλογής δεδομένων.

Ο βασικός κορμός του έξυπνου δικτύου θα είναι το δίκτυο επικοινωνιών του. Το νέο δίκτυο επικοινωνιών θα κατασκευαστεί χρησιμοποιώντας διάφορα μονοπάτια επικοινωνίας, όπως οπτικές ίνες (fiber optics), ευρυζωνικότητα πάνω από γραμμές μεταφοράς ισχύος (BPL: Broadband over Power Line) και ασύρματες τεχνολογίες. Θα συνδέει τα διάφορα στοιχεία του έξυπνου δικτύου μεταξύ τους, επιτρέποντας αμφίδρομη επικοινωνία μεταξύ τους και αυξάνοντας την πολυπλοκότητά του.

Η ενσωμάτωση των τεχνολογιών φέρνει το απομονωμένο και κλειστό δίκτυο συστημάτων ελέγχου ισχύος στο κοινό-δημόσιο δίκτυο. Η γρήγορη εξάπλωση των νέων τεχνολογιών, ειδικά αυτών που σχετίζονται με το Διαδίκτυο, ίσως εισάγουν νέες απειλές στην ασφάλεια του έξυπνου δικτύου. Οι προχωρημένες τεχνικές προσφέρουν αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνουν όμως ταυτόχρονα σημαντικά τα προβλήματα τα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών. Εκτός των απειλών του κυβερνοχώρου, όπως malware, spyware, computer viruses, που αυτή τη στιγμή απειλούν τα δίκτυα υπολογιστών και επικοινωνιών, η εισαγωγή νέων και κατανεμημένων τεχνολογιών, όπως έξυπνοι μετρητές, αισθητήρες, άλλα υποδίκτυα και σημεία πρόσβασης μπορούν να δημιουργήσουν κι άλλα ευάλωτα σημεία ή ευπάθειες (vulnerabilities) στο έξυπνο δίκτυο.

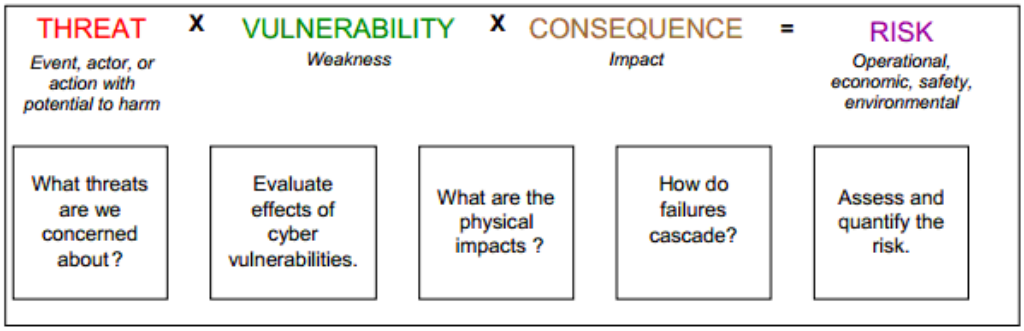
Ωστόσο, το έξυπνο δίκτυο θα εκτεθεί όχι μόνο σε νέους κινδύνους εξαιτίας των ευάλωτων σημείων του δικτύου επικοινωνιών, αλλά και σε κινδύνους που θα κληρονομηθούν από το υπάρχον ηλεκτρικό δίκτυο λόγων των φυσικών ευάλωτων σημείων αυτού.

Οι φυσικές επιθέσεις ίσως διακόψουν την παραγωγή, τη μεταφορά και τη διανομή της ηλεκτρικής ισχύος.

Οι επιθέσεις κυβερνοχώρου ίσως να επωφεληθούν την προσβασιμότητα μέσω των δικτύων HAN και NAN, προσπαθώντας να αποκτήσουν απομακρυσμένη πρόσβαση, να θέσουν σε κίνδυνο ή να ελέγξουν ηλεκτρονικές συσκευές.

Σαν κρίσιμη υποδομή, το έξυπνο δίκτυο αναμένεται να είναι ένας δελεαστικός στόχος για hacking, κλοπή υπηρεσιών, τρομοκρατίας και άλλων κακόβουλων επιθέσεων. Η ασφάλεια έχει αναγνωριστεί παγκόσμια ως ένα μείζον θέμα με πιθανώς καταστροφικές συνέπειες.

Τα τείχη προστασίας δεν εγγυώνται πλήρη ηλεκτρονική ασφάλεια, ακόμα και είναι τέλεια διαμορφωμένα. Αυτό συμβαίνει διότι δεν μπορούν να εντοπίσουν επιθέσεις που προέρχονται από μέσα και συνδέσεις μέσω της έμπιστης μεριάς.



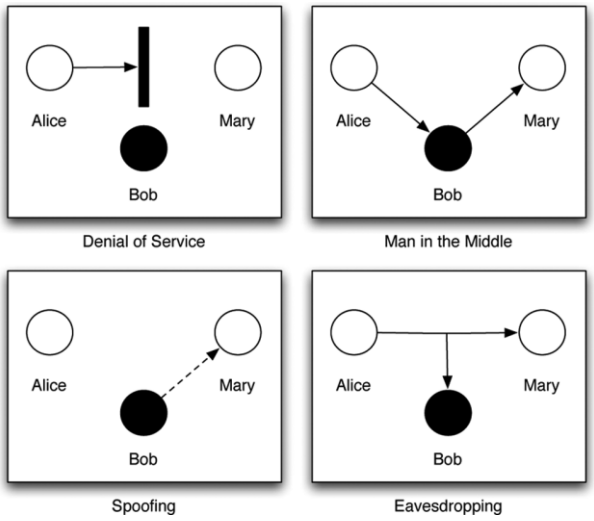
Εικόνα 2-1 Συντελεστές κινδύνου

2.2. Κατηγοριοποιήσεις επιθέσεων (attacks)

2.2.1. Βασικοί τύποι επιθέσεων

Υπάρχουν 4 βασικοί τύποι επιθέσεων:

1) *Denial-of-Service (DoS)*—είναι η επίθεση όπου ο επιτιθέμενος (Bob) αρνείται στην πηγή (Alice) την πρόσβαση στον προορισμό (Mary)(άρνηση παροχής υπηρεσιών).
2) *Man-in-the-middle*—είναι η επίθεση όπου ο Bob προσποιείται τη Mary, συνεπώς, λαμβάνει όλα τα μηνύματα από την Alice στη Mary. Ο Bob μπορεί να αλλάξει τα μηνύματα και να τα προωθήσει τροποποιημένα στη Mary.
3) *Spoofing*—είναι η επίθεση όπου ο Bob πλαστοπροσωπεί ως Alice, έτσι ώστε να μπορεί να δημιουργήσει και να στείλει μηνύματα στη Mary.
4) *Eavesdropping*—είναι η επίθεση όπου ο Bob λαμβάνει όλα τα μηνύματα που στέλνονται από την Alice στη Mary, αν και Alice και Mary δεν το γνωρίζουν (υποκλοπή συνομιλίας).



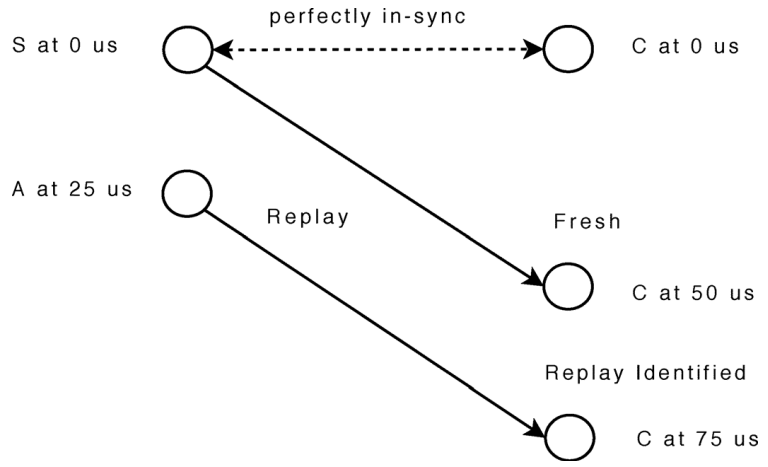
Εικόνα 2-2 Οι τέσσερις βασικοί τύποι επιθέσεων

2.2.1.1. Replay attack: συνδυασμένη επίθεση με αρχική χρήση Eavesdropping και τελικό σκοπό επίθεσης DoS

Τα ρολόγια πραγματικού χρόνου (real-time clocks) στους περισσότερους αισθητήρες χαμηλής ισχύος (π.χ. ZigBee wireless sensors) παρουσιάζουν μια φυσική ενδογενή ολίσθηση (drift) (ίσως και 1.7 s τη μέρα), η οποία δεν μπορεί να συγχρονιστεί με ακρίβεια για τον επαρκή έλεγχο του πρωτοκόλλου πιστοποίησης αυθεντικότητας (authentication protocol). Επίσης, καθώς το εύρος ζώνης (bandwidth) του δικτύου αυξάνει, τα μηνύματα απαιτούν λιγότερο χρόνο για μετάδοση και η ακρίβεια συγχρονισμού γίνεται ακόμα πιο αυστηρή. Αυτοί οι δύο παράγοντες καθιστούν την replay επίθεση πολύ πιθανή.

Στην Εικόνα 2-3, παρουσιάζεται ένα παράδειγμα όπου το replay μήνυμα ενός αντιπάλου (adversary) ορθώς αναγνωρίζεται ως χρονικά παλαιό (stale) όταν ο συλλέκτης (collector) και ένας αισθητήρας είναι τέλεια συγχρονισμένοι μεταξύ τους. Σε αυτή την εικόνα, S αντιπροσωπεύει έναν αισθητήρα, A αντιπροσωπεύει έναν αντίπαλο, C αντιπροσωπεύει ένα συλλέκτη. Σε αυτό το παράδειγμα, υποτίθεται ότι η από άκρη σε άκρη καθυστέρηση (end-to-end delay) του μηνύματος από τον S στον C είναι 50 μs. Όπως φαίνεται επίσης στην εικόνα, ένα μήνυμα μεταδίδεται από τον S τη χρονική στιγμή 0 μs και έχει μια χρονική σφραγίδα των 0 μs. Το μήνυμα φθάνει στον C τη χρονική στιγμή 50 μs. Επειδή το άθροισμα της χρονικής σφραγίδας των 0 μs συν την καθυστέρηση των 50 μs δεν είναι μικρότερο από τον τρέχοντα χρόνο (current time) στον C, ο C δηλώνει ότι το μήνυμα από τον S ως φρέσκο (fresh).

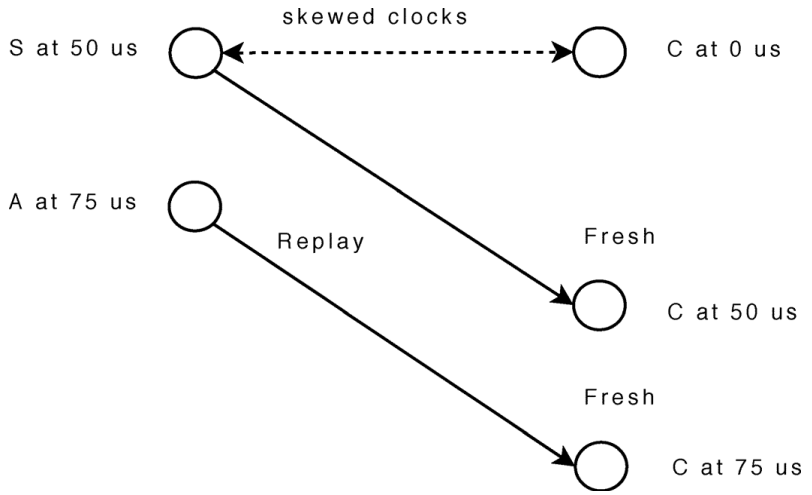
Τη χρονική στιγμή 25 μs, ο A εκδηλώνει μια replay επίθεση στέλνοντας το μήνυμα που έχει κρυφακούσει (eavesdropped message) από τον S, το οποίο έχει μια χρονική σφραγίδα των 0 μs. Υποθέτουμε ότι η από άκρη σε άκρη καθυστέρηση του μηνύματος από τον A στον C είναι επίσης 50 μs επειδή ο A είναι ανάγκη να βρίσκεται κοντά στον S για να κρυφακούει τα μηνύματα από αυτόν. Τότε, το replay μήνυμα φθάνει στον C τη χρονική στιγμή των 75 μs. Επειδή το άθροισμα της χρονικής σφραγίδας των 0 μs συν την καθυστέρηση των 50 μs είναι μικρότερο από τον τρέχοντα χρόνο στον C, ο C δηλώνει ότι το μήνυμα από τον S ως χρονικά παλαιό (stale). Έτσι, η replay επίθεση αποτυγχάνει.



Εικόνα 2-3 Αποτυχημένη replay επίθεση σε ένα τέλεια συγχρονισμένο δίκτυο

Στην Εικόνα 2-4, παρουσιάζεται ένα παράδειγμα όπου ο αντίπαλος A μπορεί να εκμεταλλευτεί την ολίσθηση του ρολογιού και να εκδηλώσει μια αποτελεσματική replay επίθεση, όταν το ρολόι ενός αισθητήρα S προηγείται του ρολογιού ενός συλλέκτη C κατά 50 μs. Όπως φαίνεται στην εικόνα αυτή, ένα μήνυμα μεταδίδεται από τον S τη χρονική στιγμή 50 μs (με αναφορά στο ρολόι του S) και περιλαμβάνει μια χρονική σφραγίδα των 50 μs. Το μήνυμα φθάνει στον C τη χρονική στιγμή των 50 μs (με αναφορά στο ρολόι του C). Επειδή το άθροισμα της χρονικής σφραγίδας των 50 μs συν την καθυστέρηση των 50 μs δεν είναι μικρότερο από τον τρέχοντα χρόνο στον C, ο C δηλώνει ότι το μήνυμα από τον S ως φρέσκο (fresh).

Τη χρονική στιγμή 75 μs (με αναφορά στο ρολόι του S), ο A εκδηλώνει μια replay επίθεση στέλνοντας το μήνυμα που έχει κρυφακούσει από τον S, το οποίο έχει μια χρονική σφραγίδα των 50 μs. Τότε, το replay μήνυμα φθάνει στον C τη χρονική στιγμή των 75 μs (με αναφορά στο ρολόι του C). Επειδή το άθροισμα της χρονικής σφραγίδας των 50 μs συν την καθυστέρηση των 50 μs δεν είναι μικρότερο από τον τρέχοντα χρόνο στον C, ο C δηλώνει ότι το μήνυμα από τον S ως φρέσκο. Έτσι, η replay επίθεση στέφεται με επιτυχία.



Εικόνα 2-4 Επιτυχημένη replay επίθεση σε ένα από-συγχρονισμένο δίκτυο

2.2.2. Επιθέσεις φυσικές, ηλεκτρονικές και συνδυασμός αυτών

1) *Φυσικές απειλές (physical)*—απαιτούν ειδικά εργαλεία και φυσική παρουσία. Οι γραμμές μεταφοράς μπορούν να υπονομευθούν οπουδήποτε κατά μήκος της γραμμής ή στον πύργο μεταφοράς. Οι γραμμές διανομής είναι τοποθετημένες σε σχετικά χαμηλό ύψος και μπορούν να διακοπούν εύκολα. Επίσης, οι έξυπνοι μετρητές είναι εξαιρετικά ευάλωτοι σε κλοπή αφού τοποθετούνται στις εγκαταστάσεις του πελάτη.
2) *Ηλεκτρονικές απειλές (cyber)*—μπορούν να εκτελεστούν από οποιοδήποτε υπολογιστή. Οι έξυπνοι μετρητές επικοινωνεί διασυνδέεται και με άλλους μετρητές μες στο δίκτυο NAN καθώς και με έξυπνες οικιακές συσκευές και συστήματα διαχείρισης ενέργειας μες στο δίκτυο HAN. Αυτές οι διασυνδέσεις αυξάνουν την έκθεση του έξυπνου δικτύου σε απομακρυσμένες απειλές, όπως παραβίαση της ιδιωτικής ζωής μέσω υποκλοπών και ανάλυσης κυκλοφορίας

δεδομένων, μη εξουσιοδοτημένη πρόσβαση σε αποθηκευμένα δεδομένα, επιθέσεις MITM και DoS, παρεμβολή ή τροποποίηση δικτύων επικοινωνιών.

3) *Συνδυασμένες απειλές (cyber-physical)*—απαιτούν συνδυασμένες γνώσεις αφού οι ηλεκτρονικές επιθέσεις μπορεί να έχουν φυσικές επιδράσεις και οι φυσικές επιθέσεις μπορεί να έχουν επίδραση στην ηλεκτρονική υποδομή. Για παράδειγμα, ένας δυσαρεστημένος ή παραπονεμένος υπάλληλος με άδεια εξουσιοδότησης στους υπολογιστές μπορεί να εισέλθει στο σύστημα ασφάλειας του υποσταθμού και να απενεργοποιήσει την περιμετρική ασφάλεια, ανοίγοντας το δρόμο για οποιαδήποτε φυσική επίθεση.

2.2.3. Κατηγοριοποίηση επιθέσεων σύμφωνα με το κίνητρο

Το κίνητρο των επιτιθέμενων μπορεί να κατηγοριοποιηθεί σε πέντε περιοχές:

1) περιέργεια για πληροφορία
2) υποκινούμενες επιθέσεις
3) ανήθικη κλοπή ενέργειας
4) κλοπή πληροφοριών κατανάλωσης ισχύος
5) οικονομικά οφέλη

External attack	Communi-cation attack	Intercept messages; launch DoS attacks to disable communication between system components.
	Component attack	Physical power equipment (generator or power lines) failure or damage.
Insider attack	Communi-cation attack	Modify or drop transmitted messages; inject false messages; delay message transmission.
	Component attack	Generate false events; control compromised system components to perform arbitrary tasks, such as coordinated attacks from multiple substations.

Εικόνα 2-5 Μορφές επιθέσεων

2.2.4. Κατηγοριοποίηση επιθέσεων σύμφωνα με τον αριθμό των επιτιθέμενων

Οι επιθέσεις μπορούν επίσης να αναλυθούν σε:

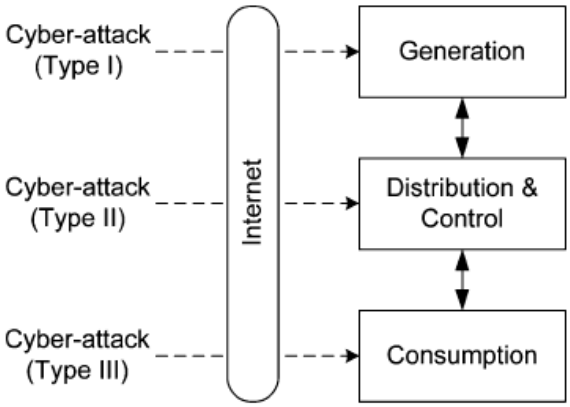
1) *ατομικές επιθέσεις (single or individual attacks)*—απομονωμένες επιθέσεις εκτελούμενες από ένα και μοναδικό άτομο. Αποτελεί πρόκληση η συλλογή όλων των απαραίτητων πληροφοριών και εργαλείων για να διαπράξει ένα μικρής κλίμακας blackout.
2) *οργανωμένες επιθέσεις (coordinated attacks)*—μελετημένες ομάδες επιτιθέμενων συνεργάζονται για να χτυπήσουν ομαδικά ένα κοινό στόχο, μια κρίσιμη υποδομή. Συνήθως στοχεύουν ένα σύνθετο αποτέλεσμα με επίδραση μεγαλύτερης κλίμακας από αυτή των ατομικών επιθέσεων. Χρησιμοποιούν μέσα όπως το Διαδίκτυο και άλλες σύγχρονες τηλεπικοινωνίες για να συντονίσουν ταυτόχρονες επιθέσεις από γεωγραφικά απομακρυσμένες περιοχές. Για παράδειγμα, ένας επιτιθέμενος μπορεί να κατεβάσει το γενικό διακόπτη ηλεκτρικής ισχύος σε ένα κτίριο, δημιουργώντας την ευκαιρία για

έναν άλλο επιτιθέμενο να εισβάλλει στο κτίριο χωρίς να ενεργοποιηθεί ο συναγερμός.

2.2.5. Κατηγοριοποίηση ηλεκτρονικών επιθέσεων σύμφωνα με το στόχο

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

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



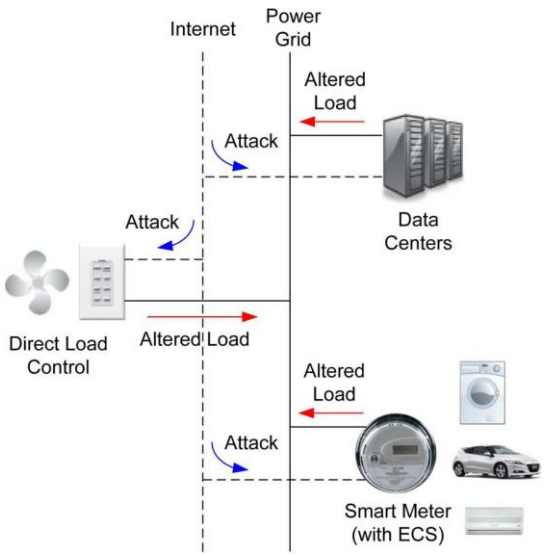
Εικόνα 2-6 Στόχοι ηλεκτρονικών επιθέσεων

2.2.6. Τύποι φορτίου προσβάσιμοι μέσω Διαδικτύου

Οι τύποι φορτίου που είναι προσβάσιμοι μέσω Διαδικτύου είναι τρεις:

1) *Κέντρα δεδομένων και φορτίο υπολογισμού*—ένα κέντρο δεδομένων περιλαμβάνει εκατοντάδες χιλιάδες computer servers, εξοπλισμούς ψύξης και μετασχηματιστές υποσταθμών. Ένα κέντρο δεδομένων μπορεί να ξεπεράσει την κατανάλωση των 50 MW, ενώ αυτή η κατανάλωση μπορεί να διπλασιαστεί όταν όλοι οι computer servers είναι απασχολημένοι με υπολογιστικές εργασίες. Γι αυτό το λόγο, επιθέσεις μέσω διαδικτύου μπορούν να κατακλύσουν τους computer servers του κέντρου δεδομένων με ψεύτικες υπολογιστικές εργασίες, με αποτέλεσμα την υπερβολική κατανάλωση ενέργειας, απότομες διακυμάνσεις φορτίου και ανισορροπία του ηλεκτρικού δικτύου.

2) *Άμεσος έλεγχος φορτίου*—αποτελεί το μερίδιο φορτίου, όπως κλιματιστικά, θερμοσίφωνας, ψυγείο, αντλίες πισίνας, που βρίσκονται υπό τον άμεσο έλεγχο του παρόχου. Ο πάροχος στέλνει σήματα-εντολές, μέσω γραμμών μεταφοράς ή Διαδικτύου, στις συσκευές αυτές για ενεργοποίηση ή απενεργοποίηση. Ο επιτιθέμενος μπορεί να καταφέρει να στείλει τέτοια σήματα-εντολές και να ελέγξει τη λειτουργία οικιακού ή βιομηχανικού φορτίου για τα οποία υποτίθεται ότι είναι υπεύθυνος ο πάροχος. Έτσι, στέλνοντας ταυτόχρονα σήματα ενεργοποίησης σε χιλιάδες συσκευές θερμοσίφωνα, ο επιτιθέμενος θα καταφέρει να προκαλέσει σημαντικό χτύπημα στη συνολική ζήτηση φορτίου. Αυτό οδηγεί σε υποβάθμιση της ποιότητας ισχύος, προβλήματα τάσης, πιθανή ζημιά στον εξοπλισμό του παρόχου και του καταναλωτή.
3) *Έμμεσος έλεγχος φορτίου*—επιτρέπει στους πελάτες να ελέγχουν το φορτίο τους ανεξάρτητα, σύμφωνα με σήματα-τιμολόγησης που στέλνονται από τον πάροχο μέσω Διαδικτύου στους έξυπνους μετρητές. Δεδομένου της πληροφορίας τιμολόγησης και βασιζόμενοι στις ενεργειακές τους ανάγκες, οι καταναλωτές προγραμματίζουν το χρόνο και το ποσό της ενεργειακής κατανάλωσης για κάθε οικιακή συσκευή. Σε αυτή την περίπτωση, ο επιτιθέμενος μπορεί να τροποποιήσει τα σήματα-τιμολόγησης, προκαλώντας αύξηση του συνολικού φορτίου με μείωση των τιμολογήσεων.



Εικόνα 2-7 Προσβάσιμα φορτία μέσω Διαδικτύου

2.3. Θέματα ασφάλειας των ασύρματων δικτύων και των έξυπνων μετρητών

Τα ασύρματα δίκτυα χρησιμοποιούνται ευρέως στο έξυπνο δίκτυο εξαιτίας της πρακτικότητας και του χαμηλού κόστους που προσφέρουν. Τα πολλαπλά μονοπάτια επικοινωνίας που διαθέτουν αποζημιώνουν για τις αποτυχίες που προκαλούνται από την κατάρρευση ορισμένων κόμβων επικοινωνίας.

Αν και οι έξυπνοι μετρητές υπόσχονται να μετασχηματίσουν το υπάρχον ηλεκτρικό δίκτυο, οι ίδιοι φέρνουν μια πληθώρα προβλημάτων ασφάλειας που πρέπει να διευθετηθούν για να εγγυηθούν ασφαλή λειτουργία του δικτύου. Για παράδειγμα,

- τα δεδομένα χρήστη ή το προφίλ κατοίκου μπορεί να συλλεχθεί κακόβουλα μέσω κακοπροαίρετης χρήσης του ηλεκτρικού ρεύματος

- το σύστημα επικοινωνιών ίσως είναι ευάλωτο σε επιθέσεις denial-of-service(DoS), που θα μπλόκαραν τη μεταφορά των μετρήσεων
- τρύπες ασφάλειας μπορούν να επιτρέψουν την εισβολή hackers μες στους έξυπνους μετρητές για να τροποποιήσουν τα δεδομένα χρήστη(οδηγώντας σε λανθασμένο υπολογισμό λογαριασμού) ή να στείλουν εντολές αποσύνδεσης προς τους ίδιους τους μετρητές.

2.4. Υπολογισμός κατάστασης (state estimation), επίθεση ανακατανομής φορτίου (load redistribution attack) και συνέπειες

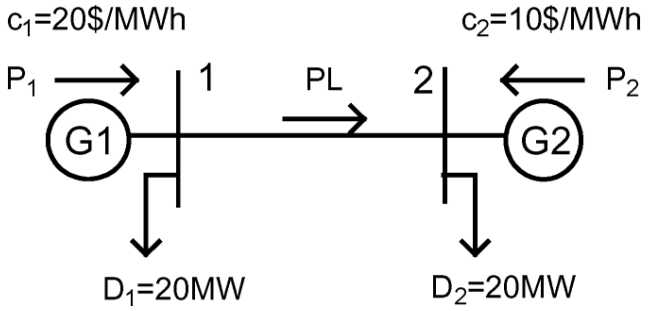
Ο υπολογισμός κατάστασης αποτελεί στοιχείο κλειδί για τη λειτουργία και τον έλεγχο ενός αξιόπιστου συστήματος. Ο υπολογισμός κατάστασης συλλέγει πληροφορίες μετρήσεων από ένα μεγάλο αριθμό μετρητών και τις αναλύει συγκεντρωτικά στο κέντρο ελέγχου. Στη συνέχεια πραγματοποιείται υπολογισμός ελαχιστοποίησης του συνολικού λειτουργικού κόστους μέσω της ανακατανομής της ισχύος παραγωγής.

Ωστόσο, πρόσφατα αποδείχτηκε ότι ο υπολογισμός κατάστασης είναι ευάλωτος σε σκόπιμες επιθέσεις μόλυνσης με λανθασμένα δεδομένα. Συνεργατικά χειρίζονται τις μετρήσεις που λαμβάνουν οι διάφοροι μετρητές, διαστρεβλώνοντας έτσι το αποτέλεσμα του υπολογισμού κατάστασης. Σαν αποτέλεσμα, ένας λανθασμένος υπολογισμός ελαχιστοποίησης του συνολικού λειτουργικού κόστους θα οδηγήσει το σύστημα σε μη οικονομική λειτουργία, συνοδευόμενη ίσως από άμεση κατάρρευση φορτίου.

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

2.4.1. Παράδειγμα επίθεσης ανακατανομής φορτίου

Ένα παράδειγμα απλού συστήματος 2 ζυγών (2-bus system), παρουσιάζεται στην παρακάτω Εικόνα 2-8. Ο ζυγός 1 επιλέγεται ως ο ζυγός αναφοράς. Η έξοδος των γεννητριών είναι P1(0 MW, 18 MW) και P2(0 MW, 30 MW). Το όριο χωρητικότητας των γραμμών μεταφοράς PL είναι 5 MW. Το κόστος κατάρρευσης φορτίου είναι cs= 40$/MWh. Υποθέτουμε ότι η αρχική κατάσταση του συστήματος είναι P1= 18 MW, P2= 22 MW και PL= -2 MW. Χωρίς επίθεση, ο υπολογισμός ελαχιστοποίησης του συνολικού λειτουργικού κόστους μέσω της ανακατανομής της ισχύος παραγωγής, θα οδηγούσε το σύστημα στη βέλτιστη κατάσταση P1'= 15 MW, P2'= 25 MW και PL'= -5 MW. Δεν θα υπήρχε καμία κατάρρευση φορτίου στο σύστημα και το συνολικό κόστος παραγωγής θα ήταν C'= 550$/h.



Εικόνα 2-8 Απλό σύστημα 2 ζυγών

Υποθέτουμε ότι μια επίθεση ανακατανομής φορτίου αλλάζει τη ζήτηση του ζυγού 1 κατά ΔD1, του ζυγού 2 κατά ΔD2 και άρα της ροής ισχύος της γραμμής κατά ΔPL. Με αυτό τον τρόπο, μεταβάλλεται λανθασμένα ο υπολογισμός κατάστασης του συστήματος, και ο υπολογισμός ελαχιστοποίησης του συνολικού λειτουργικού κόστους μέσω της ανακατανομής της ισχύος παραγωγής οδηγεί σε λανθασμένη βέλτιστη κατάσταση με πιθανή κατάρρευση φορτίου και υψηλότατο συνολικό κόστος λειτουργίας. Η άμεση καταστροφική επίδραση έξι τέτοιων επιθέσεων παρουσιάζεται στην Εικόνα 2-9.

attack case		1	2	3	4	5	6
LR attack	ΔD_1	2	4	6	8	10	-10
	ΔD_2	-2	-4	-6	-8	-10	10
	ΔPL	-2	-4	-6	-8	-10	10
false state estimation	$D_{f,1}$	22	24	26	28	30	10
	$D_{f,2}$	18	16	14	12	10	30
	PL_f	-4	-6	-8	-10	-12	8
false SCED results	$P'_{f,1}$	17	18	18	18	18	10
	$P'_{f,2}$	23	21	19	17	15	30
	PL'_f	-5	-5	-5	-5	-5	0
	$S'_{f,1}$	0	1	3	5	7	0
	$S'_{f,2}$	0	0	0	0	0	0
	C'_f	570	610	670	730	790	500
actual	PL'_t	-3	-1	1	3	5	-10

Εικόνα 2-9 Άμεση καταστροφική επίδραση σε σύστημα 2 ζυγών

Στην επίθεση 1, ο λάθος υπολογισμός βέλτιστης κατάστασης οδηγεί το σύστημα σε μη βέλτιστη ανταπόκριση παραγωγής με λειτουργικό κόστος 570$/h, το οποίο είναι 20$/h υψηλότερο από την πραγματική κατάσταση. Επίσης, σε αυτή την περίπτωση δεν υπάρχει καμιά κατάρρευση φορτίου, αφού ο λάθος υπολογισμός κατάστασης για τη ροή φορτίου της γραμμής (PL= -4 MW) βρίσκεται εντός των ορίων χωρητικότητας της γραμμής.

Στην επίθεση 2, το μέγεθος της επίθεσης αυξάνει κατά 20% το αρχικό πραγματικό φορτίο. Ο λανθασμένος βέλτιστος υπολογισμός της ροής ισχύος (PL= -6 MW) υπερβαίνει το όριο χωρητικότητας της γραμμής. Για τη διατήρηση ασφαλούς λειτουργίας, ο υπολογισμός ελαχιστοποίησης του συνολικού λειτουργικού κόστους μέσω της ανακατανομής της ισχύος παραγωγής, βασισμένος στον λανθασμένο υπολογισμό κατάστασης, οδηγεί το σύστημα σε λανθασμένη βέλτιστη κατάσταση

λειτουργίας με συνολικό κόστος λειτουργίας 610$/h και 1MW απόρριψη φορτίου στο ζυγό 1.

Καθώς το μέγεθος της επίθεσης αυξάνει σταδιακά μέχρι και το 50% του αρχικού πραγματικού φορτίου στις επιθέσεις 3 έως 5, η απόρριψη φορτίου και το λειτουργικό κόστος αυξάνουν ανάλογα.

Για τις παραπάνω περιπτώσεις, παρατηρούμε ότι για να παραπλανήσουμε το κέντρο ελέγχου και να απορρίψει μέρος φορτίου άμεσα, πρέπει να ικανοποιούνται δύο συνθήκες για την επίθεση ανακατανομής φορτίου:

1) Το μέγεθος της επίθεσης να είναι αρκετά μεγάλο.
2) Ο λανθασμένος υπολογισμός της ροής ισχύος να υπερβαίνει το αντίστοιχο όριο χωρητικότητας της γραμμής μεταφοράς.

Στην περίπτωση της επίθεσης 6, ο λανθασμένος υπολογισμός κατάστασης οδηγεί σε λανθασμένη ανταπόκριση παραγωγής. Το κέντρο ελέγχου υποθέτει ότι η ροή ισχύος στη γραμμή είναι μηδενική μετά την εφαρμογή της βέλτιστης ανακατανομής ισχύος. Ωστόσο, βασισμένοι στα πραγματικά φορτία του συστήματος, η πραγματική ροή ισχύος γίνεται PL= -10 MW υπερφορτώνοντας τη γραμμή μεταφοράς. Ωστόσο, το κέντρο ελέγχου δεν θα μπορέσει να ενημερωθεί για το πρόβλημα ασφάλειας έως ότου η επόμενη προγραμματισμένη μέτρηση συλλεχθεί. Άξιο παρατήρησης το γεγονός ότι το λειτουργικό κόστος είναι χαμηλότερο από το αρχικό πραγματικό, διότι οι γραμμές λειτουργούν αρκετά πιο κάτω από τις δυνατότητές τους.

2.5. Πιθανές ηλεκτρονικές επιθέσεις (cyber-attacks) και η επίδρασή τους στο δίκτυο ηλεκτρικής ισχύος

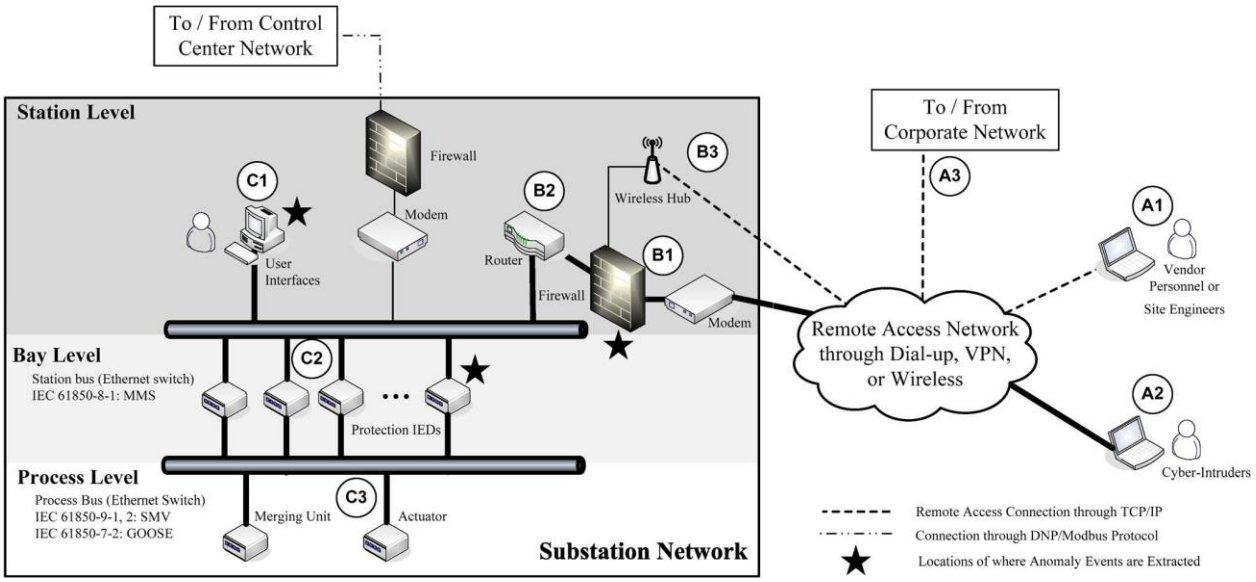
Ταξινομούμε τις επιθέσεις σε τρεις κατηγορίες-στόχους:

- *Στοιχεία*: οι συσκευές αυτοματισμού, όπως RTU και HMI, συχνά υποστηρίζουν ένα interface χρήστη για να επιτρέψει σε μηχανικούς να εκτελέσουν διαδικασίες διαμόρφωσης και διάγνωσης από απομακρυσμένα σημεία πρόσβασης(οι θύρες συντήρησης ίσως είναι βασισμένες σε IP). Η απομακρυσμένη πρόσβαση μπορεί να επιτρέψει σε έναν εισβολέα να καταλάβει τη συσκευή και να προκαλέσει ελαττωματικές καταστάσεις, όπως: 1) αλλαγή δεδομένων και παραπλάνηση του διαχειριστή του συστήματος ελέγχου, 2) ζημιά στον εξοπλισμό ενός τομέα μετά από εφαρμογή μη ακριβών δεδομένων, 3) απώλεια υπηρεσίας εάν ο εισβολέας σβήσει τη συσκευή. Για παράδειγμα, ο Stuxnet χρησιμοποιεί τρύπες ασφαλείας εμπορικών προϊόντων(π.χ. Windows XP) για να ξεκινήσει επιθέσεις.
- *Πρωτόκολλα*: Σχεδόν όλα τα σύγχρονα πρωτόκολλα δεδομένων επικοινωνιών ακολουθούν το messaging protocol που είναι καλά τεκμηριωμένο και διαθέσιμο στο δημόσιο κοινό. Το πρωτόκολλο DNP χρησιμοποιείται ευρέως από ηλεκτρικούς παρόχους στη Β.Αμερική. Κάποιος εισβολέας μπορεί να εκμεταλλευτεί αυτά τα πρωτόκολλα χρησιμοποιώντας επίθεση man-in-the-middle ή spoofing. Οι δυσμενείς συνέπειες ίσως περιλαμβάνουν αποστολή παραπλανητικών δεδομένων στη συσκευή ή στο διαχειριστή του κέντρου ελέγχου, οδηγώντας σε: 1) οικονομικές απώλειες εάν η επίθεση οδηγήσει σε υπερβολική παραγωγή, 2) κίνδυνος ασφάλειας εάν μια γραμμή ηλεκτρικής ισχύος ενεργοποιηθεί τη στιγμή που ειδικοί συντηρούν τη γραμμή, 3) καταστροφή εξοπλισμού

εάν σταλούν κακόβουλες εντολές ελέγχου που οδηγούν σε κατάσταση υπερφόρτωσης.

- *Τοπολογία*: Κάποιος εισβολέας μπορεί να εκμεταλλευτεί τα ευάλωτα σημεία μιας τοπολογίας δικτύου και να εξαπολύσει μια επίθεση denial-of-service (DoS), πλημμυρίζοντας ένα RTU με μηνύματα έγκυρου πρωτοκόλλου. Σαν αποτέλεσμα η υπολογιστική ισχύς της CPU, η μνήμη και το εύρος ζώνης θα υπερβούν τα όριά τους, και θα συντελέσουν σε καθυστέρηση ή και απώλεια ανταλλαγής δεδομένων πραγματικού χρόνου. Επίσης, οι διαχειριστές του κέντρου ελέγχου ίσως αποτύχουν να διαμορφώσουν μια ολοκληρωμένη άποψη της κατάστασης του ηλεκτρικού δικτύου, οδηγώντας σε λανθασμένη λήψη αποφάσεων.

2.6. Υποθετικά σενάρια εισβολής



Εικόνα 2-10 Υποθετικά σενάρια εισβολής

Δύο πρωτόκολλα χρησιμοποιούνται στα κέντρα ελέγχου, το DNP 3.0 over TCP/IP και το Inter-Control Center Communications Protocol (ICCP). Το πρώτο χρησιμοποιείται για ελέγχους και μετρήσεις μεταξύ κέντρων ελέγχου και υποσταθμών, ενώ το δεύτερο για ανταλλαγή δεδομένων μεταξύ των κέντρων ελέγχου.

Όπως φαίνεται στην παραπάνω εικόνα, οι ακόλουθοι συνδυασμοί αντιπροσωπεύουν τα πιθανά μονοπάτια εισβολής, μέσω απομακρυσμένων συνδέσεων, στο τοπικό δίκτυο ενός υποσταθμού:

- Ένα σημείο από τα (A1, A2, A3)-B1-B2
- Ένα σημείο από τα (A1, A2, A3)-B3-B1-B2

Κάθε συνδυασμός περιλαμβάνει συνδέσεις μέσω απομακρυσμένης σύνδεσης dial-up ή VPN με το δίκτυο του υποσταθμού και στοχεύει τη διεπαφή χρήστη(user interface) ή τις έξυπνες ηλεκτρονικές συσκευές(IED). Από τη στιγμή που το τοπικό δίκτυο διαπεραστεί, μια ηλεκτρονική επίθεση μπορεί να εκτοξευθεί μέσω:

- διεπαφής χρήστη(user interface), C1—παρέχει άμεση πρόσβαση στο δίκτυο επικοινωνιών του υποσταθμού. Μετά από μια επιτυχημένη εισβολή στη διεπαφή χρήστη με τα υψηλότερα προνόμια προσβασιμότητας, ένας εισβολέας θα μπορούσε να αξιοποιήσει την κονσόλα και να εξερευνήσει πληροφορίες απαριθμώντας διακόπτες στο τοπικό δίκτυο. Αν αναγνωριστούν οι παράμετροι ελέγχου, εντολές να ανοίξουν οι διακόπτες μπορούν να σταλούν.
- άμεσης σύνδεσης με την έξυπνη ηλεκτρονική συσκευή(IED), C2—μετά από ένα επιτυχημένο σπάσιμο του password και αποκτώντας πρόσβαση σε μια έξυπνη ηλεκτρονική συσκευή, ο εισβολέας μπορεί να ανακαλύψει τους φακέλους διαμόρφωσης του υποσταθμού που περιέχουν το μονογραμμικό σχέδιο του υποσταθμού, του δικτύου επικοινωνιών, τη σύνθεση των συγκεκριμένων συσκευών και ροές δεδομένων. Αν οι απαιτούμενες πληροφορίες αναγνωριστούν, εντολές να ανοίξουν οι διακόπτες μπορούν να σταλούν με άμεση σύνδεση με την έξυπνη ηλεκτρονική συσκευή.
- υποκλοπής και τροποποίησης πακέτων δεδομένων, C3.

2.7. Μεθοδολογία μιας χαρακτηριστικής επίθεσης

Η μεθοδολογία μιας χαρακτηριστικής επίθεσης ίσως χρησιμοποιηθεί από μια ειδική εχθρική οντότητα που επιθυμεί να προκαλέσει κάτι παραπάνω από μια διακοπή υπηρεσίας. Το να αποκτήσει ένας hacker μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα SCADA είναι μια εξαιρετικά δύσκολη εργασία που απαιτεί έναν επιδέξιο hacker και πολλές ώρες έρευνας. Για να αποκτήσει τον έλεγχο του συστήματος αυτοματισμού του ηλεκτρικού δικτύου, υπάρχουν τρία απαραίτητα βήματα: *πρόσβαση, ανακάλυψη και έλεγχος*. Επιπρόσθετα, ένα ακόμη προαιρετικό βήμα που απασχολεί μελετημένους εισβολείς είναι η απόκρυψη των επιθέσεων διαγράφοντας συγκεκριμένους φακέλους που μπορούν να εντοπίσουν και να αναφέρουν την παρουσία των εισβολέων στα συστήματα αυτοματισμού.

1) *Πρόσβαση*: Το πρώτο βήμα που απαιτείται από έναν επιτιθέμενο είναι να αποκτήσει πρόσβαση στο σύστημα SCADA. Ο επιτιθέμενος μπορεί να συγκεντρώσει όσο το δυνατόν περισσότερες πληροφορίες(π.χ. από το Διαδίκτυο), όπως ονόματα, εγκατεστημένο εξοπλισμό και άλλα χρήσιμα δεδομένα. Μετά, στοχεύει συγκεκριμένα στοιχεία του συστήματος χρησιμοποιώντας κακόβουλο λογισμικό εκμεταλλεύεται τα αδύναμα σημεία και αποκτά πρόσβαση. Η πιο κοινή μέθοδος για μη εξουσιοδοτημένη πρόσβαση είναι η εξωτερική VPN πρόσβαση στο SCADA. Η VPN πρόσβαση συνήθως χρησιμοποιείται από εξειδικευμένο προσωπικό που απαιτεί πρόσβαση από το σπίτι τους ή το γραφείο τους. Προβλήματα προκύπτουν όταν οι κωδικοί πρόσβασης του εξειδικευμένου προσωπικού υποκλαπούν με κάποιο τρόπο.

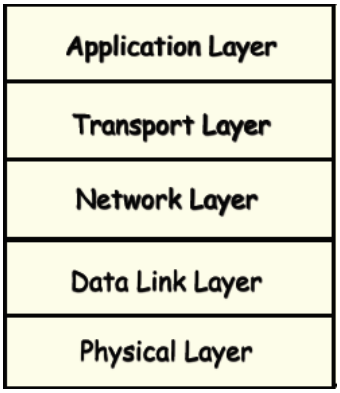
2) *Ανακάλυψη*: Αφού επιτευχθεί η πρόσβαση στο δίκτυο SCADA, το επόμενο βήμα είναι να κατανοήσεις το συγκεκριμένο δίκτυο ανακαλύπτοντας τη διαδικασία που επιτελείται. Είναι αλήθεια ότι η πολυπλοκότητα του συστήματος αποτελεί μια πολύ καλή άμυνα απέναντι στις επιθέσεις και δυσκολεύει αρκετά τον επιτιθέμενο στην κατανόησή του. Απλές πηγές πληροφορίας αρχικά αναζητούνται, όπως εξυπηρετητές ιστού, σταθμοί εργασίας μηχανικών, οθόνες HMI. Επίσης ο επιτιθέμενος μπορεί να παρακολουθεί επί μεγάλο χρονικό διάστημα τη ροή πληροφορίας που περνά από το σημείο στο οποίο είναι τοποθετημένος(ανάλυση κυκλοφορίας). Με αυτόν τον τρόπο, μπορεί να αποκαλυφθεί ένας μεγάλος πλούτος δεδομένων, όπως πιστοποιητικά FTP,

Telnet και HTTP. Ο συνδυασμός των παραπάνω θα παρέχει στον επιτιθέμενο μια καλή εικόνα σχετικά με τη λειτουργία του δικτύου.

3) *Έλεγχος*: Εάν κατανοηθεί η διαδικασία SCADA, υπάρχουν διάφοροι μέθοδοι για να ελέγξεις το σύστημα. Ένας από τους πιο δημοφιλείς στόχους είναι το HMI. Το πλεονέκτημα των κακόβουλων ενεργειών του επιτιθέμενου από τη θέση HMI είναι ότι αυτές οι ενέργειες θα εμφανίζονται ότι συμβαίνουν από τον υπεύθυνο διαχειριστή του HMI. Επίσης ένας δημοφιλής στόχος είναι ο σταθμός εργασίας μηχανικών EWS, ο οποίος χρησιμοποιείται από του μηχανικούς SCADA για να αναβαθμίσουν το σύστημα και να παρέχουν το λογισμικό και τις οθόνες στο HMI. Τέλος, άλλοι πιθανοί στόχοι αποτελούν τα συστήματα βάσεων δεδομένων και ο application server, που φιλοξενεί διάφορες εφαρμογές που χρησιμοποιούνται στο σύστημα SCADA και μπορούν να παρέχουν έλεγχο σε μέρη του συστήματος.

2.8. Μοντελοποίηση της συμπεριφοράς των επιθέσεων στο στρώμα MAC (medium access control) ασύρματων δικτύων αισθητήρων WSN

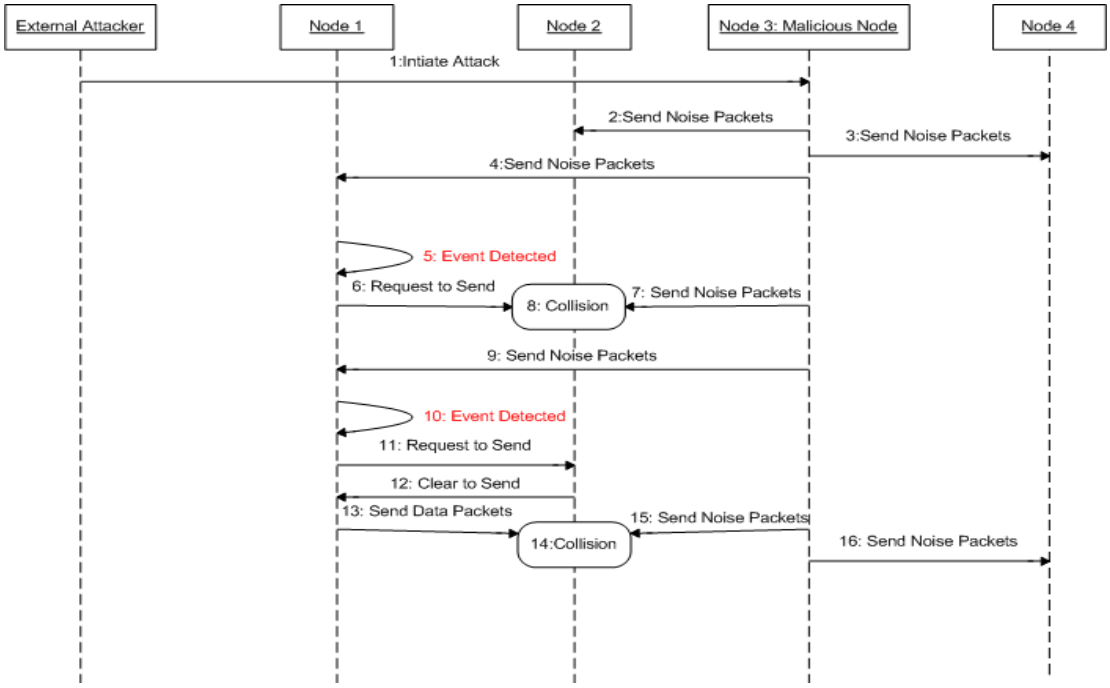
Ένα δίκτυο WSN είναι ευάλωτο σε πολλές και διαφορετικές επιθέσεις ασφάλειας σε όλα τα στρώματα επικοινωνίας και αυτές οι επιθέσεις μπορούν να δημιουργήσουν ένα μεγάλο ποσό ασυνεπειών στο δίκτυο. Για να αντιμετωπίσουμε αυτές τις επιθέσεις σε ένα WSN μέσω της ανάπτυξης καλών μηχανισμών ασφάλειας, είναι σημαντικό να κατανοήσουμε τη συμπεριφορά αυτών των επιθέσεων.



Εικόνα 2-11 Μοντέλο διαστρωμάτωσης OSI

Το στρώμα MAC παίζει σημαντικότατο ρόλο στη λειτουργία ενός WSN. Είναι υπεύθυνο για την κατανάλωση ενέργειας λόγω ασύρματης επικοινωνίας, την καθυστέρηση του δικτύου, τη χρησιμοποίηση καναλιού του δικτύου και οι επιθέσεις σε αυτό το στρώμα μπορούν να προκαλέσουν σημαντική υποβάθμιση των ανεξάρτητων κόμβων-αισθητήρων χάρη στη διαρροή ενέργειας και τη μειωμένη απόδοση λόγω καθυστέρησης. Παρακάτω παρουσιάζονται διάφορες επιθέσεις ασφάλειας που ενισχύουν τις διαρροές ενέργειας και τις καθυστερήσεις.

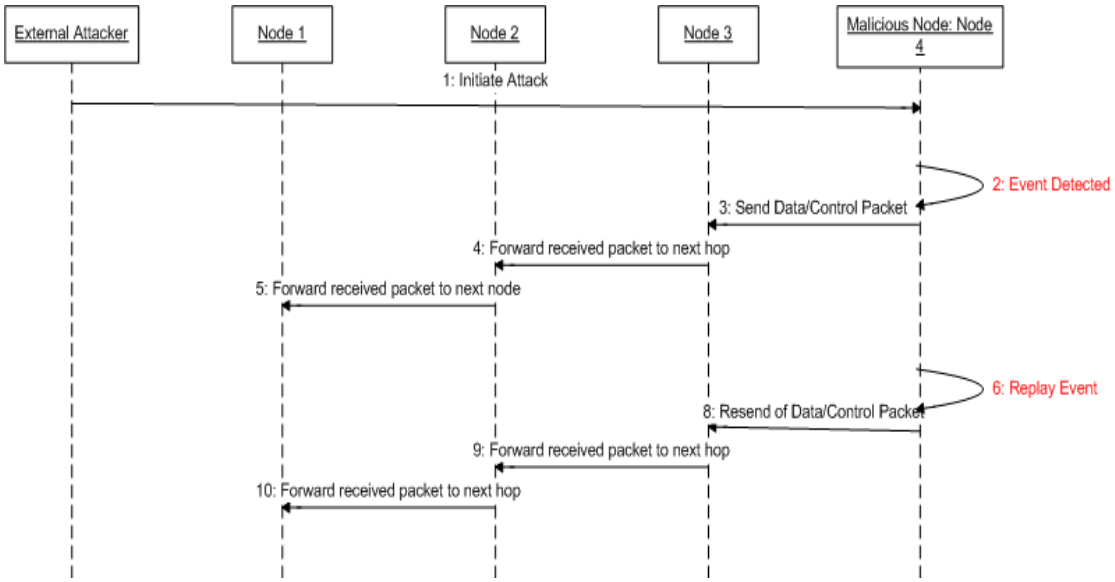
1) *Επίθεση πρόσκρουσης (collision attack)*—μπορεί εύκολα να επιτευχθεί από έναν κατειλημμένο κόμβο-αισθητήρα. Σε μια επίθεση πρόσκρουσης, ο κακόβουλος κόμβος δεν ακολουθεί τους κανόνες του πρωτοκόλλου MAC και προκαλεί προσκρούσεις με τις μεταδόσεις των γειτονικών κόμβων στέλνοντας ένα σύντομο πακέτο θορύβου(noise packet). Αυτή η επίθεση δεν καταναλώνει πολλή ενέργεια στον επιτιθέμενο, αλλά μπορεί να προκαλέσει πολλές διακοπές στη λειτουργία του δικτύου. Επίσης, είναι δύσκολο να εντοπιστεί αυτή η επίθεση εξαιτίας της φύσης ευρυ-εκπομπής (broadband) του ασύρματου περιβάλλοντος. Η παρακάτω εικόνα εξηγεί τη ροή των γεγονότων στην περίπτωση αυτών των επιθέσεων.



Εικόνα 2-12 Διάγραμμα ροής γεγονότων σε επίθεση πρόσκρουσης

Ένας εξωτερικός επιτιθέμενος ξεκινά την επίθεση πρόσκρουσης μέσω του κακόβουλου κόμβου 3. Έτσι, ξεκινά και στέλνει πακέτα θορύβου σε όλους τους κόμβους του δικτύου. Σαν αποτέλεσμα, αυξάνει την κυκλοφορία στο δίκτυο απασχολώντας κάθε κανάλι με αυτή τη δραστηριότητα. Ο κόμβος 1 εντοπίζει ένα γεγονός και στέλνει ένα πακέτο RTS(request to send) στον κόμβο 2. Την ίδια στιγμή, ο κακόβουλος κόμβος 3 στέλνει πάλι ένα πακέτο θορύβου στον κόμβο 2. Τα δυο πακέτα θα φθάσουν ταυτόχρονα στον κόμβο 2 και θα προκληθεί πρόσκρουση. Και πάλι, ο κόμβος 1 εντοπίζει ένα γεγονός και ελέγχει τη διαθεσιμότητα του καναλιού ανταλλάσσοντας μηνύματα RTS και CTS (clear to send) με τον κόμβο 2. Αμέσως μόλις ο κόμβος 1 λάβει το μήνυμα CTS από τον κόμβο 2, ο κόμβος 1 αρχίζει να στέλνει πακέτα δεδομένων προς τον κόμβο 2. Εάν, την ίδια στιγμή, ο κακόβουλος κόμβος 3 στείλει πακέτα θορύβου επίσης προς τον κόμβο 2, θα συμβούν προσκρούσεις στο δίκτυο. Ο κακόβουλος κόμβος 3 δημιουργεί συνεχώς πακέτα θορύβου που καθιστούν το κανάλι σταθερά απασχολημένο. Κατά τη διάρκεια αυτού, εάν ένας άλλος κόμβος προσπαθήσει να χρησιμοποιήσει το κανάλι, μια πρόσκρουση θα λάβει χώρα. Αυτή η πρόσκρουση των πακέτων οδηγεί σε επαναμετάδοση των πακέτων, που με τη σειρά τους οδηγεί σε αύξηση της ενεργειακής κατανάλωσης.

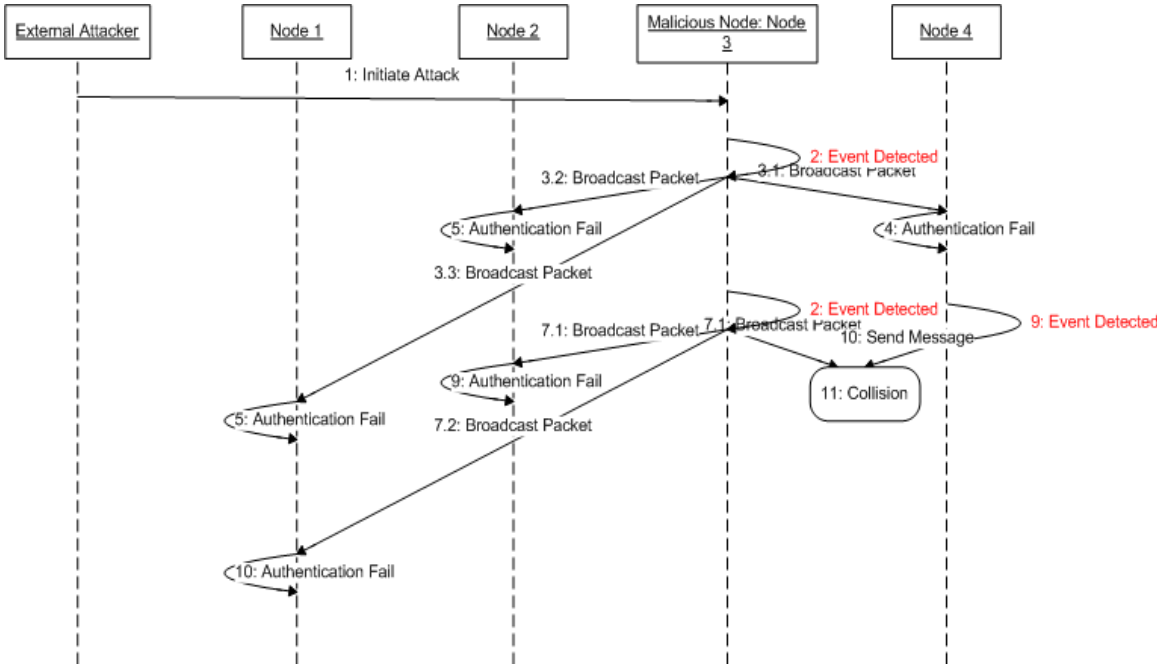
2) *Χαζή επίθεση επανάληψης (unintelligent replay attack)*—ο επιτιθέμενος δεν γνωρίζει το πρωτόκολλο MAC και δεν μπορεί να διεισδύσει στο δίκτυο. Καταγεγραμμένα γεγονότα επαναλαμβάνονται στο δίκτυο τα οποία εμποδίζουν τους κόμβους να εισέλθουν σε κατάσταση αδράνειας(sleep mode) και οδηγούν σε σπατάλη ενέργειας λαμβάνοντας και επεξεργάζοντας τα παραπάνω πακέτα. Έτσι, επαναλαμβανόμενη κυκλοφορία προωθείται μες στο δίκτυο, καταναλώνοντας ενέργεια σε κάθε κόμβο στο μονοπάτι προς τον τελικό προορισμό. Η επανάληψη των γεγονότων έχει δυσμενή επίπτωση στο χρόνο ζωής του δικτύου και την απόδοση του WSN. Η παρακάτω εικόνα εξηγεί τη ροή των γεγονότων στην περίπτωση αυτών των επιθέσεων.



Εικόνα 2-13 Διάγραμμα ροής γεγονότων σε χαζή επίθεση επανάληψης

Ένας εξωτερικός επιτιθέμενος ξεκινά την χαζή επίθεση επανάληψης μέσω του κακόβουλου κόμβου 4. Ο κακόβουλος κόμβος 4 εντοπίζει ένα γεγονός και στέλνει ένα μη πιστοποιημένο για την αυθεντικότητά του πακέτο προς τον κόμβο 1 βήμα-βήμα(hop-by-hop). Μετά από λίγο χρόνο, ο κακόβουλος κόμβος 4 επαναλαμβάνει το γεγονός και προωθεί το πακέτο εκ νέου μες στο δίκτυο. Ο κακόβουλος κόμβος δε διακρίνει πακέτα ελέγχου ή δεδομένων. Το παραπάνω γεγονός θα επαναληφθεί ξανά και ξανά, αυξάνοντας την κυκλοφορία του δικτύου και εμποδίζοντας τους κόμβους να περιέλθουν σε κατάσταση αδράνειας. Ένας αυξανόμενος αριθμός κόμβων θα βρίσκεται σε κατάσταση επαγρύπνησης(listen mode), μεγιστοποιώντας την κατανάλωση ενέργειας σε κάθε κόμβο στο μονοπάτι προς τον τελικό προορισμό. Κατά τη διάρκεια αυτού, εάν ένας άλλος κόμβος προσπαθήσει να στείλει ένα πακέτο, θα βρει το κανάλι κατειλημμένο.

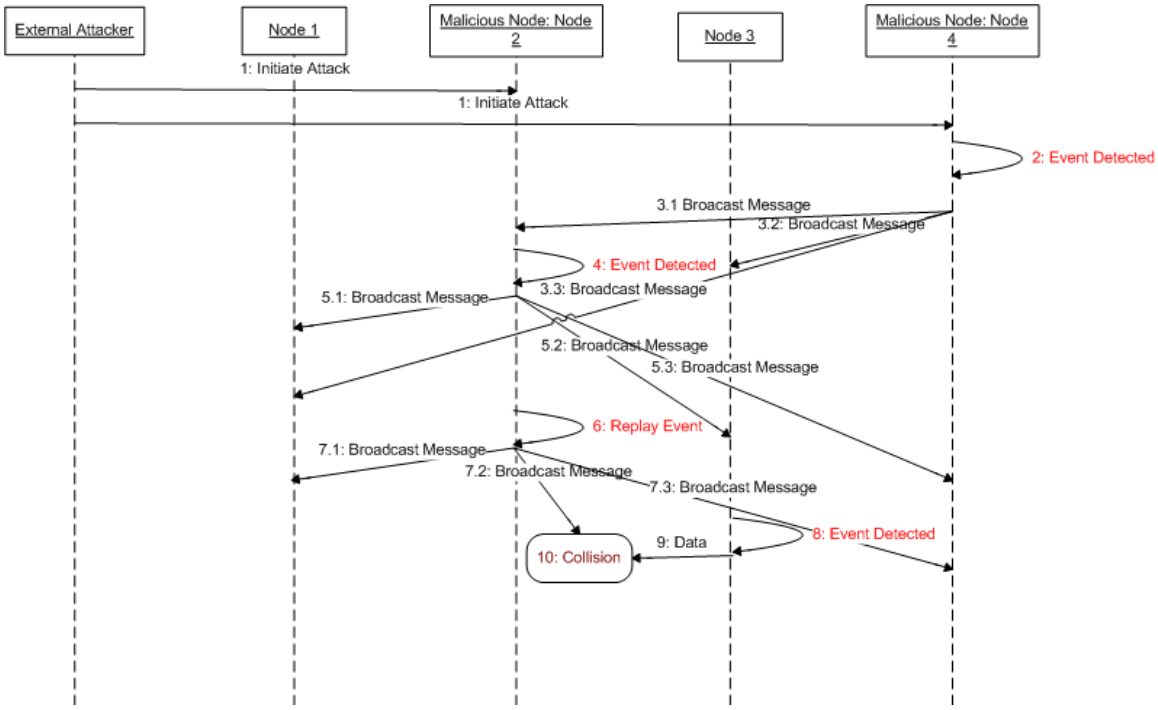
3) *Μη εξουσιοδοτημένη επίθεση ευρυ-εκπομπής (unauthenticated broadcast attack)*—ο επιτιθέμενος έχει πλήρη γνώση του πρωτοκόλλου MAC, αλλά δεν έχει την ικανότητα να διεισδύσει στο δίκτυο. Ο επιτιθέμενος εκπέμπει μη εξουσιοδοτημένη κίνηση στο δίκτυο ακολουθώντας όλους τους κανόνες του πρωτοκόλλου MAC. Αυτά τα μη εξουσιοδοτημένα και μη απαραίτητα εκπεμπόμενα μηνύματα διαταράσσουν τον φυσιολογικό κύκλο επαγρύπνησης και αδράνειας του κόμβου και τοποθετούν τους περισσότερους κόμβους σε κατάσταση επαγρύπνησης για εκτεταμένο χρονικό διάστημα. Σαν αποτέλεσμα, αυξάνεται η ενεργειακή κατανάλωση και μειώνεται ο χρόνος ζωής του δικτύου. Αυτές οι επιθέσεις προκαλούν βλάβη των servers στα πρωτόκολλα MAC που περιλαμβάνουν μικρού μεγέθους μηνύματα. Η παρακάτω εικόνα εξηγεί τη ροή των γεγονότων στην περίπτωση αυτών των επιθέσεων.



Εικόνα 2-14 Διάγραμμα ροής γεγονότων σε μη εξουσιοδοτημένη επίθεση ευρυεκπομπής

Ένας εξωτερικός επιτιθέμενος ξεκινά τη μη εξουσιοδοτημένη επίθεση ευρυεκπομπής μέσω του κακόβουλου κόμβου 3. Ο κακόβουλος κόμβος 3 εντοπίζει ένα γεγονός και εκπέμπει το πακέτο σε όλο το δίκτυο. Κάθε φορά που το πακέτο φθάνει σε έναν κόμβο, ο κόμβος θα προσπαθεί να πιστοποιήσει την αυθεντικότητά του αλλά θα αποτυγχάνει επειδή, αν και ο επιτιθέμενος έχει πλήρη γνώση του πρωτοκόλλου, δεν έχει την ικανότητα να διεισδύσει στο δίκτυο. Κάθε φορά, ο κακόβουλος κόμβος 3 εντοπίζει το γεγονός και εκπέμπει το πακέτο σε όλο το δίκτυο. Αυτή η μη αναγκαία εκπομπή των πακέτων θα καταναλώνει την ενέργεια κάθε κόμβου στο δίκτυο, καθώς οι κόμβοι θα πρέπει να είναι συνεχώς σε επαγρύπνηση. Ο κόμβος 4 εντοπίζει ένα γεγονός και στέλνει το μήνυμα προς τον κόμβο 3. Εάν την ίδια στιγμή, ο κακόβουλος κόμβος 3 εντοπίσει και εκπέμψει το γεγονός, θα προκληθεί σύγκρουση στο κανάλι ανάμεσα στον κόμβο 3 και στον κόμβο 4.

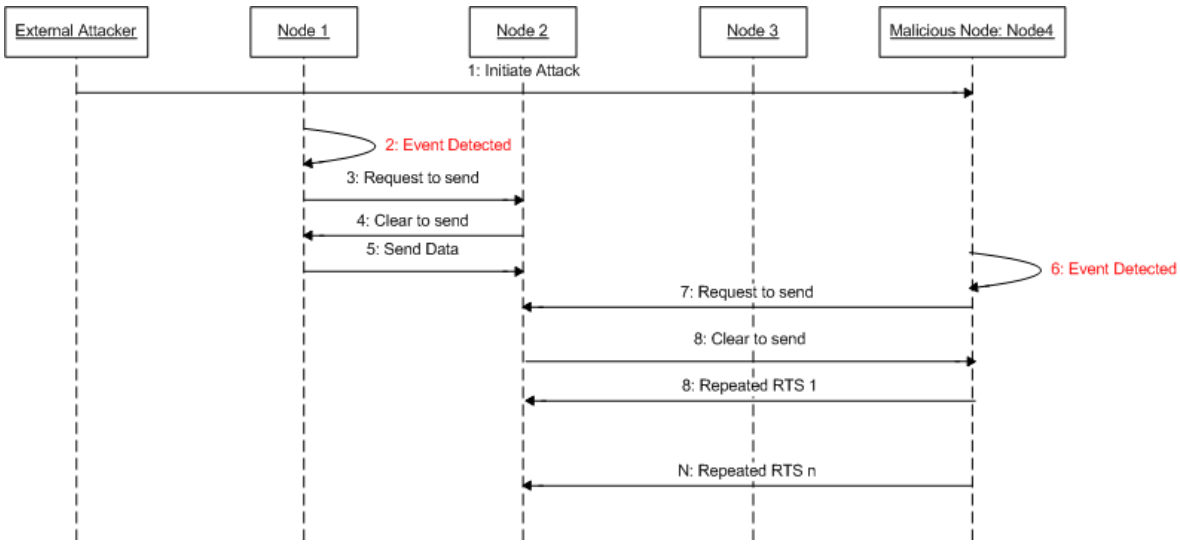
4) *Επίθεση πλήρους κυριαρχίας (full domination attack)*—ο επιτιθέμενος έχει πλήρη γνώση του πρωτοκόλλου του στρώματος MAC αλλά και την ικανότητα να διεισδύσει στο δίκτυο. Αυτός ο τύπος επίθεσης αποτελεί έναν από τους πιο καταστροφικούς στο WSN, καθώς ο επιτιθέμενος έχει την ικανότητα να παράγει κυκλοφορία άξια εμπιστοσύνης στο δίκτυο και να προκαλέσει τη μέγιστη δυνατή επίδραση αρνούμενος την κατάσταση αδράνειας(denial of sleep) στους διάφορους κόμβους. Οι επιθέσεις οργανώνονται χρησιμοποιώντας έναν ή περισσότερους κατειλημμένους κόμβους στο δίκτυο. Όλα τα είδη πρωτοκόλλων του στρώματος MAC είναι ευάλωτα σε αυτό το είδος επίθεσης. Η παρακάτω εικόνα εξηγεί τη ροή των γεγονότων στην περίπτωση αυτών των επιθέσεων.



Εικόνα 2-15 Διάγραμμα ροής γεγονότων σε επίθεση πλήρους κυριαρχίας

Ένας εξωτερικός επιτιθέμενος ξεκινά την επίθεση πλήρους κυριαρχίας μέσω των κακόβουλων κόμβων 2 και 4. Ο κακόβουλος κόμβος 4 εντοπίζει το γεγονός και εκπέμπει το μήνυμα στο δίκτυο. Το μήνυμα γίνεται αποδεκτό από όλους τους κόμβους επειδή, σε αυτή την επίθεση, ο επιτιθέμενος έχει πλήρη γνώση πρωτοκόλλου MAC αλλά και την ικανότητα να διεισδύσει στο δίκτυο. Επίσης ο κακόβουλος κόμβος 2 εντοπίζει το γεγονός και εκπέμπει το μήνυμα στο δίκτυο. Ο κακόβουλος κόμβος 2 επαναλαμβάνει το γεγονός μετά από λίγο χρόνο και το εκπέμπει σε όλο το δίκτυο. Η επαναλαμβανόμενη εκπομπή του γεγονότος θα εμποδίσει τους κόμβους να περιέλθουν σε κατάσταση αδράνειας, αυξάνοντας με αυτό τον τρόπο τη συνολική κατανάλωση ενέργειας. Ο κόμβος 3 εντοπίζει ένα γεγονός και στέλνοντας τα δεδομένα στον κόμβο 2, το πακέτο συγκρούεται με το εκπεμπόμενο μήνυμα που αποστέλλεται από τον κακόβουλο κόμβο 2.

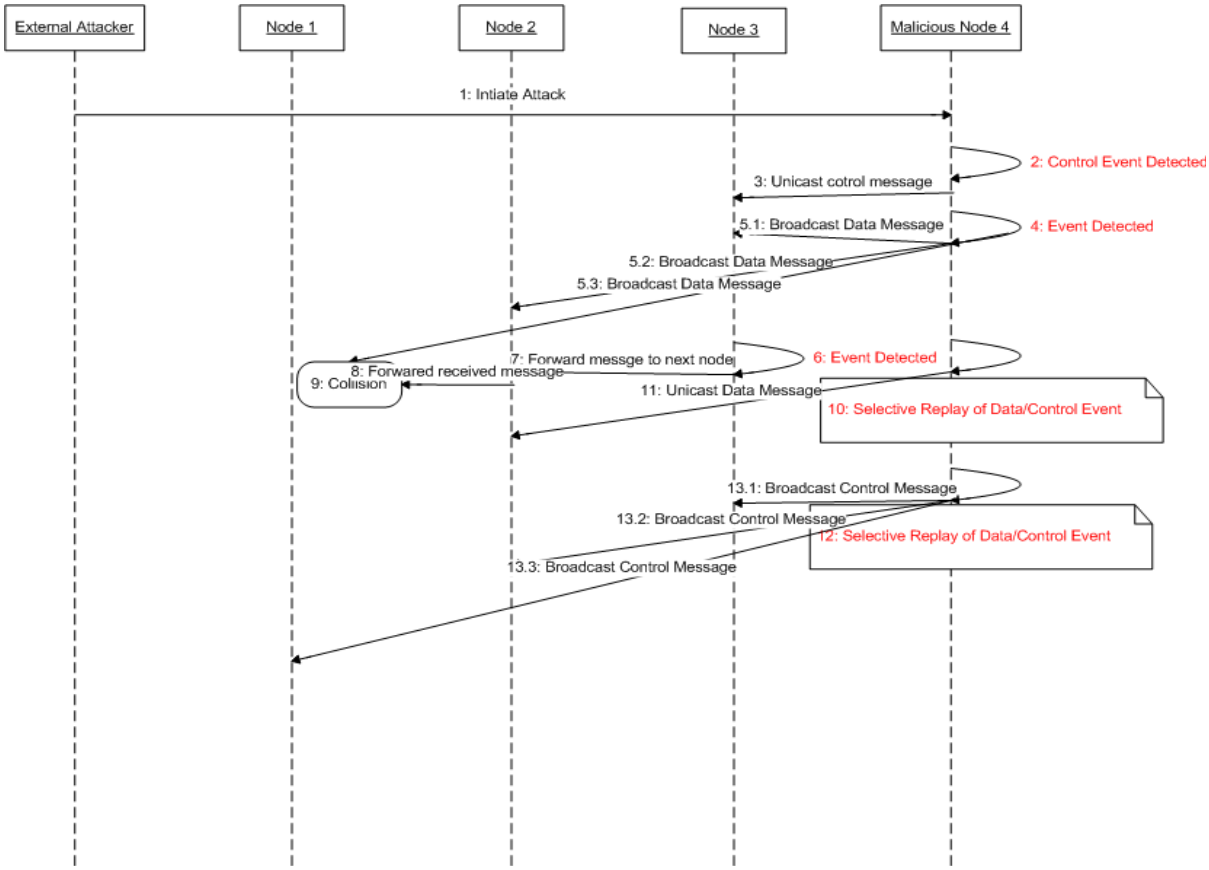
5) *Επίθεση εξάντλησης (exhaustion attack)*—ο επιτιθέμενος που ξεκινά αυτή την επίθεση έχει γνώση του πρωτοκόλλου MAC και την ικανότητα να διεισδύσει στο δίκτυο. Αυτές οι επιθέσεις είναι δυνατές μόνο στην περίπτωση πρωτοκόλλων MAC που βασίζονται σε μηνύματα RTS(request to send) και CTS(clear to send). Σε αυτή την επίθεση, ο κακόβουλος κόμβος στέλνει RTS σε έναν κόμβο και εάν ο κόμβος απαντήσει με CTS, ο κακόβουλος κόμβος θα στέλνει συνεχώς το μήνυμα RTS σε αυτό τον κόμβο, εμποδίζοντάς τον να περιέλθει σε κατάσταση αδράνειας και αντί αυτού εξαντλώντας τη συνολική ενέργεια του κόμβου. Αυτές οι επιθέσεις επηρεάζουν το χρόνο ζωής του κόμβου και μπορούν να διαχωρίσουν το δίκτυο. Η παρακάτω εικόνα εξηγεί τη ροή των γεγονότων στην περίπτωση αυτών των επιθέσεων.



Εικόνα 2-16 Διάγραμμα ροής γεγονότων σε επίθεση εξάντλησης

Ένας εξωτερικός επιτιθέμενος ξεκινά την επίθεση εξάντλησης μέσω του κακόβουλου κόμβου 4. Ο κόμβος 1 εντοπίζει το γεγονός και ανταλλάσσει μηνύματα RTS και CTS με τον κόμβο 2 και τελικά στέλνει τα δεδομένα προς τον κόμβο 2. Ο κακόβουλος κόμβος 4 εντοπίζει ένα γεγονός και στέλνει μήνυμα RTS στον κόμβο 2. Ο κόμβος 2 θα απαντήσει με CTS. Μετά από αυτό, ο κακόβουλος κόμβος θα παράγει συνεχώς ένα RTS πακέτο και θα το μεταδίδει προς τον κόμβο 2 έως ότου εξαντληθεί η συνολική ενέργεια του κόμβου 2.

6) *Ευφυής επίθεση παρεμβολής (intelligent jamming attack)*—(απλή παρεμβολή είναι η εκπομπή ραδιο-σήματος που παρεμβάλλει με τις ραδιοσυχνότητες που χρησιμοποιούνται από το δίκτυο αισθητήρων). Αποτελεί μία από τις πιο καταστροφικές επιθέσεις όπου ο επιτιθέμενος έχει πλήρη γνώση του πρωτοκόλλου, αλλά δεν έχει την ικανότητα να διεισδύσει στο δίκτυο. Ο επιτιθέμενος μολύνει το δίκτυο με μη πιστοποιημένα για την αυθεντικότητά τους πακέτα μονο-εκπομπής(unicast) και ευρυ-εκπομπής(broadcast). Αυτές οι επιθέσεις μπορούν να διακρίνουν την κίνηση ελέγχου και την κίνηση δεδομένων, σε αντίθεση με τη χαζή επίθεση επανάληψης όπου επαναλαμβάνονται τα επιλεγμένα γεγονότα(ελέγχου ή κίνησης). Η παρακάτω εικόνα εξηγεί τη ροή των γεγονότων στην περίπτωση αυτών των επιθέσεων.



Εικόνα 2-17 Διάγραμμα ροής γεγονότων σε ευφυή επίθεση παρεμβολής

Ένας εξωτερικός επιτιθέμενος ξεκινά την ευφυή επίθεση παρεμβολής μέσω του κακόβουλου κόμβου 4. Ο κακόβουλος κόμβος 4 εντοπίζει το γεγονός ελέγχου και μεταδίδει το μη πιστοποιημένο για την αυθεντικότητά του μήνυμα μονο-εκπομπής προς τον κόμβο 3. Ο κακόβουλος κόμβος 4 εντοπίζει ένα γεγονός και μεταδίδει το μη πιστοποιημένο για την αυθεντικότητά του μήνυμα ευρυ-εκπομπής μες στο δίκτυο. Ο κόμβος 3 εντοπίζει ένα γεγονός και προωθεί το μήνυμα προς τον κόμβο 1. Αυτό το μήνυμα συγκρούεται με το μήνυμα που εκπέμπεται από τον κακόβουλο κόμβο 4. Ο κακόβουλος κόμβος 4 χρησιμοποιεί τη γνώση του για το πρωτόκολλο του στρώματος MAC για επιλεκτική επανάληψη των γεγονότων δεδομένων ή ελέγχου. Έτσι, ο κόμβος 4 επαναλαμβάνει το πρώην εντοπισμένο γεγονός δεδομένων και μεταδίδει το μη πιστοποιημένο για την αυθεντικότητά του μήνυμα μονο-εκπομπής προς τον κόμβο 2. Ο κακόβουλος κόμβος 4 επαναλαμβάνει επιλεκτικά το γεγονός ελέγχου και εκπέμπει στο δίκτυο το μη πιστοποιημένο για την αυθεντικότητά του μήνυμα.

7) *Sybil attack*—ένας κακόβουλος κόμβος καταλαμβάνει παράνομα πολλαπλές ταυτότητες. Αποτελεί κίνδυνο για αλγορίθμους δρομολόγησης, συναθροίσεις πακέτων. Λειτουργεί με τον ίδιο τρόπο, ανεξαρτήτως στόχου. Για παράδειγμα, για επίθεση σε πρωτόκολλο δρομολόγησης, ο κακόβουλος κόμβος με τις πολλαπλές ταυτότητες θα δρομολογούσε πολλαπλά μονοπάτια μέσω αυτού του κόμβου.

2.9. Σημάδια ύπαρξης ευάλωτων σημείων (vulnerabilities)

- Το 1997, βασικά ψεγάδια ασφάλειας βρέθηκαν στα συστήματα υπολογιστών που ελέγχουν γεννήτριες, διακόπτες και υποσταθμούς.
- Το 1999, το Ινστιτούτου Έρευνας Ηλεκτρικής Ισχύος έδειξε ότι η αξιοπιστία του ηλεκτρικού δικτύου της Αμερικής απειλείται με αυξανόμενο ρυθμό, ενώ οι τεχνολογίες που απαιτούνται για να καταπολεμήσουν την απειλή καθυστερούν.
- Οι τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001 έχουν εκθέσει σημαντικά ευάλωτα σημεία ουσιαστικών υποδομών της Αμερικής.
- Το 2007, μια πειραματική ηλεκτρονική επίθεση ενάντια μιας γεννήτριας ισχύος προκάλεσε την αυτοκαταστροφή της.
- Πρόσφατα ανακαλύφθηκε ότι hackers εισήγαγαν λογισμικό στο ηλεκτρικό δίκτυο της Αμερικής, το οποίο θα τους επέτρεπε να διακόψουν τη λειτουργία του μια μετέπειτα χρονική στιγμή από μια απομακρυσμένη τοποθεσία, δηλώνοντας σαφώς το γεγονός ότι η υποδομή παρόχου είναι αρκετά ευάλωτη και η γενική της αποστολή να εξυπηρετεί τον πληθυσμό μπορούσε σοβαρά να τεθεί σε κίνδυνο σαν αποτέλεσμα απροσδόκητων τεχνητών ή φυσικών καταστροφών.

Ποτέ ξανά η ασφάλεια των εθνικών θεμελιωδών συστημάτων δεν μπορεί να θεωρηθεί δεδομένη.

3. Αντιμετώπιση ασφάλειας (security)

3.1. Ορισμός ασφάλειας

Οι ενεργειακοί μηχανικοί χρησιμοποιούν τον όρο ασφάλεια για να περιγράψουν την ικανότητα του κύριου όγκου του ηλεκτρικού δικτύου να αντιστέκεται σε απροσδόκητες αναταραχές, όπως βραχυκυκλώματα ή μη αναμενόμενες απώλειες στοιχείων του συστήματος χάρη σε φυσικά αίτια, ανθρώπινες φυσικές ή ηλεκτρονικές επιθέσεις.

Ο όρος ασφάλεια δεν περιέχει όμως μόνο την αξιοπιστία του συστήματος ηλεκτρικής ισχύος, αλλά περιγράφει και την αξιοπιστία συστημάτων επικοινωνιών που ενσωματώνονται για να εξυπηρετήσουν το σύστημα ηλεκτρικής ισχύος. Δηλαδή, περιλαμβάνει ακόμη την πιθανότητα να χαθεί ολοκληρωτικά ένα συγκεκριμένο μήνυμα, τη χρήση πλεοναζόντων μονοπατιών επικοινωνίας, τον αναμενόμενο χρόνο καθυστέρησης στην παράδοση ενός μηνύματος και το εύρος ζώνης μετάδοσης. Επίσης περιλαμβάνει τη διαδικασία ανάθεσης προτεραιότητας σε ορισμένα μηνύματα όταν τα κανάλια επικοινωνίας είναι κατειλημμένα (QoS: Quality of Service).

Τέλος, ο όρος ασφάλεια μπορεί να χρησιμοποιηθεί ως προστασία πληροφορίας που περιλαμβάνει μέτρα για να διασφαλίσουν την ανωνυμία της ηλεκτρονικής πληροφορίας κατά τη μετάδοση αλλά και αποθήκευση στα ψηφιακά συστήματα. Πρωταρχικής σημασίας είναι οι πληροφορίες που σχετίζονται με τις προσωπικές πληροφορίες των καταναλωτών-πελατών, οι εντολές που χρησιμοποιούνται για να ελέγξουν το ηλεκτρικό δίκτυο.

Επομένως, είναι σημαντικό οι επικοινωνίες να προστατεύονται από οποιοδήποτε είδος κακόβουλης εισβολής και ένα υψηλότερου επιπέδου σύστημα παρακολούθησης και ελέγχου να αναπτυχθεί προς όφελος της κοινωνίας. Επίσης για να λειτουργήσει το έξυπνο δίκτυο βασίζεται στις επικοινωνίες ανάμεσα σε διαφορετικά συστατικά, για τα οποία οι απαιτήσεις επικοινωνίας και ασφάλειας ποικίλουν. Έτσι, είναι ανάγκη να αναπτυχθούν διάφορα πρωτόκολλα επικοινωνίας που να ανταποκρίνονται στις διαφορετικές αυτές απαιτήσεις.

Το υπάρχον σύστημα διανομής ενέργειας είναι ευάλωτο τόσο σε φυσικές καταστροφές όσο και σε εσκεμμένες επιθέσεις. Μια επιτυχημένη τρομοκρατική προσπάθεια θα μπορούσε να διακόψει τη μεταφορά ενέργειας, έχοντας δυσμενείς επιδράσεις στην εθνική ασφάλεια, στην οικονομία και τη ζωή κάθε πολίτη. Η ασφαλής και αξιόπιστη λειτουργία του ηλεκτρικού συστήματος είναι θεμελιώδης για τα εθνικά και διεθνή οικονομικά συστήματα, την ασφάλεια και την ποιότητα ζωής.

3.2. Σημαντικές προκλήσεις

Για να απευθυνθούμε στα θέματα ασφάλειας, είναι απαραίτητο να αναγνωρίσουμε κάποιες μοναδικές προκλήσεις. Υπάρχουν τέσσερις σημαντικές προκλήσεις όταν αναπτύσσεις καινούριες λύσεις ασφάλειας δικτύου για τα συστήματα αυτοματισμού του ηλεκτρικού δικτύου.

1) Πολλά στοιχεία αυτοματισμού, όπως RTU, χρησιμοποιούν αποκλειστικά-ιδιωτικά λειτουργικά συστήματα που σχεδιάζονται για έλεγχο λειτουργικότητας και απόδοσης, αλλά όχι για ασφάλεια.

2) Τα συστήματα αυτοματισμού χρησιμοποιούν τεχνολογίες και πρωτόκολλα που σχεδιάστηκαν για συνδεσιμότητα, χωρίς εξέταση της ασφάλειας στον κυβερνοχώρο.
3) Πολλά στοιχεία αυτοματισμού, όπως RTU, κατασκευάστηκαν για να ελέγχουν τη λειτουργικότητα και ίσως δεν έχουν επιπλέον υπολογιστική ισχύ ή χώρο μνήμης για να εκτελούν λειτουργικότητες ασφάλειας. Το πρόβλημα είναι ότι αυτά τα στοιχεία προβλέπονται να λειτουργούν ίσως για παραπάνω από 30 χρόνια.
4) Το ηλεκτρικό δίκτυο γνωρίζει μια ουσιαστική αλλαγή προς το έξυπνο δίκτυο, όπου εμφανίζονται νέες εφαρμογές, όπως PMU και SM, και νέες απαιτήσεις για τη επικοινωνία δεδομένων, όπως εύρος ζώνης, καθυστέρηση και νέα πρωτόκολλα επικοινωνίας.

3.3. Στρατηγικές σχεδιασμού ασφάλειας

Οι στρατηγικές σχεδιασμού μιας αποτελεσματικής λύσης ασφάλειας για το έξυπνο δίκτυο είναι οι εξής:

- *Κλιμάκωση*—η ικανότητα του συστήματος να αυξάνει ή να μειώνει τη χωρητικότητά του για να προστατέψει μεγαλύτερο ή μικρότερο μέγεθος των συστημάτων αυτοματισμού του δικτύου ηλεκτρικής ισχύος(π.χ. περισσότερες ή λιγότερες ηλεκτρονικές συσκευές και χρήστες) με κομψό και ομαλό τρόπο. Κατά τη διάρκεια του σχεδιασμού, πρέπει να λαμβάνεται υπόψη για να διατηρήσει το ίδιο επίπεδο ανάπτυξης σε όλους τους τομείς του ηλεκτρικού δικτύου. Η απόδοση της λύσης ασφάλειας πρέπει να παραμένει σταθερή καθώς η υποδομή ηλεκτρικής ισχύος αυξάνει σε φορτίο και ποσότητα.
- *Επεκτασιμότητα*—αναφέρεται στο σχεδιασμό συστήματος με τέτοιο τρόπο ώστε να περιλαμβάνει μηχανισμούς(hooks) για εύκολη επέκταση χωρίς να απαιτούνται σημαντικές αλλαγές στην υποδομή. Με αυτόν τον τρόπο, το σύστημα θα είναι ικανό να συμπεριλάβει νέες τεχνολογίες και πρωτόκολλα επικοινωνιών, καθώς και νέα πλαίσια ασφάλειας αφού συνεχώς εξελίσσονται οι μέθοδοι επιθέσεων στον κυβερνοχώρο.
- *Δια-λειτουργικότητα*—μια ιδιότητα που αναφέρεται στην ικανότητα των διαφορετικών συστημάτων να λειτουργήσουν μαζί. Ως γνωστόν, τα συστήματα αυτοματισμού του δικτύου ηλεκτρικής ισχύος χρησιμοποιούν διάφορες τεχνολογίες όσων αφορά το υλικό, τα λειτουργικά συστήματα, τα πρωτόκολλα επικοινωνιών. Γι αυτό το λόγο το πλαίσιο ασφάλειας και τα συστατικά του πρέπει να είναι ικανά να δουλεύουν μαζί ανεξάρτητα της τεχνολογίας που υποστηρίζουν
- *Μη-διεισδυτικότητα*—αναφέρεται στην ικανότητα του συστήματος να υπόκειται σε δραστηριότητες ασφάλειας χωρίς να θέτει σε κίνδυνο τις λειτουργικότητες ελέγχου και την απόδοσή του. Επειδή πολλά συστήματα δεν έχουν επιπλέον υπολογιστική ισχύ ή χώρο μνήμης για να εκτελούν λειτουργικότητες ασφάλειας, η νέα λύση ασφάλειας είναι αναγκαίο να ενσωματωθεί στα υπάρχοντα συστήματα χωρίς συμβιβασμούς στην απόδοση, στην αξιοπιστία, στη σταθερότητα και στη διαθεσιμότητα.
- *Ευελιξία*—αναφέρεται στην ικανότητα να προσαρμόζεται στις διάφορες ανάγκες στην αναβάθμιση και σε πραγματικό χρόνο λειτουργίας. Περιλαμβάνεται η ικανότητα του συστήματος να επεκτείνεται με

καινούρια χαρακτηριστικά/συστατικά χωρίς την απώλεια της προηγούμενης λειτουργικότητας ή μείωση της ποιότητας. Σε αντίθεση με το σχετικά στατικό υπάρχον ηλεκτρικό δίκτυο, το μελλοντικό έξυπνο δίκτυο μπορεί να εξαιρετικά δυναμικό λόγω της αύξησης του αριθμού των συμμετεχόντων.

3.4. Ιδιότητες ασφάλειας

Στο έξυπνο δίκτυο υπάρχουν τρεις κρίσιμες πλευρές ασφάλειας που είναι απαραίτητο να προστατευθούν για να θεωρηθεί ασφαλές:

1) *Εμπιστευτικότητα (confidentiality)*—πρόληψη μη εξουσιοδοτημένης (unauthorized) αποκάλυψης πληροφοριών. Ουσιαστικά σημαίνει το να κρατάς την πληροφορία μυστική από μη εξουσιοδοτημένα πρόσωπα. Επομένως οι ευαίσθητες πληροφορίες δεν αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες. Για παράδειγμα, τα δεδομένα ηλεκτρονικής αγοράς και οι πληροφορίες συναλλαγής θεωρούνται ευαίσθητες πληροφορίες και θα πρέπει να είναι προσβάσιμες μόνο από εξουσιοδοτημένους αντιπρόσωπους αγοράς και όχι από άλλες οντότητες, όπως διαχειριστές συστήματος. Τέλος αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών, αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Έτσι για παράδειγμα, το γεγονός ότι κάποιος έχει φάκελο εγκληματία είναι συχνά το ίδιο σημαντικό όπως και οι λεπτομέρειες για το έγκλημα που διαπράχθηκε.
2) *ακεραιότητα (integrity)*—πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών. Ουσιαστικά σημαίνει ότι τα δεδομένα που μεταφέρονται μες στο δίκτυο επικοινωνιών δεν πρέπει να τροποποιηθούν κακόβουλα. Επίσης τα ευαίσθητα δεδομένα δεν πρέπει να διαγράφονται ούτε και να δημιουργούνται νέα δεδομένα με ένα μη εξουσιοδοτημένο και μη εντοπίσιμο τρόπο. Για παράδειγμα, ένας αντίπαλος δε θα μπορεί να τροποποιήσει τα δεδομένα ενός αισθητήρα χωρίς να εντοπιστεί.
3) *διαθεσιμότητα (availability)*—η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός πληροφοριακού συστήματος όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Δηλαδή, οι εξουσιοδοτημένες οντότητες (χρήστες) του δικτύου πρέπει να έχουν τη δυνατότητα να έχουν πρόσβαση στις υπηρεσίες του όταν τις χρειαστούν. Αυτή η υπηρεσία ασφάλεια είναι σημαντική όταν υπάρχει ένας κατειλημμένος κόμβος, για να διασφαλιστεί η φυσιολογική λειτουργία του δικτύου, απομονώνεται αυτός ο κακός κόμβος. Για παράδειγμα, τα δίκτυα επικοινωνιών πρέπει να είναι διαθέσιμα να μεταφέρουν δεδομένα και πληροφορίες(π.χ. μετρήσεις) ακόμα και κατά την παρουσία μιας επίθεσης denial-of-service (DoS).

Συγκεκριμένα για το ηλεκτρικό δίκτυο, η *διαθεσιμότητα* αποτελεί το πιο σημαντικό αντικείμενο ασφάλειας. Στο έξυπνο δίκτυο, τα κρίσιμα συστήματα πραγματικού χρόνου έχουν εκτιμώμενη μέγιστη καθυστέρηση 4 msec. Αυτά τα συστήματα παρακολουθούν συνεχώς την κατάσταση του ηλεκτρικού δικτύου και μια διακοπή στις επικοινωνίες τους μπορεί να προκαλέσει απώλεια ισχύος.

Το δεύτερο πιο σημαντικό αντικείμενο ασφάλειας, στο έξυπνο δίκτυο, αποτελεί η *ακεραιότητα*. Η ποιότητα του ηλεκτρικού ρεύματος εξαρτάται από την ποιότητα

υπολογισμού της τρέχουσας κατάστασης, επομένως και από την ποιότητα των δεδομένων που συλλέγονται από τους διάφορους αισθητήρες. Έτσι, μη εξουσιοδοτημένη τροποποίηση των δεδομένων μπορεί να προκαλέσει ζημιά στο ηλεκτρικό δίκτυο.

Το τελευταίο αντικείμενο ασφάλειας αποτελεί η *εμπιστευτικότητα*. Η απώλεια της εμπιστευτικότητας προκαλεί μικρότερους κινδύνους από την απώλεια της διαθεσιμότητας ή της ακεραιότητας. Ωστόσο, σε τομείς όπως η μυστικότητα των πληροφοριών των πελατών ή οι πληροφορίες ηλεκτρονικού εμπορίου, η εμπιστευτικότητα είναι πιο σημαντική από τις παραπάνω ιδιότητες.

Άλλες εκφάνσεις της *εμπιστευτικότητας* αποτελούν:

- Η *προστασία προσωπικών πληροφοριών (privacy)*, που αναφέρεται σε επαρκή προστασία των προσωπικών πληροφοριών και λειτουργιών έτσι ώστε μόνο εξουσιοδοτημένες οντότητες να έχουν πρόσβαση σε αυτά τα δεδομένα. Για παράδειγμα, τα δεδομένα κατανάλωσης ενέργειας του καταναλωτή χρειάζεται να προστατεύουν την ιδιωτική ζωή του καταναλωτή.
- Η *μυστικότητα (secrecy)*, που αφορά την προστασία των δεδομένων που ανήκουν σε έναν οργανισμό και όχι σε κάποιο συγκεκριμένο πρόσωπο.

3.4.1. Δευτερεύουσες έννοιες ασφάλειας

Εκτός από τις παραπάνω τρεις θεμελιώδεις έννοιες, συστήνονται ακόμη τρεις δευτερεύουσες έννοιες ασφάλειας πληροφοριακών συστημάτων:

- *Εξουσιοδοτημένη χρήση (authorized use)*—μόνο εξουσιοδοτημένα άτομα μπορούν να χρησιμοποιούν το υπολογιστικό σύστημα ή τις περιφερειακές συσκευές του και μόνο σύμφωνα με ένα προκαθορισμένο τρόπο.
- *Αυθεντικοποίηση μηνυμάτων (message authentication)*—η επιθυμία να γνωρίζουμε με βεβαιότητα κατά τη λήψη ενός μηνύματος (μέσω δικτύου) ότι το άτομο που το σύστημα αξιώνει ότι έστειλε το μήνυμα ότι πράγματι το έστειλε.
- *Αξιοπιστία (reliability)* και *σιγουριά (safety)*—η ασφάλεια (security) σχετίζεται με την αξιοπιστία και τη σιγουριά καθώς έχει να κάνει με συστήματα που πρέπει να λειτουργούν κανονικά σε αντίξοες συνθήκες, π.χ. συστήματα πυρηνικών σταθμών και ελέγχου εναέριας κυκλοφορίας.

3.5. Τρόπος αντιμετώπισης ασφάλειας

Για να επιτύχουμε αυτά τα χαρακτηριστικά, είναι απαραίτητος ο σχεδιασμός τεχνολογιών ηλεκτρονικής ασφάλειας για *προστασία, εντοπισμό* και *απόκριση*.

- Συστήματα *προστασίας* αποτελούν στοιχεία ασφάλειας, όπως διαχείριση κλειδιών, πιστοποίηση αυθεντικότητας και εξουσιοδότηση, καθώς και περιμετρική άμυνα που βοηθά στη διασφάλιση των ιδιοτήτων CIA απέναντι στις διάφορες επιθέσεις. Για παράδειγμα, η κρυπτογράφηση παρέχει εμπιστευτικότητα (και ακεραιότητα), η πιστοποίηση

αυθεντικότητας και η συνόψιση μηνύματος (message digest) παρέχουν ακεραιότητα.

- Συστήματα *εντοπισμού* αποτελούν μηχανισμοί αναγνώρισης κακόβουλων δραστηριοτήτων και επιθέσεων. Για παράδειγμα, τα συστήματα εντοπισμού εισβολέων αναζητούν κακόβουλες υπογραφές στο δίκτυο.
- Συστήματα *απόκρισης* αποτελούν οι δυναμικές αλλαγές σε πολιτικές τοίχων προστασίας για να περιοριστεί η ροή προς και από τους αντιπάλους για να αντιμετωπιστεί μια επίθεση.

Συλλογικά, τα συστήματα προστασίας, εντοπισμού και απόκρισης δημιουργούν ένα οικοσύστημα στο οποίο εκτελούνται ασφαλείς και άξιες εμπιστοσύνης λειτουργίες.

3.6. Πρόγραμμα απόκρισης σε έκτακτη ζήτηση (emergency demand response program)

Ένα πρόγραμμα απόκρισης σε έκτακτη ζήτηση μπορεί να παίξει ένα σημαντικό ρόλο στην αποτελεσματική διαχείριση ανεπάρκειας αποθεμάτων λειτουργίας και σοβαρών έκτακτων καταστάσεων για αποφυγή κατάρρευσης της τάσης του συστήματος. Αντικειμενικός σκοπός αυτού του προγράμματος είναι να βελτιώσει τα λειτουργικά αποθέματα ενέργειας επιλέγοντας τους κατάλληλους συμμετέχοντες στην απόκριση ζήτησης. Συμμετέχοντες είναι οι ζυγοί αυτοί που, μειώνοντας το φορτίο τους, θα βοηθήσουν στην ανάκαμψη της σταθερής λειτουργίας του δικτύου μετά τον επαναπροσδιορισμό παραγωγής και ζήτησης φορτίου. Επίσης επιθυμείται η ελαχιστοποίηση του συνολικού κόστους, διατηρώντας ταυτόχρονα την ασφάλεια και την αξιοπιστία του συνολικού συστήματος.

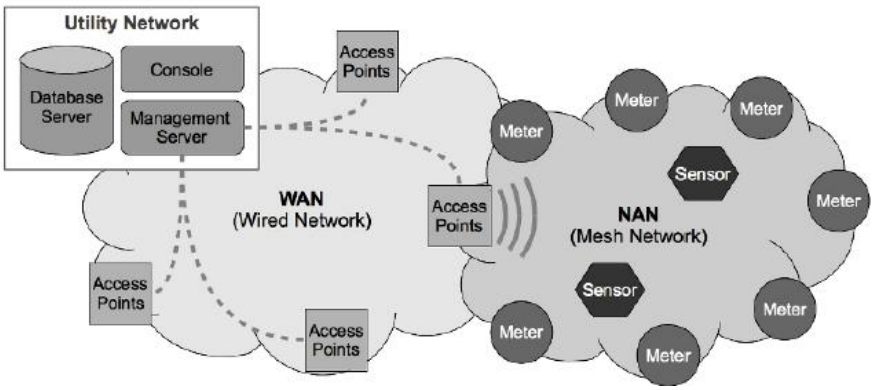
Μια πιθανή διακοπή ρεύματος μπορεί να ονομαστεί ως ένα γεγονός. Δημιουργείται λοιπόν, ένας πίνακας με ενέργειες αντίδρασης σε έκτακτη ζήτηση για διάφορα γεγονότα. Για κάθε δεδομένο γεγονός, ο πίνακας ίσως περιέχει παραμέτρους, όπως τοποθεσίες και απαιτούμενη ποσότητα μείωσης της ζήτησης, ο οποίος ενημερώνεται σε τακτά χρονικά διαστήματα. Εάν κάποιο γεγονός εντοπιστεί από το σύστημα SCADA, η απόκριση ζήτησης ενεργοποιείται αμέσως σύμφωνα με τον πίνακα αντίδρασης. Αν και το παραπάνω σενάριο φαίνεται απλό σαν ιδέα, το να ορίσεις τις παραμέτρους απόκρισης ζήτησης είναι ένα πολύπλοκο τεχνικό πρόβλημα για να εφαρμοστεί στο έξυπνο δίκτυο.

3.7. Σύστημα εντοπισμού εισβολέων (intrusion detection system)

Το σύστημα εντοπισμού εισβολέων έχει την ικανότητα να ταξινομεί τα είδη των επιθέσεων με επάρκεια και αποτελεσματικότητα μέσω της χρήσης ενός σθεναρού αλγορίθμου ταξινόμησης.

Σύμφωνα με την αρχιτεκτονική δικτύου που περιλαμβάνει HAN, NAN και WAN, κάθε κόμβος που ανήκει σε κάποιο από αυτά τα δίκτυα έχει και το ανάλογο σύστημα εντοπισμού εισβολέων του δικτύου. Τα συστήματα εντοπισμού εισβολέων του NAN περιλαμβάνουν το καλύτερο εκπαιδευμένο μοντέλο ταξινόμησης από όλα τα συστήματα εντοπισμού εισβολέων του HAN. Ανάλογα, τα συστήματα εντοπισμού εισβολέων του WAN περιλαμβάνουν το καλύτερο εκπαιδευμένο μοντέλο ταξινόμησης από όλα τα συστήματα εντοπισμού εισβολέων του NAN.

Σε κάθε περίπτωση, εάν το σύστημα εντοπισμού εισβολέων του HAN δεν καταφέρει να ταξινομήσει μια δικτυακή κυκλοφορία δεδομένων, τότε τα δεδομένα πακετάρονται και μεταδίδονται σε ένα σύστημα εντοπισμού εισβολέων του NAN. Εάν και το σύστημα εντοπισμού εισβολέων του NAN δεν καταφέρει να ταξινομήσει τη συγκεκριμένη δικτυακή κυκλοφορία δεδομένων, θα προσπαθήσει πρώτα να έρθει σε επικοινωνία με το άλλο κοντινότερο σύστημα εντοπισμού εισβολέων του NAN. Αυτή τη δυνατότητα δεν την έχει το σύστημα εντοπισμού εισβολέων του HAN. Εάν και αυτό δεν έχει αποτέλεσμα, τότε τα δεδομένα θα αποσταλούν στο σύστημα εντοπισμού εισβολέων του WAN, το οποίο έχει τη μεγαλύτερη ικανότητα και ακρίβεια στην ταξινόμηση επιθέσεων. Εάν επιτευχθεί ταξινόμηση μιας επίθεσης, τότε η ταξινόμηση κατεβαίνει ιεραρχικά προς τον κόμβο-πηγή, εκπαιδεύοντας το σύστημα εντοπισμού και κάνοντάς το πιο σθεναρό.



Εικόνα 3-1 Αρχιτεκτονική δικτύου HAN, NAN και WAN

3.8. Μηχανισμός εντοπισμού ανωμαλιών (anomaly detection mechanism)

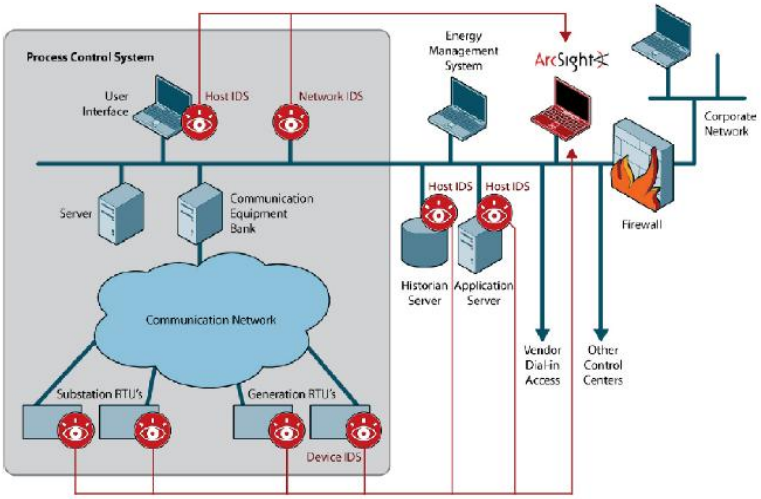
Εάν ένας επιτιθέμενος δε γνωρίζει την απαραίτητη πληροφορία (π.χ. όνομα χρήστη) για να εισβάλλει στη διεπαφή χρήστη (user interface) ή στην έξυπνη ηλεκτρονική συσκευή (IED), ίσως προσπαθήσει να τη βρει. Σαν αποτέλεσμα, καταγράφονται αποτυχημένες προσπάθειες, και η συσκευή θα κλειδωθεί εάν και όταν ο αριθμός των αποτυχημένων προσπαθειών υπερβεί ένα προκαθορισμένο κατώφλι.

Αν ο εισβολέας καταφέρει να εισέλθει, μπορεί να επιχειρήσει να αλλάξει τις ρυθμίσεις των κύριων μετασχηματιστών ή να αποσυνδέσει γραμμές μεταφοράς και διανομής. Ακόμη ίσως προσπαθήσει να επαναφέρει τις εργοστασιακές ρυθμίσεις, χάνοντας έτσι όλους τους φακέλους διαμόρφωσης που είναι κρίσιμοι για τη λειτουργία του συστήματος.

Οι τέσσερις παράμετροι που συλλαμβάνουν τους κακόβουλους εισβολείς και αποτελούν τα χαρακτηριστικά που βελτιώνουν την εγρήγορση του συστήματος είναι:

1) Αριθμός προσπαθειών εισβολής
2) Αλλαγή των αρχείων του συστήματος
3) Αλλαγή των ρυθμίσεων του συστήματος
4) Αλλαγή της κατάστασης του συστήματος

Όταν ο επιτιθέμενος προσπαθεί να εκτελέσει μια από αυτές τις λειτουργίες, ο μηχανισμός εντοπισμού ανωμαλιών εντοπίζει μια προσπάθεια να αλλάξουν οι ρυθμίσεις χωρίς εξουσιοδότηση και μπορεί να αποσυνδέσει αυτή τη συσκευή για αποφυγή ευρύτερης ζημιάς.



Εικόνα 3-2 Σύστημα εντοπισμού ανωμαλιών

3.9. Ταυτότητα (identity), διαχείριση κλειδιών (key management) και κρυπτογράφηση (encryption)

Κάθε οντότητα επικοινωνίας θα πρέπει να έχει μία μοναδική ταυτότητα. Αυτές οι ταυτότητες θα χρησιμοποιούνται για να διασφαλίζουν ότι τα μηνύματα αποστέλλονται και λαμβάνονται από μια νόμιμη έμπιστη οντότητα. Η πιστοποίηση της αυθεντικότητας θα υπογράφεται από έναν πράκτορα πιστοποίησης αυθεντικότητας και θα αποθηκεύεται σε κάθε οντότητα. Ο πράκτορας πιστοποίησης αυθεντικότητας στο δίκτυο WAN και NAN είναι ο πάροχος ηλεκτρισμού, ενώ στο δίκτυο HAN είναι ο έξυπνος μετρητής. Όταν δύο οντότητες θέλουν να έρθουν σε επικοινωνία, θα ανταλλάσσουν τα υπογεγραμμένα πιστοποιητικά αυθεντικότητάς τους για να διασφαλιστεί η ταυτότητά τους.

Η διαχείριση κλειδιών είναι πιο πολύπλοκη σε περιπτώσεις πολλαπλής εκπομπής (multicast) από περιπτώσεις μονο-εκπομπής (unicast), καθώς στην πρώτη περίπτωση τα κλειδιά κρυπτογράφησης διαμοιράζονται μεταξύ μιας ομάδας οντοτήτων. Όταν η σύνθεση της ομάδας αλλάξει, δηλαδή όταν ένα μέλος της ομάδας φύγει ή ένα νέο μέλος εισέλθει, τα κλειδιά της ομάδας πρέπει να ενημερωθούν έγκαιρα. Τα υπάρχοντα κλειδιά της ομάδας είναι απαραίτητο να αποσυρθούν και τα νέα κλειδιά της ομάδας να διανεμηθούν γρήγορα, χωρίς να διακοπεί η ροή μετρήσεων πραγματικού χρόνου.

Η κρυπτογραφία είναι μια διαδικασία που μπορεί μα προστατέψει τις συναλλαγές σε ένα ανοικτό δίκτυο όπως είναι το Internet. Η αξιοπιστία των ασφαλών συστημάτων επικοινωνιών βασίζεται στη συμμετρική κρυπτογράφηση. Συχνά, ονομάζεται κρυπτογράφηση μυστικού κλειδιού επειδή τα κλειδιά, τα οποία είναι ίδια στα δύο άκρα της ζεύξης επικοινωνιών, πρέπει να κρατηθούν μυστικά. Η διαδικασία που ακολουθείται περιγράφεται παρακάτω:

1) Τα μυστικά κλειδιά παράγονται, μεταφέρονται στα δύο άκρα της ζεύξης και αποθηκεύονται στις συσκευές κρυπτογράφησης έτσι ώστε να είναι γνωστά μόνο στον εξουσιοδοτημένο αποστολέα και παραλήπτη. Εάν ένας επιτιθέμενος καταφέρει να παράγει ένα αντίγραφο αυτού του κλειδιού, τότε

μπορεί και να αποκρυπτογραφήσει τα δεδομένα, καθιστώντας το σύστημα ανασφαλές.

2) Το μήνυμα του αποστολέα κρυπτογραφείται με το μυστικό κλειδί και μετατρέπεται σε μήνυμα κωδικών.
3) Το κρυπτογραφημένο μήνυμα μεταδίδεται πάνω στη ζεύξη επικοινωνιών.
4) Ένας υποκλοπέας που ακούει στη ζεύξη μπορεί να ανακόψει το κρυπτογραφημένο μήνυμα, αλλά χωρίς το μυστικό κλειδί δεν μπορεί να αποκρυπτογραφήσει τα δεδομένα και να διαβάσει το αρχικό μήνυμα. Έτσι, η συμμετρική κρυπτογράφηση παρέχει εμπιστευτικότητα.
5) Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το μυστικό κλειδί και έχει στη διάθεσή του το αρχικό μήνυμα.

3.10. Προστασία προσωπικών πληροφοριών ή ιδιωτικότητας (privacy protection)

Κάποιοι ισχυρίζονται ότι οι συχνά συλλεγόμενες μετρήσεις, για παράδειγμα κάθε 15 λεπτά, ίσως προσφέρουν ένα παράθυρο παρακολούθησης για τις δραστηριότητες που συμβαίνουν μες στο σπίτι, εκθέτοντας ένα πλούτο ιδιωτικών δραστηριοτήτων σε οποιονδήποτε έχει πρόσβαση στις πληροφορίες ενεργειακής κατανάλωσης.

Για παράδειγμα, η γνώση της λειτουργίας μιας συσκευής ίσως υπονοεί ότι το σπίτι κατοικείται ή ότι λείπουν οι κάτοικοί του, καθώς επίσης να γίνουν γνωστές και πληροφορίες για τον τρόπο ζωής των κατοίκων, όπως οι ώρες ύπνου.

Γι αυτό το λόγο, τα δεδομένα μέτρησης πρέπει να μπορούν να συναθροίζονται και να κρυπτογραφούνται έτσι ώστε οι ατομικές πληροφορίες να διατηρούν την ανωνυμία τους τουλάχιστον στην κλίμακα μιας πόλης.

Πολύ πρόσφατα, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας στην Αμερική εξέδωσε ένα σετ οδηγιών που εστιάζουν στην ανάπτυξη πολιτικών και πρακτικών για την προστασία της ιδιωτικής ζωής.

Μια λύση στο ζήτημα αυτό, μπορεί να προσφέρει η λειτουργία του έξυπνου μετρητή. Ο έξυπνος μετρητής μπορεί να δράσει σαν την πύλη δικτύου ανάμεσα σε εσωτερικές και εξωτερικές οντότητες. Αντί ο πάροχος να έχει τη δυνατότητα να ελέγχει άμεσα τις προσωπικές οικιακές συσκευές, μπορεί να αναζητά τον έξυπνο μετρητή για να μειώσει τη συνολική κατανάλωση ενέργειας(π.χ. κατά τη διάρκεια ωρών αιχμής, ο πάροχος θα συμβουλέψει τους έξυπνους μετρητές να περιορίσουν τις καταναλώσεις τους, προσφέροντας κίνητρα παράλληλα) και τότε ο έξυπνος μετρητής να αποφασίζει ποιες συσκευές να απενεργοποιήσει ή να περιορίσει τη λειτουργία τους. Φυσικά, οι ίδιοι οι καταναλωτές θα ιεραρχούν την προτεραιότητα των συσκευών τους. Η παραπάνω προσέγγιση ορίζει τον έξυπνο μετρητή ως τοίχο προστασίας που κρύβει τις προσωπικές συσκευές από τον πάροχο ηλεκτρισμού και προστατεύει την ιδιωτική ζωή των καταναλωτών.

3.11. Αντιμετώπιση ανάλυσης κυκλοφορίας κίνησης (traffic analysis)

Η ανάλυση κυκλοφορίας κίνησης είναι μια παθητική επίθεση που θέτει σε κίνδυνο ζητήματα κυρίως ιδιωτικής ζωής και ανωνυμίας. Σε αυτή την επίθεση, ο επιτιθέμενος δεν αλλάζει τα δεδομένα ενός μηνύματος, αλλά προσπαθεί να μάθει πληροφορία από το σύστημα και να κάνει χρήση αυτής αργότερα. Συγκεκριμένα, στοχεύει να αντιληφθεί την ταυτότητα και την τοποθεσία των συνδιαλεγόμενων παρατηρώντας

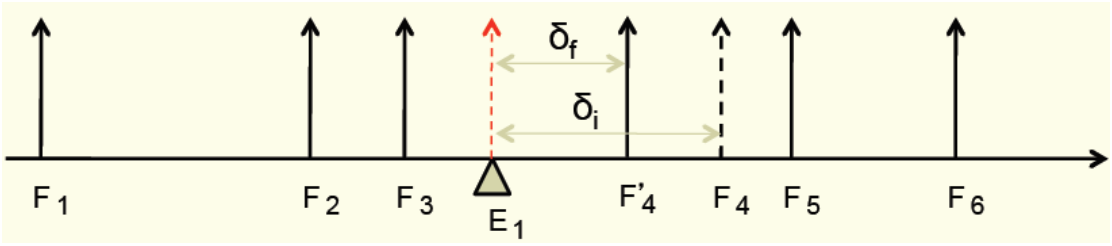
τις χρονικές στιγμές και τα μήκη των μηνυμάτων στη ζεύξη του δικτύου. Για παράδειγμα, στα δεδομένα μετρήσεων των συσκευών PMU, μπορούν να αποκαλυφθούν οι τοποθεσίες των PMUs και των κεντρικών σταθμών, καθώς επίσης και η διαδρομή που ακολουθούν τα δεδομένα. Έτσι, η πληροφορία που αντλήθηκε μπορεί να χρησιμοποιηθεί για εκτόξευση οργανωμένης επίθεσης στους μετρητές αυτούς.

Σημειώνεται ότι τα δεδομένα παράγονται περιοδικά σε καθορισμένα διαστήματα και το μέγεθος του πακέτου είναι σταθερό για συγκεκριμένες ροές, κάνοντας ευκολότερο το έργο των επιτιθέμενων να συσχετίσουν τις παραμέτρους της κυκλοφορίας, όπως χρονικές στιγμές και ποσότητα πληροφορίας. Επίσης, η κρυπτογράφηση μπορεί να αποκρύψει τα περιεχόμενα δεδομένα, αλλά δεν μπορεί να κρύψει τη χρονική στιγμή μετάδοσης της πληροφορίας.

Η συνάθροιση τυχαίου αριθμού δεδομένων στους μετρητές, παράγει ένα πακέτο τυχαίου μεγέθους και έτσι αποφεύγεται η αποστολή πακέτων σταθερού μήκους. Ωστόσο, ένα μειονέκτημα είναι ότι εισάγεται καθυστέρηση στη διαδικασία μέτρησης.

Ενώ η συνάθροιση την δεδομένων παράγει πακέτα τυχαίου μεγέθους, το διάστημα μεταξύ τους παραμένει ίδιο και μπορεί να συσχετιστεί για να εντοπιστεί μια ροή. Έτσι, προτείνεται παράλληλα με τη συνάθροιση πακέτων, και η αποστολή ψεύτικων πακέτων ανά τυχαία χρονικά διαστήματα από τους δρομολογητές, κρύβοντας την παρουσία αληθινών γεγονότων μέσα σε ψεύτικες μεταδόσεις.

Γι αυτό το λόγο, χρησιμοποιώντας συνάθροιση πακέτων εμποδίζονται οι συσχετίσεις πακέτων βασισμένες στο μέγεθος πακέτου, ενώ χρησιμοποιώντας παράλληλα συνάθροιση και εκπομπή ψεύτικων πακέτων, εμποδίζονται οι συσχετίσεις πακέτων βασισμένες στη χρονική στιγμή αποστολής και λήψης.



Εικόνα 3-3 Αποστολή ψεύτικων πακέτων ανά τυχαία χρονικά διαστήματα

4. Προστασία της προσωπικής πληροφορίας (privacy) στο έξυπνο δίκτυο

4.1. Τα δεδομένα στο έξυπνο δίκτυο

Το έξυπνο δίκτυο είναι ένα πρόσφατο παράδειγμα που αντιπροσωπεύει ένα τεράστιο αριθμό νέων τεχνολογιών που στοχεύουν να αναμορφώσουν το δίκτυο ηλεκτρικής ενέργειας. Ένας από τους στόχους του έξυπνου δικτύου είναι να μεταφέρει ευφυΐα στο υπάρχον ηλικιωμένο δίκτυο έτσι ώστε να βελτιώσει την αποτελεσματικότητα και την ανθεκτικότητά του σε νέες υψηλότερες ενεργειακές απαιτήσεις (αναμένεται ότι η κατανάλωση ηλεκτρικής ενέργειας θα τριπλασιαστεί παγκοσμίως μέχρι το 2050). Ένας τρόπος να επιτευχθεί αυτό είναι η δημιουργία αμφίδρομων δικτύων επικοινωνιών για διασύνδεση των στοιχείων του έξυπνου δικτύου. Αυτά τα δίκτυα θα δώσουν τη δυνατότητα παρακολούθησης της κατάστασης του δικτύου και της εκτέλεσης των κατάλληλων ενεργειών για παροχή σταθερότητας και λειτουργικότητας. Επίσης θα υποστηρίξουν βελτιστοποιήσεις πραγματικού χρόνου, όπως διαχείριση φορτίου, κατανεμημένη αποθήκευση ενέργειας (π.χ. ηλεκτρικά οχήματα) και κατανεμημένη παραγωγή ενέργειας (π.χ. από ανανεώσιμες πηγές ενέργειας).

Η εισαγωγή των ανανεώσιμων πηγών και των ηλεκτρικών οχημάτων στο δίκτυο αποτελούν παράγοντες που απαιτούν αυτή την αναμόρφωση. Η παραγωγή ηλεκτρικής ενέργειας που βασίζεται στις ανανεώσιμες πηγές ενέργειας, όπως ηλιακή και αιολική ενέργεια, ίσως γνωρίζουν απότομες μεταβολές λόγω των καιρικών συνθηκών. Αυτό ίσως προκαλέσει μεγάλες διακυμάνσεις τάσης που δεν είναι επιθυμητές από την άποψη της σταθερότητας του δικτύου. Από την άλλη μεριά, τα ηλεκτρικά οχήματα αποτελούν ένα αξιόλογο νέο φορτίο, αλλά ταυτόχρονα μπορούν να εξυπηρετήσουν ως αποθηκευτικές μονάδες ενέργειας και οποτεδήποτε μπορούν να εξομαλύνουν αιχμές φορτίου.

4.2. Προβλήματα προστασίας προσωπικής πληροφορίας

Το έξυπνο δίκτυο διαθέτει την ικανότητα να συλλέγει και να αποθηκεύει τις πληροφορίες (κατανάλωση ενέργειας) από το δίκτυο. Αυτό επιτυγχάνεται με συνεχείς μετρήσεις σε οικιακό επίπεδο υψηλού βαθμού ανάλυσης και πιστότητας. Οι έξυπνοι μετρητές έχουν τη δυνατότητα να μετρούν και να επικοινωνούν τεχνικά δεδομένα κατανάλωσης ενέργειας σε πραγματικό χρόνο και να διευκολύνουν με αυτό τον τρόπο τον απομακρυσμένο έλεγχο και παρακολούθηση του δικτύου.

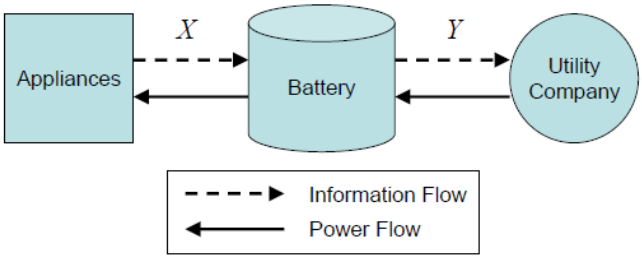
Αν και οι υπάρχοντες πολιτικοί κανόνες οπουδήποτε στον κόσμο απαγορεύουν την επαναχρησιμοποίηση συλλεγμένων δεδομένων, η αποθήκευση των δεδομένων δίνει τη δυνατότητα της κακομεταχείρισής τους. Εάν επιπλέον τα συλλεγμένα και αποθηκευμένα δεδομένα γίνουν διαθέσιμα σε διάφορες άλλες ομάδες ατόμων (εκτός των υπεύθυνων παρόχων εταιριών) όπως δικαστικές αρχές, διαφημιστικές εταιρίες και κακόβουλα άτομα, αυτό θα μπορούσε να αποτελέσει κίνδυνο για την προσωπική ζωή και ασφάλεια των καταναλωτών. Τα δεδομένα που συλλέγονται από έναν οικιακό έξυπνο μετρητή μπορούν ενδεχομένως να αποκαλύψουν ευαίσθητες

προσωπικές πληροφορίες σχετικά με τους ιδιοκτήτες. Η πάροχος εταιρία μπορεί να αναλύσει τα δεδομένα φορτίου κάθε νοικοκυριού και με αυτό τον τρόπο να ανακαλύψει τις οικιακές συσκευές και τις ώρες λειτουργίας τους. Τα συνεχώς συλλεγόμενα δεδομένα μέτρησης ίσως παρέχουν ένα παράθυρο εισβολής για τις δραστηριότητες που συμβαίνουν μέσα στα σπίτια, εκθέτοντας έναν πλούτο προσωπικών δραστηριοτήτων σε οποιονδήποτε έχει πρόσβαση στις πληροφορίες ηλεκτρικής κατανάλωσης. Για παράδειγμα, η γνώση της λειτουργίας μιας οικιακής συσκευής ίσως υπονοεί απασχόληση ή κενότητα μιας οικίας καθώς και πληροφορίες τρόπου ζωής, όπως ώρες ύπνου.

Η ανάγκη για την προστασία των προσωπικών δεδομένων στο έξυπνο δίκτυο αναγνωρίζεται από πολλά σωματεία προτυποποίησης, όπως το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογιών (NIST) στις Ηνωμένες Πολιτείες Αμερικής. Ενώ αναζητούνται ρωμαλέες πολιτικές για την προστασία των προσωπικών δεδομένων που θα καθορίσουν τη χρησιμοποίηση των δεδομένων μεταφοράς στο έξυπνο δίκτυο, κάποια σενάρια προτείνονται που έχουν σκοπό να συνεισφέρουν προς αυτή την κατεύθυνση. Για παράδειγμα, τα δεδομένα μέτρησης μπορούν να συναθροίζονται και να κρυπτογραφούνται με τέτοιο τρόπο ώστε οι ατομικές πληροφορίες να είναι ανώνυμες σε κλίμακα ενός τμήματος πόλης. Επίσης, τα δεδομένα μέτρησης μπορούν να διαχωριστούν σε χαρακτηριστικά δεδομένα χαμηλής συχνότητας (π.χ. τα δεδομένα που χρησιμοποιούνται για τιμολόγηση) και σε ανώνυμα τεχνικά δεδομένα υψηλής συχνότητας (π.χ. τα δεδομένα που χρησιμοποιούνται για τη διαχείριση απόκρισης σε ζήτηση). Και πάλι όμως, στα προηγούμενα παραδείγματα, η προστασία των προσωπικών δεδομένων εξαρτάται από τις σχέσεις εμπιστοσύνης και τις πολιτικές διακίνησης δεδομένων που διέπουν τα εμπλεκόμενα άτομα.

4.3. Ένα απλό σενάριο διαχείρισης του οικιακού ηλεκτρικού φορτίου

Για την προστασία των προσωπικών δεδομένων, έχει προταθεί ένα απλό σενάριο διαχείρισης του οικιακού ηλεκτρικού φορτίου. Υπάρχει η δυνατότητα απόκτησης ελέγχου της ροής ισχύος μέσα σε ένα σπίτι, δίνοντας τη δυνατότητα σε μια επαναφορτιζόμενη μπαταρία να τροφοδοτεί ένα μέρος της ζήτησης ηλεκτρικής ενέργειας και το υπόλοιπο μέρος να τροφοδοτείται κανονικά από το δίκτυο. Δηλαδή, οι μετρήσεις προσωπικών δεδομένων μπορούν να προστατευθούν χρησιμοποιώντας μια μπαταρία για να αποκρύψει ενεργειακά προφίλ χρηστών.



Εικόνα 4-1 Ροές ισχύος ελεγχόμενες από την μπαταρία

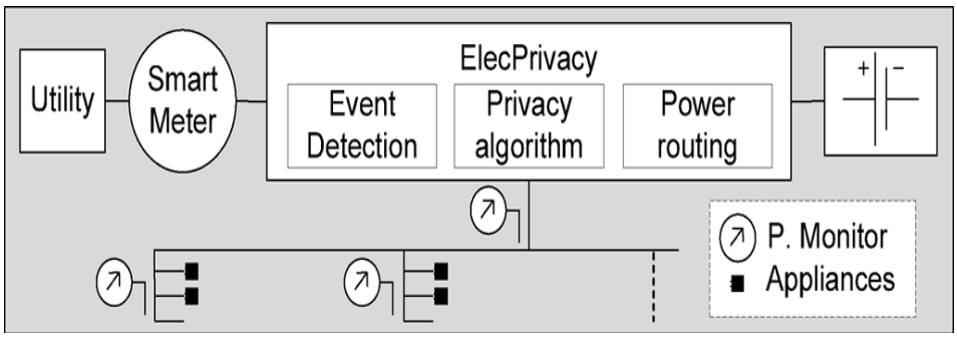
Το νοικοκυριό μπορεί να τροποποιήσει μερικώς το προφίλ κατανάλωσης φορτίου του χρησιμοποιώντας μια επαναφορτιζόμενη μπαταρία. Η ροή της πληροφορίας γίνεται από αριστερά προς τα δεξιά, όπως παρουσιάζεται στην Εικόνα 4-1. Η είσοδος φορτίου X της μπαταρίας είναι το συνολικό φορτίο των οικιακών συσκευών. Η έξοδος φορτίου Y της μπαταρίας είναι ο συνδυασμός του φορτίου των οικιακών συσκευών και της μπαταρίας, το οποίο φορτίο αναφέρεται στον έξυπνο μετρητή και κατόπιν στην εταιρία παροχής. Η ισχύς, από την άλλη μεριά, ρέει από δεξιά προς τα αριστερά, από την εταιρία παροχής ηλεκτρικής ενέργειας και μέσω της μπαταρίας προς τις οικιακές συσκευές. Οποιαδήποτε στιγμή, η μπαταρία μπορεί να εκτελέσει ένα συνδυασμό από τις ακόλουθες ενέργειες (ή καμία από αυτές) ανάλογα με τη χωρητικότητά της:

- Μεταφορά ηλεκτρικής ενέργειας από την εταιρία παροχής κατευθείαν προς τις οικιακές συσκευές
- Αποθήκευση ηλεκτρικής ενέργειας από την εταιρία παροχής για μελλοντική χρήση
- Τροφοδότηση των οικιακών συσκευών με προηγούμενη αποθηκευμένη ηλεκτρική ενέργεια

Με αυτό τον τρόπο, η φόρτιση και η αποφόρτιση της μπαταρίας μπορεί να διαχειριστεί την έξοδο φορτίου Y, αποκρύπτοντας κάποιες από τις πληροφορίες κάποιες από τις πληροφορίες που περιέχονται στην είσοδο φορτίου X. Ο αλγόριθμος που προτείνεται για τον τρόπο φόρτισης/αποφόρτισης της μπαταρίας περιγράφεται παρακάτω και κύριος σκοπός του είναι την έξοδο φορτίου Y στην πιο πρόσφατη τιμή της όποτε αυτό καθίσταται δυνατό.

4.4. Σύστημα προστασίας προσωπικών δεδομένων "ElecPrivacy"

Αυτό το σύστημα προστασίας προσωπικών δεδομένων προϋποθέτει την ύπαρξη μιας μονάδας αποθήκευσης ενέργειας, όπως ένα ηλεκτρικό όχημα, και έναν μηχανισμό δρομολόγησης ηλεκτρικής ενέργειας, ο οποίος ασκεί επιλεκτικό έλεγχο και αναμιγνύει ροές ηλεκτρικής ισχύος ενός πλήθους ηλεκτρικών πηγών για να καλύψει τη ζήτηση ενέργειας. Για παράδειγμα, εάν επιθυμούμε να χρησιμοποιήσουμε την ενέργεια της μπαταρίας για να αποκρύψουμε την καταναλωτική ζήτηση μιας οικιακής συσκευής, η ενέργεια της μπαταρίας θα μειώσει τη σύνθετη αιχμή ζήτησης ισχύος.



Εικόνα 4-2 Σύστημα προστασίας προσωπικών δεδομένων "ElecPrivacy"

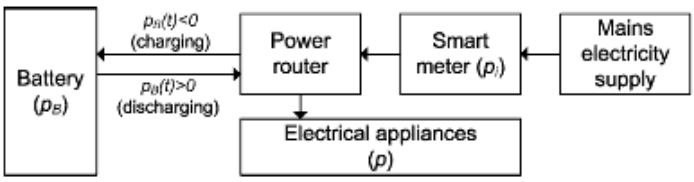
Στην Εικόνα 4-2, φαίνεται μια συνοπτική παρουσίαση αυτού του συστήματος προστασίας προσωπικών δεδομένων, αποτελούμενο από τα εξής υποσυστήματα:

- *Μηχανισμός μέτρησης* — χρησιμοποιείται για να παρέχει ένα σύνολο μετρήσεων ηλεκτρικής ενέργειας από τον έξυπνο μετρητή ή από τις έξυπνες οικιακές συσκευές. Μπορεί να εφαρμοστεί μαζί με ένα σύνολο από οθόνες ηλεκτρικής ενέργειας προσκολλημένες στις διαφορετικές συσκευές.
- *Εντοπισμός γεγονότος* — αναλύει δεδομένα μετρήσεων με σκοπό να εντοπίσει ένα τρέχον, ή να προβλέψει ένα επερχόμενο, γεγονός που ίσως περιέχει προσωπική πληροφορία (μια αλλαγή στην κατανάλωση ενέργειας από το άνοιγμα/κλείσιμο μιας οικιακής συσκευής).
- *Αλγόριθμος προστασίας προσωπικών δεδομένων* — συντελεί δρομολόγηση ενέργειας για να αποκρύψει ένα γεγονός κατανάλωσης που εντοπίστηκε.
- *Δρομολόγηση ηλεκτρικής ενέργειας* — αναμιγνύει μια ιδιωτική πηγή ενέργειας (όχι της παρόχου εταιρίας, π.χ. μια επαναφορτιζόμενη μπαταρία) με την ενέργεια από τον πάροχο για να ανταποκριθεί στην καταναλωτική ζήτηση των οικιακών συσκευών.

Τέλος, ο κύριος στόχος αυτού του συστήματος είναι αρχικά ο εντοπισμός μιας απειλής των προσωπικών δεδομένων και εν συνεχεία η απόκρισή του εκτελώντας δρομολόγηση ηλεκτρικής ενέργειας για να αποκρύψει τα φορτία των οικιακών ηλεκτρικών συσκευών. Ο μη εντοπισμός των γεγονότων διαφόρων ατομικών οικιακών συσκευών προσφέρει προστασία της ιδιωτικής ζωής και της προσωπικής συμπεριφοράς, δηλαδή του δικαιώματος των ατόμων να κρατούν κάθε γνώση των δραστηριοτήτων τους και των επιλογών τους μακριά από κάθε άλλον.

4.5. Αλγόριθμος προστασίας προσωπικών δεδομένων

Θεωρούμε την απλή περίπτωση όπου μια μπαταρία αποφορτίζεται ή επαναφορτίζεται με μέση ισχύ $p_B(t)$ σε ένα διάστημα Δt για να αποκρύψει μια δεδομένη κατανάλωση φορτίου $p(t)$. Με τη χρήση του μηχανισμού ανάμιξης ισχύος μπαταρίας, το ίχνος οικιακής κατανάλωσης ηλεκτρικής ισχύος γίνεται $p_i = p - p_B$, όπου αυτό το μοντέλο απεικονίζεται στην Εικόνα 4-3. Όσο μεγαλύτερο το μέγεθος της μπαταρίας, τόσο μεγαλύτερη καταναλωτική ισχύς αποκρύπτεται.



Εικόνα 4-3 Μοντέλο ανάμιξης ισχύος μπαταρίας

Υποθέτουμε ότι το ίχνος οικιακής κατανάλωσης ηλεκτρικής ισχύος p_i ορίζεται από τον μετασχηματισμό C του πραγματικού χρόνου φορτίου ζήτησης p, έτσι ώστε $p_i =$

*C*p. Αναφερόμαστε στον μετασχηματισμό *C* ως τον αλγόριθμο προστασίας των προσωπικών δεδομένων.

Ο προτεινόμενος αλγόριθμος χρησιμοποιεί την μπαταρία για να αντισταθεί απέναντι στις αλλαγές του φορτίου ζήτησης. Δηλαδή, ο αλγόριθμος αναγκάζει την μπαταρία είτε να αποφορτίζει είτε να επαναφορτίζει όταν το απαιτούμενο φορτίο p(t) είναι μεγαλύτερο ή μικρότερο αντίστοιχα από το προηγούμενο μετρημένο φορτίο p_i (t – Δt). Η ισχύς και η διάρκεια αποφόρτισης/επαναφόρτισης της μπαταρίας διαμορφώνονται έτσι ώστε να εξισορροπούνται οι διαφορές ισχύος, εάν τα όρια της μπαταρίας το επιτρέπουν.

Current battery charge level: $p_B(t) = e_i(t) - e(t - \Delta t) + p(t)\Delta t$
if $D(t) = p(t) - p_i(t - \Delta t) > 0$ (discharging case) **then**
  if There is enough battery energy/power to provide $D(t)$ for Δt **then**
    Mix in battery power so that $p_i(t) = p_i(t - \Delta t)$
  else
    Use maximum battery power while $B(t) > 0$
  end if
end if
if $C(t) = p_i(t - \Delta t) - p(t) > 0$ (charging case) **then**
  if Enough battery 'emptiness' to absorb $C(t)$ for Δt **then**
    Recharge battery so that $p_i(t) = p_i(t - \Delta t)$
  else
    Fully recharge battery
  end if
end if

Εικόνα 4-4 Αλγόριθμος προστασίας προσωπικών δεδομένων

Μια συνέπεια της χρησιμοποίησης του αλγορίθμου προστασίας προσωπικών δεδομένων είναι ότι τροποποιεί τα μοντέλα πρόβλεψης κατανάλωσης ή ζήτησης ηλεκτρικής ενέργειας όπως υπολογίζονται από την εκάστοτε πάροχο εταιρία. Επειδή το κόστος παραγωγής ηλεκτρικής ενέργειας εξαρτάται από τη ζήτηση, αυτό σημαίνει ότι η τιμή της παραγωγής ηλεκτρικής ενέργειας μπορεί να είναι διαφορετική συγκρινόμενη με την περίπτωση που ο αλγόριθμος προστασίας προσωπικών δεδομένων χρησιμοποιείται. Επίσης στο έξυπνο δίκτυο, άλλοι παράγοντες που επηρεάζουν τα μοντέλα πρόβλεψης κατανάλωσης ηλεκτρικής ενέργειας είναι οι ανανεώσιμες πηγές ενέργειας και τα ηλεκτρικά οχήματα που επηρεάζουν και αυτά θετικά την τιμή παραγωγής ηλεκτρικής ενέργειας.

5. Κρυπτογραφία (Cryptography)

5.1. Αναγνώριση και Αυθεντικοποίηση

Προϋπόθεση για τη σωστή εφαρμογή και λειτουργία των μηχανισμών ασφάλειας σε ένα σύστημα αποτελεί η ύπαρξη αξιόπιστου συστήματος αναγνώρισης και αυθεντικοποίησης των χρηστών. Τα αποτελέσματα της αναγνώρισης και της αυθεντικοποίησης αποτελούν τη βάση για την εξουσιοδότηση των χρηστών προκειμένου κατόπιν να χρησιμοποιήσουν τους πόρους του πληροφοριακού συστήματος.

5.1.1. Αναγνώριση (identification)

Ένα ασφαλές σύστημα πρέπει με κάποιον τρόπο να αναγνωρίζει τις ταυτότητες των χρηστών καθώς αυτοί ζητούν να χρησιμοποιήσουν τις υπηρεσίες του. Για παράδειγμα, η αναγνώριση χρηστών απαιτείται για:

- Έλεγχο πρόσβασης σε υπολογιστές.
- Περιορισμό πρόσβασης σε κτίρια και προστατευμένες περιοχές μέσα σε κτίρια.
- Ελεγχόμενη χρήση των τραπεζικών τερματικών, όπως τα ATMs (Automatic Teller Machines).

5.1.2. Αυθεντικοποίηση (authentication)

Αυθεντικοποίηση ονομάζεται η διαδικασία επιβεβαίωσης της ταυτότητας ενός χρήστη. Το σύστημα αυθεντικοποίησης χρηστών αποτελεί την πρώτη γραμμή άμυνας ενάντια σε επίδοξους εισβολείς και αποσκοπεί στο να αποτρέψει μη εξουσιοδοτημένους χρήστες από το να επιτύχουν πρόσβαση στο σύστημα, απαιτώντας κάθε φορά από τους χρήστες να επικυρώνουν την εξουσιοδότησή τους πριν χρησιμοποιήσουν το σύστημα.

5.1.2.1. Τεχνικές αυθεντικοποίησης

Οι κυριότερες τεχνικές αυθεντικοποίησης χρήστη μπορούν να ταξινομηθούν στις παρακάτω βασικές κατηγορίες:

- Αυθεντικοποίηση από στοιχεία που έχει ο χρήστης—συνθηματικά (passwords), προσωπικοί αριθμοί αναγνώρισης (PINs) για τραπεζικές συναλλαγές, μαγνητικές και έξυπνες κάρτες.
- Αυθεντικοποίηση από χαρακτηριστικά του ίδιου του χρήστη—επιβεβαίωση υπογραφής, επιβεβαίωση δακτυλικού αποτυπώματος, αναγνώριση φωνής, αναγνώριση αμφιβληστροειδούς χιτώνα.

5.2. Τεχνικές κρυπτογραφίας

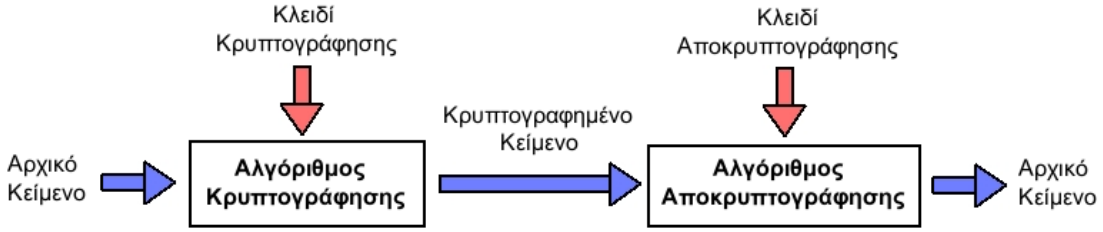
Η διαδεδομένη χρήση του διαδικτύου σε εφαρμογές που περιλαμβάνουν επικοινωνίες ευαίσθητων δεδομένων εισάγει την ανάγκη για λύσεις στα προβλήματα ασφάλειας που υπάρχουν.

Για την προστασία των πληροφοριών που μεταδίδονται μέσω δικτύων ψηφιακών επικοινωνιών χρησιμοποιούνται σήμερα ευρέως συστήματα κρυπτογραφίας δημοσίου κλειδιού και μυστικού κλειδιού.

Η εκτεταμένη χρήση της κρυπτογραφίας επιτρέπει για τις διακινούμενες πληροφορίες:

1) *Κρυπτογράφηση (encryption)* και *αποκρυπτογράφηση (decryption)*
2) *Ανίχνευση αλλοιώσεων (tamper detection)*
3) *Αυθεντικοποίηση (authentication)* του αποστολέα

Επιπλέον, μαζί με τη συνδρομή των ψηφιακών πιστοποιητικών και των ψηφιακών υπογραφών, διασφαλίζεται τόσο η εμπιστευτικότητα όσο και η ακεραιότητα των διακινούμενων δεδομένων.



Εικόνα 5-1 Τυπικό σύστημα κρυπτογράφησης

5.2.1. Κρυπτογραφία Μυστικού Κλειδιού (Συμμετρική Κρυπτογραφία)

Οι αλγόριθμοι συμμετρικής κρυπτογραφίας βασίζονται στην ύπαρξη ενός μόνο μυστικού κλειδιού που είναι γνωστό μόνο στα συναλλασσόμενα μέρη. Αυτό το κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση του μηνύματος.

Η συμμετρική κρυπτογραφία εγγυάται την *εμπιστευτικότητα* (confidentiality) των δεδομένων αφού κρυπτογραφεί το μήνυμα με ένα μυστικό κλειδί. Το μήνυμα που παράγεται αποκρυπτογραφείται από τον παραλήπτη με τη βοήθεια του ίδιου κλειδιού, το οποίο πρέπει να μένει μυστικό μεταξύ των δύο.

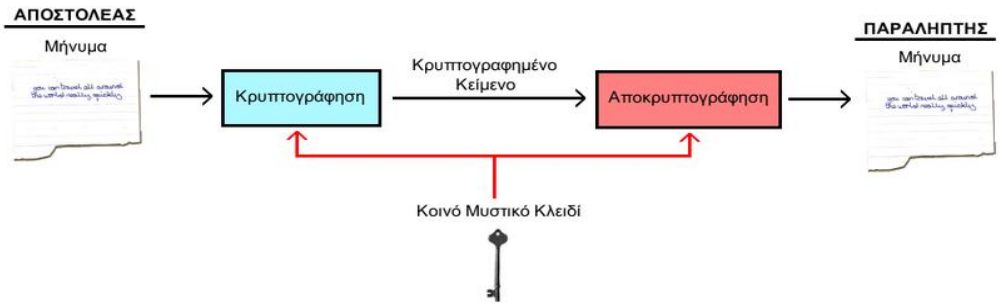
Το βασικό πλεονέκτημα των συμμετρικών αλγορίθμων είναι ότι οι χρήστες δεν καταλαβαίνουν κάποια σημαντική χρονική καθυστέρηση λόγω της κρυπτογράφησης / αποκρυπτογράφησης. Αρκεί να διατηρείται μυστικό το διαμοιρασμένο (shared) κλειδί.

Παρόλο που η συμμετρική κρυπτογράφηση εγγυάται την εμπιστευτικότητα, δεν μπορεί να εγγυηθεί για το πώς θα γίνει η ανταλλαγή του κλειδιού με ασφάλεια. Επομένως, όταν αποστολέας και παραλήπτης δεν γνωρίζονται, θα πρέπει να υπάρχει ένα ασφαλές κανάλι επικοινωνίας για τη μεταφορά του κλειδιού.

Ένα ακόμη σοβαρό πρόβλημα αφορά την *αναγνώριση ή ταυτοποίηση (identification)* μεταξύ του αποστολέα και του παραλήπτη. Το πρόβλημα της ταυτοποίησης έγκειται στο ότι πολλοί άνθρωποι μπορεί να έχουν πρόσβαση στο κοινό κλειδί. Όταν κάποιος από αυτούς λάβει ένα κρυπτογραφημένο μήνυμα, ξέρει

ότι ήρθε από κάποιον από αυτούς όμως δεν μπορεί να αποδείξει ποιος πραγματικά του έστειλε το μήνυμα.

Επομένως, υπάρχει σημαντικό πρόβλημα διαχείρισης των κλειδιών και ιδιαίτερα σε ότι αφορά την αρχική διανομή τους.

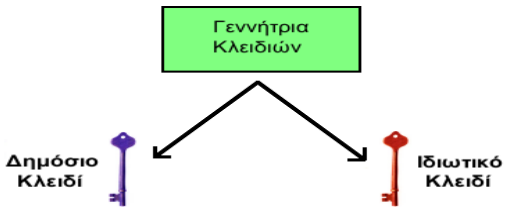


Εικόνα 5-2 Κρυπτογράφηση συμμετρικού κλειδιού

5.2.2. Κρυπτογραφία Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογραφία)

Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν διαμοιράζονται ένα μυστικό κλειδί, αλλά αντιθέτως έχουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες. Η κρυπτογράφηση δημοσίου κλειδιού περιλαμβάνει τη χρήση δύο κλειδιών:

- Ενός δημοσίου κλειδιού (public key)
- Ενός προσωπικού κλειδιού (private key)



Εικόνα 5-3 Χρήση δημοσίου και ιδιωτικού κλειδιού

Τα δεδομένα κρυπτογραφούνται με το δημόσιο κλειδί του παραλήπτη και αποστέλλονται. Όταν παραληφθούν αποκρυπτογραφούνται με το προσωπικό κλειδί του παραλήπτη. Τα δυο κλειδιά έχουν μαθηματική σχέση μεταξύ τους. Είναι υπολογιστικά όμως αδύνατο να βρει κανείς το κλειδί της αποκρυπτογράφησης από τη γνώση και μόνο του κλειδιού κρυπτογράφησης.

Πλεονέκτημα της κρυπτογράφησης δημοσίου κλειδιού είναι ότι το δημόσιο κλειδί διανέμεται ελεύθερα με αποτέλεσμα την εύκολη σύσταση ασφαλών καναλιών επικοινωνίας μεταξύ δυο απομακρυσμένων χρηστών, χωρίς αυτοί να χρειάζεται να συναντηθούν ή να μεσολαβήσει κάποιο έμπιστο τρίτο μέρος μεταξύ τους. Μειονέκτημά της αποτελεί το γεγονός ότι απαιτεί είναι αργή γιατί απαιτεί περισσότερους υπολογισμούς κρυπτογράφησης / αποκρυπτογράφησης.

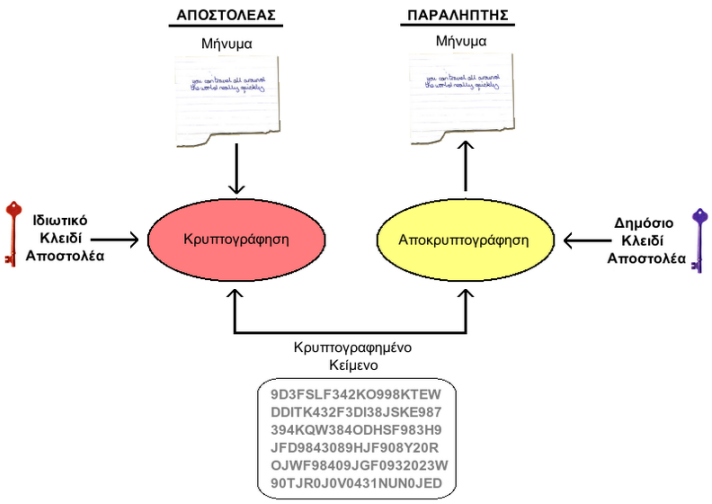
Για αυτό, χρησιμοποιείται η κρυπτογράφηση δημοσίου κλειδιού για την ανταλλαγή / διανομή συμμετρικών κλειδιών και στη συνέχεια χρησιμοποιείται η συμμετρική κρυπτογράφηση για την ουσιαστική επικοινωνία.

5.2.2.1. Τρόποι Κρυπτογράφησης Δημοσίου Κλειδιού

Κάθε χρήστης παράγει το δικό του ζεύγος κλειδιών (key pair), δηλαδή το δημόσιο και το ιδιωτικό κλειδί. Κατόπιν, γνωστοποιεί σε όλους τους χρήστες το δημόσιο κλειδί του προκειμένου να μπορούν να του αποστείλουν εμπιστευτικά (κρυπτογραφημένα) μηνύματα. Με αυτό τον τρόπο, οποιοσδήποτε έχει το δημόσιο κλειδί κρυπτογράφησης μπορεί να στείλει μυστικά μηνύματα, αλλά μόνο ο δημιουργός του ζεύγους κλειδιών μπορεί να τα αποκρυπτογραφήσει, αφού είναι ο μοναδικός κάτοχος του ιδιωτικού κλειδιού αποκρυπτογράφησης.

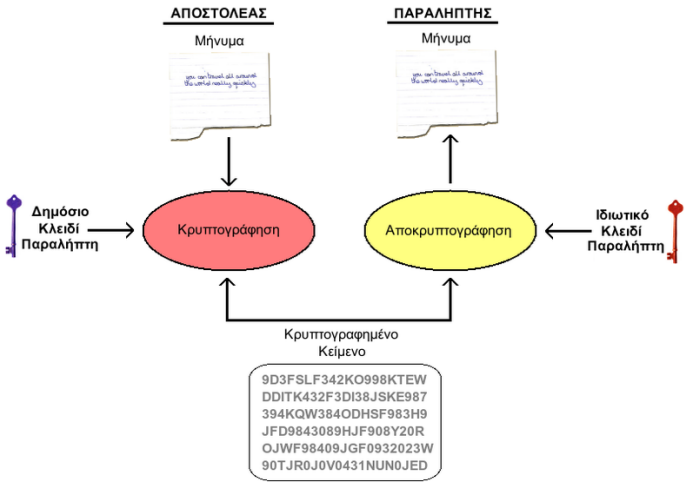
Η διαδικασία κρυπτογράφησης με τη χρήση του ζεύγους των κλειδιών μπορεί να γίνει με τρεις τρόπους:

1) Ο αποστολέας μπορεί να χρησιμοποιήσει το ιδιωτικό κλειδί του για την κρυπτογράφηση της πληροφορίας. Ο παραλήπτης που έχει ήδη διαθέσιμο το δημόσιο κλειδί του αποστολέα μπορεί να αποκρυπτογραφήσει το μήνυμα. Με αυτό τον τρόπο, μπορεί ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (authentication), αφού γνωρίζει το ιδιωτικό κλειδί που χρησιμοποιήθηκε. Παρόλα αυτά, δεν μπορεί να είναι σίγουρος για την εμπιστευτικότητα (confidentiality) των δεδομένων, γιατί οποιοσδήποτε θα μπορούσε να χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα και να αποκρυπτογραφήσει το μήνυμα.



Εικόνα 5-4 Αυθεντικοποίηση αλλά όχι Εμπιστευτικότητα

2) Εάν ο αποστολέας χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για την κρυπτογράφηση, τότε μόνο ο παραλήπτης με το ιδιωτικό κλειδί του μπορεί να αποκρυπτογραφήσει το μήνυμα. Αυτή η διαδικασία εξασφαλίζει την εμπιστευτικότητα της πληροφορίας, όμως δεν μπορεί να αποκαλύψει την ταυτότητα του αποστολέα αφού οποιοσδήποτε θα μπορούσε να έχει το δημόσιο κλειδί που έκανε την κρυπτογράφηση.



Εικόνα 5-5 Εμπιστευτικότητα αλλά όχι Αυθεντικοποίηση

3) Όταν οι παραπάνω δυο μέθοδοι συνδυαστούν μπορεί να επιτευχθεί τόσο η εμπιστευτικότητα της πληροφορίας όσο και η ταυτοποίηση των εμπλεκόμενων μερών. Ο αποστολέας μπορεί να κρυπτογραφήσει τα δεδομένα πρώτα με το ιδιωτικό του κλειδί και στη συνέχεια με το δημόσιο κλειδί του παραλήπτη. Όταν ο παραλήπτης λάβει το μήνυμα, χρησιμοποιεί το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στη συνέχεια αποκρυπτογραφεί το αποτέλεσμα με το δημόσιο κλειδί του αποστολέα (ταυτοποίηση).

5.3. Ψηφιακές Υπογραφές (Digital Signatures)

Η κρυπτογράφηση / αποκρυπτογράφηση αντιμετωπίζει το πρόβλημα της υποκλοπής (eavesdropping), αλλά όχι αυτά της παραποίησης και της προσποίησης. Για την αντιμετώπιση της παραποίησης χρησιμοποιείται μια μαθηματική συνάρτηση που ονομάζεται *μονόδρομος τεμαχισμός* (one-way hash) ή *σύνοψη μηνύματος* (message digest). Το αποτέλεσμα της εφαρμογής του μονόδρομου τεμαχισμού σε ένα μήνυμα είναι ένας αριθμός σταθερού μήκους, μοναδικός για κάθε μήνυμα και χωρίς τη δυνατότητα εξαγωγής του μηνύματος από τη γνώση μόνο του αριθμού αυτού (μονόδρομος).

Ο μονόδρομος τεμαχισμός κάθε μηνύματος κρυπτογραφείται με το προσωπικό / ιδιωτικό κλειδί του αποστολέα. Ο κρυπτογραφημένος αυτός τεμαχισμός μαζί με την πληροφορία για τον αλγόριθμο τεμαχισμού αποτελούν την ψηφιακή υπογραφή του αποστολέα.

Στη μεριά του παραλήπτη, αποκρυπτογραφείται η ψηφιακή υπογραφή με το δημόσιο κλειδί του αποστολέα. Με βάση τον γνωστό, και στα δυο μέρη, αλγόριθμο τεμαχισμού επαναϋπολογίζεται ο τεμαχισμός του μηνύματος. Κατόπιν, συγκρίνονται οι δυο τεμαχισμοί, αυτός που παραλήφθηκε και αυτός που υπολογίστηκε. Αν δεν είναι ίδιοι, τότε είτε έχει αλλαχθεί το μήνυμα είτε η ψηφιακή υπογραφή δεν αντιστοιχεί στο δημόσιο κλειδί του αποστολέα. Αν είναι ίδιοι, τότε ο παραλήπτης είναι βέβαιος ότι το δημόσιο κλειδί που χρησιμοποιεί αντιστοιχεί με το ιδιωτικό κλειδί που χρησιμοποιήθηκε για τη δημιουργία της ψηφιακής υπογραφής και επιβεβαιώνεται η ακεραιότητα του μηνύματος.

5.4. Ψηφιακά Πιστοποιητικά (Digital Certificates)

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

Πιστοποίηση (certification) είναι η διαδικασία της αντιστοίχησης και δέσμευσης ενός δημοσίου κλειδιού σε ένα άτομο, οργανισμό ή μια άλλη οντότητα. Για το σκοπό αυτό χρησιμοποιούνται τα ψηφιακά πιστοποιητικά, τα οποία αποτελούν τελικά το μέσο με το οποίο μεταδίδονται με ασφαλή τρόπο οι τιμές των δημόσιων κλειδιών και οι πληροφορίες κατόχου που σχετίζονται με αυτά.

Τα ψηφιακά πιστοποιητικά είναι ηλεκτρονικά έγγραφα που χρησιμοποιούνται για την αναγνώριση ενός προσώπου / εξυπηρετητή / οργανισμού και τη συσχέτισή του με ένα δημόσιο κλειδί.

Η απόκτηση ενός ηλεκτρονικού πιστοποιητικού γίνεται μετά από αίτηση σε μια Αρχή Πιστοποίησης (Certificate Authority). Η Αρχή Πιστοποίησης επιβεβαιώνει την ταυτότητα του αιτούντος και εκδίδει το πιστοποιητικό, που περιλαμβάνει:

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

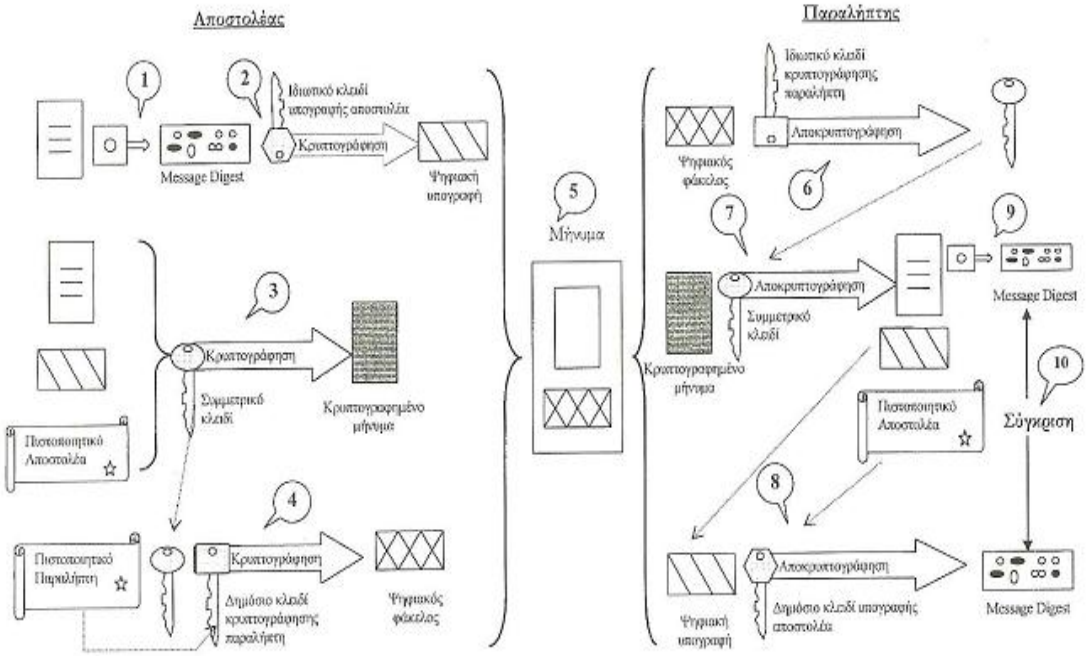
5.5. Συνολική Διαδικασία Κρυπτογράφησης

Για τη μετάδοση ενός μηνύματος από τον αποστολέα στον παραλήπτη, εφαρμόζεται η παρακάτω διαδικασία κρυπτογράφησης:

1) Ο αποστολέας εφαρμόζει στο αρχικό μήνυμα μια συνάρτηση κατακερματισμού (hash function) και παράγεται μια μοναδική τιμή που αποτελεί τη σύνοψη μηνύματος (message digest).
2) Ο αποστολέας κρυπτογραφεί τη σύνοψη μηνύματος με το ιδιωτικό κλειδί του και με αυτό τον τρόπο προκύπτει η ψηφιακή υπογραφή του.
3) Ο αποστολέας δημιουργεί ένα τυχαίο συμμετρικό κλειδί και το χρησιμοποιεί για να κρυπτογραφήσει το μήνυμα που θέλει να στείλει, την ψηφιακή υπογραφή του και ένα αντίγραφο του ψηφιακού πιστοποιητικού του, που περιέχει το δημόσιο κλειδί του.
4) Το ψηφιακό πιστοποιητικό του παραλήπτη, το οποίο ο αποστολέας πρέπει να διαθέτει πριν ξεκινήσει η διαδικασία, περιέχει το δημόσιο κλειδί του. Για να επιτευχθεί η ασφαλής μετάδοση του συμμετρικού κλειδιού, ο αποστολέας το κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη. Το κρυπτογραφημένο κλειδί που προκύπτει αποτελεί τον ψηφιακό φάκελο, και αποστέλλεται μαζί με το κρυπτογραφημένο μήνυμα του βήματος 3.
5) Το μήνυμα που στέλνεται στον παραλήπτη αποτελείται από:
   - Το συμμετρικά κρυπτογραφημένο μήνυμα (μαζί με την ψηφιακή υπογραφή και το ψηφιακό πιστοποιητικό του αποστολέα).

- Το ασύμμετρα (με το δημόσιο κλειδί του παραλήπτη) κρυπτογραφημένο συμμετρικό κλειδί (ψηφιακός φάκελος).

6) Ο παραλήπτης λαμβάνει το μήνυμα και αποκρυπτογραφεί τον ψηφιακό φάκελο με το ιδιωτικό του κλειδί, έτσι ώστε να αποκτήσει το συμμετρικό κλειδί.
7) Αποκρυπτογραφεί με το συμμετρικό κλειδί το κρυπτογραφημένο μήνυμα, μαζί με την υπογραφή και το πιστοποιητικό του αποστολέα.
8) Αποκρυπτογραφεί την ψηφιακή υπογραφή με το δημόσιο κλειδί του αποστολέα, που περιέχεται στο πιστοποιητικό που μόλις έλαβε. Έτσι, αποκτά τη γνήσια σύνοψη του κρυπτογραφημένου μηνύματος που παρέλαβε.
9) Χρησιμοποιεί την ίδια συνάρτηση κατακερματισμού που χρησιμοποίησε και ο αποστολέας και παράγει μια καινούρια σύνοψη για το αποκρυπτογραφημένο μήνυμα.
10) Τελικά, συγκρίνει τη δική του σύνοψη μηνύματος με αυτή που προέκυψε από την ψηφιακή υπογραφή του αποστολέα.



Εικόνα 5-6 Διαδικασία Κρυπτογράφησης

6. Ασύρματες Συνεργατικές Επικοινωνίες (Wireless Cooperative Communications)

6.1. Εισαγωγή

Συνεργασία είναι η διαδικασία του να εργάζεσαι μαζί συλλογικά, το αντίθετο του να δουλεύεις ξεχωριστά με ανταγωνισμό. Η ιδέα της συνεργασίας των ασύρματων επικοινωνιών δημιουργήθηκε ως απάντηση στην υποστήριξη της κινητικότητας των χρηστών και των περιορισμένων πόρων ενέργειας και ράδιο-φάσματος, που θέτουν προκλήσεις στις υπηρεσίες των ασύρματων δικτύων επικοινωνιών όσον αφορά τη χωρητικότητα και την απόδοσή του.

Ο όρος ασύρματες συνεργατικές επικοινωνίες (wireless cooperative communications) συνήθως αναφέρεται σε ένα ασύρματο σύστημα όπου οι κόμβοι χρηστών μοιράζονται και συντονίζουν τους ασύρματους πόρους τους (radio resources) με σκοπό να αυξήσουν την ποιότητα μετάδοσης. Στις συνεργατικές επικοινωνίες, ένας κόμβος δρα ως η πηγή και ένας άλλος ως ο προορισμός, ενώ οι υπόλοιποι κόμβοι εξυπηρετούν ως κόμβοι μεταφοράς. Επίσης, κάθε κόμβος αναμετάδοσης έχει το δικαίωμα να δρα ως πηγή ή προορισμός. Αυτή η ιδέα είναι ιδιαίτερα ελκυστική σε κάθε ασύρματο περιβάλλον, στο οποίο η ποιότητα καναλιού ποικίλλει και οι πόροι ενέργειας/φάσματος είναι περιορισμένοι. Η υψηλή απόδοση των ασυρμάτων συνεργατικών επικοινωνιών απαιτεί την κατάλληλη κατανομή φάσματος και ισχύος μεταξύ της πηγής και των ενδιάμεσων κόμβων μεταφοράς.

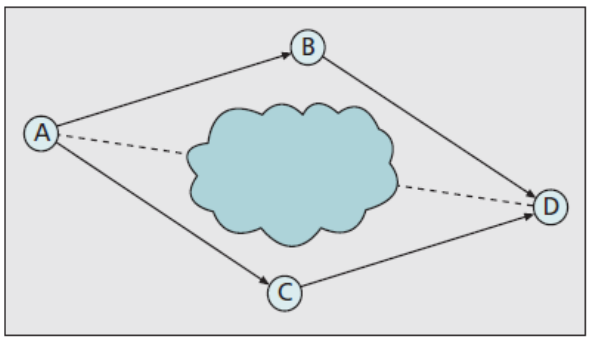
Η ιδέα της συνεργασίας των ασύρματων δικτύων επικοινωνιών μπορεί να γίνει αποτελεσματική στην αντιμετώπιση των περιορισμών απόδοσης των ασύρματων δικτύων λόγω της κινητικότητας των χρηστών και της ανεπάρκειας ενεργειακών πόρων. Η συνεργασία διαφορετικών οντοτήτων μπορεί να αυξήσει την αξιοπιστία των καναλιών μέσω της χωρικής ποικιλομορφίας, να βελτιώσει την ρυθμαπόδοση μέσω της συνάθροισης προσφερόμενων πόρων, να επιτύχει αδιάκοπη παροχή υπηρεσιών. Οι συνεργατικές επικοινωνίες μπορούν να βελτιώσουν τη συνδεσιμότητα των κόμβων του δικτύου, να αυξήσουν την απόδοση της ζεύξης, να εξοικονομήσουν την κατανάλωση ενέργειας του δικτύου, ακόμα και να αλλάξουν την τοπολογία του δικτύου για να επιτρέψουν συντομότερη δρομολόγηση.

Πράγματι, οι περισσότερες τρέχουσες εργασίες για τα ασύρματα δίκτυα προσπαθούν να δημιουργήσουν, να προσαρμόσουν και να διαχειριστούν ένα δίκτυο πάνω σε ένα λαβύρινθο μη συνεργατικών ασύρματων ζεύξεων point-to-point. Τέτοιες αρχιτεκτονικές φαίνονται σαν πολύπλοκα δίκτυα απλών ζεύξεων. Ωστόσο, πρόσφατες πρόοδοι στις συνεργατικές επικοινωνίες θα προσφέρουν πολλά πλεονεκτήματα ευελιξίας έναντι των παραδοσιακών τεχνικών. Η συνεργασία ανακουφίζει από συγκεκριμένα προβλήματα δικτύου, όπως λύση συγκρούσεων και δρομολόγησης, επιτρέποντας πιο απλά δίκτυα πιο πολύπλοκων ζεύξεων παρά πολύπλοκα δίκτυα απλών ζεύξεων.

Είναι αδύνατο για κάποιες ασύρματες κινητές συσκευές να υποστηρίζουν πολλαπλές κεραίες λόγω περιορισμών μεγέθους και κόστους. Όμως, οι συνεργατικές επικοινωνίες επιτρέπουν σε συσκευές με μια μοναδική κεραία να συνεργάζονται μεταξύ τους εκμεταλλευόμενες τη χωρική ποικιλομορφία και αποκομίζοντας τα οφέλη των MIMO συστημάτων (πολλαπλών εισόδων-πολλαπλών εξόδων), όπως η ανθεκτικότητα στην εξασθένηση, η υψηλή απόδοση, η χαμηλή ισχύ μετάδοσης και τα προσαρμοστικά δίκτυα.

Η συνεργασία μπορεί να πάρει διάφορες μορφές, συμπεριλαμβανομένου των συνεργατικών επικοινωνιών φυσικού στρώματος (physical-layer cooperative communications), συνεργατικών επικοινωνιών στρώματος ζεύξης δεδομένων, συνεργατικού και διανοητικού μέσου πρόσβασης του στρώματος ζεύξης δεδομένων (link-layer cooperative and cognitive medium access), συνεργατικής δρομολόγησης και εξισορρόπησης φορτίου του στρώματος δικτύου (network-layer cooperative routing and load balancing), του συνεργατικού από άκρη σε άκρη ελέγχου συμφόρησης του στρώματος μεταφοράς (transport-layer collaborative end-to-end congestion control), των συνεργατικών υπηρεσιών peer-to-peer (peer-to-peer file sharing→e.g., Bittorrent). Για να παραμείνουν ανταγωνιστικοί, οι πάροχοι ασύρματων υπηρεσιών θα πρέπει να μπορούν να παρέχουν υψηλής ποιότητας υπηρεσίες για όλες τις εφαρμογές, που περιλαμβάνουν φωνή, μηνύματα, δεδομένα και βίντεο.

Οι συνεργατικές επικοινωνίες έχουν πρόσφατα προσελκύσει την ιδιαίτερη προσοχή ως μια αποτελεσματική στρατηγική μετάδοσης, που ωφελείται της χρήσης ευρυεκπομπής του ασύρματου δικτύου. Η βασική ιδέα είναι ότι επιτρέπει στους κόμβους ενός ασύρματου δικτύου να μοιράζονται πληροφορίες και να μεταδίδουν συνεργατικά σαν μια εικονική διάταξη κεραίων παρέχοντας χωρική ποικιλομορφία που βελτιώνει σημαντικά την απόδοση του συστήματος. Για παράδειγμα, όπως φαίνεται στην Εικόνα 6-1, ο κόμβος A θα ήθελε να στείλει κάποιες πληροφορίες στον κόμβο D. Εάν το κανάλι μεταξύ των κόμβων A και D είναι μπλοκαρισμένο ή προκαλεί σημαντική εξασθένηση, τότε θα ήταν δύσκολο για τον κόμβο A να επικοινωνήσει με τον κόμβο D με όρους point-to-point στην ασύρματη επικοινωνία. Ωστόσο, εάν οι δύο κοντινοί κόμβοι B και C μπορούν να βοηθήσουν τον κόμβο A, ενεργώντας ως ενδιάμεσοι κόμβοι μεταφοράς και προωθώντας την πληροφορία προς τον κόμβο D, τότε η επικοινωνία μεταξύ των δύο κόμβων A και D είναι εφικτή. Με ένα τέτοιο συνεργατικό τρόπο, είναι δυνατόν για τον προορισμό να λάβει τη μεταδιδόμενη πληροφορία.



Εικόνα 6-1 Συνεργατικές επικοινωνίες με πηγή τον κόμβο A, κόμβοι μεταφοράς B και C, προορισμός ο κόμβος D

6.2. Πρωτόκολλα Συνεργατικών Επικοινωνιών

Η βασική ιδέα των συνεργατικών επικοινωνιών είναι να επιτρέψουν σε κοντινούς κόμβους χρηστών να βοηθήσουν τη μεταφορά μηνυμάτων από άλλους κόμβους. Με αυτό τον τρόπο, οι κόμβοι, που γνωρίζουν βαθιά εξασθένηση στη ζεύξη τους προς τον προορισμό τους, μπορούν να αξιοποιήσουν τα ποιοτικά κανάλια που παρέχονται από τους ενδιάμεσους κόμβους μεταφοράς.

Τα πιο δημοφιλή, χάρη στην απλότητα και τον ευκολονόητο σχεδιασμό τους, πρωτόκολλα συνεργατικών επικοινωνιών που έχουν προταθεί, είναι τα εξής:

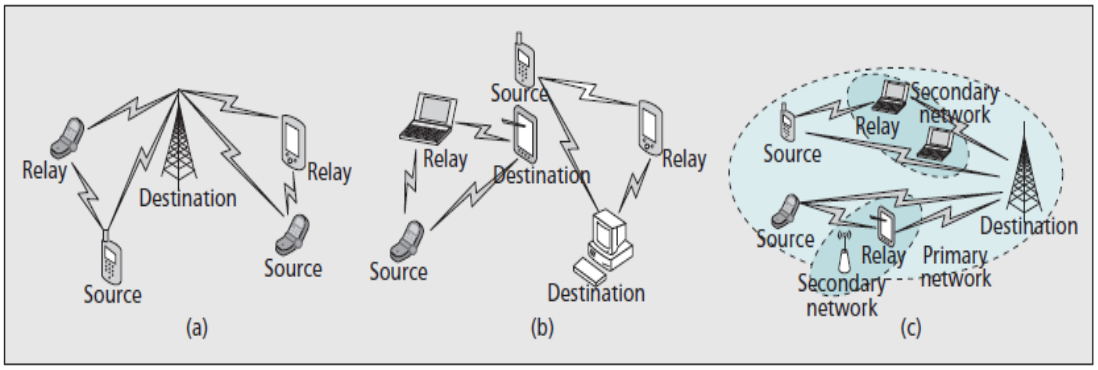
- *Ενίσχυση και προώθηση AF* (amplify-and-forward)—οι ενδιάμεσοι κόμβοι μεταφοράς απλά ενισχύουν το λαμβανόμενο σήμα και το προωθούν κατευθείαν προς τον προορισμό. Στον προορισμό, η ποιότητα σήματος του μεταφερόμενου μηνύματος είναι μειωμένη σε σχέση με την ποιότητα του σήματος της ζεύξης πηγής-ενδιάμεσου κόμβου μεταφοράς, επειδή και το σήμα και ο θόρυβος ενισχύονται στους ενδιάμεσους κόμβους μεταφοράς. Ο κόμβος προορισμού συνδυάζει τις κυματομορφές που έστειλαν η πηγή και ο ενδιάμεσος κόμβος μεταφοράς και κάνει την τελική απόφαση για τη μεταδιδόμενη πληροφορία.
- *Αποκωδικοποίηση και προώθηση DF* (decode-and-forward)—οι ενδιάμεσοι κόμβοι μεταφοράς θα αποκωδικοποιήσουν και θα αναπαράγουν ένα καινούριο μήνυμα προς τον προορισμό. Στον προορισμό, ένας κόμβος μεταφέρει τα μηνύματα από την πηγή μόνο εάν είναι ικανός να αποκωδικοποιήσει τα μηνύματα με αξιόπιστο τρόπο. Έτσι, οι ενδιάμεσοι κόμβοι μεταφοράς επιλέγονται να αναμεταδώσουν τα μηνύματα της πηγής μόνο εάν το κανάλι πηγής-ενδιάμεσου κόμβου είναι επαρκώς αξιόπιστο. Ο κόμβος προορισμού συνδυάζει μαζί την απευθείας μετάδοσης πληροφορία και την αναγεννημένη πληροφορία.

Και στις δυο περιπτώσεις, η πηγή μεταδίδει το μήνυμά της προς τον προορισμό, και χάρη στη φύση ευρυ-εκπομπής (broadcast nature) των ασύρματων καναλιών, οι άλλοι κόμβοι μπορούν επίσης να λάβουν το μήνυμα.

Η πηγή και οι ενδιάμεσοι κόμβοι μεταφοράς μεταδίδουν τα σήματά τους μέσω ορθογώνιων καναλιών χρησιμοποιώντας σενάρια πολλαπλής πρόσβασης διαίρεσης χρόνου (TDMA), πολλαπλής πρόσβασης διαίρεσης συχνότητας (FDMA) ή πολλαπλής πρόσβασης διαίρεσης κώδικα (CDMA).

Εάν μια ομάδα ενδιάμεσων κόμβων μεταφοράς έχουν την άδεια να επιλεχθούν, τα σενάρια επιλογής κόμβων ταξινομούνται στις ακόλουθες δύο κατηγορίες:

- Επιλογή μοναδικής συνεργασίας (selection cooperation)—όπου περιορίζεται η προώθηση σε ένα και μοναδικό κόμβο από ένα σύνολο πιθανών ενδιάμεσων κόμβων μεταφοράς.
- Επιλογή αναμετάδοσης (selection relaying)—όπου επιτρέπεται σε ένα υποσύνολο πιθανών ενδιάμεσων κόμβων μεταφοράς να προωθήσουν τα μηνύματα της πηγής προς τον προορισμό.



Εικόνα 6-2 Δίκτυα όπου οι συνεργατικές επικοινωνίες μπορούν να εφαρμοστούν: a)κυψελωτό δίκτυο, b)ad-hoc δίκτυο, c)διανοητικό ράδιο-δίκτυο

6.3. Διανοητικά ράδιο-δίκτυα (cognitive radio networks)

Η τρέχουσα χρησιμοποίηση φάσματος στα ασύρματα δίκτυα βασίζεται σε μια σταθερή πολιτική εργασία. Η αναφορά της Ομοσπονδιακής Επιτροπής Επικοινωνιών FCC (Federal Communication Commission) σχετικά με τη μέτρηση χρησιμοποίησης φάσματος έχει αποκαλύψει ότι, αν και η ζήτηση φάσματος ραδιοσυχνοτήτων αυξάνεται με εκρηκτικό ρυθμό, ένα μεγάλο τμήμα των ανατεθειμένων ζωνών συχνοτήτων υπό-αξιοποιείται σημαντικά. Η αναπτυσσόμενη διανοητική ράδιο-τεχνολογία (cognitive radio technology) είναι γνωστή ως μια πολλά υποσχόμενη προσέγγιση για να αντιμετωπίσει αποτελεσματικά την ανεπάρκεια φάσματος, και σαν αποτέλεσμα ένα παράδειγμα επικοινωνιών για πολύπλοκα πληροφοριακά συστήματα, όπως το έξυπνο δίκτυο. Σε ένα διανοητικό ράδιο-δίκτυο, οι δευτερεύοντες χρήστες SUs (secondary users) που δε διαθέτουν νόμιμη άδεια επιτρέπεται να έχουν ευκαιριακά πρόσβαση σε κενές θέσεις του φάσματος που ανατίθεται για τους νόμιμους πρωτεύοντες χρήστες PUs (primary users). Ο σχεδιασμός ενός τέτοιου δικτύου είναι ιδιαίτερα απαιτητικός. Το σύστημα δευτερευόντων χρηστών θα πρέπει να είναι ικανό να ανακαλύπτει όσο το δυνατόν περισσότερες ευκαιρίες φάσματος και παράλληλα να αποφεύγει αυστηρώς την παρεμβολή του προς τους πρωτεύοντες χρήστες.

Η ανίχνευση διαθέσιμου φάσματος (spectrum sensing) είναι μια σημαντική τεχνολογία για τα διανοητικά ράδιο-δίκτυα να εντοπίσουν αποτελεσματικά και με ακρίβεια πρωτεύοντες χρήστες και να αποφύγουν την παρεμβολή προς αυτούς. Ωστόσο, πολλοί απρόβλεπτοι παράγοντες όπως η αστάθεια του καναλιού και η αβεβαιότητα του θορύβου, μπορούν να υποβαθμίσουν σημαντικά την απόδοση της ανίχνευσης διαθέσιμου φάσματος.

Η απόδοση της ανίχνευσης φάσματος χαρακτηρίζεται από δύο παράγοντες:

- Αίσθηση ακρίβειας (sensing accuracy)—αναφέρεται στην ακρίβεια εντοπισμού των σημάτων των πρωτευόντων χρηστών έτσι ώστε να μην παρεμβάλλονται οι πρωτεύουσες μεταδόσεις. Αντιπροσωπεύεται από την πιθανότητα εντοπισμού.
- Αίσθηση αποτελεσματικότητας (sensing efficiency)—αναφέρεται στον αριθμό των ανακαλυφθέντων ευκαιριών φάσματος καταναλώνοντας μια μονάδα κόστους σε όρους απώλειας ή απόδοσης.

Η αίσθηση ακρίβειας και η αίσθηση αποτελεσματικότητας αποτελούν δυο αντίθετες απόψεις που αντανακλούν στην απόδοση της ανίχνευσης διαθέσιμου φάσματος. Ας υποθέσουμε ένα απλό παράδειγμα όπου πολλαπλοί δευτερεύοντες χρήστες ανιχνεύουν ακριβώς το ίδιο ασύρματο κανάλι. Παρατηρείται ότι οι περισσότεροι δευτερεύοντες χρήστες οδηγούν σε υψηλότερη αίσθηση ακρίβειας αλλά και σε λιγότερη αίσθηση αποτελεσματικότητας λόγω αναπόφευκτης σύγκρουσης μετάδοσης. Επειδή η συνολική απόδοση του συστήματος εξαρτάται και από τα δύο μεγέθη, είναι απαραίτητο να υπάρξει ένας βέλτιστος συμβιβασμός (trade-off) μεταξύ αίσθησης ακρίβειας και αίσθησης αποτελεσματικότητας.

Στα διανοητικά ράδιο-δίκτυα, έχουν μελετηθεί δύο τύποι παραδειγμάτων συνεργασίας:

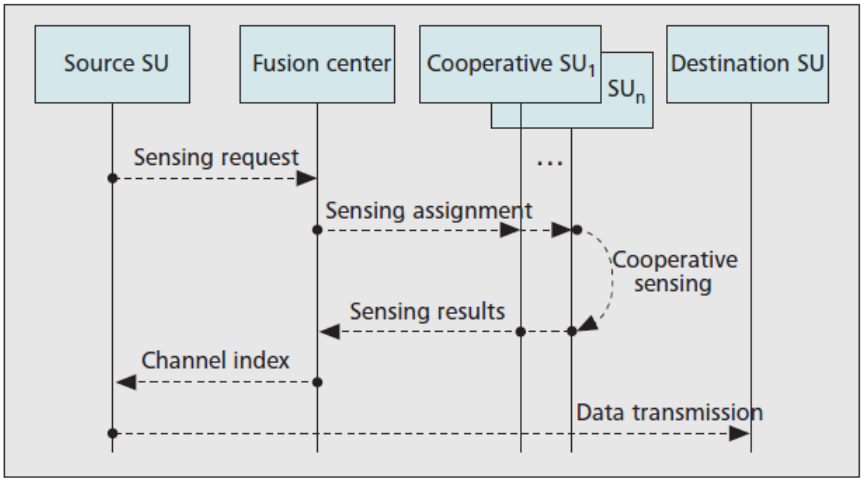
- Συνεργασία μεταξύ πρωτευόντων και δευτερευόντων χρηστών (PU-SU cooperation)—οι πρωτεύοντες χρήστες είναι ενήμεροι της ύπαρξης των δευτερευόντων χρηστών. Το σύστημα πρωταρχικής χρήσης καθορίζει την πολιτική ενοικίασης φάσματος για το σύστημα δευτερεύουσας χρήσης. Οι δευτερεύοντες χρήστες αξιοποιούν ένα μικρό κομμάτι του νόμιμου φάσματος, και σε ανταπόδοση, συνεργάζονται με τους πρωτεύοντες χρήστες για να βελτιώσουν την ποιότητα των πρωταρχικών μεταδόσεων.
- Συνεργασία μεταξύ μόνο των δευτερευόντων χρηστών (inter-SU cooperation)—όπου δεν υπάρχει καμία επικοινωνία μεταξύ πρωτευόντων και δευτερευόντων χρηστών.

6.3.1. Συνεργατική ανίχνευση διαθέσιμου φάσματος

Στη συνεργατική ανίχνευση διαθέσιμου φάσματος, οι πολλαπλοί χρήστες του δευτερεύοντος συστήματος συνεργάζονται για να καταπολεμήσουν τις απρόβλεπτες καταστάσεις στο ασύρματο περιβάλλον και να βελτιώσουν την αίσθηση ακρίβειας και αποτελεσματικότητας. Σε αυτό το μηχανισμό συνεργασίας, ορίζονται διάφορα στοιχεία του δευτερεύοντος συστήματος:

- *Πηγή* (Source SU)—ο δευτερεύων χρήστης που διαθέτει τα δεδομένα πακέτων προς μετάδοση.
- *Προορισμός* (Destination SU)—ο δευτερεύων χρήστης που πρόκειται να λάβει τα δεδομένα πακέτων από την πηγή.
- *Συνεργάτες* (Cooperative SUs)—οι δευτερεύοντες χρήστες που ορίστηκαν να εκτελέσουν τη συνεργατική ανίχνευση φάσματος.
- *Κέντρο σύντηξης* (Fusion Center)—το στοιχείο που είναι υπεύθυνο για τη λήψη και το συνδυασμό των αποτελεσμάτων ανίχνευσης ώστε να πάρει την τελική απόφαση.

Η Εικόνα 6-3 παρουσιάζει τη διαδικασία συνεργατικής ανίχνευσης διαθέσιμου φάσματος. Η πηγή, που σκοπεύει να μεταδώσει πακέτα, θα στείλει ένα μήνυμα αναζήτησης (request) στο κέντρο σύντηξης, απαιτώντας την έναρξη της διαδικασίας συνεργατικής ανίχνευσης διαθέσιμου φάσματος. Το κέντρο σύντηξης αναθέτει επιλεκτικά διάφορους συνεργάτες. Τα αποτελέσματα ανίχνευσης των συνεργατών στέλνονται στο κέντρο σύντηξης την τελική απόφαση συνεργασίας. Αμέσως μόλις ανακαλυφθούν οι ευκαιρίες φάσματος, τα πακέτα μπορούν να μεταδοθούν από την πηγή προς τον προορισμό μέσω του καναλιού που εντοπίστηκε από το κέντρο σύντηξης.



Εικόνα 6-3 Διαδικασία συνεργατικής ανίχνευσης διαθέσιμου φάσματος

6.3.2. Ταξινόμηση μηχανισμών συνεργασίας

Οι μηχανισμοί συνεργασίας στη συνεργατική ανίχνευση διαθέσιμου φάσματος είναι διαφορετικοί στον τρόπο που:

- Οι συνεργάτες επιλέγονται και προγραμματίζονται για συνεργασία
- Τα αποτελέσματα ανίχνευσης διαθέσιμου φάσματος μεταφέρονται στο κέντρο σύντηξης
- Τα αποτελέσματα ανίχνευσης διαθέσιμου φάσματος συνδυάζονται

Ανάλογα με τον αριθμό των ανιχνευμένων καναλιών σε μια περίοδο, η συνεργατική ανίχνευση διαθέσιμου φάσματος θα μπορούσε γενικά να κατηγοριοποιηθεί σε:

- *Αλληλοδιάδοχη* συνεργατική ανίχνευση (sequential cooperative sensing)—όλοι οι συνεργάτες προγραμματίζονται να ανιχνεύουν ακριβώς το ίδιο κανάλι σε κάθε περίοδο ανίχνευσης. Τα κανάλια ανιχνεύονται ένα προς ένα διαδοχικά.
- *Παράλληλη* συνεργατική ανίχνευση (parallel cooperative sensing)—περισσότερα από ένα κανάλια ανιχνεύονται σε κάθε περίοδο ανίχνευσης. Οι συνεργάτες χωρίζονται σε ομάδες και κάθε ομάδα ανιχνεύει ένα κανάλι.

Στην παράλληλη συνεργατική ανίχνευση, πολλαπλά κανάλια εντοπίζονται σε μια περίοδο ανίχνευσης. Έτσι, ο χρόνος για να βρεθούν όλα τα διαθέσιμα κανάλια είναι πολύ συντομότερος από το χρόνο που χρειάζεται στην αλληλοδιάδοχη συνεργατική ανίχνευση. Στην πρώτη περίπτωση, αυξάνεται σημαντικά η αποτελεσματικότητα ανίχνευσης, ενώ στη δεύτερη περίπτωση αυξάνεται η ακρίβεια ανίχνευσης. Για να υπάρξει ένα είδος συμβιβασμού μεταξύ των δύο παραγόντων, προτείνεται η ημι-παράλληλη συνεργατική ανίχνευση.

Βασιζόμενοι στις στιγμές όπου οι λειτουργίες ανίχνευσης εκτελούνται, η συνεργασία δευτερευόντων χρηστών μπορεί να κατηγοριοποιηθεί σε:

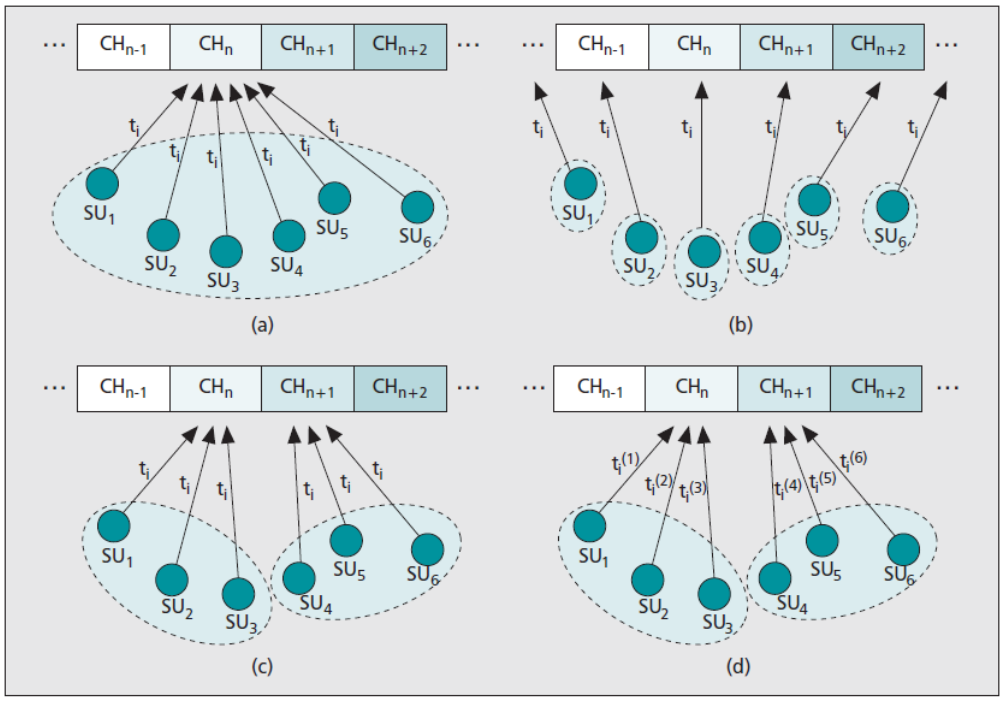
- *Σύγχρονη* συνεργατική ανίχνευση (Synchronous cooperative sensing)—όλοι οι συνεργάτες έχουν την ίδια περίοδο ανίχνευσης και εκτελούν

ανίχνευση διαθέσιμου φάσματος ταυτόχρονα. Όλα τα αποτελέσματα ανίχνευσης διαθέσιμου φάσματος έχουν ταυτόσημη χρονική επισήμανση επιδεικνύοντας τη χρονική στιγμή που η λειτουργία ανίχνευσης συμβαίνει.

- *Ασύγχρονη* συνεργατική ανίχνευση (Asynchronous cooperative sensing)—κάθε συνεργάτης εκτελεί ανίχνευση διαθέσιμου φάσματος σύμφωνα με τη δικιά του περίοδο ανίχνευσης. Σαν αποτέλεσμα, οι χρονικές στιγμές όπου οι δευτερεύοντες χρήστες εκτελούν ανίχνευση ίσως είναι διαφορετικές. Ανάλογα, τα αποτελέσματα ανίχνευσης διαθέσιμου φάσματος έχουν διαφορετικές χρονικές επισημάνσεις.

Cooperative scheme	Sensing overhead	Sensing delay	Network throughput	Interference to PUs	Operation mode
Sequential	Moderate	Large	Low	Light	Centralized
Parallel	Moderate	Small	High	Moderate	Centralized
Synchronous	Moderate	Large	Low	Light	Centralized
Asynchronous	Small	Small	High	Moderate	Centralized or decentralized

Εικόνα 6-4 Σύγκριση μεταξύ συνεργατικών σεναρίων ανίχνευσης διαθέσιμου φάσματος



Εικόνα 6-5 Απεικόνιση των μηχανισμών συνεργασίας: a)Αλληλοδιάδοχη συνεργατική ανίχνευση, b)Πλήρης-Παράλληλη συνεργατική ανίχνευση , c)Ημι-Παράλληλη συνεργατική ανίχνευση, d)Ασύγχρονη συνεργατική ανίχνευση

6.4. Διανοητικά ράδιο-δίκτυα στο έξυπνο δίκτυο

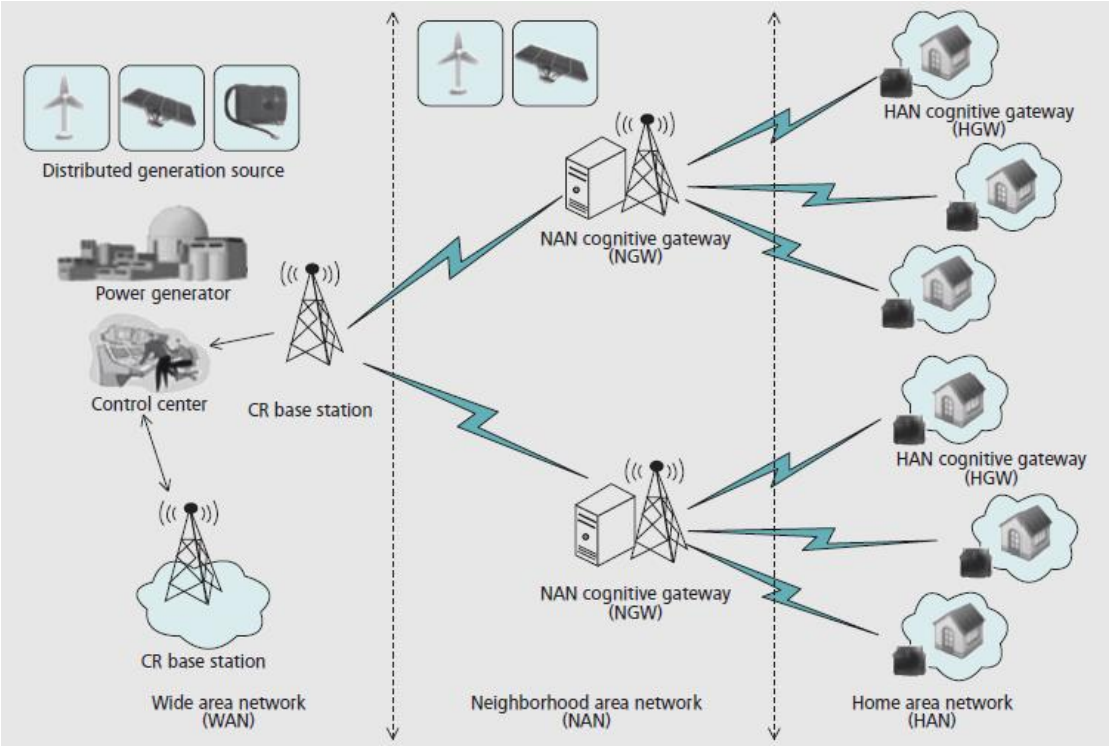
Τα έξυπνα δίκτυα πρέπει να μεταφέρουν αξιόπιστες και πραγματικού χρόνου πληροφορίες στα κέντρα ελέγχου των παρόχων. Λόγω των μοναδικών προκλήσεων που θέτει το έξυπνο δίκτυο, το υπάρχον δίκτυο επικοινωνιών είναι ανέφικτο να ανταποκριθεί στις νέες απαιτήσεις. Η επαναστατική αρχιτεκτονική επικοινωνιών περιλαμβάνει το διανοητικό ράδιο-δίκτυο για το έξυπνο δίκτυο. Το διανοητικό ράδιο-δίκτυο αναφέρεται στην ικανότητα των ασύρματων συστημάτων για αναδιαμόρφωση (reconfiguration) ανάλογα με το περιβάλλον και τις ιδιαιτερότητές του.

Τα κίνητρα της χρήσης του διανοητικού ράδιο-δικτύου στο έξυπνο δίκτυο είναι τα ακόλουθα:

- Η κύρια πρόκληση σε ένα HAN είναι τα αυξανόμενα έντονα ράδιο-συστήματα. Υπάρχουν ήδη αρκετά είδη ράδιο-συστημάτων που λειτουργούν στη ζώνη συχνοτήτων 2.4 GHz βιομηχανικών, επιστημονικών και ιατρικών χρήσεων (ISM—industrial, scientific, medical), όπως ZigBee, Bluetooth, WiFi. Η συνύπαρξη αυτών των συστημάτων θα μπορούσε να προκαλέσει σημαντικές παρεμβολές του ενός με το άλλο. Επιπλέον, οικιακές συσκευές (π.χ. φούρνοι μικροκυμάτων) μπορούν να επιτρέψουν τη διαρροή ισχυρών ηλεκτρομαγνητικών κυμάτων. Σαν αποτέλεσμα, το φάσμα συνωστίζεται σε μεγάλο βαθμό σε ένα HAN. Επίσης, οι έξυπνοι μετρητές σε ένα HAN συνήθως λειτουργούν στη συχνότητα των 2.4 GHz ISM για οικονομικούς λόγους. Η σοβαρή παρεμβολή και ο οξύς ανταγωνισμός για την περιορισμένη αυτή ζώνη συχνοτήτων σίγουρα θα θέσει σε κίνδυνο τις αξιόπιστες επικοινωνίες του έξυπνου δικτύου. Είναι ωφέλιμο να εισάγουμε διανοητική ράδιο-τεχνολογία στα HAN. Βασιζόμενοι στην προσαρμοζόμενη χωρητικότητα του διανοητικού ράδιο-δικτύου, η παρεμβολή μεταξύ διαφορετικών ράδιο-συστημάτων θα μπορούσε να μειωθεί αξιόλογα με τη βοήθεια έξυπνου προγραμματισμού μεταδόσεων και συντονισμού ισχύος εκπομπής.
- Τα παραγόμενα δεδομένα που σχετίζονται με την ενέργεια θα αυξηθούν υπερβολικά στο κοντινό μέλλον. Αυτό θέτει μια σημαντική πρόκληση για κάθε υπάρχον δίκτυο επικοινωνιών, καθώς επίσης και για το έξυπνο δίκτυο που πρέπει να συλλέγει, να μεταδίδει και να αποθηκεύει τόσο μεγάλης κλίμακας δεδομένα. Η χρησιμοποίηση του ράδιο-δικτύου στο έξυπνο δίκτυο θα βελτιώσει την αξιοποίηση φάσματος και τη χωρητικότητα των επικοινωνιών για να υποστηρίξει μεταδόσεις δεδομένων μεγάλης κλίμακας.
- Οι επικοινωνίες του έξυπνου δικτύου θα καλύψουν περιοχές οικιών, περιοχές γειτονιών καθώς και ευρύτερες περιοχές. Συνεπώς, θα χρειάζεται έξυπνες συσκευές και τερματικά που να διαχειρίζονται αποτελεσματικά τις επικοινωνίες μέσα σε κάθε υποπεριοχή και μεταξύ διαφορετικού εύρους υπηρεσίες. Για τη σύγκλιση αυτού του «ετερογενούς» δικτύου, οι συσκευές έξυπνου δικτύου θα πρέπει να εξοπλιστούν με διανοητική ράδιο-λειτουργικότητα για να δώσουν τη δυνατότητα αναδιαμόρφωσης και ενημερότητας των κόμβων.

Θέτοντας σε εφαρμογή τη διανοητική ράδιο-τεχνολογία, η συγκεκριμένη υποδομή υπόσχεται να αξιοποιήσει με τον καλύτερο δυνατό τρόπο όλους τους διαθέσιμους

πόρους φάσματος στο έξυπνο δίκτυο. Οι υποχρησιμοποιούμενες συχνότητες θα εκμεταλλευθούν με το βέλτιστο δυνατό τρόπο και θα αυξηθούν η ευελιξία, η αποτελεσματικότητα και η αξιοπιστία του έξυπνου δικτύου.



Εικόνα 6-6 Αρχιτεκτονική διανοητικού ράδιο-δικτύου στο έξυπνο δίκτυο

6.4.1. Διανοητικές επικοινωνίες στο HAN

Το HAN αποτελείται από μια διανοητική πύλη δικτύου (cognitive gateway), έξυπνους μετρητές, αισθητήρες, ενεργοποιητές και άλλες έξυπνες συσκευές. Οι τεχνολογίες που χρησιμοποιούνται είναι είτε ενσύρματες είτε ασύρματες.

Η διανοητική πύλη δικτύου πρέπει να μπορεί να συνδιαλέγεται έξυπνα με τα διάφορα περιβάλλοντα ραδιοσυχνοτήτων, να συνδέεται με προσαρμοστικό τρόπο και να τροποποιεί τις παραμέτρους των πομπών της. Στη μια κατεύθυνση, θα συλλέγει περιοδικά δεδομένα μέτρησης από διάφορες συσκευές μέσα στο HAN και θα μεταφέρει τα συλλεγμένα δεδομένα έξω από το NAN. Στην άλλη κατεύθυνση, λαμβάνει δεδομένα από το NAN και τα μεταφέρει προς τους έξυπνους μετρητές ή τα παρουσιάζει στους πελάτες.

Επίσης, δίνει τη δυνατότητα σε άλλες συσκευές να γίνουν μέλος του δικτύου, αναθέτει κανάλια και δικτυακές διευθύνσεις σε κάθε συσκευή και συντονίζει τις επικοινωνίες μεταξύ των συσκευών μέσα στο HAN. Μέσα στο HAN, η διανοητική πύλη δικτύου διαχειρίζεται τις ζώνες συχνοτήτων του φάσματος για να παρέχει το βέλτιστο ρυθμό δεδομένων με χαμηλή παρεμβολή.

6.4.2. *Διανοητικές επικοινωνίες στο NAN*

Τα NAN συλλέγουν πληροφορίες ενεργειακής κατανάλωσης από νοικοκυριά σε μια γειτονιά και τα μεταφέρουν στην πάροχο εταιρία μέσω WAN. Σε ένα NAN, η διανοητική πύλη δικτύου συνδέει διάφορε διανοητικές πύλες δικτύου από πολλαπλά HAN.

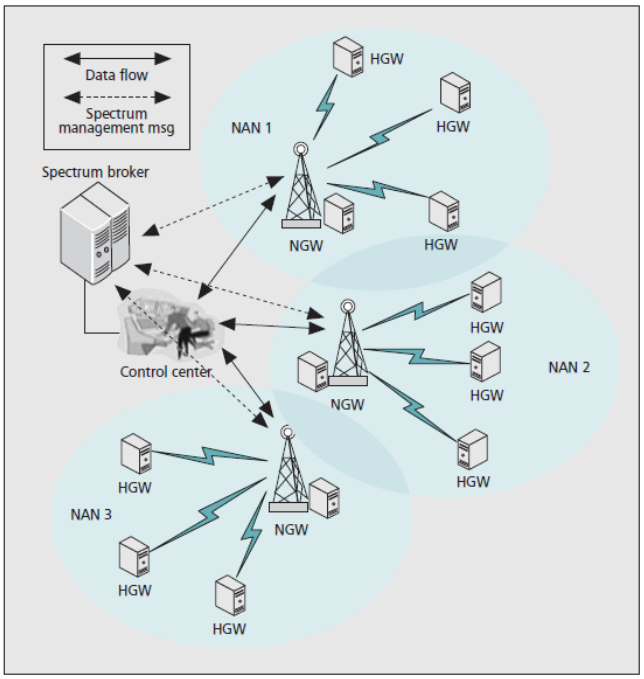
Κάποιες αδειοδοτημένες ζώνες συχνοτήτων αγοράζονται από κάποιον τηλεπικοινωνιακό φορέα. Η διανοητική πύλη δικτύου του NAN κατανέμει αυτές τις ζώνες συχνοτήτων προς τις διανοητικές πύλες δικτύου του HAN ανάλογα με τη ζήτηση μετάδοσης.

6.4.3. *Διανοητικές επικοινωνίες στο WAN*

Πολλαπλά NAN συνθέτουν ένα WAN και κάθε NAN ανταλλάσσει πληροφορίες με το κέντρο ελέγχου μέσω του WAN, όπως φαίνεται και στην παρακάτω εικόνα. Το κέντρο ελέγχου είναι συνδεδεμένο με διανοητικούς σταθμούς βάσης που είναι διασκορπισμένη σε μια μεγάλη περιοχή (π.χ. μια πόλη).

Για να βελτιωθεί η αξιοποίηση του φάσματος και να μειωθεί το κόστος της αγοράς νέων ζωνών συχνοτήτων, αδειοδοτημένες και μη (δευτερεύοντες χρήστες) ζώνες συχνοτήτων χρησιμοποιούνται με προγραμματισμό και αδιάκοπη εναλλαγή. Εάν ένα WAN καλύπτει μια μεγάλη περιοχή εξυπηρέτησης, αρκετά NAN μπορούν να μοιράζονται την ίδια ζώνη συχνοτήτων χωρίς να παρεμβάλλουν το ένα στο άλλο.

Για παράδειγμα, στην Εικόνα 6-7, υπάρχουν 3 NAN και 10 ζώνες συχνοτήτων αγοράζονται από τον τηλεπικοινωνιακό φορέα. Σύμφωνα με τις διαφορετικέ απαιτήσεις ρυθμαπόδοσης δεδομένων, θα κατανεμηθούν 4 ζώνες συχνοτήτων στο NAN1 και 6 ζώνες συχνοτήτων στο NAN2. Επειδή το NAN1 και το NAN3 βρίσκονται μακριά το ένα με το άλλο, οι 4 ζώνες που κατανεμήθηκαν στο NAN1 οι ίδιες θα κατανεμηθούν και στο NAN3.



Εικόνα 6-7 Αρχιτεκτονική WAN (Wide Area Network)

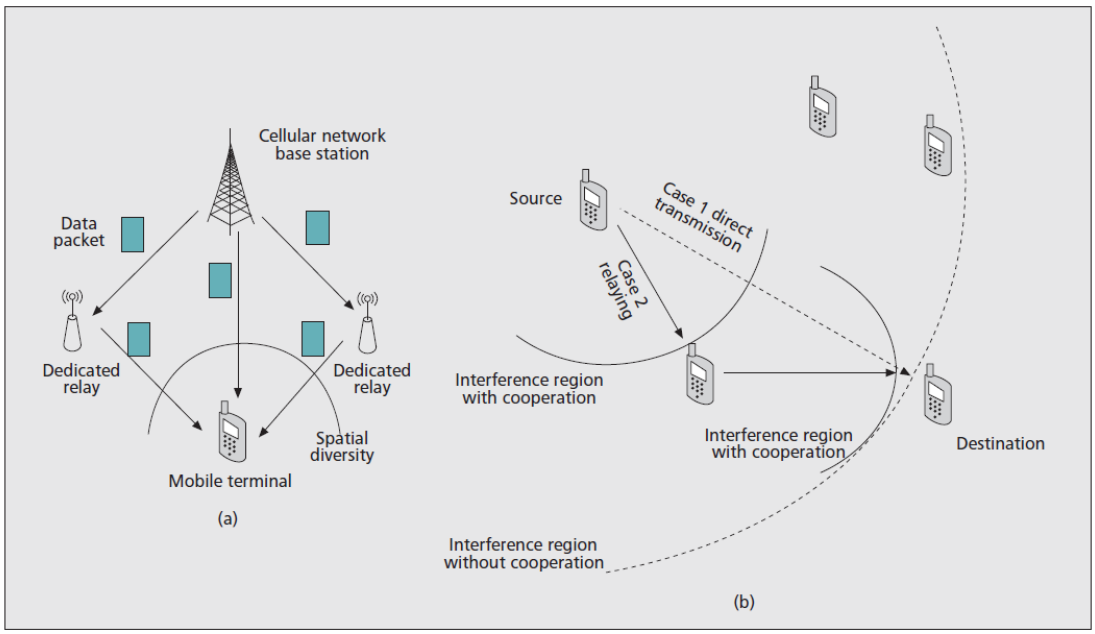
6.5. Πιθανά οφέλη συνεργασίας

Βελτιωμένη αξιοπιστία καναλιού—μετριάζοντας τις φθορές του καναλιού

Το ασύρματο κανάλι επικοινωνίας υποφέρει από διάφορα φαινόμενα που μειώνουν την αξιοπιστία του. Αυτά τα φαινόμενα περιλαμβάνουν απώλεια μονοπατιού (path loss), σκίαση (shadowing) και απόσβεση (fading). Η συνεργασία στα ασύρματα δίκτυα μπορεί να αυξήσει την αξιοπιστία των επικοινωνιών ενάντια στις φθορές που υφίσταται το κανάλι. Αυτή η βελτιωμένη αξιοπιστία μπορεί να επιτευχθεί εκμεταλλευόμενοι τη συνεργατική χωρική ποικιλομορφία (cooperative spatial diversity). Όταν το κανάλι ανάμεσα στην πραγματική πηγή και τον προορισμό είναι αναξιόπιστο, άλλες δικτυακές οντότητες μπορούν να συνεργαστούν με την πηγή ώστε να δημιουργήσουν μια εικονική διάταξη κεραιών (virtual antenna array) και να προωθήσουν τα δεδομένα προς τον προορισμό. Σαν αποτέλεσμα, διαφορετικά μονοπάτια μετάδοσης με ανεξάρτητους συντελεστές καναλιών δημιουργούνται ανάμεσα στους κόμβους της πηγής και του προορισμού μέσω των συνεργατικών οντοτήτων. Με αυτό τον τρόπο, ο προορισμός λαμβάνει διάφορα αντίγραφα του μεταδιδόμενου σήματος πάνω από ανεξάρτητα μεταξύ τους κανάλια. Βασιζόμενος στη χωρική ποικιλομορφία, ο προορισμός μπορεί να συνδυάσει τα λαμβανόμενα δεδομένα από αυτές τις οντότητες με βέλτιστο εντοπισμό έτσι ώστε να βελτιώσει την ακρίβεια μετάδοσης. Η συγκεκριμένη ιδέα απεικονίζεται στην Εικόνα 6-8α για μια μετάδοση από ένα σταθμό βάσης προς ένα κινητό τερματικό, όπου η πηγή μεταδίδει πακέτα δεδομένων προς τον προορισμό με τη βοήθεια συνεργατικών οντοτήτων. Σε αυτό το πλαίσιο, η συνεργατική οντότητα είναι ένας κόμβος αναμετάδοσης με βελτιωμένες συνθήκες καναλιού απέναντι στην κατευθείαν κανάλι μετάδοσης από την πηγή στον προορισμό.

Βελτιωμένη αξιοπιστία καναλιού—μείωση παρεμβολής

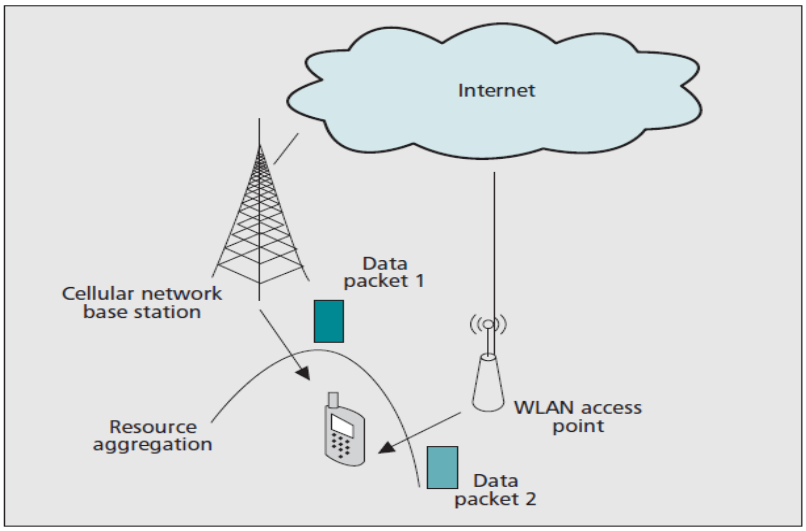
Η φύση ευρυεκπομπής του ασύρματου μέσου επικοινωνιών έχει ως αποτέλεσμα την παρεμβολή στους διαφορετικούς κόμβους στην περιοχή κάλυψης (περιοχή παρεμβολής) των κόμβων μεταξύ τους. Μια τέτοια παρεμβολή μειώνει το λόγο σήματος προς παρεμβολή και θόρυβο (SNIR) στους δέκτες και σαν αποτέλεσμα υποβαθμίζει την ικανότητά τους για αποτελεσματικότερο εντοπισμό. Χάρη στη συνεργασία που διενεργείται από τους συνεργατικούς κόμβους αναμετάδοσης, η πραγματική ισχύς μετάδοσης από την πραγματική πηγή μπορεί να μειωθεί σημαντικά λόγω των καλύτερων συνθηκών καναλιού των ζεύξεων αναμετάδοσης που μειώνουν σε μεγάλο βαθμό την περιοχή παρεμβολής, όπως φαίνεται στην Εικόνα 6-8β. Αυτό βοηθά στη βελτίωση της ενεργειακής αποτελεσματικότητας του συστήματος επικοινωνιών. Εκτός της μείωσης της περιοχής παρεμβολής, η συνεργασία μπορεί να επιλύσει το πρόβλημα του κρυμμένου τερματικού (hidden terminal).



Εικόνα 6-8 Συνεργασία προς βελτίωση της αξιοπιστίας του καναλιού: a)χωρική ποικιλομορφία, b)μείωση παρεμβολής

Βελτιωμένη ρυθμαπόδοση συστήματος

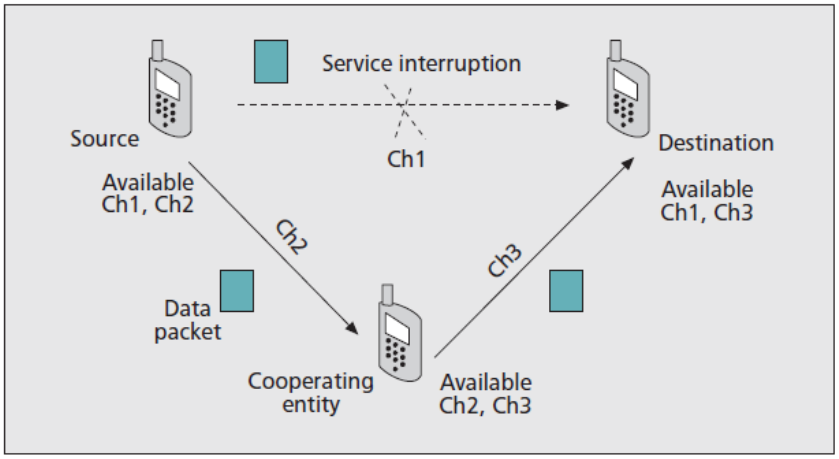
Η βελτιωμένη ρυθμαπόδοση του συστήματος ίσως είναι το άμεσο όφελος από την αύξηση της αξιοπιστίας του καναλιού μέσω συνεργατικών μεταδόσεων στο φυσικό στρώμα. Επίσης, αυτή η συνεργασία μπορεί να αυξήσει την υπάρχουσα ρυθμαπόδοση μέσω της συνάθροισης των προσφερόμενων πόρων από διαφορετικές συνεργατικές οντότητες. Σε αυτή την περίπτωση, τα πακέτα δεδομένων μεταδίδονται κατά μήκος πολλαπλών μονοπατιών προς τον προορισμό. Σε αντίθεση με το προηγούμενο σενάριο συνεργασίας, τα πακέτα δεδομένων που μεταδίδονται μέσω των διαφορετικών μονοπατιών δεν αποτελούν το ίδιο αντίγραφο του μεταδιδόμενου σήματος. Αντί αυτού, διαφορετικά μονοπάτια μετάδοσης μεταφέρουν διαφορετικά πακέτα δεδομένων. Αυτό έχει ως αποτέλεσμα την αύξηση του συνολικού ρυθμού μετάδοσης δεδομένων μεταξύ πηγής και προορισμού. Σε αυτή την περίπτωση, οι συνεργατικές οντότητες μπορεί να είναι κινητά τερματικά, σταθμοί βάσης ή σημεία πρόσβασης με επαρκείς πόρους (π.χ. εύρος ζώνης), έτσι ώστε όταν αυτοί οι πόροι συναθροιστούν, ο συνολικός ρυθμός μετάδοσης δεδομένων από την πηγή στον προορισμό μπορεί να αυξηθεί. Αυτή η στρατηγική μπορεί να υποστηρίξει εφαρμογές με υψηλές απαιτήσεις ρυθμού μετάδοσης. Στην Εικόνα 6-9 για παράδειγμα, πόροι από τη συνεργασία κυψελωτού δικτύου και ασύρματου τοπικού δικτύου WLAN συναθροίζονται για να παρέχουν υψηλό ρυθμό μετάδοσης δεδομένων για το κινητό τερματικό.



Εικόνα 6-9 Συνεργατική συνάθροιση πόρων μέσω ενός κυψελωτού δικτύου και ενός WLAN

Αδιάκοπη παροχή υπηρεσιών

Οι κινητοί χρήστες είναι πιο ευαίσθητοι στη διακοπή κλήσης (call dropping) παρά στην εμπλοκή κλήσης (call blocking). Η διακοπή κλήσης διακόπτει τη ροή της υπηρεσίας για διαφορετικούς λόγους κάθε φορά. Οι συνεργατικές στρατηγικές στα στρώματα ζεύξης δεδομένων, δικτύου και μεταφοράς μπορεί να εγγυηθεί συνεχή ροή υπηρεσιών μιας διαρκούς κλήσης. Στην Εικόνα 6-10, όταν η υπηρεσία διακόπτεται κατά μήκος ενός μονοπατιού (Ch1), μπορεί ακόμη να συνεχιστεί κάνοντας χρήση ενός άλλου συνεργατικού μονοπατιού (Ch2, Ch3). Σε αυτό το πλαίσιο, μια συνεργατική οντότητα μπορεί να είναι ένα κινητό τερματικό, ένας σταθμός βάσης ή ένα σημείο πρόσβασης, τα οποία μπορούν να δημιουργήσουν ένα υποκατάστατο μονοπάτι ανάμεσα στην πηγή και τον προορισμό.



Εικόνα 6-10 Συνεργασία για αδιάκοπη παροχή υπηρεσιών

6.6. Μηχανισμοί απόδοσης κινήτρων

Στα παραδοσιακά συστήματα πολλαπλών χρηστών (multi-user systems), η συνεργατική κατανομή πόρων ίσως δεν εφαρμόζεται επειδή οι κόμβοι χρηστών είναι ανεξάρτητοι ο ένας με τον άλλον και τείνουν να είναι ατομιστές (selfish) σε περίπτωση ανταγωνισμού των πόρων. Επειδή, η διαδικασία αναμετάδοσης για τους ενδιάμεσους κόμβους αντιπροσωπεύει ένα κόστος πόρων επικοινωνίας, ένας κόμβος αναμετάδοσης έχει την πρόθεση να καταναλώσει τους πόρους του μόνο και μόνο για να μεγιστοποιήσει το δικό του όφελος. Για αυτό το λόγο, είναι σημαντικό να σχεδιαστούν μηχανισμοί απόδοσης κινήτρων (incentive mechanisms) για να κινητοποιήσουν τη συνεργασία μεταξύ των ατομιστών κόμβων. Μια κατάλληλη στρατηγική απόδοσης κινήτρων σε μια ομάδα ατομιστών κόμβων θα μπορούσε να ωφελήσει όλους μέσα από τη συνεργασία. Επίσης, η τελική κατανομή πόρων αναφέρεται ως το *κοινωνικό βέλτιστο* (social optimal), το οποίο σημαίνει πως κανένας δεν μπορεί να βελτιώσει την απόδοσή του σε βάρος της υποβάθμισης της απόδοσης των άλλων κόμβων. Τέλος, έρευνες εκτελούνται με στόχο να βοηθήσουν ένα σύνολο ατομιστών κόμβων να βρουν τις κατάλληλες στρατηγικές συνεργασίας που θα μπορούσαν να οδηγήσουν σε κοινωνικά βέλτιστη κατανομή πόρων.

Σε στρατιωτικές εφαρμογές, μπορεί να θεωρηθεί συνεργασία μεταξύ των κόμβων επειδή οι κόμβοι ανήκουν στην ίδια εξουσία και με αυτό τον τρόπο εθελοντικά συνεργάζονται για να επιτύχουν ένα κοινό στόχο. Ωστόσο, σε εμπορικές εφαρμογές, όπου οι κόμβοι συνήθως ανήκουν σε διαφορετικές ανεξάρτητες οντότητες, δεν υπάρχει λόγος να θεωρήσουμε ότι οι κόμβοι θα συνεργαστούν. Πράγματι, οι κόμβοι είναι ατομιστές και καταναλώνουν τους πόρους τους μόνο όταν αυτή η διαδικασία θα μεγιστοποιήσει τα δικά τους οφέλη.

Οι συνεργατικές επικοινωνίες κερδίζουν δημοσιότητα επειδή έχουν τη μεγάλη δυνατότητα να αυξάνουν τη χωρητικότητα των ασύρματων δικτύων. Παρά όλα αυτά, οι εφαρμογές τους σπάνια εμφανίζονται στην πραγματική ζωή. Το κύριο χαρακτηριστικό που εμποδίζει την εξάπλωση των εφαρμογών τους είναι η έλλειψη κινήτρων προς τους ασύρματους κόμβους ώστε να ενεργήσουν ως ενδιάμεσοι κόμβοι μεταφοράς.

Υπάρχουν τρεις κύριοι μηχανισμοί που παρέχουν τέτοιου είδους κίνητρα:

- *Μηχανισμός βασιζόμενος στη φημολογία* (reputation-based mechanism)—μια κεντρική εξουσία (π.χ. ένας σταθμός βάσης) καταγράφει τη συνεργατική συμπεριφορά των κόμβων και τιμωρεί τους μη συνεργάσιμους κόμβους. Οι κόμβοι ατομιστές, που είναι απρόθυμοι να συνεργαστούν και έτσι αυξάνουν τη δικιά τους ωφέλεια σε σύγκρουση με την προσπάθεια για αποτελεσματική χρήση των πόρων του συστήματος, θα τιμωρηθούν και θα αναγκαστούν να μειώσουν την ισχύ μετάδοσής τους. Αντίθετα, οι κόμβοι που ανταποκρίνονται σε προσφορά συνεργασίας προς όφελος των διαθέσιμων πόρων του συστήματος, θα ανταμείβονται με δυνατότητα μετάδοσης μεγαλύτερης ισχύος.
- *Μηχανισμός βασιζόμενος στην ανταλλαγή πόρων* (resource-exchange-based mechanism)—η πηγή καταλαμβάνει κάποιους κόμβους σαν αναμεταδότες για συνεργατική επικοινωνία. Σαν ανταπόδοση, η πηγή παρέχει τους δικούς της πόρους για να βοηθήσει τους κόμβους αναμετάδοσης να επιτύχουν συγκεκριμένους σκοπούς. Η στρατηγική για κάθε κόμβο είναι

να αποφασίσει για το μέγεθος ισχύος που θα χρησιμοποιήσει για μετάδοση των δικών του δεδομένων και για το μέγεθος ισχύος που θα χρησιμοποιήσει για αναμετάδοση δεδομένων άλλων κόμβων. Η ωφέλεια ενός κόμβου ορίζεται ως η διαφορά μεταξύ του επιτυχημένου ρυθμού μετάδοσης και της ενέργειας την οποία δαπάνησε.

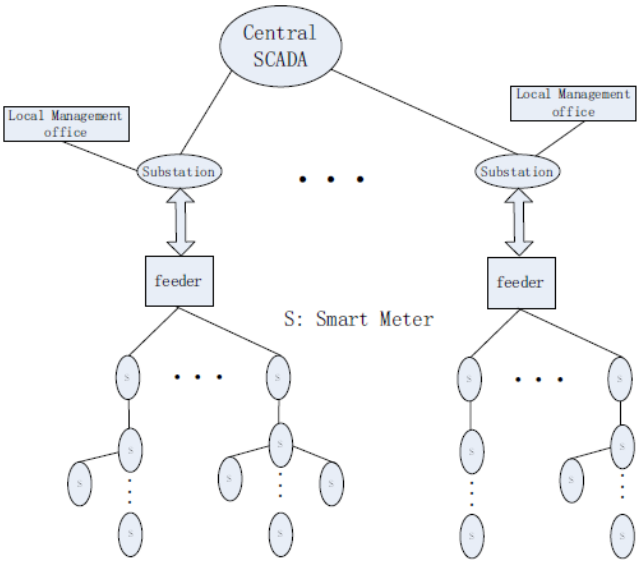
- *Μηχανισμός βασιζόμενος στην τιμολόγηση* (pricing-based mechanism)—ένα εικονικό συνάλλαγμα υποτίθεται σε αυτό το δίκτυο. Οι κόμβοι αναμετάδοσης πωλούν τους πόρους τους (π.χ. ισχύς, εύρος ζώνης, χρόνος) για μια συγκεκριμένη τιμή. Η πηγή πληρώνει τους κόμβους αναμετάδοσης για να χρησιμοποιήσει τους πόρους αυτών.

7. Το έξυπνο δίκτυο μέτρησης (advanced metering infrastructure of smart grid)

7.1. Αρχιτεκτονική συστήματος επικοινωνιών για το έξυπνο δίκτυο μέτρησης

Τα συστήματα ελέγχου επιτήρησης και απόκτησης δεδομένων (SCADA) έχουν εφαρμοστεί εδώ και δεκαετίες για να παρακολουθούν και να ελέγχουν τα δίκτυα ηλεκτρικής ισχύος. Το κέντρο ελέγχου SCADA διαχειρίζεται την προμήθεια ηλεκτρικού ρεύματος προς τους υποσταθμούς μέσω των γραμμών μεταφοράς υψηλής τάσης. Στους υποσταθμούς λαμβάνει χώρα η υποβάθμιση της υψηλής τάσης στη μέση τάση και τη διανομή της ηλεκτρικής ενέργειας μέσω των feeder γραμμών διανομής. Στο τέρμα των feeder γραμμών διανομής, ο τελικός καταναλωτής μπορεί να τροφοδοτήσει το σπίτι του με ηλεκτρικό ρεύμα.

Σε κάθε σπίτι, ο έξυπνος μετρητής συγκεντρώνει τα δεδομένα κατανάλωσης ηλεκτρικής ισχύος από όλες τις έξυπνες ηλεκτρικές συσκευές του σπιτιού και τις προωθεί στο τοπικό γραφείο διαχείρισης της παρόχου εταιρίας (utility company). Αυτά τα δεδομένα επεξεργάζονται ως πληροφορία λογαριασμού (billing information), συναθροίζονται και προωθούνται στο κέντρο ελέγχου SCADA και το διαχειριστή παροχής μέσω οπτικών ινών. Με αυτή την πληροφορία πραγματικού χρόνου, ο διαχειριστής παροχής μπορεί να παρακολουθήσει την κατάσταση ολόκληρου του έξυπνου δικτύου και να προσαρμόσει βέλτιστα την παραγωγή, μεταφορά και διανομή, να εξομαλύνει την αυξημένη ζήτηση και να αποφύγει πιθανές διακοπές ρεύματος στην πλευρά του παρόχου. Έπειτα, τα μηνύματα διαχείρισης πραγματικού χρόνου διανέμονται στους αντίστοιχους καταναλωτές μέσω των έξυπνων μετρητών. Με αυτό τον τρόπο, οι έξυπνες οικιακές συσκευές αναπρογραμματίζουν ανάλογα τις εργασίες τους και τα χρονικά διαστήματα λειτουργίας τους, έτσι ώστε να αποφευχθούν οι πιθανότητες διακοπής του ηλεκτρικού ρεύματος στη μεριά του καταναλωτή.



Εικόνα 7-1 Αρχιτεκτονική συστήματος επικοινωνιών για το έξυπνο δίκτυο μέτρησης

Το δίκτυο επικοινωνιών στη χαμηλή τάση συνήθως εφαρμόζεται με ασύρματες τεχνολογίες, όπως IEEE 802.11 Wi-Fi (HAN), για μια ομάδα τελικών καταναλωτών. Κάθε τελικός καταναλωτής θεωρείται ότι αντιπροσωπεύεται από έναν έξυπνο μετρητή. Οι έξυπνοι αυτοί μετρητές συνδέονται σε μια feeder γραμμή διανομής, η οποία δρα σαν μια πύλη δικτύου που οδηγεί τις συλλεγμένες μετρήσεις στο τοπικό γραφείο διαχείρισης στην πίσω πλευρά του υποσταθμού χρησιμοποιώντας τεχνολογία IEEE 802.16 WiMax (WAN).

Η τεχνολογία επικοινωνιών μεταξύ των έξυπνων μετρητών και της feeder γραμμής διανομής μπορεί να είναι ένα ασύρματο δίκτυο πολλαπλών κόμβων (multi-hop wireless network), επειδή η ασύρματη δικτύωση είναι ο πιο οικονομικός τρόπος για να συνδέσεις μια ομάδα έξυπνων μετρητών σε μια κοινωνία. Για ένα ασύρματο δίκτυο πολλαπλών κόμβων, ένα ασύρματο σενάριο δρομολόγησης μπορεί να δημιουργηθεί για να συνδέσει τους έξυπνους μετρητές αποτελεσματικά.

7.2. Ζητήματα ασφάλειας για το έξυπνο δίκτυο μέτρησης

Τα σενάρια ασφάλειας που περιλαμβάνουν μηχανισμούς πιστοποίησης αυθεντικότητας είναι ανεπαρκή. Δεν υπάρχει πρακτικός μηχανισμός που να ανταποκρίνεται στο πρόβλημα κλιμάκωσης (scalability) για τις πιστοποιήσεις αυθεντικότητας των έξυπνων μετρητών. Για παράδειγμα, για να πιστοποιηθεί η αυθεντικότητα ενός έξυπνου μετρητή ως Home Area Network gateway (HAN GW), ένας άλλος έξυπνος μετρητής, ο Building Area Network gateway (BAN GW), θα πρέπει να επικοινωνήσει με τον HAN GW με ασφάλεια. Αυτή η επικοινωνία χρειάζεται να κρυπτογραφηθεί με μυστικά κλειδιά των HAN GW και BAN GW. Εντωμεταξύ, ο BAN GW θα πρέπει να πιστοποιήσει την αυθεντικότητά του με τον Neighboring Area Network gateway (NAN GW) και η ροή δεδομένων ανάμεσά τους θα πρέπει να κρυπτογραφηθεί επίσης.

Οι κρυπτογραφικές δαπάνες, όπως η ψηφιακή υπογραφή και το ψηφιακό πιστοποιητικό καταλαμβάνουν ένα σημαντικό μερίδιο σε σχέση με την απλή διαδικασία των δεδομένων ενός πακέτου. Επίσης, οι κρυπτογραφικές λειτουργίες συνηγορούν σε σημαντική αύξηση του υπολογιστικού κόστους, ειδικά στην πλευρά του αποδέκτη που πιστοποιεί το μήνυμα. Στο έξυπνο δίκτυο, ένας έξυπνος μετρητής στέλνει μια μέτρηση μετά από ένα διάστημα 500 msec. Η παραγωγή μιας ψηφιακής υπογραφής κάθε 500 msec δεν αποτελεί σημαντικό πρόβλημα, χρησιμοποιώντας έναν προσωπικό υπολογιστή, για τα σενάρια ψηφιακής υπογραφής που βασίζονται σε υποδομή δημοσίου κλειδιού (public key infrastructure). Ωστόσο, για ένα δίκτυο που συνδέει εκατοντάδες κτίρια, καθένα από τα οποία διαθέτει ένα τεράστιο αριθμό διαμερισμάτων, ο αριθμός των μηνυμάτων-μετρήσεων που απαιτούνται να πιστοποιηθούν από τον NAN GW ίσως είναι αρκετά μεγαλύτερος της χωρητικότητάς του. Επίσης, οι έξυπνοι μετρητές γίνονται ευάλωτοι σε ηλεκτρονικές επιθέσεις, αφού η χρήση ασύρματων και IP τεχνολογιών δίνουν τη δυνατότητα σε online διαχείριση αυτών.

Η ψηφιακή υπογραφή και πιστοποίηση κάθε μηνύματος σίγουρα μπορεί να επιτύχει ασφαλείς επικοινωνίες. Ωστόσο, οι κρυπτογραφικές λειτουργίες που εφαρμόζονται καθιστούν τα σενάρια ασφάλειας, όπως PKI (public key infrastructure) μη κλιμακώσιμα και μη διαχειρίσιμα οικονομικά χάρη στην πυκνότητα κυκλοφορίας δεδομένων και τους περιορισμένους πόρους του έξυπνου δικτύου. Γι αυτό το λόγο, απαιτούνται ασφαλή σενάρια επικοινωνίας μικρού υπολογιστικού κόστους,

προσαρμοσμένα για τις επικοινωνίες του έξυπνου δικτύου, που θα επιτρέπουν την ασφαλή και γρήγορη επεξεργασία και διαχείριση των μηνυμάτων-μετρήσεων.

7.3. Ασφαλές και αξιόπιστο συνεργατικό σενάριο επικοινωνίας για το έξυπνο δίκτυο μέτρησης

Ένα συνεργατικό σενάριο επικοινωνίας μεταξύ των έξυπνων μετρητών που διασυνδέονται μεταξύ τους μέσω ενός ασύρματου δικτύου πολλαπλών κόμβων (multihop wireless network) μπορεί να αναπτυχθεί για να διασφαλίσει ασφαλείς και αξιόπιστες επικοινωνίες στο έξυπνο δίκτυο μέτρησης (advanced metering infrastructure), αντιμετωπίζοντας παράλληλα τις διάφορες ηλεκτρονικές απειλές (cyber threats):

- *Αμοιβαίες πιστοποιήσεις αυθεντικότητας (mutual authentications)* όταν ένας έξυπνος μετρητής εγκαθίσταται και γίνεται μέλος του ευρύτερου δικτύου μέτρησης. Με αυτό τον τρόπο παρέχονται έμπιστες υπηρεσίες, διασφαλίζεται η ακεραιότητα (integrity) και ιδιωτικότητα (privacy) των δεδομένων.
- *Κρυπτογράφηση δεδομένων (data encryption)* χρησιμοποιώντας τα αντίστοιχα κλειδιά που αναπαράγονται στη διαδικασία πιστοποίησης αυθεντικότητας. Με αυτό τον τρόπο επιτυγχάνεται η εμπιστευτικότητα των δεδομένων που μεταφέρονται.
- *Σενάριο μεταφοράς δεδομένων (data transmission scheme)* που διευκολύνει τη συλλογή δεδομένων και τη διαχείριση μεταφοράς μηνυμάτων μεταξύ των έξυπνων μετρητών και ενός τοπικού συλλέκτη (local collector) δεδομένων. Με αυτό τον τρόπο επιτυγχάνεται μικρότερη από άκρη σε άκρη καθυστέρηση (end-to-end delay) και μικρότερη απώλεια πακέτων (packet loss) σε σχέση με τη βασική μέθοδο ασφάλειας.

7.3.1. Διαδικασία αρχικοποίησης (initialization process)

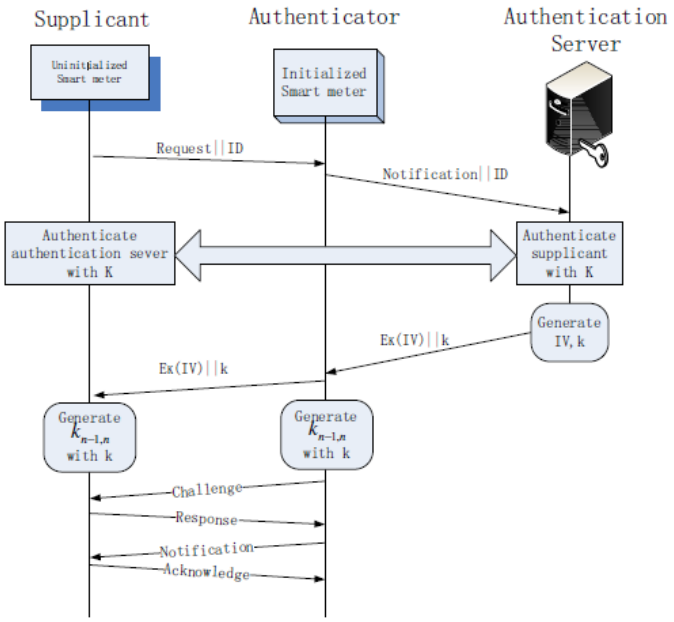
Ένας νέο-εγκατεστημένος έξυπνος μετρητής, πριν γίνει μέλος του πιστοποιημένου για την αυθεντικότητά του δικτύου έξυπνων μετρητών, πρέπει να πιστοποιηθεί η αυθεντικότητα του ιδίου από τον εξυπηρετητή πιστοποίησης αυθεντικότητας (authentication server), που βρίσκεται στο τοπικό γραφείο διαχείρισης, ως μια νόμιμη συσκευή και ως ένας τελικός πελάτης. Ο γειτονικός πιστοποιημένος για την αυθεντικότητά του έξυπνος μετρητής παίζει το ρόλο του νόμιμου μεσολαβητή (authenticator) στη διαδικασία αρχικοποίησης για να μεταφέρει τα μηνύματα της πιστοποίησης αυθεντικότητας μεταξύ του υποβάλλοντος (supplicant) και του εξυπηρετητή πιστοποίησης αυθεντικότητας.

Και οι δυο, ο υποβάλλων έξυπνος μετρητής και ο εξυπηρετητής πιστοποίησης αυθεντικότητας, έχουν ένα ταυτόσημο κλειδί K, το οποίο δεν αποκαλύπτεται ποτέ σε κανέναν άλλο, ούτε καν στον μεσολαβητή. Αυτό συμβαίνει διότι τόσο οι αμοιβαίες πιστοποιήσεις αυθεντικότητας ταυτότητας όσο και οι επακόλουθες κρυπτογραφήσεις/αποκρυπτογραφήσεις δεδομένων μεταξύ του υποβάλλοντος και του εξυπηρετητή πιστοποίησης αυθεντικότητας βασίζονται σε αυτό το κλειδί K. Εάν πιστοποιηθεί η αυθεντικότητα της ταυτότητας του υποβάλλοντος ως μια έγκυρη

συσκευή, τα αντίστοιχα διαπιστευτήρια του υποβάλλοντος εγκαθιδρύονται μεταξύ του εξυπηρετητή πιστοποίησης αυθεντικότητας και του υποβάλλοντος.

Έπειτα, ο εξυπηρετητής πιστοποίησης αυθεντικότητας θα αναπαράγει ένα αρχικό διάνυσμα IV (initial vector) και ένα κλειδί k. Το αρχικό διάνυσμα IV και το κλειδί k θα κρυπτογραφηθούν με το κλειδί K, έτσι ώστε ο υποβάλλων να μπορεί να αποκρυπτογραφήσει και να μπορεί να αποκτήσει το αρχικό διάνυσμα IV και το κλειδί k. Εντωμεταξύ, ο εξυπηρετητής πιστοποίησης αυθεντικότητας στέλνει το κλειδί k στο μεσολαβητή κρυπτογραφημένο με το δικό τους κλειδί K', το οποίο δημιουργήθηκε όταν ο τρέχων μεσολαβητής είχε πιστοποιήσει την αυθεντικότητά του με τον εξυπηρετητή πιστοποίησης αυθεντικότητας. Έτσι, ο μεσολαβητής γνωρίζει το κλειδί k.

Με αυτό το κλειδί k, ο υποβάλλων και ο μεσολαβητής μπορούν να δημιουργήσουν το κλειδί $k_{n-1,n}$ ατομικά και μετά να διεξάγουν μια διαδικασία τετραπλής χειραψίας(four-way handshake) για να πραγματοποιήσουν και μια άλλη πιστοποίηση αυθεντικότητας μεταξύ υποβάλλοντος και μεσολαβητή. Μετά την επιτυχημένη πιστοποίηση αυθεντικότητας, το κλειδί $k_{n-1,n}$ είναι επικυρωμένο τόσο στην πλευρά του υποβάλλοντος όσο και στην πλευρά του μεσολαβητή και όλα είναι έτοιμα για επακόλουθες ανταλλαγές μηνυμάτων.



Εικόνα 7-2 Διαδικασία αρχικοποίησης για έναν νέο-εγκατεστημένο έξυπνο μετρητή

Επειδή κάθε έξυπνος μετρητής πρέπει να πραγματοποιήσει τη διαδικασία αρχικοποίησης, ο εξυπηρετητής πιστοποίησης αυθεντικότητας μπορεί να συγκεντρώσει όλες τις απαραίτητες πληροφορίες για την τοπολογία του ασύρματου δικτύου πολλαπλών κόμβων έξυπνων μετρητών. Ο ίδιος εξυπηρετητής μπορεί να δημιουργήσει μια βέλτιστη διαδρομή για τη δρομολόγηση των μηνυμάτων, ειδοποιώντας τους αντίστοιχους μετρητές που περιλαμβάνονται στη διαδρομή δυναμικά.

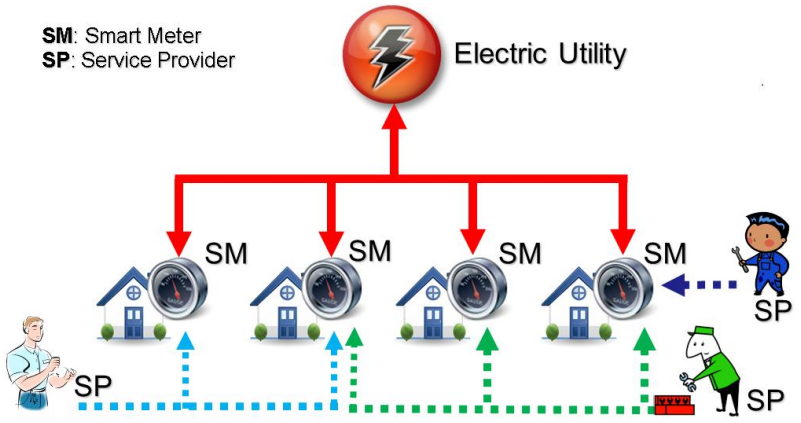
7.3.1.1. Ο έξυπνος μετρητής (smart meter) ως τείχος προστασίας (firewall) μεταξύ εσωτερικού και εξωτερικού κόσμου

Ο έξυπνος μετρητής μπορεί να χρησιμοποιηθεί ως ένα τείχος προστασίας που διευθύνει την εισερχόμενη και εξερχόμενη κυκλοφορία, διασφαλίζοντας την ιδιωτική ζωή των ιδιοκτητών-χρηστών και την ακεραιότητα των μηνυμάτων που ανταλλάσσονται. Λειτουργεί ως μεσολαβητής για να μεταφέρει τις οδηγίες του ηλεκτρικού παρόχου (electric utility) προς τις έξυπνες ηλεκτρικές οικιακές συσκευές. Επίσης, δίνει τη δυνατότητα στους παρόχους υπηρεσίας (service providers) να παρακολουθούν και να προσφέρουν τεχνική βοήθεια στους πελάτες τους χρησιμοποιώντας την υπάρχουσα υποδομή επικοινωνιών. Όλα αυτά τα χαρακτηριστικά επιτυγχάνονται εγκαθιδρύοντας μια σχέση εμπιστοσύνης μεταξύ ηλεκτρικού παρόχου και έξυπνου μετρητή.

Τον εσωτερικό κόσμο αποτελεί το Home Area Network (HAN) που αποτελείται από τις επικοινωνίες μεταξύ των έξυπνων ηλεκτρικών οικιακών συσκευών, ενώ τον εξωτερικό κόσμο αποτελεί το Wide Area Network (WAN) που αποτελείται από τις επικοινωνίες μεταξύ των νοικοκυριών, των παρόχων και των διαχειριστών του συστήματος.

Ο έξυπνος μετρητής θα προστατεύει την ιδιωτική ζωή των χρηστών αποκρύπτοντας ατομικά στοιχεία από τον ηλεκτρικό πάροχο. Αντί ο ηλεκτρικός πάροχος να ελέγχει άμεσα τις οικιακές συσκευές, θα αναζητά τον έξυπνο μετρητή ώστε να μειώσει τη συνολική κατανάλωση ενέργειας και να αποφασίσει ποιες οικιακές συσκευές να κλείσει ή να περιορίσει τη λειτουργία τους. Οι πελάτες θα είναι αυτοί που θα αποφασίζουν την προτεραιότητα κάθε συσκευής τους.

Ακόμη, ο έξυπνος μετρητής θα χρησιμοποιείται για να επικοινωνεί με τους παρόχους υπηρεσίας, οι οποίοι έχουν υπογράψει συμβόλαιο για να συντηρούν συγκεκριμένες ηλεκτρικές συσκευές. Δηλαδή, θα καταγράφει και θα ζευγαρώνει έναν πάροχο υπηρεσίας με τις αντίστοιχες συσκευές για να δημιουργήσει ένα μονοπάτι επικοινωνίας μεταξύ τους. Θα παρέχει μηνύματα μόνο μεταξύ των παρόχων υπηρεσίας που έχουν υπογράψει συμβόλαιο με τις οικιακές συσκευές για τις οποίες είναι υπεύθυνοι. Για παράδειγμα, ένα ηλεκτρικό αυτοκίνητο μπορεί να εκπέμψει μηνύματα λάθους (error messages) σε ένα συγκεκριμένο και πιστοποιημένο για την αυθεντικότητά του μηχανικό υπηρεσίας μέσω του έξυπνου μετρητή.



Εικόνα 7-3 Έξυπνοι μετρητές και μηχανικοί-τεχνικοί υπηρεσίας

Ο ηλεκτρικός πάροχος θα στέλνει οδηγίες σχετικές με την κατανάλωση προς τους έξυπνους μετρητές και θα συλλέγουν από αυτούς στοιχεία κατανάλωσης ανά τακτά χρονικά διαστήματα. Για παράδειγμα, κατά τη διάρκεια των περιόδων αιχμής, ο ηλεκτρικός πάροχος θα καθοδηγεί τους έξυπνους μετρητές να περιορίσουν τις καταναλώσεις τους, προμηθεύοντάς τους με κίνητρα. Μετά, θα αποτελεί ευθύνη του έξυπνου μετρητή να διακανονίσει τη λειτουργία των οικιακών συσκευών του. Αυτή η προσέγγιση κρύβει τις ιδιωτικές συσκευές από τον πάροχο και προστατεύει την ιδιωτική ζωή των χρηστών.

Οι πάροχοι υπηρεσιών θα καταγράφονται σε έναν ηλεκτρικό πάροχο και θα παρέχουν ψηφιακά πιστοποιητικά για την αυθεντικότητα της ταυτότητάς τους καθώς και κλειδιά επικοινωνίας για να μπορούν εξυπηρετήσουν τους χρήστες. Έπειτα, θα μπορούν να υπογράψουν συμβόλαια με ιδιωτικούς χρήστες για τις συσκευές που θα υποστηρίζουν. Ο έξυπνος μετρητής θα περιορίσει την επικοινωνία των οικιακών συσκευών μόνο με παρόχους υπηρεσιών των οποίων τα πιστοποιητικά είναι έγκυρα.

7.3.1.2. Ζητήματα ασφάλειας

1) Ταυτότητα και διαχείριση κλειδιών (identity and key management)—κάθε οντότητα επικοινωνίας είτε στο HAN είτε στο WAN θα έχει μια μοναδική ταυτότητα. Αυτές οι ταυτότητες θα χρησιμοποιούνται για να διασφαλίσουν ότι τα μηνύματα εκπέμπονται και λαμβάνονται από νόμιμες οντότητες άξιες εμπιστοσύνης. Επιπλέον, ο έξυπνος μετρητής, ο ηλεκτρικός πάροχος, οι πάροχοι υπηρεσιών και κάποιες από τις οικιακές συσκευές θα έχουν πιστοποιητικά για τα δημόσιά τους κλειδιά και τα ζευγάρια ιδιωτικών κλειδιών θα κρατούνται εμπιστευτικά. Ο ηλεκτρικός πάροχος θα είναι η αρχή εξουσιοδότησης της πιστοποίησης που θα παρέχει πιστοποιητικά για οντότητες μέσα στο WAN. Το πιστοποιητικό του ηλεκτρικού παρόχου θα αποθηκεύεται σε κάθε έξυπνο μετρητή πριν την εγκατάσταση και τα πιστοποιητικά για τους έξυπνους μετρητές και τους παρόχους υπηρεσιών θα υπογράφονται από τον ηλεκτρικό πάροχο. Μετά τη συμφωνία για σύναψη συμβολαίου ανάμεσα σε έναν έξυπνο μετρητή και έναν πάροχο υπηρεσίας, και οι δύο οντότητες ανταλλάσσουν υπογεγραμμένα πιστοποιητικά για να διασφαλίσουν την ταυτότητα και τη νομιμότητα των δημόσιων κλειδιών τους. Παρόμοια, ο έξυπνος μετρητής θα είναι η αρχή εξουσιοδότησης που θα χειρίζεται τα πιστοποιητικά μέσα στο HAN. Εάν χρειάζεται, τα πιστοποιητικά για τις έξυπνες οικιακές συσκευές θα υπογράφονται από τον έξυπνο μετρητή και θα χρησιμοποιούνται για την επικοινωνία με τους παρόχους υπηρεσιών.
2) Διασφάλιση ιδιωτικής ζωής (privacy assurance)—αμέσως μόλις ο έξυπνος μετρητής πιστοποιήσει την αυθεντικότητα μιας απομακρυσμένης οντότητας, μπορεί να δημιουργήσει ένα ασφαλές κανάλι επικοινωνίας χρησιμοποιώντας αποθηκευμένα κλειδιά για να κρυπτογραφήσει/ αποκρυπτογραφήσει τα μεταδιδόμενα μηνύματα. Η κύρια ανησυχία για την προστασία της ιδιωτικής ζωής τοποθετείται στην περιοχή WAN, όπου εξωτερικές οντότητες συγκεντρώσουν πληροφορίες κατανάλωσης χρηστών. Ουσιαστικά, ο έξυπνος μετρητής θα παρέχει δεδομένα που θα είναι επαρκή για την απομακρυσμένη οντότητα του παρόχου υπηρεσιών να κάνει τη δουλειά της.

3) Διασφάλιση ακεραιότητας (integrity assurance)—επειδή ο έξυπνος μετρητής θα δρα ως μια πύλη δικτύου μεταξύ του HAN και του WAN και θα εξυπηρετεί ως ένα τείχος προστασίας για το HAN, είναι σημαντικό να διακατέχεται από υψηλή ασφάλεια ακεραιότητας. Η δημιουργία μιας σχέσης εμπιστοσύνης με τον έξυπνο μετρητή παρέχει μια καλύτερη ασφάλεια τόσο για εξωτερικές όσο και για εσωτερικές οντότητες. Ο ηλεκτρικός πάροχος και οι πάροχοι υπηρεσιών προστατεύονται από επιθέσεις που εξαπολύονται από κακόβουλους έξυπνους μετρητές.

7.3.1.3. Ασφαλείς μηχανισμοί επικοινωνίας

- Επικοινωνίες ηλεκτρικού παρόχου-έξυπνου μετρητή—ο ηλεκτρικός πάροχος θα συγκεντρώσει πληροφορίες κατανάλωσης από του έξυπνους μετρητές για τη διαχείριση του έξυπνου δικτύου. Κάθε έξυπνος μετρητής θα προμηθεύει τον πάροχο με συνεχείς αναφορές στοιχείων κατανάλωσης ηλεκτρικής ενέργειας, όπως ελάχιστη, μέγιστη, μέση κατανάλωση ισχύος των χρηστών. Το διάστημα και η συχνότητα αυτών των αναφορών καθορίζεται από τον πάροχο, έτσι ώστε οι συγκρούσεις πακέτων και οι συνωστισμοί να ελαχιστοποιούνται. Η επικοινωνία μεταξύ αυτών των δύο οντοτήτων πραγματοποιείται μέσω μονο-εκπομπής (unicast), αφού έχει εγκατασταθεί και πιστοποιηθεί η αυθεντικότητα της ταυτότητάς τους.
  Στην περίπτωση διαταραχής της κατανάλωσης ή παράδοσης ηλεκτρικής ισχύος, ο έξυπνος μετρητής θα αποστείλει μηνύματα έκτακτης ανάγκης (urgent messages) προς τον ηλεκτρικό πάροχο. Αυτά τα μηνύματα θα ενεργοποιήσουν αντίστοιχους συναγερμούς, έτσι ώστε να ληφθούν οι απαραίτητες προφυλάξεις και τα κατάλληλα μέτρα από τον πάροχο. Για παράδειγμα, εάν ένας έξυπνος μετρητής αναφέρει στον πάροχο το επείγον περιστατικό εκδήλωσης πυρκαγιάς σε ένα σπίτι-νοικοκυριό, τότε ο πάροχος θα αποστείλει σήματα πολυ-εκπομπής (multicast) ή ευρυ-εκπομπής(broadcast) στους έξυπνους μετρητές της γύρω περιοχής του επείγοντος περιστατικού.
- Επικοινωνίες έξυπνου μετρητή-οικιακών συσκευών—στο επίπεδο HAN, οι απαιτήσεις ασφάλειας είναι λιγότερο αυστηρές από το επίπεδο WAN. Ο έξυπνος μετρητής θα αποτελεί την αρχή εξουσιοδότησης στο HAN και θα παρέχει πιστοποιητικά στις έξυπνες συσκευές όταν χρειάζεται. Όταν μια έξυπνη συσκευή συστήνεται στο σύστημα, θα καταγράφεται στον έξυπνο μετρητή. Ο έξυπνος μετρητής θα αποθηκεύει την ταυτότητα των συσκευών αυτών και θα διατηρεί την ακεραιότητά τους.
  Ο έξυπνος μετρητής θα καθοδηγεί ξεχωριστά τις οικιακές συσκευές να σταματήσουν να λειτουργούν ή να μεταβάλλουν τον κύκλο λειτουργίας τους. Αντίστροφα, οι έξυπνες συσκευές θα στέλνουν αναφορές κατανάλωσης και μηνύματα λάθους στον έξυπνο μετρητή. Εάν ληφθεί ένα μήνυμα λάθους από συσκευή που έχει υπογράψει συμβόλαιο με κάποιο πάροχο υπηρεσιών, ο έξυπνος μετρητής θα στείλει μήνυμα αναζήτησης(request message) στον αντίστοιχο πάροχο υπηρεσιών.
  Επίσης, η τοποθέτηση προτεραιότητας μπορεί να διαμορφωθεί από τον χρήστη εάν πιστεύει ότι μια συσκευή είναι πιο σημαντική από μια άλλη.

Για παράδειγμα, ένα ψυγείο μπορεί να έχει προτεραιότητα απέναντι στο πλυντήριο πιάτων ή το στεγνωτήριο ρούχων.

- Επικοινωνίες παρόχου υπηρεσιών-έξυπνου μετρητή—οι πάροχοι υπηρεσιών παρακολουθούν και συντηρούν τις ηλεκτρικές οικιακές συσκευές μέσω του έξυπνου μετρητή. Κάθε πάροχος υπηρεσιών που θέλει να συμμετέχει στο σύστημα, πρέπει πρώτα να καταγραφεί στον ηλεκτρικό πάροχο και έπειτα να υπογράψει συμβόλαιο με ιδιωτικούς χρήστες για συγκεκριμένες συσκευές. Ο έξυπνος μετρητής γίνεται τότε ένας πληρεξούσιος μεταξύ των οικιακών συσκευών και παρόχου υπηρεσιών που έχουν υπογράψει συμβόλαιο μεταξύ τους.
  Επιτρέποντας σε ένα πάροχο υπηρεσιών περιορισμένη πρόσβαση στις πληροφορίες των συσκευών ενός νοικοκυριού, κάποιο μέρος της ιδιωτικής ζωής αποκαλύπτεται. Αυτή η αποκάλυψη ίσως ελαχιστοποιηθεί, παρέχοντας στον πάροχο υπηρεσίας μόνο επαρκείς πληροφορίες για να εκτελέσει τη δουλειά του. Για παράδειγμα, οι πάροχοι υπηρεσιών μπορούν να προσφέρουν αναβάθμιση σε συγκεκριμένα στοιχεία λογισμικού των έξυπνων συσκευών.

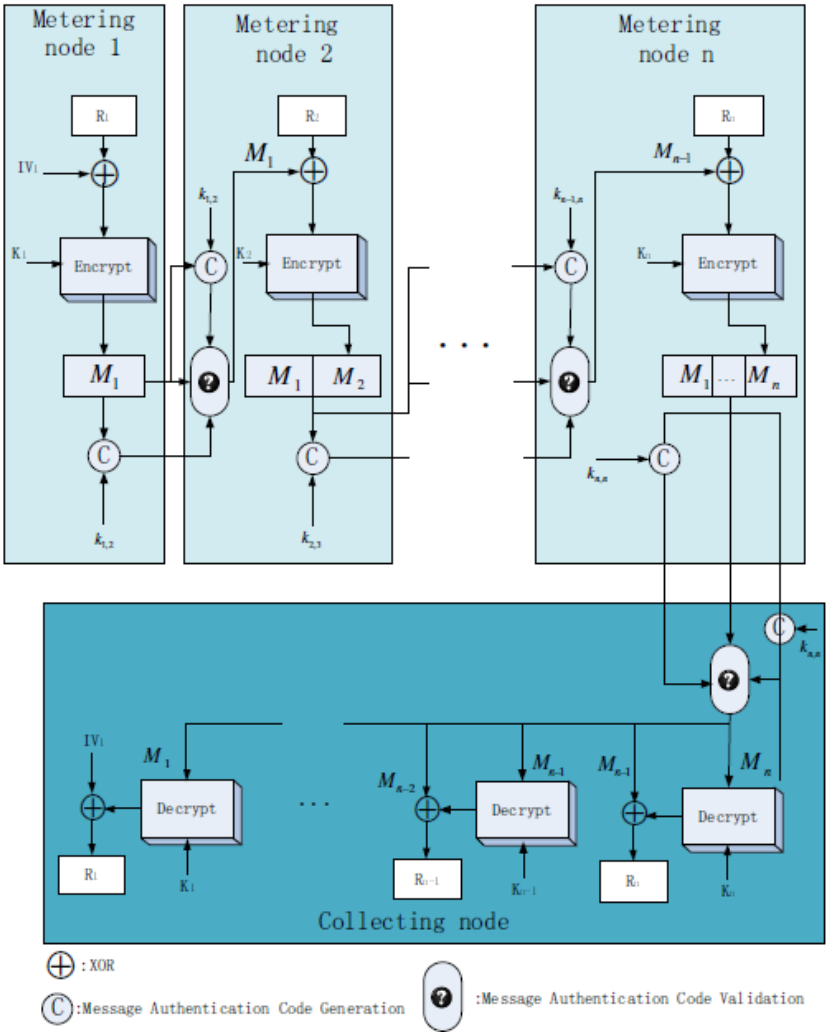
7.3.2. Διαδικασία συλλογής μηνυμάτων-μετρήσεων (meter-reading collection process)

Υποθέτουμε ότι μια ομάδα έξυπνων μετρητών δημιουργεί μια τοπολογία αλυσίδας (route chain topology) με τη σειρά κόμβος 1, κόμβος 2, …, κόμβος n και ο κόμβος συλλογής (collecting node). Η εικόνα απεικονίζει τη διαδικασία κρυπτογράφησης/αποκρυπτογράφησης και πιστοποίησης αυθεντικότητας των μηνυμάτων κατά τη συλλογή των μετρήσεων.

Ο έξυπνος μετρητής-κόμβος 1, που βρίσκεται στην αρχή της αλυσίδας, πραγματοποιεί την πράξη XOR μεταξύ της μέτρησής του και του αρχικού του διανύσματος IV. Το αποτέλεσμα αυτής της πράξης χρησιμοποιείται ως είσοδος για κρυπτογράφηση με το κλειδί K_1 ώστε να δημιουργήσει το κρυπτογραφημένο μήνυμα M_1. Η λειτουργία πιστοποίησης αυθεντικότητας των μηνυμάτων χρησιμοποιεί το κρυπτογραφημένο μήνυμα M_1 και το κλειδί του $k_{1,2}$ για να δημιουργήσει τον αντίστοιχο κώδικα πιστοποίησης αυθεντικότητας του μηνύματος, ο οποίος θα επισυναφθεί μαζί με το κρυπτογραφημένο μήνυμα M_1. Τότε, αυτός ο συνδυασμός θα σταλεί στο γειτονικό έξυπνο μετρητή-κόμβο 2, ο οποίος αποτελεί το επόμενο βήμα της διαδρομής προς τον κόμβο συλλογής.

Ο έξυπνος μετρητής-κόμβος 2 δημιουργεί το δικό του κώδικα πιστοποίησης αυθεντικότητας του μηνύματος χρησιμοποιώντας το κλειδί του $k_{1,2}$ και το λαμβανόμενο κρυπτογραφημένο μήνυμα M_1. Εάν ο παραγόμενος κώδικας πιστοποίησης αυθεντικότητας του μηνύματος ταιριάζει με τον λαμβανόμενο αντίστοιχο κώδικα, τότε πιστοποιείται η ακεραιότητα του λαμβανόμενου κρυπτογραφημένου μηνύματος M_1. Τότε, το κρυπτογραφημένο μήνυμα M_1 λειτουργεί ως μια είσοδος για την πράξη XOR στον έξυπνο μετρητή-κόμβο 2. Την άλλη είσοδο αποτελεί η μέτρηση του έξυπνου μετρητή-κόμβου 2. Παρόμοια διαδικασία συμβαίνει σε όλους τους ενδιάμεσους κόμβους στη διαδρομή της αλυσίδας μέχρι να φθάσει στον κόμβο συλλέκτη (εξυπηρετητής πιστοποίησης αυθεντικότητας), ο οποίος έχει στην κατοχή του όλα τα K_n της διαδρομής. Μετά την πιστοποίηση αυθεντικότητας του μηνύματος του έξυπνου μετρητή-κόμβου n, ο

κόμβος συλλέκτης μπορεί να αποκρυπτογραφήσει άμεσα όλα τα μηνύματα-μετρήσεις από τον έξυπνο μετρητή-κόμβο 1 έως τον έξυπνο μετρητή-κόμβο n της αλυσίδας.



Εικόνα 7-4 Διαδικασία συλλογής μηνυμάτων-μετρήσεων

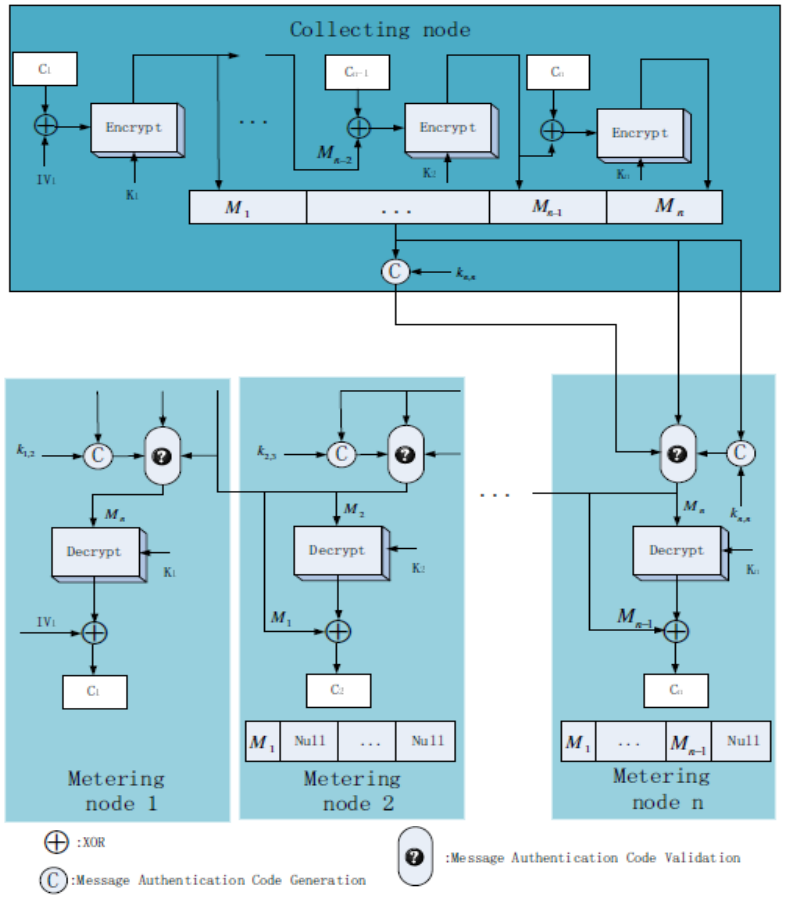
Ο κόμβος συλλέκτης θα συναθροίσει τα λαμβανόμενα μηνύματα-μετρήσεις και θα προωθήσει αυτά τα επεξεργασμένα δεδομένα μέσω προκαθορισμένων γραμμών σε ανώτερα στρώματα. Όλες οι μετρήσεις στις feeder γραμμές μεταφοράς συγκεντρώνονται στο τοπικό γραφείο διαχείρισης, όπου η μετρήσεις πραγματικού χρόνου ταξινομούνται εκ νέου για λόγους κοστολόγησης κατανάλωσης ρεύματος νοικοκυριών. Επίσης, οι πληροφορία αυτών των μετρήσεων θα χρησιμοποιηθεί και από το κέντρο ελέγχου SCADA για βέλτιστη διαχείριση της ενέργειας.

7.3.3. Διαδικασία διανομής μηνυμάτων διαχείρισης (management message distribution process)

Το κέντρο ελέγχου SCADA και το τοπικό γραφείο διαχείρισης του υποσταθμού θα προσαρμόσουν την παραγωγή, μεταφορά και διανομή ηλεκτρικής ισχύος στο έξυπνο

δίκτυο σύμφωνα με τις συλλεγμένες μετρήσεις. Τα μηνύματα διαχείρισης και ελέγχου θα διανεμηθούν σε συγκεκριμένους έξυπνους μετρητές για να προγραμματίσουν τη λειτουργία των έξυπνων οικιακών συσκευών.

Η αντίστροφη διαδικασία ροής πραγματοποιείται για να μοιραστούν τα συγκεκριμένα μηνύματα διαχείρισης από τον κόμβο συλλέκτη στους αντίστοιχους έξυπνους μετρητές κόμβους της διαδρομής της αλυσίδας.



Εικόνα 7-5 Διαδικασία διανομής μηνυμάτων διαχείρισης

7.3.4. Εκτίμηση προσφοράς συνεργατικού σεναρίου επικοινωνίας

Στο παραπάνω συνεργατικό σενάριο επικοινωνίας για το έξυπνο δίκτυο μέτρησης, οι διαδικασίες πιστοποίησης αυθεντικότητας και κρυπτογράφησης πραγματοποιούνται βήμα-βήμα, κόμβο-κόμβο (hop-by-hop) στη διαδρομή επικοινωνίας. Επίσης, επιτυγχάνονται τα παρακάτω αποτελέσματα:

- *Πιστοποίηση αυθεντικότητας συσκευής (device authentication)*—η ταυτότητα και η νομιμότητα των έξυπνων μετρητών και των σχετιζόμενων καταναλωτών πιστοποιείται πριν γίνει μέλος του διασυνδεδεμένου (interconnected) δικτύου έξυπνων μετρητών και λάβει τις κατάλληλες υπηρεσίες του παρόχου (utility service).

- *Εμπιστευτικότητα δεδομένων (data confidentiality)*—οι μετρήσεις και τα μηνύματα διαχείρισης και ελέγχου κρατούνται μυστικά έτσι ώστε να αποκρύπτουν την ιδιωτική ζωή των καταναλωτών και τις επιχειρησιακές πληροφορίες του παρόχου από μη εξουσιοδοτημένες οντότητες.
- *Ακεραιότητα μηνυμάτων (message integrity)*—το έξυπνο δίκτυο πιστοποιεί ότι οι μετρήσεις και τα μηνύματα διαχείρισης και ελέγχου μεταφέρονται μη τροποποιημένα μες στο έξυπνο δίκτυο μέτρησης.
- *Συντηρητική μυστικοπάθεια (maintaining secrecy)*—κάποια μυστικά του έξυπνου μετρητή κρατούνται για τον ίδιο και μόνο(μετρήσεις), ενώ κάποια άλλα μυστικά μοιράζονται με συγκεκριμένους εταίρους για την εξασφάλιση ασφαλών επικοινωνιών (κλειδιά).
- *Αντιμετώπιση πιθανών ηλεκτρονικών επιθέσεων (cyber attacks)*—ένας έξυπνος μετρητής, έχοντας στην κατοχή του τα ψηφιακά διαπιστευτήρια της νομιμότητάς του, εγγυάται ότι παρέχει ασφαλείς συνδέσεις επικοινωνίας με ολόκληρο το δίκτυο έξυπνων μετρητών. Ακόμη και αν ένας έξυπνος μετρητής τεθεί σε κίνδυνο, ο επιτιθέμενος δεν μπορεί να χρησιμοποιήσει τον κατειλημμένο έξυπνο μετρητή για περαιτέρω πρόσβαση στις πληροφορίες άλλων έξυπνων μετρητών.

7.3.5. Σύγκριση με το βασικό σενάριο ασφάλειας

Επίσης, υπήρξαν και θετικά αποτελέσματα προσομοίωσης του συνεργατικού σεναρίου επικοινωνίας, χρησιμοποιώντας 10 κόμβους-έξυπνους μετρητές στην τοπολογία της αλυσίδας. Το παραπάνω σενάριο συγκρίθηκε με το βασικό σενάριο ασφάλειας, όπου καθένας από τους έξυπνους μετρητές επικοινωνεί με τον κόμβο συλλέκτη μέσω ενός ιδιωτικού κλειδιού και μιας ανεξάρτητης από άκρη σε άκρη κρυπτογράφησης.

Παρατηρείται ότι το προτεινόμενο σενάριο είναι ανώτερο του βασικού σεναρίου ασφάλειας καθώς ο αριθμός των κόμβων-έξυπνων μετρητών αυξάνει. Η ασύρματη παρεμβολή χειροτερεύει καθώς όλο και περισσότερες συσκευές εμπλέκονται ταυτόχρονα. Στο προτεινόμενο σενάριο, κάθε συμμετέχων έξυπνος μετρητής, κατά τη διαδικασία αρχικοποίησης, μπορεί να προγραμματίσει το συγκεκριμένο διάστημα που θα μεταδώσει. Γι αυτό το λόγο, όλοι οι συμμετέχοντες έξυπνοι μετρητές θα μεταδώσουν με προκαθορισμένη σειρά για να αποφευχθεί η παρεμβολή τόσο στη μετάδοση όσο και στη λήψη. Έτσι, επιτυγχάνεται χαμηλή από άκρη σε άκρη καθυστέρηση, ενώ στο βασικό σενάριο ασφάλειας χειροτερεύει όσο αυξάνει ο αριθμός των κόμβων.

Παρατηρείται σημαντική διαφορά στο ρυθμό απώλειας πακέτων. Το προτεινόμενο σενάριο μπορεί να κρατήσει σε πολύ χαμηλό επίπεδο το ρυθμό απώλειας πακέτων (περίπου 0%), ενώ το βασικό σενάριο ασφάλειας υποβαθμίζεται δραματικά καθώς ο αριθμός των κόμβων αυξάνει. Ξεπερνάει το 20% όταν ο αριθμός των κόμβων φτάνει στους 9, το οποίο είναι προφανώς καταστροφικό για τη λειτουργία εφαρμογών όπως online μετρήσεις, παρακολούθηση και προστασία.

8. Προσομοίωση Δικτύου Smart Grid (Simulation of Smart Grid Network)

8.1. Τα στοιχεία της προσομοίωσης

Η τοπολογία της προσομοίωσης που εκτέλεσα στηρίζεται στην ιδέα της λειτουργίας του έξυπνου δικτύου, συμπεριλαμβανομένου των ζητημάτων ασφάλειας και συνεργατικών υπηρεσιών που το απασχολούν.

Τα σύνθετα στοιχεία που δημιούργησα και συμμετέχουν στην προσομοίωση είναι τα εξής:

- Έξυπνοι μετρητές (smart meters)
- Κινούμενοι χρήστες (mobile users)
- Συλλέκτες δεδομένων (data collectors)
- Σημεία πρόσβασης (access points)
- Τοπικά δίκτυα και πύλες δικτύου (LANs and gateways)
- Διαδίκτυο (internet)
- Απομακρυσμένοι εξυπηρετητές (remote servers)
- Υπάλληλοι κέντρου ελέγχου (control center's officers)
- Επιτιθέμενοι (attackers)
- mtu (master transmission unit)
- Διαμερίσματα και ιδιοκτήτες (buildings and owners)
- Έξυπνο δίκτυο (smart grid)

Διάφορα στοιχεία που συνθέτουν τα παραπάνω δημιουργημένα στοιχεία και συναντώνται συχνά στην προσομοίωση δικτύου είναι τα εξής:

Εικόνα 8-1 ChannelControl

Το παραπάνω απλό στοιχείο εμφανίζεται στη δημιουργία του σύνθετου δικτύου SmartGrid. Το ChannelControl έχει ακριβώς ένα παράδειγμα σε κάθε δικτυακό μοντέλο που περιέχει κινητούς ή ασύρματους κόμβους. Το στοιχείο αυτό πληροφορείται για την θέση και την κίνηση των κόμβων και αποφασίζει ποιοι κόμβοι σε απόσταση επικοινωνίας ή παρεμβολής. Έπειτα, αυτή η πληροφορία χρησιμοποιείται από τις διεπιφάνειες ραδιοσυχνοτήτων των κόμβων κατά τις μεταδόσεις.

Οι παράμετροι του ChannelControl είναι οι εξής:

```
bool coreDebug = default(false); // debug switch for core framework
double playgroundSizeX = default(600); // x size of the playground (in meters)
double playgroundSizeY = default(400); // y size of the playground (in meters)
double pMax @unit("mW") = default(20mW); // maximum sending power used for this network
double sat @unit("dBm") = default(-110dBm); // signal attenuation threshold (in dBm)
```

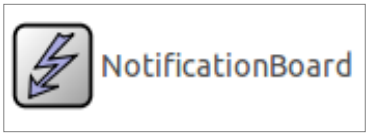
```
double alpha = default(2); // path loss coefficient
double carrierFrequency @unit("Hz") = default(2.4GHz); // carrier frequency of the channel (in Hz)
int numChannels = default(1); // number of radio channels (frequencies)
```

Εικόνα 8-2 FlatNetworkConfigurator

Το παραπάνω απλό στοιχείο εμφανίζεται στη δημιουργία του σύνθετου δικτύου SmartGrid. Το FlatNetworkConfigurator διαμορφώνει τις IP διευθύνσεις και τους πίνακες δρομολόγησης για ένα "επίπεδο" δίκτυο ("flat" network). "Επίπεδο" σημαίνει ότι όλα τα στοιχεία θα έχουν την ίδια διεύθυνση δικτύου και θα διαφέρουν μόνο στο τμήμα host. Δηλαδή, αναθέτει IP διευθύνσεις στα στοιχεία που βρίσκονται στο ίδιο δίκτυο, ανακαλύπτει την τοπολογία του δικτύου και υπολογίζει τα κοντινότερα μονοπάτια. Για την τελευταία περίπτωση, διαμορφώνει ένα γράφο από τα στοιχεία του δικτύου και εφαρμόζει τον αλγόριθμο του Dijstra σε αυτόν.

Οι παράμετροι του FlatNetworkConfigurator είναι οι εξής:

```
string networkAddress = default("192.168.0.0"); // network part of the address
string netmask = default("255.255.0.0"); // host part of addresses are autoconfigured
```



Εικόνα 8-3 NotificationBoard

Το παραπάνω απλό στοιχείο εμφανίζεται σε όλα τα σύνθετα δημιουργημένα στοιχεία. Χρησιμοποιώντας το NotificationBoard, τα στοιχεία της προσομοίωσης έχουν τη δυνατότητα να γνωστοποιούν το ένα στο άλλο για διάφορα γεγονότα που συμβαίνουν, όπως αλλαγές στον πίνακα δρομολόγησης, αλλαγές στην κατάσταση του ασύρματου καναλιού (π.χ. διαθέσιμο, μετάδοση, λήψη), αλλαγές στη θέση κινούμενων κόμβων, κ.ά. Λειτουργεί ως μεσολαβητής μεταξύ του στοιχείου, που οι αλλαγές κατάστασης μπορούν να συμβούν, και των στοιχείων που ενδιαφέρονται να μάθουν για αυτές τις αλλαγές.

Εικόνα 8-4 InterfaceTable

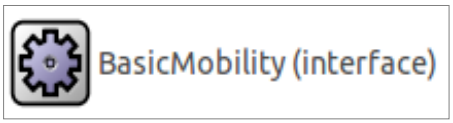
Το παραπάνω απλό στοιχείο εμφανίζεται σε όλα τα σύνθετα δημιουργημένα στοιχεία. Το InterfaceTable διατηρεί τον πίνακα όλων των διεπιφανειών δικτύου (network interfaces). Εκτός των καταγεγραμμένων διεπιφανειών, μια διεπιφάνεια ανατροφοδότησης (loopback) επίσης δημιουργείται. Ο πίνακας αυτός περιέχει μόνο ανεξάρτητες πρωτοκόλλου ιδιότητες των διεπιφανειών—τα δεδομένα των IP διευθύνσεων συγκεκριμένα διατηρούνται στο στοιχείο RoutingTable.

Εικόνα 8-5 Routingtable

Το παραπάνω απλό στοιχείο εμφανίζεται σε όλα τα σύνθετα δημιουργημένα στοιχεία. Το Routingtable αποθηκεύει τον πίνακα δρομολόγησης (η ανά διεπιφάνεια διαμόρφωση αποθηκεύεται στο στοιχείο InterfaceTable.

Εικόνα 8-6 NullMobility

Το παραπάνω απλό στοιχείο εμφανίζεται σε όλα τα σύνθετα δημιουργημένα στοιχεία εκτός του σύνθετου στοιχείου User. Το NullMobility δεν κάνει τίποτα, απλά χρησιμοποιείται για τους κόμβους που παραμένουν στάσιμοι.

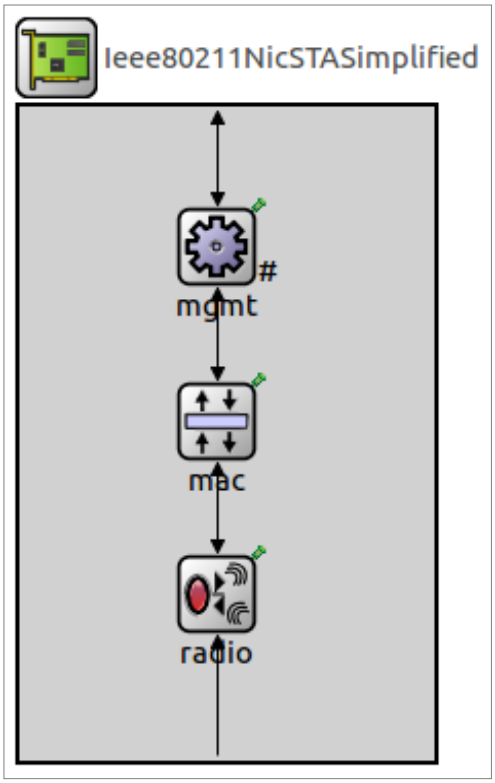


Εικόνα 8-7 BasicMobility

Το παραπάνω απλό στοιχείο εμφανίζεται μόνο στο σύνθετο στοιχείο User. Το BasicMobility δίνει τη δυνατότητα εφαρμογής μοντέλων κινητικότητας, όπως κυκλική, γραμμική, τυχαία, ορθογώνια κινητικότητα.

Στην προσομοίωση, χρησιμοποιήθηκε κυκλική κινητικότητα των χρηστών, που παρουσιάζει τις παρακάτω παραμέτρους:

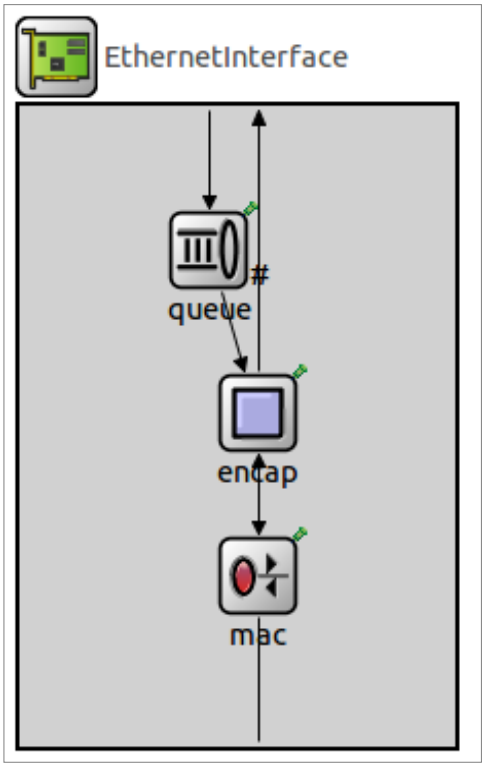
```
bool debug = default(false); // debug switch
double cx = default(100); // x coord of the center of the circle
double cy = default(100); // y coord of the center of the circle
double r = default(100); // radius of the circle
double speed @unit("mps") = default(2mps); // speed of the host (in m/s)
double startAngle @unit("deg") = default(0); // starting angle (degrees)
double updateInterval @unit("s") = default(100ms); // time interval to update the hosts position
```



Εικόνα 8-8 Ασύρματη κάρτα σύνδεσης δικτύου υποδομής 802.11

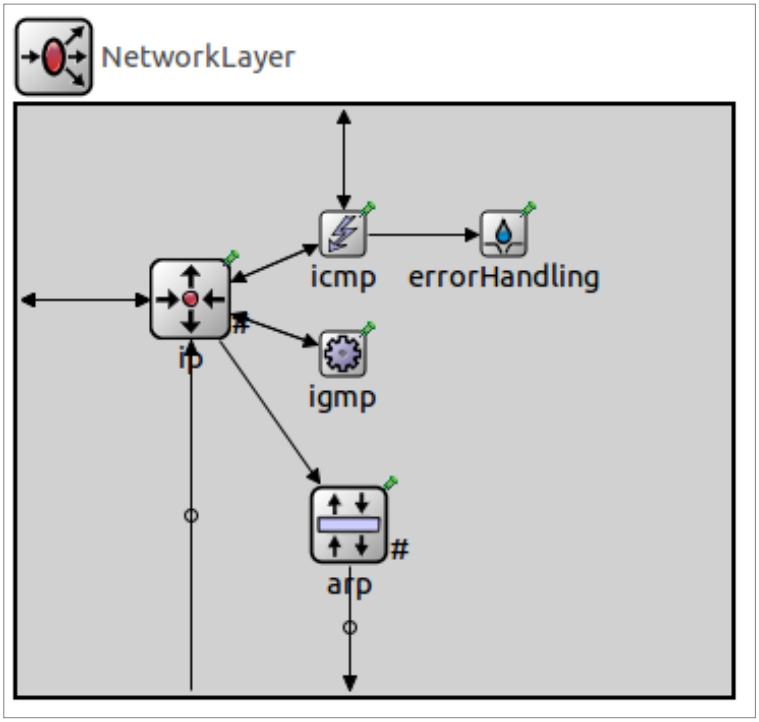
Το παραπάνω σύνθετο στοιχείο εμφανίζεται σε όλα τα σύνθετα δημιουργημένα στοιχεία. Το στοιχείο αυτό εφαρμόζει μια ασύρματη κάρτα σύνδεσης δικτύου υποδομής 802.11. Αποτελείται από 3 απλά στοιχεία και όλα μαζί εμφανίζουν τις παρακάτω παραμέτρους:

```
string accessPointAddress; // MAC address of associate AP
int frameCapacity = default(100);

string address = default("auto"); // MAC address as hex string (12 hex digits), or "auto". "auto" values will be replaced by a generated MAC address in init stage 0.
String queueModule = default(""); // name of optional external queue module
int maxQueueSize; // max queue length in frames; only used if queueModule==""
double bitrate @unit("bps");
int rtsThresholdBytes @unit("B") = default(2346B); // longer messages will be sent using RTS/CTS
int retryLimit = default(-1); // maximum number of retries per message, -1 means default
int cwMinData = default(-1); // contention window for normal data frames, -1 means default
int cwMinBroadcast = default(-1); // contention window for broadcast messages, -1 means default
int mtu = default(1500);

int channelNumber = default(0); // channel identifier
double transmitterPower @unit("mW") = default(20mW); // power used for transmission of messages (in mW)
double bitrate @unit("bps"); // (in bits/s)
double thermalNoise @unit("dBm") = default(-110dBm); // base noise level (dBm)
double pathLossAlpha = default(2); // used by the path loss calculation
double shadowingDeviation @unit("dB") = default(0dB); // used by the shadowing model calculation
double snirThreshold @unit("dB") = default(4dB); // if signal-noise ratio is below this threshold, frame is considered noise (in dB)
double sensitivity @unit("mW"); // received signals with power below sensitivity are ignored
```



Εικόνα 8-9 Ενσύρματη κάρτα σύνδεσης δικτύου υποδομής Ethernet

Το παραπάνω σύνθετο στοιχείο εμφανίζεται σε όλα τα σύνθετα δημιουργημένα στοιχεία. Το στοιχείο αυτό εφαρμόζει μια ενσύρματη κάρτα σύνδεσης δικτύου υποδομής Ethernet. Δεν χρησιμοποιείται στην προσομοίωση, αλλά προτείνεται ως εναλλακτική επιλογή.



Εικόνα 8-10 NetworkLayer

Το παραπάνω σύνθετο στοιχείο εμφανίζεται σε όλα τα σύνθετα δημιουργημένα στοιχεία. Το στοιχείο αυτό προσομοιώνει το στρώμα δικτύου ενός IP κόμβου. Συνδέεται με το στρώμα ζεύξης δεδομένων (ασύρματη ή ενσύρματη διεπιφάνεια). Προσφέρει διεπιφάνειες προς το στρώμα μεταφοράς τύπου TCP, UDP, Ping.
Κάποιες από τις εμφανιζόμενες παραμέτρους είναι οι εξής:

```
int timeToLive = default(32);
double retryTimeout @unit("s") = default(1s); // number seconds ARP waits between retries to resolve an \IP address
int retryCount = default(3); // number of times ARP will attempt to resolve an \IP address
double cacheTimeout @unit("s") = default(120s); // number seconds unused entries in the cache will time out
bool proxyARP = default(true); // sets proxy \ARP mode (replying to \ARP requests for the addresses for which a routing table entry exists)
```

Εικόνα 8-11 PingApp

Το παραπάνω απλό στοιχείο εμφανίζεται σε όλα τα σύνθετα δημιουργημένα στοιχεία. Το PingApp παράγει αναζητήσεις πινγκ (ping requests). Κάθε ping request στέλνεται με ένα σειριακό αριθμό και οι απαντήσεις αναμένονται να επιστρέψουν με τον ίδια σειριακό αριθμό.

Παρακάτω, παρουσιάζονται οι παράμετροι αυτού του στοιχείου:

```
string destAddr = default(""); // destination IP or Ipv6 address
string srcAddr = default(""); // source IP or Ipv6 address (useful with multi-homing)
double packetSize @unit("B") = default(56B); // of ping payload, in bytes
volatile double interval @unit("s") = default(1s); // time to wait between pings (can be random)
double hopLimit = default(32); // TTL or hopLimit for IP packets
double count = default(0); // stop after count ping requests, 0 means continuously
double startTime @unit("s") = default(uniform(0s,this.interval)); // send first ping at startTime
double stopTime @unit("s") = default(0s); // send no pings after stopTime, 0 means forever
```

Εικόνα 8-12 TCP

Το παραπάνω απλό στοιχείο εμφανίζεται στα περισσότερα σύνθετα δημιουργημένα στοιχεία. Προφανώς, προσομοιώνει το TCP πρωτόκολλο στο στρώμα μεταφοράς.

Ακολουθούν κάποιες παράμετροι αυτού του στοιχείου:

```
int advertisedWindow = default(14*this.mss); // in bytes, corresponds with the maximal receiver buffer capacity (Note: normally, NIC queues should be at least this size)
bool nagleEnabled = default(true); // Nagle's algorithm (RFC 896) enabled/disabled
int mss = default(536); // Maximum Segment Size (RFC 793) (header option)
string tcpAlgorithmClass = default("TCPReno"); //
TCPReno/TCPTahoe/TCPNewReno/TCPNoCongestionControl/DumbTCP
```

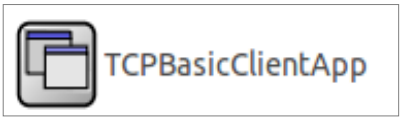
```
string sendQueueClass = default("TCPVirtualDataSendQueue"); //
TCPVirtualDataSendQueue/TCPMsgBasedSendQueue
string receiveQueueClass = default("TCPVirtualDataRcvQueue"); //
TCPVirtualDataRcvQueue/TCPMsgBasedRcvQueue
bool recordStats = default(true); // recording of seqNum etc. into output vectors enabled/disabled
```

Εικόνα 8-13 TCP_hack

Το παραπάνω απλό στοιχείο εμφανίζεται μόνο στο σύνθετο δημιουργημένο στοιχείο του SmartMeter και αποτελεί το μοναδικό στοιχείο που χρησιμοποιήθηκε από τη βιβλιοθήκη του SCADASim (όλα τα υπόλοιπα εξήχθησαν από τη βιβλιοθήκη του INET Framework). Προφανώς όπως και το παραπάνω στοιχείο, προσομοιώνει το TCP πρωτόκολλο στο στρώμα μεταφοράς. Ωστόσο, υπάρχει μια διαφορά μεταξύ τους. Αυτή είναι το γεγονός ότι το συγκεκριμένο στοιχείο υποστηρίζει έναν περιορισμένο αριθμό ταυτόχρονων συνδέσεων που γίνονται αποδεκτές από τον εξυπηρετητή και την υποδοχή του που ακούει σε μια θύρα (listening socket).

Ακολουθούν κάποιες παράμετροι αυτού του στοιχείου:

```
nagleEnabled = default(true); // Nagle's algorithm (RFC 896) enabled/disabled
mss = default(1024); // maximum segment size
advertisedWindow = default(14*this.mss); // in bytes (Note: normally, NIC queues should be at least
this size)
tcpAlgorithmClass = default("TCPReno"); //
TCPTahoe/TCPReno/TCPNoCongestionControl/DumbTCP
sendQueueClass = default("TCPMsgBasedSendQueue");    //
TCPVirtualDataSendQueue/TCPMsgBasedSendQueue
receiveQueueClass = default("TCPMsgBasedRcvQueue"); //
TCPVirtualDataRcvQueue/TCPMsgBasedRcvQueue
recordStats = default(true); // recording seqNum etc. into output vectors on/off
int maxThreadCount; // how many concurrent Threads are accepted
```



Εικόνα 8-14 TCPBasicClientApp

Το παραπάνω απλό στοιχείο εμφανίζεται στα σύνθετα στοιχεία που αποτελούν πελάτες TCP σύνδεσης. Αυτοί είναι οι έξυπνοι μετρητές, οι κινούμενοι χρήστες, καθώς και οι υπεύθυνοι υπάλληλοι του κέντρου ελέγχου. Ειδικότερα, το στοιχείο αυτό επικοινωνεί με τον αντίστοιχο εξυπηρετητή σε sessions. Κατά τη διάρκεια ενός session, ο πελάτης ανοίγει μια μοναδική TCP σύνδεση με τον εξυπηρετητή, στέλνει διάφορα request (περιμένοντας πάντοτε να φθάσει ολοκληρωμένη απάντηση πριν στείλει ένα νέο request), και τελικά κλείνει τη σύνδεση.

Ακολουθούν κάποιες παράμετροι αυτού του στοιχείου:

```
string address = default(""); // may be left empty ("")
int port = default(-1); // port number to listen on
string connectAddress = default("");  // server address (may be symbolic)
int connectPort = default(1000); // port number to connect to
double startTime @unit("s") = default(1s); // time first session begins
volatile int numRequestsPerSession = default(1);  // number of requests sent per session
volatile int requestLength @unit(B) = default(200B); // length of a request
volatile int replyLength @unit("B") = default(1MiB); // length of a reply
volatile double thinkTime @unit("s"); // time gap between requests
volatile double idleInterval @unit(s); // time gap between sessions
volatile double reconnectInterval @unit("s") = default(30s);  // if connection breaks, waits this much
before trying to reconnect
```

Επίσης, αποτελεί στοιχείο του οποίου ο κώδικας τροποποιήθηκε έτσι ώστε να ανταποκρίνεται στις ανάγκες της προσομοίωσης (το μέρος του κώδικα που τροποποιήθηκε είναι γραμμένο πλάγια, έντονα και υπογεγραμμένο). Πιο συγκεκριμένα, υπολογίζεται ο χρόνος καθυστέρησης κάθε εισερχόμενου πακέτου απάντησης από τον εξυπηρετητή.

TCPBasicClientApp.h

```
#ifndef __INET_TCPBASICCLIENTAPP_H
#define __INET_TCPBASICCLIENTAPP_H

#include <omnetpp.h>
#include "TCPGenericCliAppBase.h"


/**
 * An example request-reply based client application.
 */
class INET_API TCPBasicClientApp : public TCPGenericCliAppBase
{
 protected:

   // statistics
   cOutVector httpdelay;

   cMessage *timeoutMsg;
   bool earlySend;  // if true, don't wait with sendRequest() until established()
   int numRequestsToSend; // requests to send in this session

   /** Utility: sends a request to the server */
   virtual void sendRequest();

 public:
   TCPBasicClientApp();
   virtual ~TCPBasicClientApp();

 protected:
   /** Redefined to schedule a connect(). */
   virtual void initialize();

   /** Redefined. */
   virtual void handleTimer(cMessage *msg);

   /** Redefined. */
```

```
    virtual void socketEstablished(int connId, void *yourPtr);

    /** Redefined. */
    virtual void socketDataArrived(int connId, void *yourPtr, cPacket *msg, bool urgent);

    /** Redefined to start another session after a delay. */
    virtual void socketClosed(int connId, void *yourPtr);

    /** Redefined to reconnect after a delay. */
    virtual void socketFailure(int connId, void *yourPtr, int code);
};

#endif

#include "TCPBasicClientApp.h"
```

TCPBasicClientApp.cc

```
#define MSGKIND_CONNECT  0
#define MSGKIND_SEND     1


Define_Module(TCPBasicClientApp);

void TCPBasicClientApp::initialize()
{
    TCPGenericCliAppBase::initialize();

    httpdelay.setName("http delay");

    timeoutMsg = new cMessage("timer");
    numRequestsToSend = 0;
    earlySend = false;  // TBD make it parameter
    WATCH(numRequestsToSend);
    WATCH(earlySend);

    timeoutMsg->setKind(MSGKIND_CONNECT);
    scheduleAt((simtime_t)par("startTime"), timeoutMsg);
}

void TCPBasicClientApp::socketDataArrived(int connId, void *ptr, cPacket *msg, bool urgent)
{
    TCPGenericCliAppBase::socketDataArrived(connId, ptr, msg, urgent);

    httpdelay.record(simTime() - msg->getCreationTime());

    if (numRequestsToSend>0)
    {
        EV << "reply arrived\n";
        timeoutMsg->setKind(MSGKIND_SEND);
        scheduleAt(simTime()+(simtime_t)par("thinkTime"), timeoutMsg);
    }
    else
    {
        EV << "reply to last request arrived, closing session\n";
        close();
    }
```

Εικόνα 8-15 TCPGenericSrvApp

Το παραπάνω απλό στοιχείο εμφανίζεται στα σύνθετα στοιχεία που αποτελούν πελάτες TCP σύνδεσης. Αυτοί είναι οι έξυπνοι μετρητές, οι κινούμενοι χρήστες, οι απομακρυσμένοι εξυπηρετητές, καθώς και οι υπεύθυνοι υπάλληλοι του κέντρου ελέγχου. Το στοιχείο δέχεται έναν αριθμό εισερχόμενων συνδέσεων, ανάλογα με την περίπτωση, και περιμένει να λάβει μηνύματα από τους πελάτες.

Ακολουθούν κάποιες παράμετροι αυτού του στοιχείου:

```
string address = default(""); // local address; may be left empty ("")
int port = default(1000);     // port number to listen on
double replyDelay @unit("s") = default(0s);
```

Εικόνα 8-16 TCPSinkApp

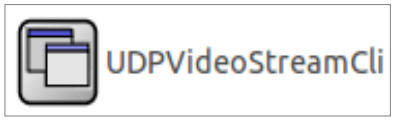
Το παραπάνω στοιχείο εμφανίζεται σε ένα και μοναδικό στοιχείο, το MasterTransmissionUnit. Αποδέχεται τις εισερχόμενες TCP συνδέσεις και απορρίπτει οτιδήποτε φθάνει σε αυτό.

Ακολουθούν κάποιες παράμετροι αυτού του στοιχείου:

```
string address = default(""); // may be left empty ("")
int port = default(1000); // port number to listen on
```

Εικόνα 8-17 UDP

Το παραπάνω απλό στοιχείο εμφανίζεται στα στοιχεία που αποτελούν πελάτες ή εξυπηρετητές VideoStream. Προφανώς, προσομοιώνει το UDP πρωτόκολλο στο στρώμα μεταφοράς.



Εικόνα 8-18 UDPVideoStreamCli

Το παραπάνω απλό στοιχείο εμφανίζεται στα στοιχεία που αποτελούν πελάτες VideoStream, δηλαδή στους κινούμενους χρήστες.

Ακολουθούν κάποιες παράμετροι αυτού του στοιχείου:

```
int localPort;
string serverAddress;
int serverPort;
double startTime @unit("s") = default(1s);
volatile double nextTime @unit("s") = default(1s);
```

Επίσης, αποτελεί στοιχείο του οποίου ο κώδικας τροποποιήθηκε έτσι ώστε να ανταποκρίνεται στις ανάγκες της προσομοίωσης (το μέρος του κώδικα που τροποποιήθηκε είναι γραμμένο πλάγια, έντονα και υπογεγραμμένο). Πιο συγκεκριμένα, ο πελάτης μπορεί να αναζητά και να κατεβάζει όχι μόνο ένα βίντεο και να ξεκουράζεται, όπως ίσχυε μέχρι τώρα, αλλά να συνεχίζει να αναζητά και να κατεβάζει όσα βίντεο επιθυμεί ανά επιλεγόμενο χρονικό διάστημα. Επίσης, από εδώ και πέρα, η αναζήτηση του εξυπηρετητή από τον οποίο θα κατεβάσει το βίντεο θα είναι τυχαία επιλογή μέσα από μια λίστα εξυπηρετητών.

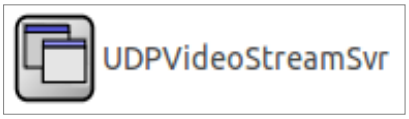
UDPVideoStreamCli.h

```
#ifndef __INET_UDPVIDEOSTREAM_H
#define __INET_UDPVIDEOSTREAM_H

#include <vector>
#include <omnetpp.h>
#include "UDPAppBase.h"
#include "IPvXAddress.h"

/**
 * A "Realtime" VideoStream client application.
 *
 * Basic video stream application. Clients connect to server and get a stream of
 * video back.
 */
class INET_API UDPVideoStreamCli : public UDPAppBase
{
  protected:
    // statistics
    cOutVector eed;

  protected:
    ///@name Overridden cSimpleModule functions
    //@{
    virtual void initialize();
    virtual void finish();
    virtual void handleMessage(cMessage *msg);
    //@}

  protected:
    virtual void requestStream();
    virtual void receiveStream(cPacket *msg);

  protected:
    std::vector<IPvXAddress> serverAddress;

    // chooses random destination address
    virtual IPvXAddress chooseDestAddress();
};

#endif
```

UDPVideoStreamCli.cc

```
#include "UDPVideoStreamCli.h"
#include "IPAddressResolver.h"


Define_Module(UDPVideoStreamCli);


void UDPVideoStreamCli::initialize()
{
   eed.setName("video stream eed");
   simtime_t startTime = par("startTime");

   simtime_t nextTime = par("nextTime");
   simtime_t sum = par("sum");
   int i;

   if (startTime>=0)
      scheduleAt(startTime, new cMessage("UDPVideoStreamStart"));

   sum = startTime;
   if (nextTime>=0)
      for(i=0; i<10; i++){
         scheduleAt(sum + nextTime, new cMessage("UDPVideoStreamStart"));
         sum = sum + nextTime;
      }
}


void UDPVideoStreamCli::requestStream()
{
   int svrPort = par("serverPort");
   int localPort = par("localPort");
   const char *address = par("serverAddress");

   cStringTokenizer tokenizer(address);
      const char *token;
      while ((token = tokenizer.nextToken())!=NULL)
         serverAddress.push_back(IPAddressResolver().resolve(token));

   if (serverAddress.empty())
      return;

   IPvXAddress randomsvrAddr = chooseDestAddress();

//    IPvXAddress svrAddr = IPAddressResolver().resolve(address);
//    if (svrAddr.isUnspecified())
//    {
//       EV << "Server address is unspecified, skip sending video stream request\n";
//       return;
//    }

   EV << "Requesting video stream from " << randomsvrAddr << ":" << svrPort << "\n";

   bindToPort(localPort);

   cPacket *msg = new cPacket("VideoStrmReq");
   sendToUDP(msg, localPort, randomsvrAddr, svrPort);
}
```

```
IPvXAddress UDPVideoStreamCli::chooseDestAddress()
{
   int k = intrand(serverAddress.size());
   return serverAddress[k];
}
```



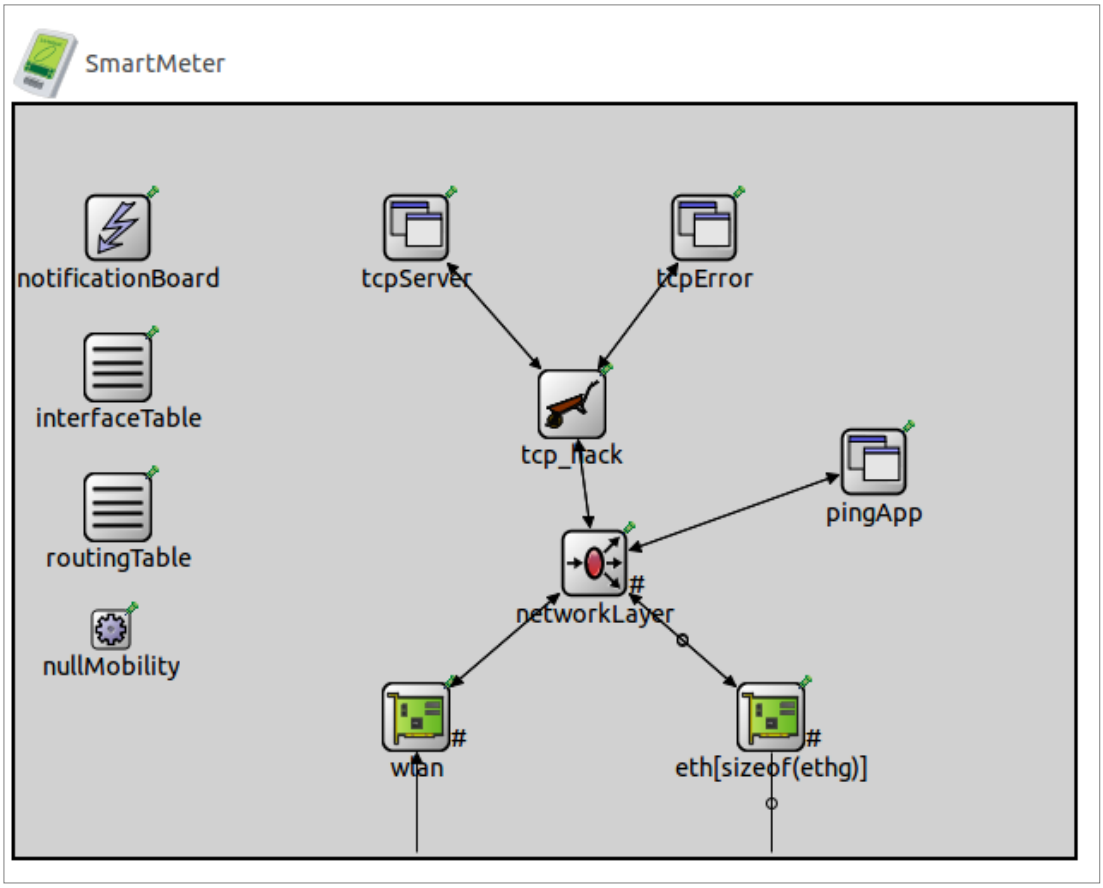
Εικόνα 8-19 UDPVideoStreamSvr

Το παραπάνω απλό στοιχείο εμφανίζεται στα στοιχεία που αποτελούν εξυπηρετητές VideoStream, δηλαδή στους κινούμενους χρήστες και στους απομακρυσμένους εξυπηρετητές.

Ακολουθούν κάποιες παράμετροι αυτού του στοιχείου:

```
int serverPort; // port to listen on
volatile double waitInterval @unit("s"); // interval between sending video stream packets
volatile int packetLen @unit("B");
volatile int videoSize @unit("B");
```

Έξυπνοι μετρητές



Εικόνα 8-20 Έξυπνος μετρητής

Η κατασκευή του σύνθετου στοιχείου των έξυπνων μετρητών είναι η εξής:

Στο στρώμα ζεύξης δεδομένων υπάρχει η δυνατότητα για ασύρματη και ενσύρματη σύνδεση. Περιλαμβάνεται μια ασύρματη κάρτα σύνδεσης δικτύου wlan τύπου Ieee80211NicSTASimplified και μια ενσύρματη κάρτα σύνδεσης δικτύου eth τύπου EthernetInterface. Στη συγκεκριμένη προσομοίωση χρησιμοποιείται μόνο η ασύρματη δυνατότητα.

Κάποιες παράμετροι της ασύρματης κάρτας, που ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini, είναι:

- Η μεγάλη χωρητικότητα των 1000000000 πλαισίων.
- Η διεύθυνση MAC των έξυπνων μετρητών ορίζεται αυτόματα.
- Κάθε τετράδα έξυπνων μετρητών έχει το δικό της σημείο πρόσβασης αλλά και το δικό της αναγνωριστικό αριθμό καναλιού. Για παράδειγμα, οι έξυπνοι μετρητές 1 έως 4 έχουν ως σημείο πρόσβασης το συλλέκτη δεδομένων 1 και αριθμό αναγνωριστικού καναλιού 1, οι έξυπνοι μετρητές 5 έως 8 έχουν ως σημείο πρόσβασης το συλλέκτη δεδομένων 2 και αριθμό αναγνωριστικού καναλιού 2, κ.ο.κ.

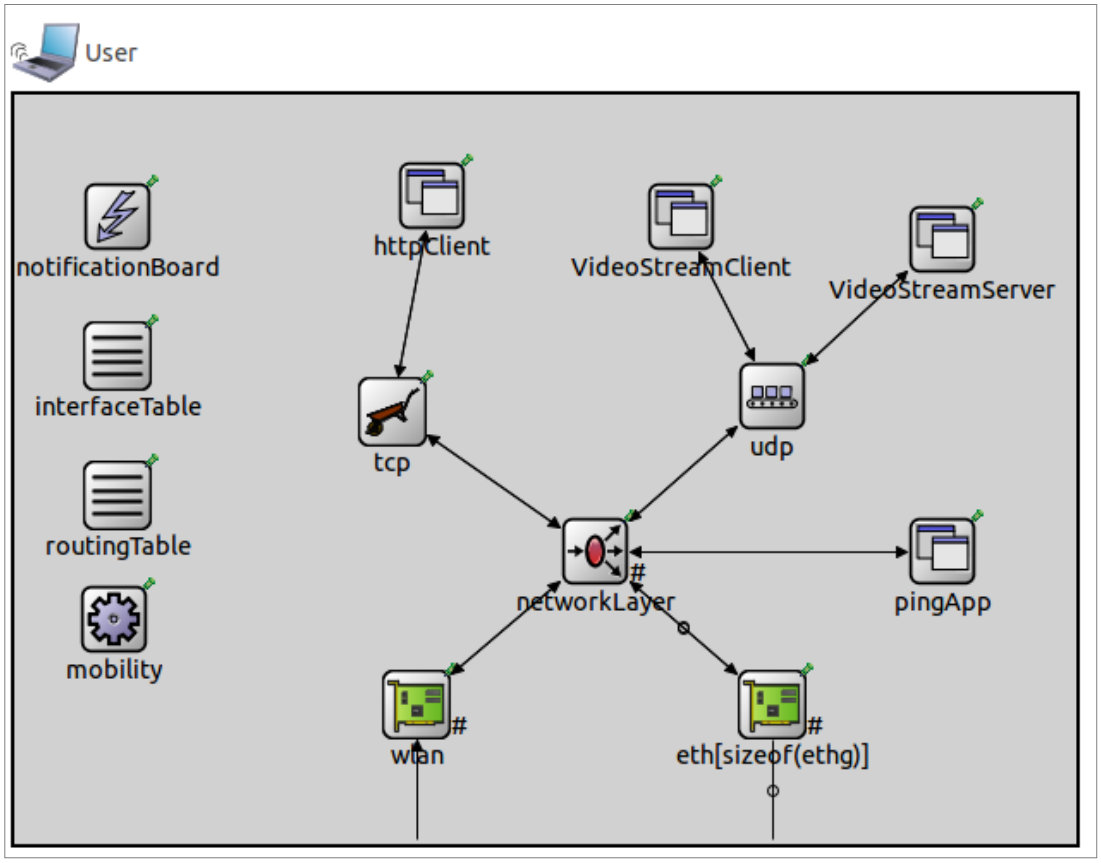
Το στοιχείο pingApp τύπου PingApp χρησιμοποιείται έτσι ώστε είτε να αναζητά ο ιδιοκτήτης κάθε διαμερίσματος τον αντίστοιχο έξυπνο μετρητή του είτε ο έξυπνος μετρητής να αναζητά την παρουσία άλλων στοιχείων του έξυπνου δικτύου (π.χ. οικιακές συσκευές, άλλους έξυπνους μετρητές, κ.ά.).

Στο στρώμα μεταφοράς, χρησιμοποιείται το στοιχείο tcp_hack τύπου TCP_hack που αποτελεί το μοναδικό στοιχείο που αντλήθηκε από τη βιβλιοθήκη του SCADASim, ενώ όλα τα υπόλοιπα στοιχεία βρέθηκαν στη βιβλιοθήκη του INET Framework. Ο μέγιστος αριθμός παράλληλων συνδέσεων TCP, που μπορεί να εξυπηρετήσει το στοιχείο tcpServer του έξυπνου μετρητή, ορίστηκε ο αριθμός 4. Όπως θα παρουσιαστεί αργότερα, το δεδομένο αυτό βοηθά στην εφαρμογή του σεναρίου της επίθεσης άρνησης υπηρεσιών (DoS—Denial of Service) του στοιχείου tcpServer του έξυπνου μετρητή προς τους υπαλλήλους του κέντρου ελέγχου.

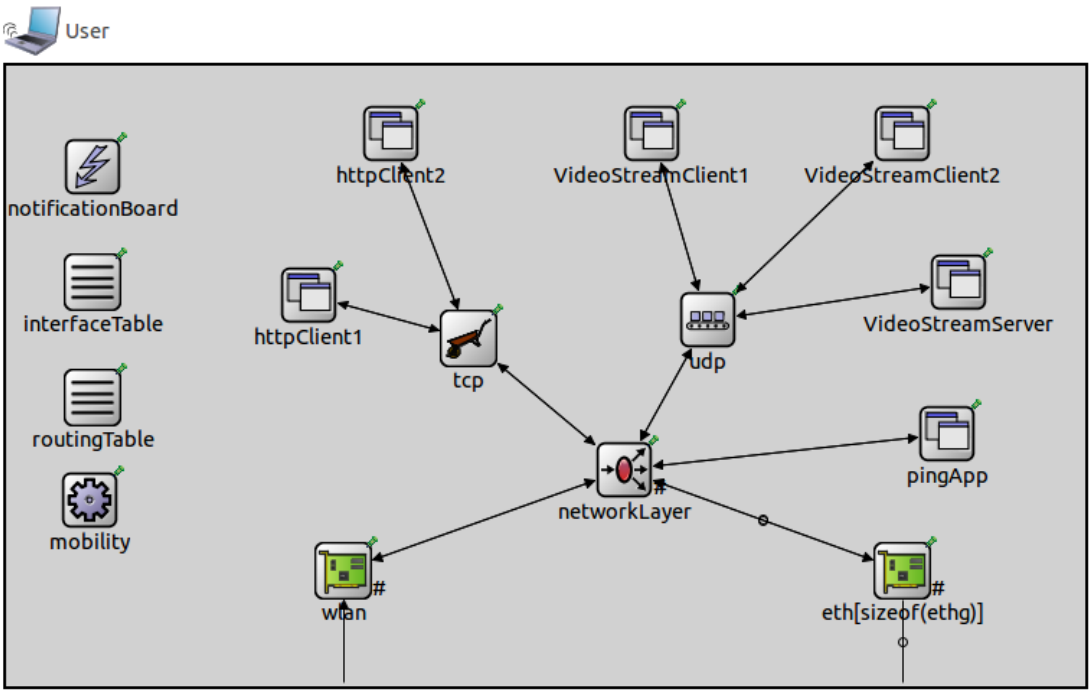
Στο στρώμα εφαρμογών, χρησιμοποιούνται τα στοιχεία tcpServer τύπου TCPGenericSrvApp και tcpError τύπου TCPBasicClientApp. Ο tcpServer είναι ένας εξυπηρετητής που ακούει σε ένα συγκεκριμένο αριθμό θύρας, τον αριθμό 1000. Αναζητείται συνήθως από τους υπαλλήλους του κέντρου ελέγχου ανά σταθερό χρονικό διάστημα (30 sec) και επιστρέφει στο κέντρο ελέγχου τα δεδομένα μέτρησης 1 KiloBytes. Ο tcpError είναι ένας τύπος πελάτη που αναζητά μια συγκεκριμένη διεύθυνση και θύρα του εξυπηρετητή βοήθειας του κέντρου ελέγχου, τη θύρα 3000. Χρησιμοποιείται είτε για ενημερώσεις του έξυπνου μετρητή είτε για επισημάνσεις προβλημάτων, όπως διακοπή ρεύματος. Όπως γίνεται φανερό, δεν γίνονται αναζητήσεις ανά σταθερό χρονικό διάστημα, ενώ το μέγεθος του πακέτου αποστολής είναι 3000 Bytes.

Όλες οι παράμετροι ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini παρακάτω.

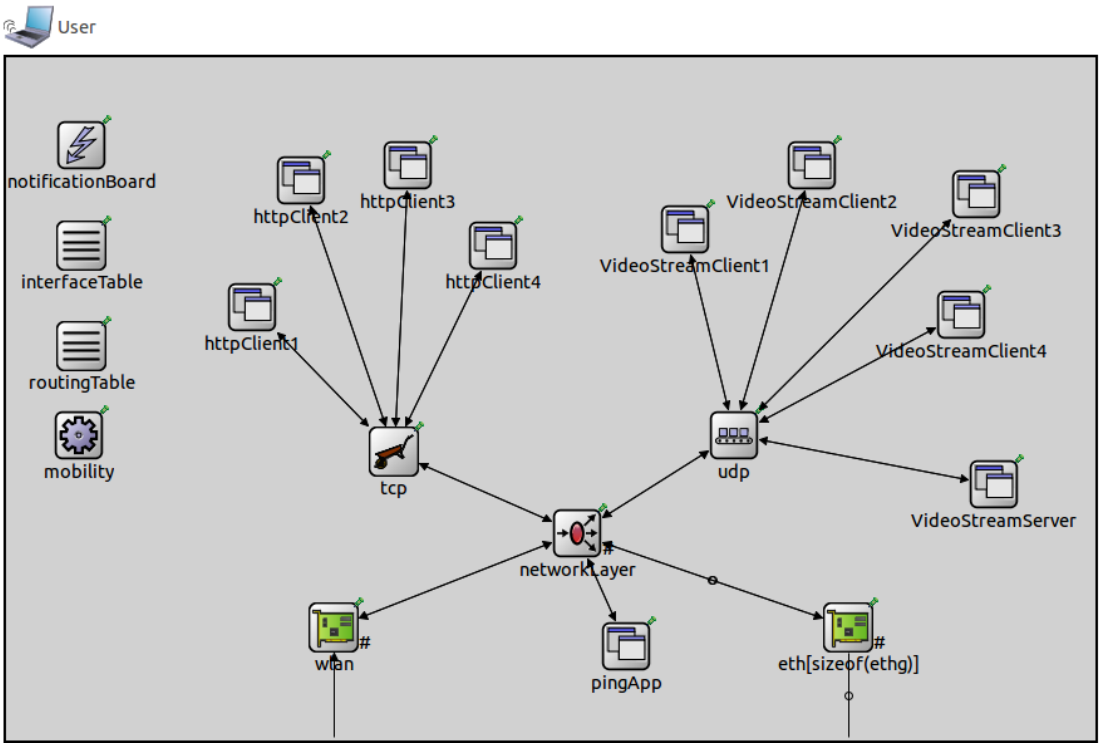
Κινούμενοι χρήστες



Εικόνα 8-21 Κινούμενος χρήστης 1ου (βασικού) σεναρίου



Εικόνα 8-22 Κινούμενος χρήστης 2ου σεναρίου



Εικόνα 8-23 Κινούμενος χρήστης 3ου σεναρίου

Η κατασκευή του σύνθετου στοιχείου των κινούμενων χρηστών είναι η εξής:

Στο στρώμα ζεύξης δεδομένων υπάρχει η δυνατότητα για ασύρματη και ενσύρματη σύνδεση. Περιλαμβάνεται μια ασύρματη κάρτα σύνδεσης δικτύου wlan τύπου Ieee80211NicSTASimplified και μια ενσύρματη κάρτα σύνδεσης δικτύου eth τύπου EthernetInterface. Στη συγκεκριμένη προσομοίωση χρησιμοποιείται μόνο η ασύρματη δυνατότητα.

Κάποιες παράμετροι της ασύρματης κάρτας, που ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini, είναι:

- Η μεγάλη χωρητικότητα των 1000000000 πλαισίων.
- Η διεύθυνση MAC των έξυπνων μετρητών ορίζεται αυτόματα.
- Κάθε τετράδα κινούμενων χρηστών έχει το δικό της σημείο πρόσβασης αλλά και το δικό της αναγνωριστικό αριθμό καναλιού. Για παράδειγμα, οι κινούμενοι χρήστες 1 έως 4 έχουν ως σημείο πρόσβασης το συλλέκτη δεδομένων 1 και αριθμό αναγνωριστικού καναλιού 1, οι κινούμενοι χρήστες 5 έως 8 έχουν ως σημείο πρόσβασης το συλλέκτη δεδομένων 2 και αριθμό αναγνωριστικού καναλιού 2, κ.ο.κ.

Το στοιχείο pingApp τύπου PingApp χρησιμοποιείται έτσι ώστε είτε να αναζητά ο κάθε κινούμενος χρήστης τα στοιχεία του διαδικτύου που αυτός επιθυμεί (π.χ. άλλους κινούμενους χρήστες, απομακρυσμένους εξυπηρετητές, κ.ά.)

Στο στρώμα μεταφοράς, χρησιμοποιείται το στοιχείο tcp τύπου TCP, που εξυπηρετεί απεριόριστο αριθμό συνδέσεων αφού δεν μας ενδιαφέρει κάποιο σενάριο επίθεσης στους κινούμενους χρήστες.

Στο στρώμα εφαρμογών, χρησιμοποιούνται το στοιχείο httpClient τύπου TCPBasicClientApp. Ο httpClient είναι ένας τύπος πελάτη που αναζητά μια συγκεκριμένη διεύθυνση και θύρα ενός απομακρυσμένου εξυπηρετητή http, τη θύρα 2000. Χρησιμοποιείται κυρίως για αναζητήσεις ιστοσελίδων ή εγγράφων στο

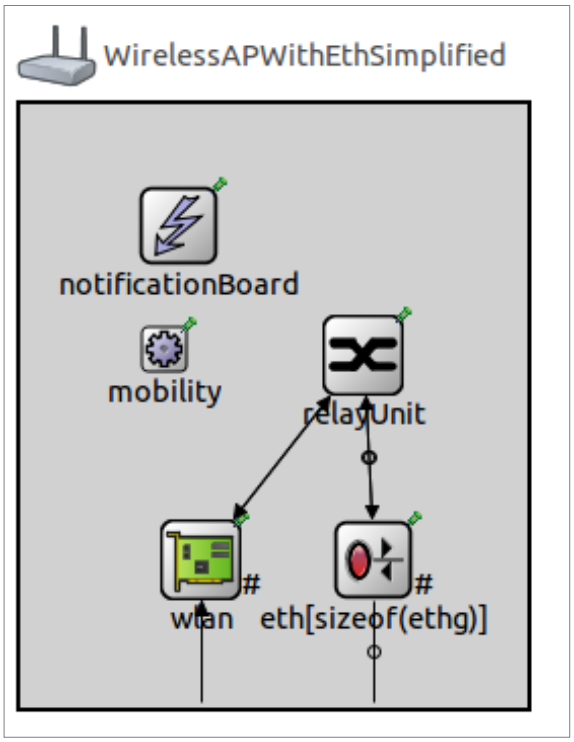
διαδίκτυο. Οι αναζητήσεις πραγματοποιούνται ανά μέσο χρονικό διάστημα 5 sec, ενώ το μέγεθος του πακέτου αποστολής είναι 5 KiloBytes.

Στο στρώμα μεταφοράς, χρησιμοποιείται επίσης το στοιχείο udp τύπου UDP, που προσομοιώνει το πρωτόκολλο μεταφοράς UDP. Στο στρώμα εφαρμογών, χρησιμοποιούνται τα στοιχεία VideoStreamClient τύπου UDPVideoStreamCli και VideoStreamServer τύπου UDPVideoStreamSvr. Ο VideoStreamServer είναι ένας εξυπηρετητής που ακούει σε ένα συγκεκριμένο αριθμό θύρας, τον αριθμό 2. Αναζητείται από άλλους κινούμενους χρήστες σε περίπτωση που επιλεχθεί να τους εξυπηρετήσει με το βίντεο που επιθυμούν να κατεβάσουν, το οποίο συνολικό μέγεθος του βίντεο είναι 200 KiloBytes και στέλνεται σε πακέτα των 50 KiloBytes . Ο VideoStreamClient είναι ένας τύπος πελάτη που αναζητά μια συγκεκριμένη διεύθυνση και θύρα του εξυπηρετητή από τον οποίο θα κατεβάσει το επιθυμητό βίντεο, τη θύρα 2. Οι αναζητήσεις βίντεο πραγματοποιούνται ανά μέσο χρονικό διάστημα 6 sec και η επιλογή του εξυπηρετητή (κινούμενου χρήστη ή απομακρυσμένου εξυπηρετητή) γίνεται τυχαία. Το γεγονός ότι οι κινούμενοι χρήστες αποτελούν ταυτόχρονα πελάτες και εξυπηρετητές βίντεο βοηθά στην εφαρμογή των συνεργατικών υπηρεσιών peer-to-peer.

Τέλος, οι χρήστες κινούνται κυκλικά με συγκεκριμένη ταχύτητα γύρω από κάθε συλλέκτη δεδομένων. Για παράδειγμα, οι κινούμενοι χρήστες 1 έως 4 κινούνται κυκλικά γύρω από το συλλέκτη δεδομένων 1, οι κινούμενοι χρήστες 5 έως 8 κινούνται κυκλικά γύρω από το συλλέκτη δεδομένων 2, κ.ο.κ.

Όλες οι παράμετροι ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini παρακάτω.

Συλλέκτες δεδομένων, σημεία πρόσβασης, διαδίκτυο, τοπικά δίκτυα και πύλες δικτύου



Εικόνα 8-24 Σημείο πρόσβασης με δυνατότητα ενσύρματης και ασύρματης λειτουργίας

Η κατασκευή των παραπάνω σύνθετων στοιχείων είναι η εξής:

Στο στρώμα ζεύξης δεδομένων υπάρχει η δυνατότητα για ασύρματη και ενσύρματη σύνδεση. Περιλαμβάνεται μια ασύρματη κάρτα σύνδεσης δικτύου wlan τύπου Ieee80211NicSTASimplified και μια ενσύρματη κάρτα σύνδεσης δικτύου eth τύπου EthernetInterface. Τα συγκεκριμένα στοιχεία λειτουργούν ως εξής:

- Εάν η πληροφορία προέρχεται από ασύρματη μετάδοση πομπού, εισέρχεται μέσω της ασύρματης κάρτας σύνδεσης δικτύου και μεταφέρεται ασύρματα ή ενσύρματα μέχρι να φθάσει στον παραλήπτη.
- Εάν η πληροφορία προέρχεται από ενσύρματη μετάδοση πομπού, εισέρχεται μέσω της ενσύρματης κάρτας σύνδεσης δικτύου και μεταφέρεται ασύρματα ή ενσύρματα μέχρι να φθάσει στον παραλήπτη.

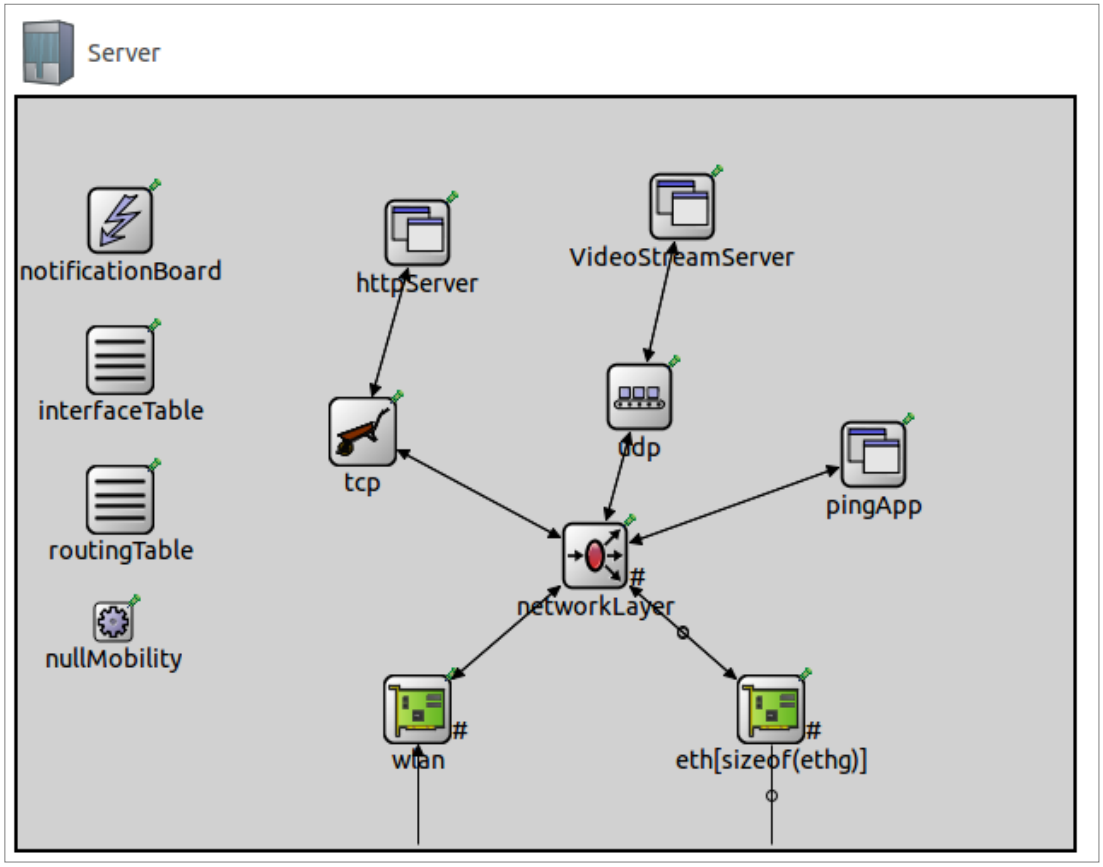
Τα στοιχεία αυτά αναλαμβάνουν τη μεταφορά κάθε είδους πληροφορίας που ρέει μέσα στο δίκτυο επικοινωνιών του έξυπνου δικτύου.

Η διεύθυνση MAC των σημείων πρόσβασης ορίζεται από τον υπεύθυνο της προσομοίωσης.

Η ενσύρματη κάρτα σύνδεσης δικτύου προσφέρει μεταφορά δεδομένων σε γραμμές duplex Ethernet με ρυθμό μετάδοσης δεδομένων 10 ή 100 Mbps.

Όλες οι παράμετροι ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini παρακάτω.

Απομακρυσμένοι εξυπηρετητές



Εικόνα 8-25 Απομακρυσμένος εξυπηρετητής

Η κατασκευή του σύνθετου στοιχείου των απομακρυσμένων εξυπηρετητών είναι η εξής:

Στο στρώμα ζεύξης δεδομένων υπάρχει η δυνατότητα για ασύρματη και ενσύρματη σύνδεση. Περιλαμβάνεται μια ασύρματη κάρτα σύνδεσης δικτύου wlan τύπου Ieee80211NicSTASimplified και μια ενσύρματη κάρτα σύνδεσης δικτύου eth τύπου EthernetInterface. Στη συγκεκριμένη προσομοίωση χρησιμοποιείται μόνο η ασύρματη δυνατότητα.

Κάποιες παράμετροι της ασύρματης κάρτας, που ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini, είναι:

- Η μεγάλη χωρητικότητα των 1000000000 πλαισίων.
- Η διεύθυνση MAC των απομακρυσμένων εξυπηρετητών ορίζεται αυτόματα.
- Οι απομακρυσμένοι εξυπηρετητές έχουν το ίδιο σημείο πρόσβασης lan αλλά και το ίδιο αναγνωριστικό αριθμό καναλιού.

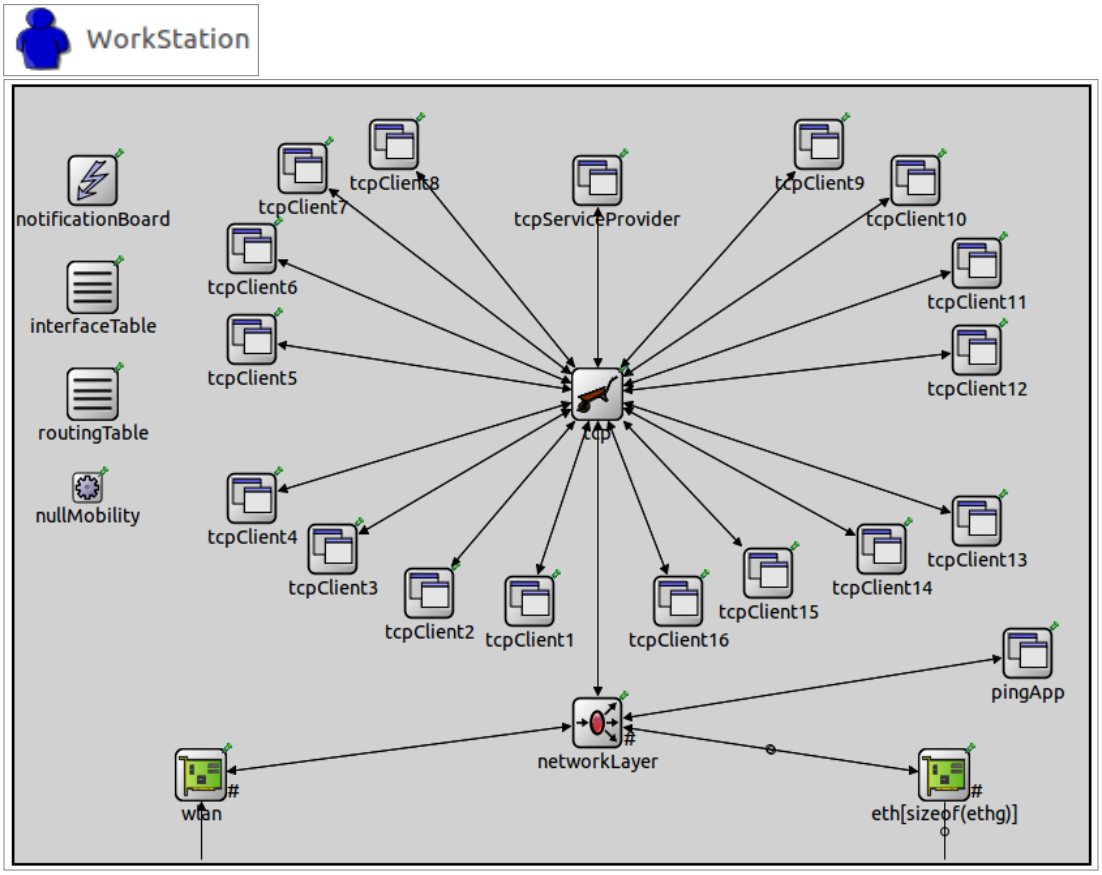
Το στοιχείο pingApp τύπου PingApp χρησιμοποιείται έτσι ώστε είτε να αναζητά ο κάθε εξυπηρετητής τα στοιχεία του διαδικτύου που αυτός επιθυμεί (π.χ. Άλλους απομακρυσμένους εξυπηρετητές, κ.ά.)

Στο στρώμα μεταφοράς, χρησιμοποιείται το στοιχείο tcp τύπου TCP και το στοιχείο udp τύπου UDP, που προσομοιώνουν τα αντίστοιχα πρωτόκολλα μεταφοράς.

Στο στρώμα εφαρμογών, χρησιμοποιούνται το στοιχείο httpServer τύπου TCPGenericSrvApp και το στοιχείο VideoStreamServer τύπου UDPVideoStreamSvr. Με αυτό τον τρόπο, εξυπηρετεί μοναδικά http συνδέσεις (ακούγοντας στη θύρα 2000) όταν κάποιοι χρήστες αναζητούν ιστοσελίδες ή έγγραφα στο διαδίκτυο, αποστέλλοντας συνήθως πακέτα των 8 KiloBytes. Επίσης, εξυπηρετεί VideoStream συνδέσεις (ακούγοντας στη θύρα 2), αλλά όχι μοναδικά διότι οι πελάτες μπορούν να κατεβάζουν το επιθυμητό βίντεο και από άλλους χρήστες που το περιέχουν. Το συνολικό μέγεθος του βίντεο είναι 200 KiloBytes και στέλνεται σε πακέτα των 50 KiloBytes.

Όλες οι παράμετροι ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini παρακάτω.

Υπάλληλοι κέντρου ελέγχου



Εικόνα 8-26 Κέντρο Ελέγχου έξυπνου δικτύου

Η κατασκευή του σύνθετου στοιχείου των υπαλλήλων του κέντρου ελέγχου είναι η εξής:

Στο στρώμα ζεύξης δεδομένων υπάρχει η δυνατότητα για ασύρματη και ενσύρματη σύνδεση. Περιλαμβάνεται μια ασύρματη κάρτα σύνδεσης δικτύου wlan τύπου Ieee80211NicSTASimplified και μια ενσύρματη κάρτα σύνδεσης δικτύου eth τύπου EthernetInterface.Στη συγκεκριμένη προσομοίωση χρησιμοποιείται μόνο η ασύρματη δυνατότητα.

Κάποιες παράμετροι της ασύρματης κάρτας, που ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini, είναι:

- Η μεγάλη χωρητικότητα των 1000000000 πλαισίων.
- Η διεύθυνση MAC των υπαλλήλων του κέντρου ελέγχου ορίζεται αυτόματα.
- Οι υπάλληλοι του κέντρου ελέγχου έχουν το ίδιο σημείο πρόσβασης gateway αλλά και τον ίδιο αναγνωριστικό αριθμό καναλιού.

Το στοιχείο pingApp τύπου PingApp χρησιμοποιείται έτσι ώστε είτε να αναζητά ο κάθε υπάλληλος άλλα στοιχεία του δικτύου που αυτός επιθυμεί (π.χ. άλλους υπαλλήλους του κέντρου ελέγχου, συσκευές έξυπνων μετρητών, κ.ά.)

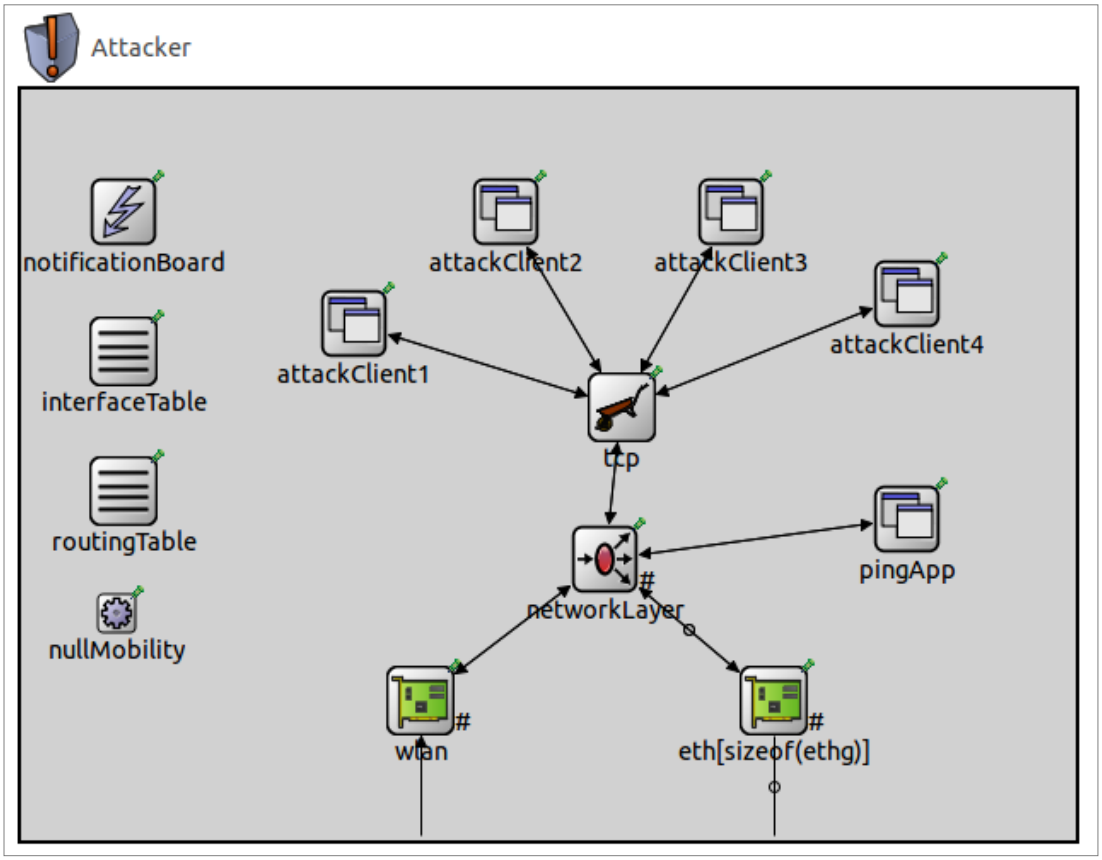
Στο στρώμα μεταφοράς, χρησιμοποιείται το στοιχείο tcp τύπου TCP, που προσομοιώνει το αντίστοιχο πρωτόκολλο μεταφοράς.

Στο στρώμα εφαρμογών, χρησιμοποιούνται τα στοιχεία tcpServiceProvider τύπου TCPGenericSrvApp και tcpClient{1..16} τύπου TCPBasicClientApp. Ο tcpServiceProvider είναι ένας εξυπηρετητής που ακούει σε ένα συγκεκριμένο αριθμό

θύρας, τον αριθμό 3000. Αναζητείται σε περιπτώσεις προβλήματος από τους έξυπνους μετρητές για τους οποίους είναι υπεύθυνος και επιστρέφει στους μετρητές τις υπηρεσίες του σε δεδομένα των 1 KiloBytes. Ο tcpClient είναι ένας τύπος πελάτη που αναζητά μια συγκεκριμένη διεύθυνση και θύρα του έξυπνου μετρητή, τη θύρα 1000. Κάθε tcpClient είναι δεσμευμένος με έναν έξυπνο μετρητή. Ο έξυπνος μετρητής του στέλνει τις μετρήσεις του και τότε ο tcpClient του επιστρέφει δεδομένα των 15 KiloBytes, που περιλαμβάνουν πληροφορίες χρήσιμες για τους πελάτες (λογαριασμοί, προγραμματισμός οικιακών συσκευών, τιμολογήσεις ενέργειας των επόμενων 30 λεπτών). Οι αναζητήσεις πραγματοποιούνται ανά σταθερό χρονικό διάστημα των 30 sec.

Όλες οι παράμετροι ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini παρακάτω.

Επιτιθέμενοι



Εικόνα 8-27 Επιτιθέμενος

Η κατασκευή του σύνθετου στοιχείου των επιτιθέμενων είναι η εξής:

Στο στρώμα ζεύξης δεδομένων υπάρχει η δυνατότητα για ασύρματη και ενσύρματη σύνδεση. Περιλαμβάνεται μια ασύρματη κάρτα σύνδεσης δικτύου wlan τύπου Ieee80211NicSTASimplified και μια ενσύρματη κάρτα σύνδεσης δικτύου eth τύπου

EthernetInterface.Στη συγκεκριμένη προσομοίωση χρησιμοποιείται μόνο η ασύρματη δυνατότητα.

Κάποιες παράμετροι της ασύρματης κάρτας, που ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini, είναι:

- Η μεγάλη χωρητικότητα των 1000000000 πλαισίων.
- Η διεύθυνση MAC των επιτιθέμενων ορίζεται αυτόματα.
- Κάθε ομάδα δύο επιτιθέμενων έχει το ίδιο σημείο πρόσβασης αλλά και τον ίδιο αναγνωριστικό αριθμό καναλιού. Για παράδειγμα, οι επιτιθέμενοι 1 και 2 έχουν ως σημείο πρόσβασης το accessPont1 και αναγνωριστικό αριθμό καναλιού 17, οι επιτιθέμενοι 3 και 4 έχουν ως σημείο πρόσβασης το accessPont2 και αναγνωριστικό αριθμό καναλιού 18, κ.ο.κ.

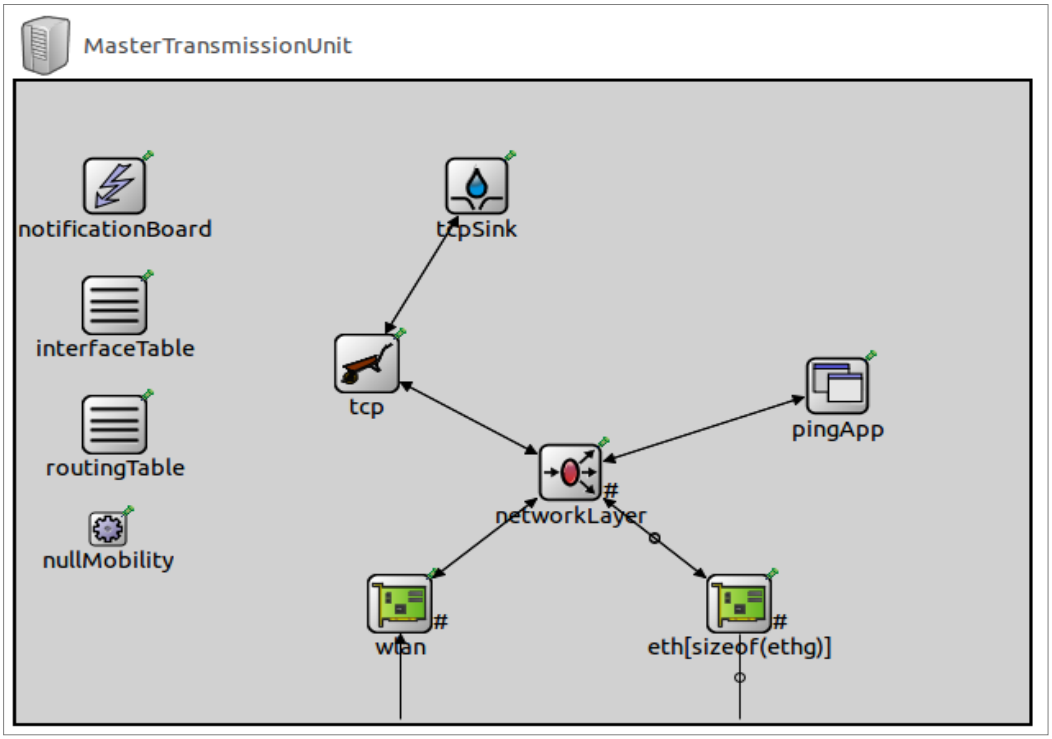
Το στοιχείο pingApp τύπου PingApp χρησιμοποιείται έτσι ώστε είτε να αναζητά ο κάθε επιτιθέμενος άλλα στοιχεία του δικτύου που αυτός επιθυμεί (π.χ. έξυπνους μετρητές στόχους, κ.ά.)

Στο στρώμα μεταφοράς, χρησιμοποιείται το στοιχείο tcp τύπου TCP, που προσομοιώνει το αντίστοιχο πρωτόκολλο μεταφοράς.

Στο στρώμα εφαρμογών, χρησιμοποιούνται τα στοιχεία attackClient{1..4} τύπου TCPBasicClientApp. Ο attackClient είναι σαν τον tcpClient. Ένας τύπος πελάτη που αναζητά μια συγκεκριμένη διεύθυνση και θύρα του έξυπνου μετρητή, τη θύρα 1000. Ωστόσο, οι ομοιότητές τους σταματούν εκεί. Οι attackClient{1..4} στέλνουν 4 συνεχόμενες αναζητήσεις στον ίδιο έξυπνο μετρητή και του προκαλούν πληρότητα παράλληλων συνδέσεων. Απασχολούν τον έξυπνο μετρητή για περισσότερα από 2 λεπτά στέλνοντάς του δεδομένα των 100 Bytes.

Όλες οι παράμετροι ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini παρακάτω.

Mtu



Εικόνα 8-28 Μονάδα συντήρησης δεδομένων κέντρου ελέγχου

Η κατασκευή του σύνθετου στοιχείου της κύριας μονάδας μεταφοράς είναι η εξής:

Στο στρώμα ζεύξης δεδομένων υπάρχει η δυνατότητα για ασύρματη και ενσύρματη σύνδεση. Περιλαμβάνεται μια ασύρματη κάρτα σύνδεσης δικτύου wlan τύπου Ieee80211NicSTASimplified και μια ενσύρματη κάρτα σύνδεσης δικτύου eth τύπου EthernetInterface.Στη συγκεκριμένη προσομοίωση χρησιμοποιείται μόνο η ασύρματη δυνατότητα.

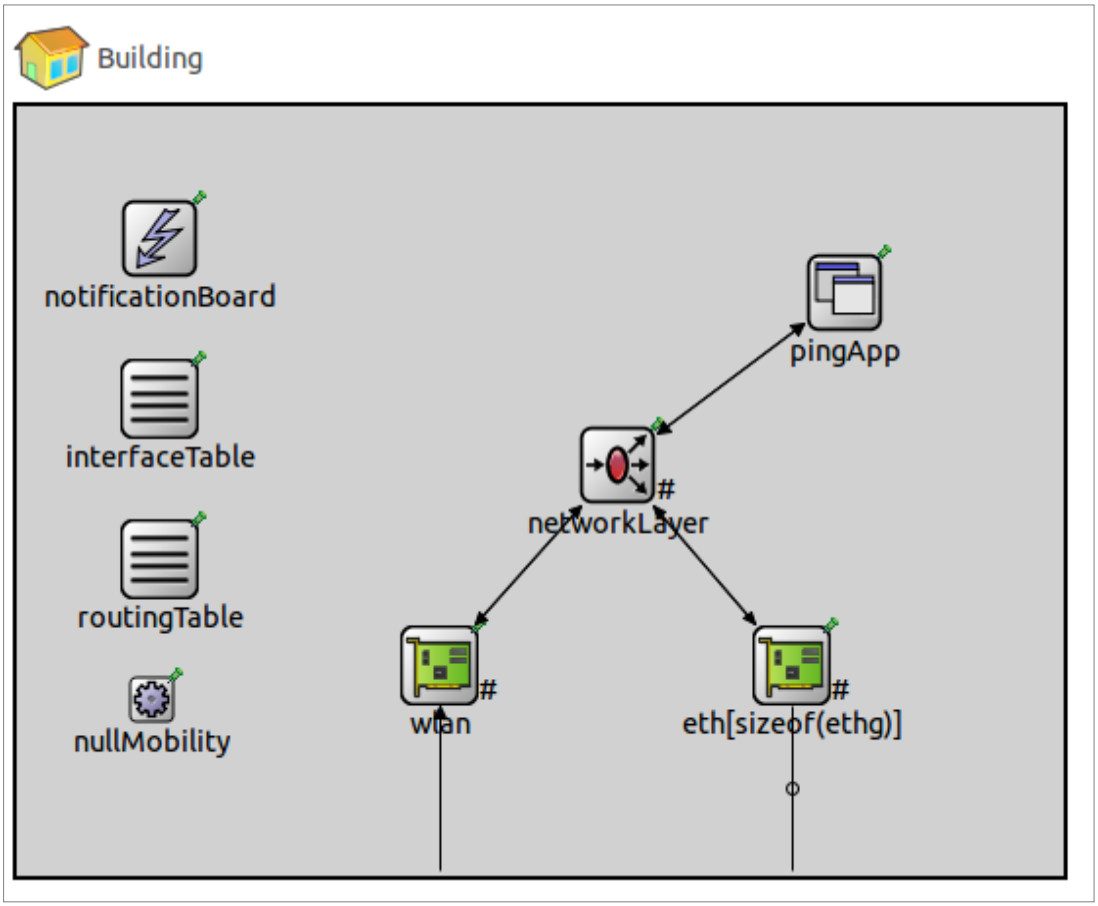
Το στοιχείο pingApp τύπου PingApp χρησιμοποιείται έτσι ώστε είτε να αναζητάται από τους υπαλλήλους του κέντρου ελέγχου.

Στο στρώμα μεταφοράς, χρησιμοποιείται το στοιχείο tcp τύπου TCP, που προσομοιώνει το αντίστοιχο πρωτόκολλο μεταφοράς.

Στο στρώμα εφαρμογών, χρησιμοποιείται το στοιχείο tcpSink τύπου TCPSinkApp. Το στοιχείο αυτό δέχεται τα δεδομένα συνομιλίας μεταξύ των έξυπνων μετρητών και των υπαλλήλων του κέντρου ελέγχου.

Όλες οι παράμετροι ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini παρακάτω.

Διαμερίσματα



Εικόνα 8-29 Διαμέρισμα-ιδιοκτήτης έξυπνου μετρητή

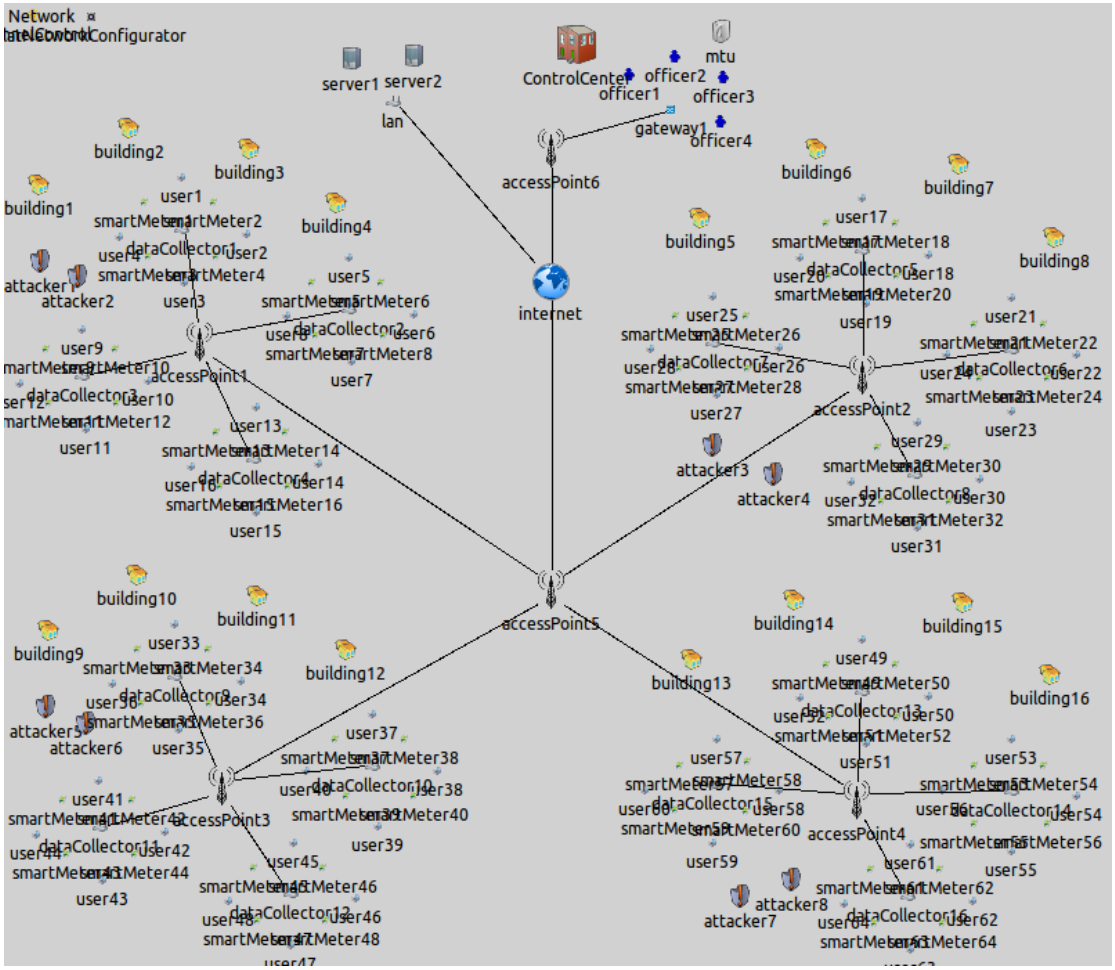
Η κατασκευή του σύνθετου στοιχείου του διαμερίσματος ή ιδιοκτήτη είναι η εξής:

Στο στρώμα ζεύξης δεδομένων υπάρχει η δυνατότητα για ασύρματη και ενσύρματη σύνδεση. Περιλαμβάνεται μια ασύρματη κάρτα σύνδεσης δικτύου wlan τύπου Ieee80211NicSTASimplified και μια ενσύρματη κάρτα σύνδεσης δικτύου eth τύπου EthernetInterface.Στη συγκεκριμένη προσομοίωση χρησιμοποιείται μόνο η ασύρματη δυνατότητα.

Το στοιχείο pingApp τύπου PingApp χρησιμοποιείται έτσι ώστε είτε να αναζητείται από τους ιδιοκτήτες του διαμερίσματος ο αντίστοιχος έξυπνος μετρητής τους.

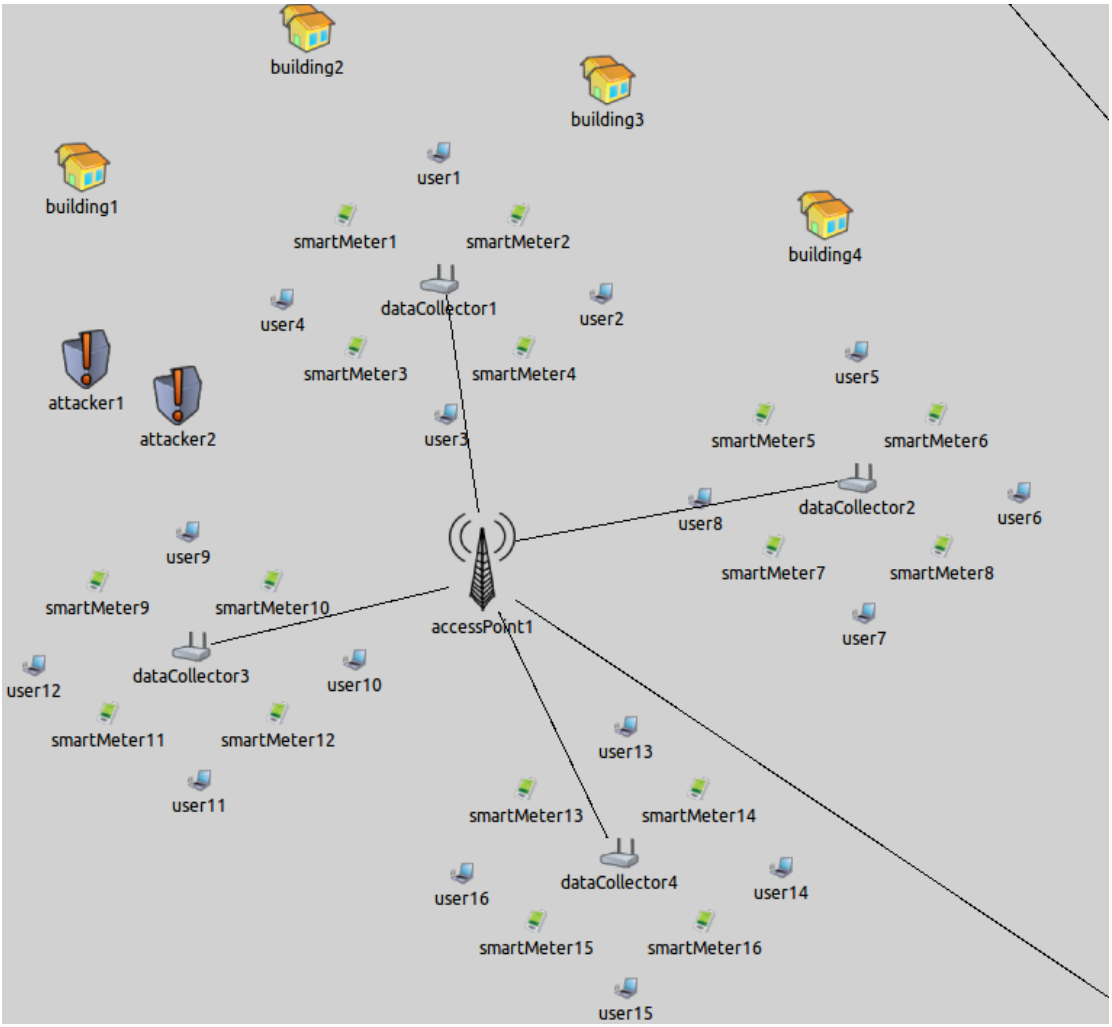
Όλες οι παράμετροι ορίζονται και παρουσιάζονται ολοκληρωμένα στο αρχείο omnetpp.ini παρακάτω.

Έξυπνο δίκτυο



Εικόνα 8-30 Έξυπνο Δίκτυο

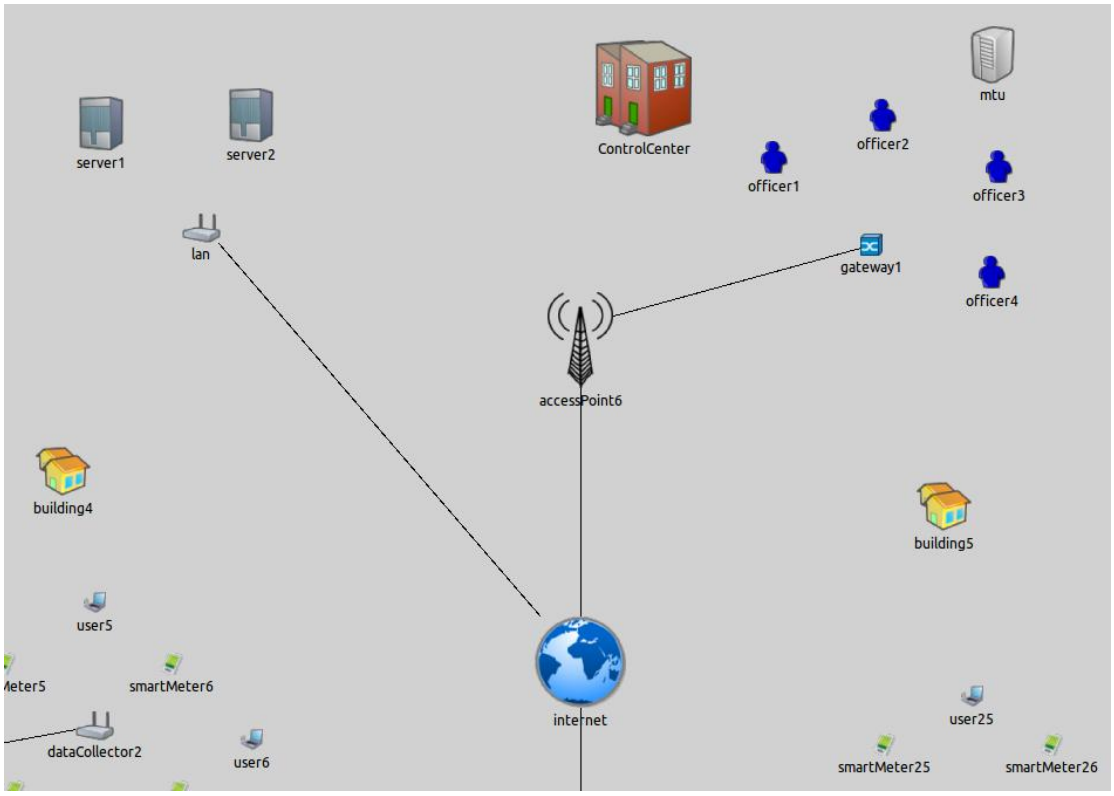
Στην παραπάνω εικόνα, παρουσιάζεται το τελικό δίκτυο προσομοίωσης. Όλα τα στοιχεία, που προαναφέρθηκαν, λαμβάνουν δράση στο παραπάνω δίκτυο. Ωστόσο, επειδή η παραπάνω εικόνα δεν είναι τόσο εύκολη στην αντίληψη, παρουσιάζεται παρακάτω μια γειτονιά-υποδίκτυο από τις 4 συνολικά γειτονιές-υποδίκτυα της μικρής πόλης.



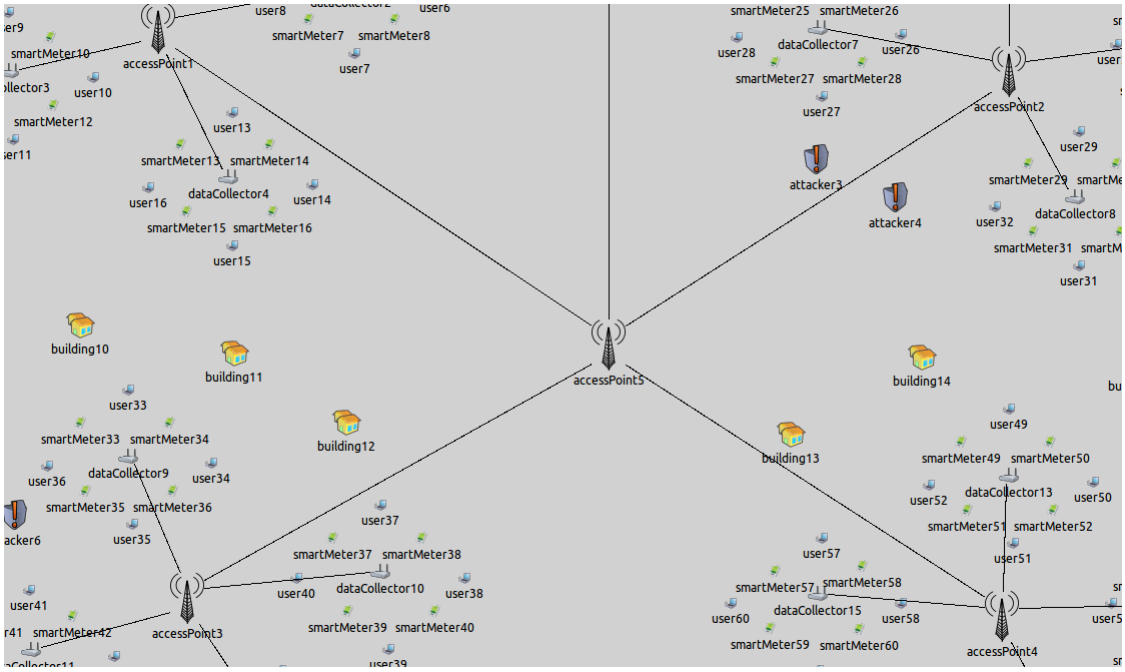
Εικόνα 8-31 Υποδίκτυο-γειτονιά έξυπνου δικτύου

Σε καθένα από τα 4 υποδίκτυα, υπάρχουν τα παραπάνω στοιχεία.

Παρακάτω παρουσιάζονται άλλες δυο εικόνες για την καλύτερη κατανόηση του συνολικού δικτύου.



Εικόνα 8-32 Κέντρο Ελέγχου και Απομακρυσμένοι Εξυπηρετητές



Εικόνα 8-33 Διασύνδεση των 4 υποδικτύων-γειτονιών

8.2. Το αρχείο omnetpp.ini

```
[General]
network = SmartGrid
tkenv-plugin-path = ../../../etc/plugins


#Ethermac
**.eth[*].txrate= 10Mbps
**.eth[*].duplexEnabled = true
**.eth[*].mtu = 1500

# mac
**.mac.maxQueueSize = 1
**.mac.rtsThresholdBytes = 3000B
**.mac.bitrate = 11Mbps
**.mac.retryLimit = 1
**.mac.cwMinData = -1
**.mac.cwMinBroadcast = -1
**.mac.mtu = 1500

# radio
**.radio.bitrate = 11Mbps
**.radio.transmitterPower = 20.0mW
**.radio.thermalNoise = -110dBm
**.radio.sensitivity = -85mW
**.radio.pathLossAlpha = 2
**.radio.snirThreshold = 4dB

# mobility
**.user*.mobilityType = "CircleMobility"
**.user*.mobility.speed = 50mps
**.user*.mobility.updateInterval = 0.1s
**.user*.mobility.r = 150

**.user{1..4}.mobility.cx = 442
**.user{1..4}.mobility.cy = 566
**.user1.mobility.startAngle = 90deg
**.user2.mobility.startAngle = 0deg
**.user3.mobility.startAngle = 270deg
**.user4.mobility.startAngle = 180deg

**.user{5..8}.mobility.cx = 860
**.user{5..8}.mobility.cy = 765
**.user5.mobility.startAngle = 90deg
**.user6.mobility.startAngle = 0deg
**.user7.mobility.startAngle = 270deg
**.user8.mobility.startAngle = 180deg

**.user{9..12}.mobility.cx = 195
**.user{9..12}.mobility.cy = 932
**.user9.mobility.startAngle = 90deg
**.user10.mobility.startAngle = 0deg
**.user11.mobility.startAngle = 270deg
**.user12.mobility.startAngle = 180deg

**.user{13..16}.mobility.cx = 622
**.user{13..16}.mobility.cy = 1139
**.user13.mobility.startAngle = 90deg
**.user14.mobility.startAngle = 0deg
```

```
**.user15.mobility.startAngle = 270deg
**.user16.mobility.startAngle = 180deg

**.user{17..20}.mobility.cx = 2142
**.user{17..20}.mobility.cy = 617
**.user17.mobility.startAngle = 90deg
**.user18.mobility.startAngle = 0deg
**.user19.mobility.startAngle = 270deg
**.user20.mobility.startAngle = 180deg

**.user{21..24}.mobility.cx = 2514
**.user{21..24}.mobility.cy = 867
**.user21.mobility.startAngle = 90deg
**.user22.mobility.startAngle = 0deg
**.user23.mobility.startAngle = 270deg
**.user24.mobility.startAngle = 180deg

**.user{25..28}.mobility.cx = 1769
**.user{25..28}.mobility.cy = 848
**.user25.mobility.startAngle = 90deg
**.user26.mobility.startAngle = 0deg
**.user27.mobility.startAngle = 270deg
**.user28.mobility.startAngle = 180deg

**.user{29..32}.mobility.cx = 2271
**.user{29..32}.mobility.cy = 1177
**.user29.mobility.startAngle = 90deg
**.user30.mobility.startAngle = 0deg
**.user31.mobility.startAngle = 270deg
**.user32.mobility.startAngle = 180deg

**.user{33..36}.mobility.cx = 426
**.user{33..36}.mobility.cy = 1681
**.user33.mobility.startAngle = 90deg
**.user34.mobility.startAngle = 0deg
**.user35.mobility.startAngle = 270deg
**.user36.mobility.startAngle = 180deg

**.user{37..40}.mobility.cx = 918
**.user{37..40}.mobility.cy = 1905
**.user37.mobility.startAngle = 90deg
**.user38.mobility.startAngle = 0deg
**.user39.mobility.startAngle = 270deg
**.user40.mobility.startAngle = 180deg

**.user{41..44}.mobility.cx = 237
**.user{41..44}.mobility.cy = 2057
**.user41.mobility.startAngle = 90deg
**.user42.mobility.startAngle = 0deg
**.user43.mobility.startAngle = 270deg
**.user44.mobility.startAngle = 180deg

**.user{45..48}.mobility.cx = 715
**.user{45..48}.mobility.cy = 2224
**.user45.mobility.startAngle = 90deg
**.user46.mobility.startAngle = 0deg
**.user47.mobility.startAngle = 270deg
**.user48.mobility.startAngle = 180deg

**.user{49..52}.mobility.cx = 2142
```

```
**.user{49..52}.mobility.cy = 1718
**.user49.mobility.startAngle = 90deg
**.user50.mobility.startAngle = 0deg
**.user51.mobility.startAngle = 270deg
**.user52.mobility.startAngle = 180deg

**.user{53..56}.mobility.cx = 2514
**.user{53..56}.mobility.cy = 1968
**.user53.mobility.startAngle = 90deg
**.user54.mobility.startAngle = 0deg
**.user55.mobility.startAngle = 270deg
**.user56.mobility.startAngle = 180deg

**.user{57..60}.mobility.cx = 1769
**.user{57..60}.mobility.cy = 1949
**.user57.mobility.startAngle = 90deg
**.user58.mobility.startAngle = 0deg
**.user59.mobility.startAngle = 270deg
**.user60.mobility.startAngle = 180deg

**.user{61..64}.mobility.cx = 2253
**.user{61..64}.mobility.cy = 2230
**.user61.mobility.startAngle = 90deg
**.user62.mobility.startAngle = 0deg
**.user63.mobility.startAngle = 270deg
**.user64.mobility.startAngle = 180deg

# channel physical parameters
**.playgroundSizeX = 3200
**.playgroundSizeY = 2700
**.coreDebug = false
**.channelControl.carrierFrequency = 2.4GHz
**.channelControl.pMax = 20.0mW
**.channelControl.sat = -110dBm
**.channelControl.alpha = 2
**.channelControl.numChannels = 30

**.smartMeter{1..4}.wlan.radio.channelNumber = 1
**.user{1..4}.wlan.radio.channelNumber = 1
**.dataCollector1.wlan.radio.channelNumber = 1

**.smartMeter{5..8}.wlan.radio.channelNumber = 2
**.user{5..8}.wlan.radio.channelNumber = 2
**.dataCollector2.wlan.radio.channelNumber = 2

**.smartMeter{9..12}.wlan.radio.channelNumber = 3
**.user{9..12}.wlan.radio.channelNumber = 3
**.dataCollector3.wlan.radio.channelNumber = 3

**.smartMeter{13..16}.wlan.radio.channelNumber = 4
**.user{13..16}.wlan.radio.channelNumber = 4
**.dataCollector4.wlan.radio.channelNumber = 4

**.smartMeter{17..20}.wlan.radio.channelNumber = 5
**.user{17..20}.wlan.radio.channelNumber = 5
**.dataCollector5.wlan.radio.channelNumber = 5

**.smartMeter{21..24}.wlan.radio.channelNumber = 6
**.user{21..24}.wlan.radio.channelNumber = 6
**.dataCollector6.wlan.radio.channelNumber = 6
```

```
**.smartMeter{25..28}.wlan.radio.channelNumber = 7
**.user{25..28}.wlan.radio.channelNumber = 7
**.dataCollector7.wlan.radio.channelNumber = 7

**.smartMeter{29..32}.wlan.radio.channelNumber = 8
**.user{29..32}.wlan.radio.channelNumber = 8
**.dataCollector8.wlan.radio.channelNumber = 8

**.smartMeter{33..36}.wlan.radio.channelNumber = 9
**.user{33..36}.wlan.radio.channelNumber = 9
**.dataCollector9.wlan.radio.channelNumber = 9

**.smartMeter{37..40}.wlan.radio.channelNumber = 10
**.user{37..40}.wlan.radio.channelNumber = 10
**.dataCollector10.wlan.radio.channelNumber = 10

**.smartMeter{41..44}.wlan.radio.channelNumber = 11
**.user{41..44}.wlan.radio.channelNumber = 11
**.dataCollector11.wlan.radio.channelNumber = 11

**.smartMeter{45..48}.wlan.radio.channelNumber = 12
**.user{45..48}.wlan.radio.channelNumber = 12
**.dataCollector12.wlan.radio.channelNumber = 12

**.smartMeter{49..52}.wlan.radio.channelNumber = 13
**.user{49..52}.wlan.radio.channelNumber = 13
**.dataCollector13.wlan.radio.channelNumber = 13

**.smartMeter{53..56}.wlan.radio.channelNumber = 14
**.user{53..56}.wlan.radio.channelNumber = 14
**.dataCollector14.wlan.radio.channelNumber = 14

**.smartMeter{57..60}.wlan.radio.channelNumber = 15
**.user{57..60}.wlan.radio.channelNumber = 15
**.dataCollector15.wlan.radio.channelNumber = 15

**.smartMeter{61..64}.wlan.radio.channelNumber = 16
**.user{61..64}.wlan.radio.channelNumber = 16
**.dataCollector16.wlan.radio.channelNumber = 16

**.attacker1.wlan.radio.channelNumber = 17
**.attacker2.wlan.radio.channelNumber = 17
**.building{1..4}.wlan.radio.channelNumber = 17
**.accessPoint1.wlan.radio.channelNumber = 17

**.attacker3.wlan.radio.channelNumber = 18
**.attacker4.wlan.radio.channelNumber = 18
**.building{5..8}.wlan.radio.channelNumber = 18
**.accessPoint2.wlan.radio.channelNumber = 18

**.attacker5.wlan.radio.channelNumber = 19
**.attacker6.wlan.radio.channelNumber = 19
**.building{9..12}.wlan.radio.channelNumber = 19
**.accessPoint3.wlan.radio.channelNumber = 19

**.attacker7.wlan.radio.channelNumber = 20
**.attacker8.wlan.radio.channelNumber = 20
**.building{13..16}.wlan.radio.channelNumber = 20
**.accessPoint4.wlan.radio.channelNumber = 20
```

```
**.accessPoint5.wlan.radio.channelNumber = 21
**.internet.wlan.radio.channelNumber = 22
**.accessPoint6.wlan.radio.channelNumber = 23

**.lan.wlan.radio.channelNumber = 24
**.server1.wlan.radio.channelNumber = 24
**.server2.wlan.radio.channelNumber = 24

**.gateway1.wlan.radio.channelNumber = 25
**.mtu.wlan.radio.channelNumber = 25
**.officer1.wlan.radio.channelNumber = 25
**.officer2.wlan.radio.channelNumber = 25
**.officer3.wlan.radio.channelNumber = 25
**.officer4.wlan.radio.channelNumber = 25

# tcp
**.tcp.sendQueueClass = "TCPMsgBasedSendQueue"
#TCPVirtualDataSendQueue/TCPMsgBasedSendQueue
**.tcp.receiveQueueClass = "TCPMsgBasedRcvQueue"
# TCPVirtualDataRcvQueue/TCPMsgBasedRcvQueue
**.tcp_hack.maxThreadCount = 4

# tcpClient
**.tcpClient*.address = ""
**.tcpClient*.port = -1
**.tcpClient*.connectPort = 1000
**.tcpClient*.numRequestsPerSession = 1
**.tcpClient*.requestLength = 15000B
**.tcpClient*.replyLength = 3000B
**.tcpClient*.reconnectInterval = 30s
**.tcpClient*.thinkTime = 30s  # time gap between requests
**.tcpClient*.idleInterval = 15s  # time gap between sessions

**.officer1.tcpClient1.connectAddress = "smartMeter1"
**.officer1.tcpClient2.connectAddress = "smartMeter2"
**.officer1.tcpClient3.connectAddress = "smartMeter3"
**.officer1.tcpClient4.connectAddress = "smartMeter4"
**.officer1.tcpClient5.connectAddress = "smartMeter5"
**.officer1.tcpClient6.connectAddress = "smartMeter6"
**.officer1.tcpClient7.connectAddress = "smartMeter7"
**.officer1.tcpClient8.connectAddress = "smartMeter8"
**.officer1.tcpClient9.connectAddress = "smartMeter9"
**.officer1.tcpClient10.connectAddress = "smartMeter10"
**.officer1.tcpClient11.connectAddress = "smartMeter11"
**.officer1.tcpClient12.connectAddress = "smartMeter12"
**.officer1.tcpClient13.connectAddress = "smartMeter13"
**.officer1.tcpClient14.connectAddress = "smartMeter14"
**.officer1.tcpClient15.connectAddress = "smartMeter15"
**.officer1.tcpClient16.connectAddress = "smartMeter16"

**.officer2.tcpClient1.connectAddress = "smartMeter17"
**.officer2.tcpClient2.connectAddress = "smartMeter18"
**.officer2.tcpClient3.connectAddress = "smartMeter19"
**.officer2.tcpClient4.connectAddress = "smartMeter20"
**.officer2.tcpClient5.connectAddress = "smartMeter21"
**.officer2.tcpClient6.connectAddress = "smartMeter22"
**.officer2.tcpClient7.connectAddress = "smartMeter23"
**.officer2.tcpClient8.connectAddress = "smartMeter24"
**.officer2.tcpClient9.connectAddress = "smartMeter25"
```

```
**.officer2.tcpClient10.connectAddress = "smartMeter26"
**.officer2.tcpClient11.connectAddress = "smartMeter27"
**.officer2.tcpClient12.connectAddress = "smartMeter28"
**.officer2.tcpClient13.connectAddress = "smartMeter29"
**.officer2.tcpClient14.connectAddress = "smartMeter30"
**.officer2.tcpClient15.connectAddress = "smartMeter31"
**.officer2.tcpClient16.connectAddress = "smartMeter32"

**.officer3.tcpClient1.connectAddress = "smartMeter33"
**.officer3.tcpClient2.connectAddress = "smartMeter34"
**.officer3.tcpClient3.connectAddress = "smartMeter35"
**.officer3.tcpClient4.connectAddress = "smartMeter36"
**.officer3.tcpClient5.connectAddress = "smartMeter37"
**.officer3.tcpClient6.connectAddress = "smartMeter38"
**.officer3.tcpClient7.connectAddress = "smartMeter39"
**.officer3.tcpClient8.connectAddress = "smartMeter40"
**.officer3.tcpClient9.connectAddress = "smartMeter41"
**.officer3.tcpClient10.connectAddress = "smartMeter42"
**.officer3.tcpClient11.connectAddress = "smartMeter43"
**.officer3.tcpClient12.connectAddress = "smartMeter44"
**.officer3.tcpClient13.connectAddress = "smartMeter45"
**.officer3.tcpClient14.connectAddress = "smartMeter46"
**.officer3.tcpClient15.connectAddress = "smartMeter47"
**.officer3.tcpClient16.connectAddress = "smartMeter48"

**.officer4.tcpClient1.connectAddress = "smartMeter49"
**.officer4.tcpClient2.connectAddress = "smartMeter50"
**.officer4.tcpClient3.connectAddress = "smartMeter51"
**.officer4.tcpClient4.connectAddress = "smartMeter52"
**.officer4.tcpClient5.connectAddress = "smartMeter53"
**.officer4.tcpClient6.connectAddress = "smartMeter54"
**.officer4.tcpClient7.connectAddress = "smartMeter55"
**.officer4.tcpClient8.connectAddress = "smartMeter56"
**.officer4.tcpClient9.connectAddress = "smartMeter57"
**.officer4.tcpClient10.connectAddress = "smartMeter58"
**.officer4.tcpClient11.connectAddress = "smartMeter59"
**.officer4.tcpClient12.connectAddress = "smartMeter60"
**.officer4.tcpClient13.connectAddress = "smartMeter61"
**.officer4.tcpClient14.connectAddress = "smartMeter62"
**.officer4.tcpClient15.connectAddress = "smartMeter63"
**.officer4.tcpClient16.connectAddress = "smartMeter64"

**.officer1.tcpClient1.startTime = 0.4s
**.officer1.tcpClient2.startTime = 0.45s
**.officer1.tcpClient3.startTime = 0.5s
**.officer1.tcpClient4.startTime = 0.55s
**.officer1.tcpClient5.startTime = 0.6s
**.officer1.tcpClient6.startTime = 0.65s
**.officer1.tcpClient7.startTime = 0.7s
**.officer1.tcpClient8.startTime = 0.75s
**.officer1.tcpClient9.startTime = 0.8s
**.officer1.tcpClient10.startTime = 0.85s
**.officer1.tcpClient11.startTime = 0.9s
**.officer1.tcpClient12.startTime = 0.95s
**.officer1.tcpClient13.startTime = 1.0s
**.officer1.tcpClient14.startTime = 1.05s
**.officer1.tcpClient15.startTime = 1.1s
**.officer1.tcpClient16.startTime = 1.15s

**.officer2.tcpClient1.startTime = 0.41s
```

```
**.officer2.tcpClient2.startTime = 0.46s
**.officer2.tcpClient3.startTime = 0.51s
**.officer2.tcpClient4.startTime = 0.56s
**.officer2.tcpClient5.startTime = 0.61s
**.officer2.tcpClient6.startTime = 0.66s
**.officer2.tcpClient7.startTime = 0.71s
**.officer2.tcpClient8.startTime = 0.76s
**.officer2.tcpClient9.startTime = 0.81s
**.officer2.tcpClient10.startTime = 0.86s
**.officer2.tcpClient11.startTime = 0.91s
**.officer2.tcpClient12.startTime = 0.96s
**.officer2.tcpClient13.startTime = 1.01s
**.officer2.tcpClient14.startTime = 1.06s
**.officer2.tcpClient15.startTime = 1.11s
**.officer2.tcpClient16.startTime = 1.16s

**.officer3.tcpClient1.startTime = 0.42s
**.officer3.tcpClient2.startTime = 0.47s
**.officer3.tcpClient3.startTime = 0.52s
**.officer3.tcpClient4.startTime = 0.57s
**.officer3.tcpClient5.startTime = 0.62s
**.officer3.tcpClient6.startTime = 0.67s
**.officer3.tcpClient7.startTime = 0.72s
**.officer3.tcpClient8.startTime = 0.77s
**.officer3.tcpClient9.startTime = 0.82s
**.officer3.tcpClient10.startTime = 0.87s
**.officer3.tcpClient11.startTime = 0.92s
**.officer3.tcpClient12.startTime = 0.97s
**.officer3.tcpClient13.startTime = 1.02s
**.officer3.tcpClient14.startTime = 1.07s
**.officer3.tcpClient15.startTime = 1.12s
**.officer3.tcpClient16.startTime = 1.17s

**.officer4.tcpClient1.startTime = 0.43s
**.officer4.tcpClient2.startTime = 0.48s
**.officer4.tcpClient3.startTime = 0.53s
**.officer4.tcpClient4.startTime = 0.58s
**.officer4.tcpClient5.startTime = 0.63s
**.officer4.tcpClient6.startTime = 0.68s
**.officer4.tcpClient7.startTime = 0.73s
**.officer4.tcpClient8.startTime = 0.78s
**.officer4.tcpClient9.startTime = 0.83s
**.officer4.tcpClient10.startTime = 0.88s
**.officer4.tcpClient11.startTime = 0.93s
**.officer4.tcpClient12.startTime = 0.98s
**.officer4.tcpClient13.startTime = 1.03s
**.officer4.tcpClient14.startTime = 1.08s
**.officer4.tcpClient15.startTime = 1.13s
**.officer4.tcpClient16.startTime = 1.18s

# tcpServer
**.tcpServer.address = ""
**.tcpServer.port = 1000
**.tcpServer.replyDelay = 0s

# tcpSink
**.tcpSink.address = ""
**.tcpSink.port = 1000
```

```
# tcpError
**.tcpError.address = ""
**.tcpError.port = -1
**.tcpError.connectPort = 3000
**.tcpError.numRequestsPerSession = 1
**.tcpError.requestLength = 50B
**.tcpError.replyLength = 1000B
**.tcpError.reconnectInterval = 30s
**.tcpError.thinkTime = 30s  # time gap between requests
**.tcpError.idleInterval = exponential(3600s)  # time gap between sessions

**.smartMeter{1..16}.tcpError.connectAddress = "officer1"
**.smartMeter{17..32}.tcpError.connectAddress = "officer2"
**.smartMeter{33..48}.tcpError.connectAddress = "officer3"
**.smartMeter{49..64}.tcpError.connectAddress = "officer4"

**.smartMeter9.tcpError.startTime = 45s
**.smartMeter24.tcpError.startTime = 33s
**.smartMeter40.tcpError.startTime = 68s
**.smartMeter57.tcpError.startTime = 92s

**.smartMeter{1..8}.tcpError.startTime = 4500s
**.smartMeter{10..23}.tcpError.startTime = 4500s
**.smartMeter{25..39}.tcpError.startTime = 4500s
**.smartMeter{41..56}.tcpError.startTime = 4500s
*.smartMeter{58..64}.tcpError.startTime = 4500s

# tcpServiceProvider
**.tcpServiceProvider.address = ""
**.tcpServiceProvider.port = 3000
**.tcpServiceProvider.replyDelay = 0s

# httpClient
**.httpClient*.address = ""
**.httpClient*.port = -1
**.httpClient*.connectPort = 2000
**.user*.httpClient*.numRequestsPerSession = 1
**.httpClient*.requestLength = 5000B
**.httpClient*.replyLength = 30000B
**.httpClient*.reconnectInterval = 30s
**.user*.httpClient*.thinkTime = exponential(4s)  # time gap between requests
**.user*.httpClient*.idleInterval = uniform(2s, 4s)  # time gap between sessions

**.user{1..32}.httpClient*.connectAddress = "server1"
**.user{33..64}.httpClient*.connectAddress = "server2"

**.user*.httpClient*.startTime = uniform(2s, 4s)

# httpServer
**.httpServer.address = ""
**.httpServer.port = 2000
**.httpServer.replyDelay = 0s

# VideoStreamClient
**.VideoStreamClient*.localPort=1
**.VideoStreamClient*.serverPort=2

**.user{1..4}.VideoStreamClient*.serverAddress = "user5 user6 user7 user8 user21 user22 user23
user24 user37 user38 user39 user40 user53 user54 user55 user56 server1"
```

```
**.user{5..8}.VideoStreamClient*.serverAddress = "user1 user2 user3 user4 user17 user18 user19
user20 user33 user34 user35 user36 user49 user50 user51 user52 server1"
**.user{9..12}.VideoStreamClient*.serverAddress = "user13 user14 user15 user16 user29 user30
user31 user32 user45 user46 user47 user48 user61 user62 user63 user64 server1"
**.user{13..16}.VideoStreamClient*.serverAddress = "user9 user10 user11 user12 user25 user26
user27 user28 user41 user42 user43 user44 user57 user58 user59 user60 server1"
**.user{17..20}.VideoStreamClient*.serverAddress = "user5 user6 user7 user8 user21 user22 user23
user24 user37 user38 user39 user40 user53 user54 user55 user56 server1"
**.user{21..24}.VideoStreamClient*.serverAddress = "user1 user2 user3 user4 user17 user18 user19
user20 user33 user34 user35 user36 user49 user50 user51 user52 server1"
**.user{25..28}.VideoStreamClient*.serverAddress = "user13 user14 user15 user16 user29 user30
user31 user32 user45 user46 user47 user48 user61 user62 user63 user64 server1"
**.user{29..32}.VideoStreamClient*.serverAddress = "user9 user10 user11 user12 user25 user26
user27 user28 user41 user42 user43 user44 user57 user58 user59 user60 server1"
**.user{33..36}.VideoStreamClient*.serverAddress = "user5 user6 user7 user8 user21 user22 user23
user24 user37 user38 user39 user40 user53 user54 user55 user56 server2"
**.user{37..40}.VideoStreamClient*.serverAddress = "user1 user2 user3 user4 user17 user18 user19
user20 user33 user34 user35 user36 user49 user50 user51 user52 server2"
**.user{41..44}.VideoStreamClient*.serverAddress = "user13 user14 user15 user16 user29 user30
user31 user32 user45 user46 user47 user48 user61 user62 user63 user64 server2"
**.user{45..48}.VideoStreamClient*.serverAddress = "user9 user10 user11 user12 user25 user26
user27 user28 user41 user42 user43 user44 user57 user58 user59 user60 server2"
**.user{49..52}.VideoStreamClient*.serverAddress = "user5 user6 user7 user8 user21 user22 user23
user24 user37 user38 user39 user40 user53 user54 user55 user56 server2"
**.user{53..56}.VideoStreamClient*.serverAddress = "user1 user2 user3 user4 user17 user18 user19
user20 user33 user34 user35 user36 user49 user50 user51 user52 server2"
**.user{57..60}.VideoStreamClient*.serverAddress = "user13 user14 user15 user16 user29 user30
user31 user32 user45 user46 user47 user48 user61 user62 user63 user64 server2"
**.user{61..64}.VideoStreamClient*.serverAddress = "user9 user10 user11 user12 user25 user26
user27 user28 user41 user42 user43 user44 user57 user58 user59 user60 server2"

**.user*.VideoStreamClient*.startTime=uniform(2s, 6s)

**.user*.VideoStreamClient*.nextTime=uniform(4s, 6s)

# VideoStreamServer
**.VideoStreamServer.serverPort=2
**.VideoStreamServer.waitInterval=exponential(0.1s)
**.VideoStreamServer.packetLen=50000B
**.VideoStreamServer.videoSize=200000B

# PingApp
**.building2.pingApp.destAddr = "smartMeter6"
**.building4.pingApp.destAddr = "smartMeter12"
**.building6.pingApp.destAddr = "smartMeter18"
**.building8.pingApp.destAddr = "smartMeter27"
**.building10.pingApp.destAddr = "smartMeter33"
**.building12.pingApp.destAddr = "smartMeter44"
**.building14.pingApp.destAddr = "smartMeter50"
**.building16.pingApp.destAddr = "smartMeter60"

**.building2.pingApp.startTime = 40s
**.building6.pingApp.startTime = 40s
**.building10.pingApp.startTime = 40s
**.building14.pingApp.startTime = 40s
**.building4.pingApp.startTime = 40.5s
**.building8.pingApp.startTime = 40.5s
**.building12.pingApp.startTime = 40.5s
**.building16.pingApp.startTime = 40.5s
```

```
**.pingApp.interval = 2s
**.pingApp.stopTime = 61s
**.pingApp.count = 1
**.pingApp.packetSize = 56B

# attackClient
**.attackClient*.address = ""
**.attackClient*.port = -1
**.attackClient*.connectPort = 1000
**.attackClient*.numRequestsPerSession = 4
**.attackClient*.requestLength = 100B
**.attackClient*.replyLength = 10B
**.attackClient*.reconnectInterval = 30s
**.attackClient*.thinkTime = 30s  # time gap between requests
**.attackClient*.idleInterval = 30s  # time gap between sessions

**.attacker1.attackClient*.connectAddress = "smartMeter3"
**.attacker2.attackClient*.connectAddress = "smartMeter11"
**.attacker3.attackClient*.connectAddress = "smartMeter18"
**.attacker4.attackClient*.connectAddress = "smartMeter26"
**.attacker5.attackClient*.connectAddress = "smartMeter34"
**.attacker6.attackClient*.connectAddress = "smartMeter44"
**.attacker7.attackClient*.connectAddress = "smartMeter55"
**.attacker8.attackClient*.connectAddress = "smartMeter60"

**.attacker1.attackClient1.startTime = 0.1s
**.attacker1.attackClient2.startTime = 0.2s
**.attacker1.attackClient3.startTime = 0.25s
**.attacker1.attackClient4.startTime = 0.3s

**.attacker3.attackClient1.startTime = 0.1s
**.attacker3.attackClient2.startTime = 0.2s
**.attacker3.attackClient3.startTime = 0.25s
**.attacker3.attackClient4.startTime = 0.3s

**.attacker5.attackClient1.startTime = 0.1s
**.attacker5.attackClient2.startTime = 0.2s
**.attacker5.attackClient3.startTime = 0.25s
**.attacker5.attackClient4.startTime = 0.3s

**.attacker7.attackClient1.startTime = 0.1s
**.attacker7.attackClient2.startTime = 0.2s
**.attacker7.attackClient3.startTime = 0.25s
**.attacker7.attackClient4.startTime = 0.3s

**.attacker2.attackClient1.startTime = 0.11s
**.attacker2.attackClient2.startTime = 0.21s
**.attacker2.attackClient3.startTime = 0.26s
**.attacker2.attackClient4.startTime = 0.31s

**.attacker4.attackClient1.startTime = 0.11s
**.attacker4.attackClient2.startTime = 0.21s
**.attacker4.attackClient3.startTime = 0.26s
**.attacker4.attackClient4.startTime = 0.31s

**.attacker6.attackClient1.startTime = 0.11s
**.attacker6.attackClient2.startTime = 0.21s
**.attacker6.attackClient3.startTime = 0.26s
**.attacker6.attackClient4.startTime = 0.31s
```

```
**.attacker8.attackClient1.startTime = 0.11s
**.attacker8.attackClient2.startTime = 0.21s
**.attacker8.attackClient3.startTime = 0.26s
**.attacker8.attackClient4.startTime = 0.31s

# mac address
**.smartMeter*.wlan.mac.address = "auto"
**.officer*.wlan.mac.address= "auto"
**.user*.wlan.mac.address = "auto"
**.server*.wlan.mac.address = "auto"
**.attacker*.wlan.mac.address = "auto"
**.building*.wlan.mac.address = "auto"

**.dataCollector1.wlan.mac.address = "10:00:00:00:00:00"
**.dataCollector2.wlan.mac.address = "11:00:00:00:00:00"
**.dataCollector3.wlan.mac.address = "12:00:00:00:00:00"
**.dataCollector4.wlan.mac.address = "13:00:00:00:00:00"
**.dataCollector5.wlan.mac.address = "14:00:00:00:00:00"
**.dataCollector6.wlan.mac.address = "15:00:00:00:00:00"
**.dataCollector7.wlan.mac.address = "16:00:00:00:00:00"
**.dataCollector8.wlan.mac.address = "17:00:00:00:00:00"
**.dataCollector9.wlan.mac.address = "18:00:00:00:00:00"
**.dataCollector10.wlan.mac.address = "19:00:00:00:00:00"
**.dataCollector11.wlan.mac.address = "20:00:00:00:00:00"
**.dataCollector12.wlan.mac.address = "21:00:00:00:00:00"
**.dataCollector13.wlan.mac.address = "22:00:00:00:00:00"
**.dataCollector14.wlan.mac.address = "23:00:00:00:00:00"
**.dataCollector15.wlan.mac.address = "24:00:00:00:00:00"
**.dataCollector16.wlan.mac.address = "25:00:00:00:00:00"

**.accessPoint1.wlan.mac.address= "26:00:00:00:00:00"
**.accessPoint2.wlan.mac.address= "27:00:00:00:00:00"
**.accessPoint3.wlan.mac.address= "28:00:00:00:00:00"
**.accessPoint4.wlan.mac.address= "29:00:00:00:00:00"
**.accessPoint5.wlan.mac.address= "30:00:00:00:00:00"
**.accessPoint6.wlan.mac.address= "31:00:00:00:00:00"
**.internet.wlan.mac.address= "32:00:00:00:00:00"
**.lan.wlan.mac.address= "33:00:00:00:00:00"
**.gateway1.wlan.mac.address= "34:00:00:00:00:00"

#mgmt
**.attacker*.wlan.mgmt.frameCapacity = 1000000000
**.smartMeter*.wlan.mgmt.frameCapacity = 1000000000
**.user*.wlan.mgmt.frameCapacity = 1000000000
**.dataCollector*.wlan.mgmt.frameCapacity = 1000000000
**.server*.wlan.mgmt.frameCapacity = 1000000000

**.smartMeter{1..4}.wlan.mgmt.accessPointAddress = "10:00:00:00:00:00"
**.user{1..4}.wlan.mgmt.accessPointAddress = "10:00:00:00:00:00"

**.smartMeter{5..8}.wlan.mgmt.accessPointAddress = "11:00:00:00:00:00"
**.user{5..8}.wlan.mgmt.accessPointAddress = "11:00:00:00:00:00"

**.smartMeter{9..12}.wlan.mgmt.accessPointAddress = "12:00:00:00:00:00"
**.user{9..12}.wlan.mgmt.accessPointAddress = "12:00:00:00:00:00"

**.smartMeter{13..16}.wlan.mgmt.accessPointAddress = "13:00:00:00:00:00"
**.user{13..16}.wlan.mgmt.accessPointAddress = "13:00:00:00:00:00"

**.smartMeter{17..20}.wlan.mgmt.accessPointAddress = "14:00:00:00:00:00"
```

```
**.user{17..20}.wlan.mgmt.accessPointAddress = "14:00:00:00:00:00"

**.smartMeter{21..24}.wlan.mgmt.accessPointAddress = "15:00:00:00:00:00"
**.user{21..24}.wlan.mgmt.accessPointAddress = "15:00:00:00:00:00"

**.smartMeter{25..28}.wlan.mgmt.accessPointAddress = "16:00:00:00:00:00"
**.user{25..28}.wlan.mgmt.accessPointAddress = "16:00:00:00:00:00"

**.smartMeter{29..32}.wlan.mgmt.accessPointAddress = "17:00:00:00:00:00"
**.user{29..32}.wlan.mgmt.accessPointAddress = "17:00:00:00:00:00"

**.smartMeter{33..36}.wlan.mgmt.accessPointAddress = "18:00:00:00:00:00"
**.user{33..36}.wlan.mgmt.accessPointAddress = "18:00:00:00:00:00"

**.smartMeter{37..40}.wlan.mgmt.accessPointAddress = "19:00:00:00:00:00"
**.user{37..40}.wlan.mgmt.accessPointAddress = "19:00:00:00:00:00"

**.smartMeter{41..44}.wlan.mgmt.accessPointAddress = "20:00:00:00:00:00"
**.user{41..44}.wlan.mgmt.accessPointAddress = "20:00:00:00:00:00"

**.smartMeter{45..48}.wlan.mgmt.accessPointAddress = "21:00:00:00:00:00"
**.user{45..48}.wlan.mgmt.accessPointAddress = "21:00:00:00:00:00"

**.smartMeter{49..52}.wlan.mgmt.accessPointAddress = "22:00:00:00:00:00"
**.user{49..52}.wlan.mgmt.accessPointAddress = "22:00:00:00:00:00"

**.smartMeter{53..56}.wlan.mgmt.accessPointAddress = "23:00:00:00:00:00"
**.user{53..56}.wlan.mgmt.accessPointAddress = "23:00:00:00:00:00"

**.smartMeter{57..60}.wlan.mgmt.accessPointAddress = "24:00:00:00:00:00"
**.user{57..60}.wlan.mgmt.accessPointAddress = "24:00:00:00:00:00"

**.smartMeter{61..64}.wlan.mgmt.accessPointAddress = "25:00:00:00:00:00"
**.user{61..64}.wlan.mgmt.accessPointAddress = "25:00:00:00:00:00"

**.attacker{1..2}.wlan.mgmt.accessPointAddress = "26:00:00:00:00:00"
**.building{1..4}.wlan.mgmt.accessPointAddress = "26:00:00:00:00:00"

**.attacker{3..4}.wlan.mgmt.accessPointAddress = "27:00:00:00:00:00"
**.building{5..8}.wlan.mgmt.accessPointAddress = "27:00:00:00:00:00"

**.attacker{5..6}.wlan.mgmt.accessPointAddress = "28:00:00:00:00:00"
**.building{9..12}.wlan.mgmt.accessPointAddress = "28:00:00:00:00:00"

**.attacker{7..8}.wlan.mgmt.accessPointAddress = "29:00:00:00:00:00"
**.building{13..16}.wlan.mgmt.accessPointAddress = "29:00:00:00:00:00"

**.ControlCenter.wlan.mgmt.accessPointAddress = "31:00:00:00:00:00"

**.server*.wlan.mgmt.accessPointAddress = "33:00:00:00:00:00"

**.officer*.wlan.mgmt.accessPointAddress = "34:00:00:00:00:00"
**.mtu.wlan.mgmt.accessPointAddress = "34:00:00:00:00:00"
```

8.3. Βασικό σενάριο προσομοίωσης

Βέλτιστη λειτουργία του έξυπνου δικτύου

Εμπλεκόμενα μέρη: έξυπνοι μετρητές και κέντρο ελέγχου

Στη μικρή πόλη, υπάρχουν διασκορπισμένοι έξυπνοι μετρητές (smart meters). Οι έξυπνοι μετρητές συλλέγουν σε πραγματικό χρόνο τα δεδομένα μέτρησης της ενέργειας κατανάλωσης των νοικοκυριών και τα προωθούν μέσω του έξυπνου δικτύου επικοινωνιών στο κέντρο ελέγχου της παρόχου εταιρίας για αναλυτική επεξεργασία.
Μια ομάδα 4 έξυπνων μετρητών (π.χ. τα διαμερίσματα μιας μέσης πολυκατοικίας) μεταδίδει με ασύρματο τρόπο μέσω WiFi τις πληροφορίες της (μετρήσεις ή μηνύματα λάθους) σε ένα συλλέκτη δεδομένων (data collector).
Ο συλλέκτης δεδομένων συγκεντρώνει τις πληροφορίες και τις μεταφέρει με ενσύρματο τρόπο μέσω Ethernet στο σημείο πρόσβασης (access point) της γειτονιάς.
Κάθε γειτονιά αποτελείται από 4 σημεία πρόσβασης.
Στη συνέχεια, οι πληροφορίες από τα σημεία πρόσβασης κάθε γειτονιάς μεταδίδονται με ενσύρματο τρόπο μέσω Ethernet σε ένα κεντρικό σημείο πρόσβασης της πόλης.
Η μικρή πόλη αποτελείται από 4 γειτονιές.
Μεταξύ του κεντρικού σημείου πρόσβασης της πόλης και του σημείου πρόσβασης του κέντρου ελέγχου παρεμβάλλεται ένα τεράστιο δίκτυο επικοινωνιών, το Διαδίκτυο (Internet).
Έπειτα, οι πληροφορίες κατευθύνονται στην πύλη δικτύου των υπεύθυνων υπαλλήλων της εταιρείας και με ασύρματο τρόπο μέσω WiFi στους ίδιους τους προσωπικούς υπολογιστές των υπαλλήλων για άμεση ανάλυση.
Υπάρχουν 4 υπεύθυνοι υπάλληλοι στο κέντρο ελέγχου, ένας για την εξυπηρέτηση των έξυπνων μετρητών κάθε γειτονιάς.
Η δουλειά των υπαλλήλων είναι να επεξεργαστούν τις λαμβανόμενες πληροφορίες και να απαντήσουν στους αποστολείς ακολουθώντας την αντίθετη διαδρομή επικοινωνιών.
Η απάντησή τους θα περιλαμβάνει είτε πληροφορίες προς τους καταναλωτές, μέσω των έξυπνων μετρητών, για το λογαριασμό τους ή την κοστολόγηση της κατανάλωσης ενέργειας για το επόμενο χρονικό διάστημα, είτε παροχή υπηρεσιών και αποκατάστασης τεχνικού λάθους προς τους έξυπνους μετρητές ή τις οικιακές συσκευές.

Επίθεση άρνησης υπηρεσιών (DoS)

Εμπλεκόμενα μέρη: έξυπνοι μετρητές και επιτιθέμενοι

Στη μικρή πόλη, υπάρχουν διασκορπισμένοι κάποιοι επιτιθέμενοι (attackers). Σε κάθε γειτονιά υπάρχουν δυο επιτιθέμενοι. Αυτοί προσπαθούν να αποτρέψουν έναν ή περισσότερους έξυπνους μετρητές από το να παρέχουν τις υπηρεσίες τους (Denial of Service) είτε προς τους καταναλωτές είτε προς τους διαχειριστές τους στο κέντρο ελέγχου.
Ένας επιτιθέμενος στέλνει πολλά συνεχόμενα TCP Requests σε έναν συγκεκριμένο έξυπνο μετρητή. Σημειώνεται πως μια επιτυχημένη σύνδεση TCP μεταξύ

επιτιθέμενου και έξυπνου μετρητή με τη διαδικασία της τριπλής χειραψίας (SYN, SYNACK, ACK) διαρκεί για χρονικό διάστημα τουλάχιστον 2 min. Αυτό συμβαίνει διότι ο επιτιθέμενος, από τη στιγμή που συνδέεται επιτυχώς με τον έξυπνο μετρητή, τον κρατά απασχολημένο με συνεχείς ερωτήσεις-απαντήσεις.
Λαμβάνοντας υπόψη ότι ένας έξυπνος μετρητής έχει τη δυνατότητα να εξυπηρετεί ένα περιορισμένο αριθμό παράλληλων συνδέσεων TCP, γίνεται κατανοητό πως αν φτάσει στο όριό του τότε δεν θα μπορεί να συνδεθεί με το κέντρο ελέγχου, η οποία διαδικασία συμβαίνει κάθε 30 sec. Με αυτό τον τρόπο, δεν θα υπάρχει η δυνατότητα βέλτιστης λειτουργίας του έξυπνου δικτύου για ορισμένο χρονικό διάστημα.

Συνεργατικές υπηρεσίες peer-to-peer

Εμπλεκόμενα μέρη: κινούμενοι χρήστες και υπηρεσίες πελάτη-εξυπηρετητή

Στη μικρή πόλη, υπάρχουν διασκορπισμένοι κινούμενοι χρήστες (users). Στην πρώτη περίπτωση, 4 κινούμενοι χρήστες κινούνται κυκλικά γύρω από κάθε συλλέκτη δεδομένων. Στη δεύτερη περίπτωση, 8 κινούμενοι χρήστες κινούνται κυκλικά γύρω από κάθε συλλέκτη δεδομένων. Στην τρίτη περίπτωση, 16 κινούμενοι χρήστες κινούνται κυκλικά γύρω από κάθε συλλέκτη δεδομένων. Μπορούμε να υποθέσουμε ότι οι κινούμενοι χρήστες, που κινούνται κυκλικά και με σταθερή ταχύτητα γύρω από κάθε συλλέκτη δεδομένων, αποτελούν κάτοικοι των κοντινών πολυκατοικιών ή περαστικοί. Επίσης, χρησιμοποιούν μια συσκευή με σύνδεση στο Διαδίκτυο (π.χ. προσωπικός υπολογιστής ή κινητό τηλέφωνο).
Κάθε κινούμενος χρήστης μεταδίδει με ασύρματο τρόπο μέσω WiFi την αίτησή του για σύνδεση με έναν εξυπηρετητή προς τον συλλέκτη δεδομένων. Η αίτηση αυτή του πελάτη μπορεί να είναι ένα HTTP Request (TCP σύνδεση) προς έναν απομακρυσμένο εξυπηρετητή για αναζήτηση και προβολή μιας ιστοσελίδας. Ο απομακρυσμένος εξυπηρετητής τοποθετείται εκτός ορίων της πόλης και βρίσκεται μέσω του Internet. Ακόμη η αίτηση αυτή του πελάτη μπορεί να είναι ένα VideoStream Request (UDP σύνδεση) προς έναν τυχαίο εξυπηρετητή για αναζήτηση και κατέβασμα ενός βίντεο. Εκτός του απομακρυσμένου εξυπηρετητή όπως προηγουμένως, το βίντεο αυτό μπορεί να αναζητείται και από έναν οποιοδήποτε κινούμενο χρήστη της συγκεκριμένης ή άλλης γειτονιάς, ο οποίος διαθέτει το συγκεκριμένο βίντεο και εκτελώντας με αυτό τον τρόπο χρέη εξυπηρετητή (peer-to-peer συνεργασίες).

Απλή αναζήτηση έξυπνου μετρητή

Εμπλεκόμενα μέρη: διαμέρισμα και αντίστοιχος έξυπνος μετρητής

Κάθε διαμέρισμα έχει και τον αντίστοιχο έξυπνο μετρητή του για την καταγραφή της οικιακής κατανάλωσής του. Κάθε διαμέρισμα έχει τη δυνατότητα να αναζητά τον έξυπνο μετρητή του, επιβεβαιώνοντας με αυτό τον τρόπο την ύπαρξή του και τη σύνδεσή του με τις οικιακές συσκευές του διαμερίσματος. Αυτή η δυνατότητα δίνεται με την αποστολή ενός Ping Request (ICMP Protocol) προς τον έξυπνο μετρητή. Η απόκριση του έξυπνου μετρητή σημαίνει πως όλα κυλούν ομαλά.

8.4. Αποτελέσματα Προσομοίωσης Δικτύου SmartGrid

Το δίκτυο προσομοίωσης SmartGrid, όπως φαίνεται από την Εικόνα 8-30, αποτελείται από 4 γειτονιές υποδίκτυα (sub-networks), όπου είναι τοποθετημένοι οι έξυπνοι μετρητές, οι κινούμενοι χρήστες, τα διαμερίσματα, κ.ά.

Παρακάτω, παρουσιάζονται σε πίνακες και γραφικές παραστάσεις τα αποτελέσματα, όπως ποσότητα εισερχόμενων και εξερχόμενων δεδομένων, ρυθμός εισερχόμενης και εξερχόμενης πληροφορίας, χρησιμοποίηση κόμβων, χρόνος καθυστέρησης άφιξης πακέτων. Αυτά τα αποτελέσματα αφορούν τα κεντρικά σημεία πρόσβασης (AccessPoints), τους έξυπνους μετρητές (SmartMeters) και τους κινούμενους χρήστες (Users).

Γίνεται σύγκριση 3 σεναρίων προσομοίωσης:

- 16 χρήστες σε κάθε υποδίκτυο (16x4)
- 32 χρήστες σε κάθε υποδίκτυο (32x4)
- 64 χρήστες σε κάθε υποδίκτυο (64x4)

8.4.1. Ρυθμός λήψης / αποστολής δεδομένων ανά σημείο πρόσβασης

Τα σημεία πρόσβασης που λαμβάνουν μέρος σε κάθε υποδίκτυο είναι οι 4 συλλέκτες δεδομένων (DataCollectors{1..16}) και το κεντρικό σημείο πρόσβασης της γειτονιάς (AccessPoint{1..4}).

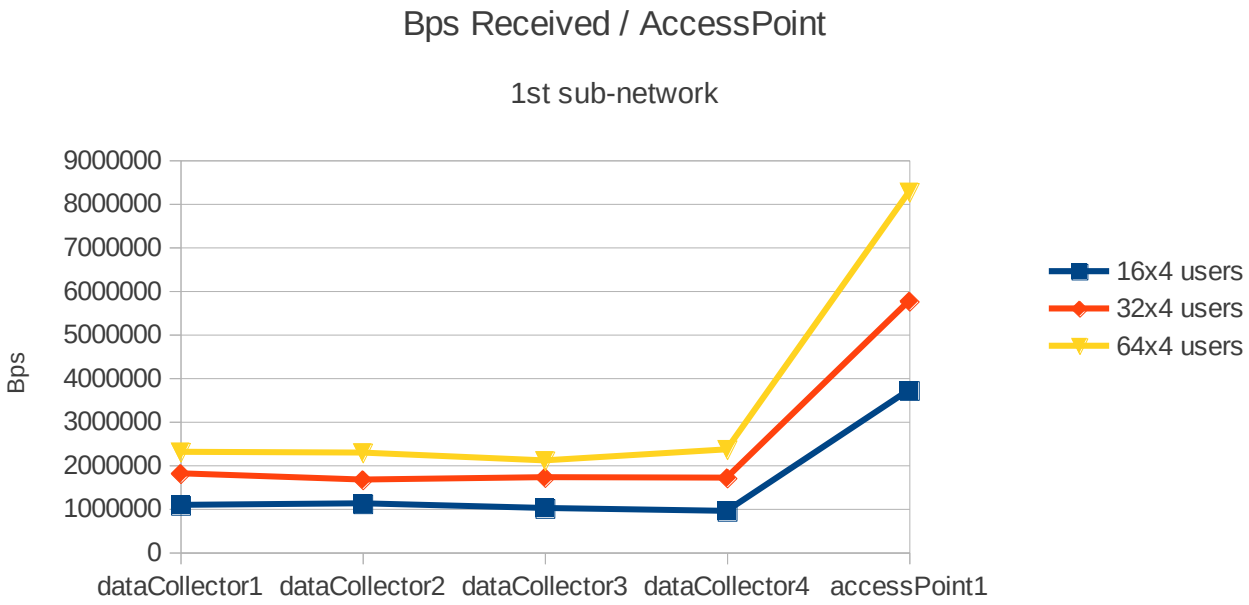
1η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων ρυθμού λήψης δεδομένων ανά σημείο πρόσβασης:

(Bps)	***16x4 users***	***32x4 users***	***64x4 users***
dataCollector1	1081336.90591	1806196.7747102	2300209.6459146
dataCollector2	1117042.0024893	1663901.1161918	2281393.6062743
dataCollector3	1010160.8462809	1716426.3807457	2102350.5624128
dataCollector4	943332.52362759	1705863.0873199	2355402.2955238
accessPoint1	3717114.04741436	5761051.2196553	8261575.8048879

Πίνακας 8-1 Ρυθμός λήψης δεδομένων / σημείο πρόσβασης (υποδίκτυο 1)

Επίσης, παρουσιάζεται το γράφημα του ρυθμού λήψης δεδομένων ανά σημείο πρόσβασης:



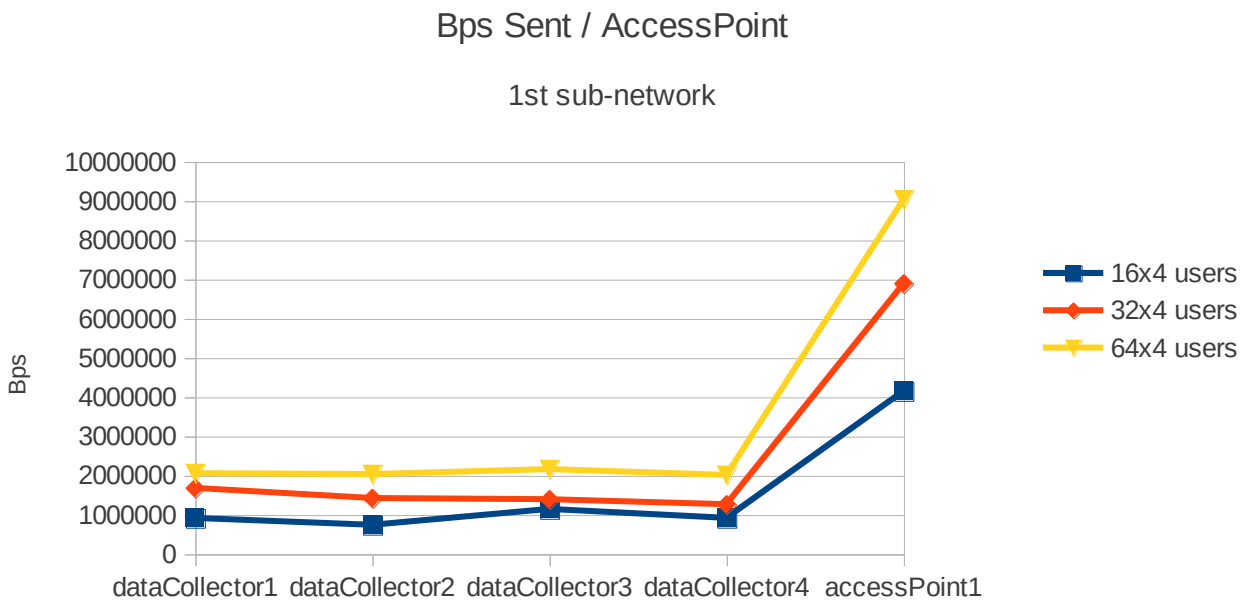
Γράφημα 8-1 Ρυθμός λήψης δεδομένων / σημείο πρόσβασης (υποδίκτυο 1)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων ρυθμού αποστολής δεδομένων ανά σημείο πρόσβασης:

(Bps)	***16x4 users***	***32x4 users***	***64x4 users***
dataCollector1	914667.16627932	1680531.6632788	2056962.4667925
dataCollector2	739383.01943179	1422738.4499216	2033937.6182854
dataCollector3	1144905.759166	1392422.7151307	2160140.28416
dataCollector4	918158.10253725	1265358.3913242	2010535.43565
accessPoint1	4151872.27830779	6892387.3589676	9039356.1101255

Πίνακας 8-2 Ρυθμός αποστολής δεδομένων / σημείο πρόσβασης (υποδίκτυο 1)

Επίσης, παρουσιάζεται το γράφημα του ρυθμού αποστολής δεδομένων ανά σημείο πρόσβασης:



Γράφημα 8-2 Ρυθμός αποστολής δεδομένων / σημείο πρόσβασης (υποδίκτυο 1)

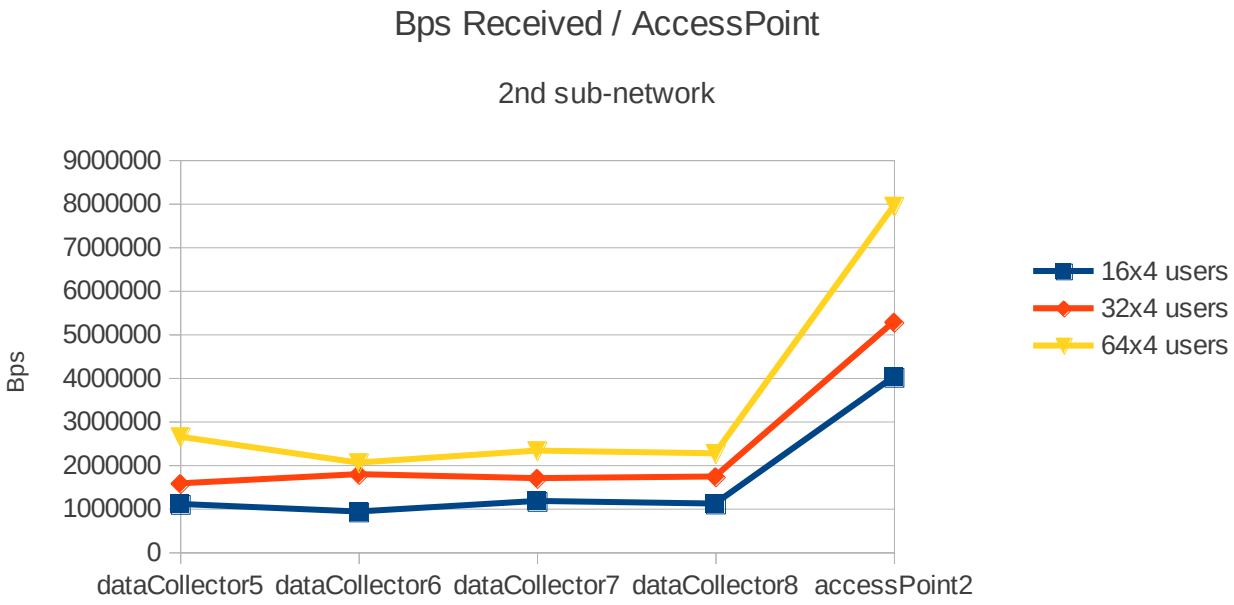
2η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων ρυθμού λήψης δεδομένων ανά σημείο πρόσβασης:

(Bps)	***16x4 users***	***32x4 users***	***64x4 users***
dataCollector5	1099309.720967	1571142.9624691	2642778.3676135
dataCollector6	925855.17565229	1781878.1596269	2046377.6444931
dataCollector7	1167363.1113134	1690600.018994	2322823.5602226
dataCollector8	1107215.8609239	1729756.098639	2259562.0936146
accessPoint2	4015343.89726187	5274362.9151937	7933623.6473155

Πίνακας 8-3 Ρυθμός λήψης δεδομένων / σημείο πρόσβασης (υποδίκτυο 2)

Επίσης, παρουσιάζεται το γράφημα του ρυθμού λήψης δεδομένων ανά σημείο πρόσβασης:



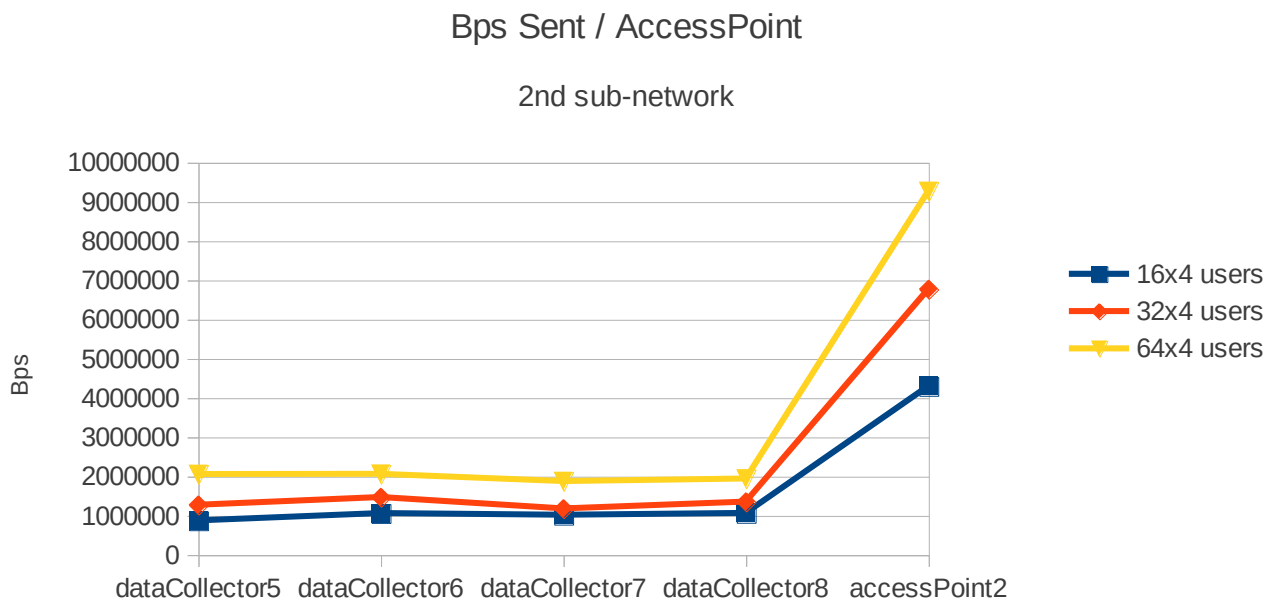
Γράφημα 8-3 Ρυθμός λήψης δεδομένων / σημείο πρόσβασης (υποδίκτυο 2)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων ρυθμού αποστολής δεδομένων ανά σημείο πρόσβασης:

(Bps)	***16x4 users***	***32x4 users***	***64x4 users***
dataCollector5	873358.86500587	1272546.4548982	2055841.9310985
dataCollector6	1060927.5554783	1469501.2635102	2061428.0762003
dataCollector7	1016720.051776	1179806.7013382	1876186.8859476
dataCollector8	1064337.4250017	1352508.4954471	1940166.7540691
accessPoint2	4299743.86885659	6773377.239729	9271541.6659438

Πίνακας 8-4 Ρυθμός αποστολής δεδομένων / σημείο πρόσβασης (υποδίκτυο 2)

Επίσης, παρουσιάζεται το γράφημα του ρυθμού αποστολής δεδομένων ανά σημείο πρόσβασης:



Γράφημα 8-4 Ρυθμός αποστολής δεδομένων / σημείο πρόσβασης (υποδίκτυο 2)

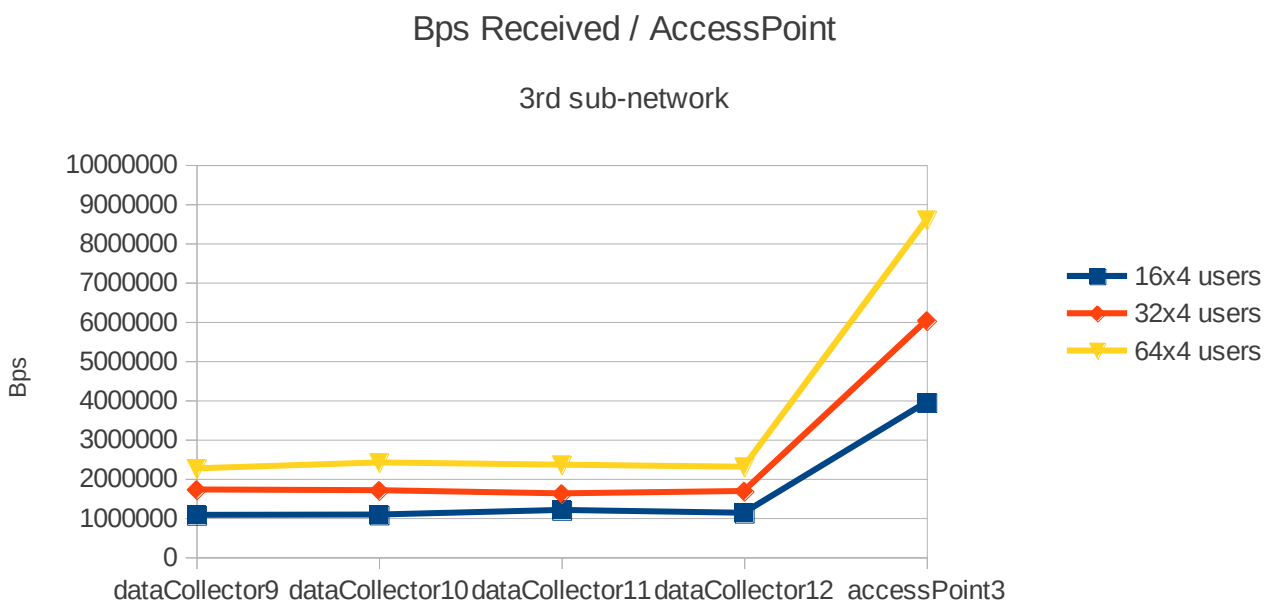
3η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων ρυθμού λήψης δεδομένων ανά σημείο πρόσβασης:

(Bps)	***16x4 users***	***32x4 users***	***64x4 users***
dataCollector9	1069650.4961195	1717469.5899723	2255281.0179289
dataCollector10	1076491.5685174	1697241.6777354	2405206.1337803
dataCollector11	1195580.2016194	1616486.8301746	2347474.2788216
dataCollector12	1122357.2069422	1678449.5115301	2296301.3710143
accessPoint3	3943069.9700464	6026366.6328751	8590009.5634749

Πίνακας 8-5 Ρυθμός λήψης δεδομένων / σημείο πρόσβασης (υποδίκτυο 3)

Επίσης, παρουσιάζεται το γράφημα του ρυθμού λήψης δεδομένων ανά σημείο πρόσβασης:



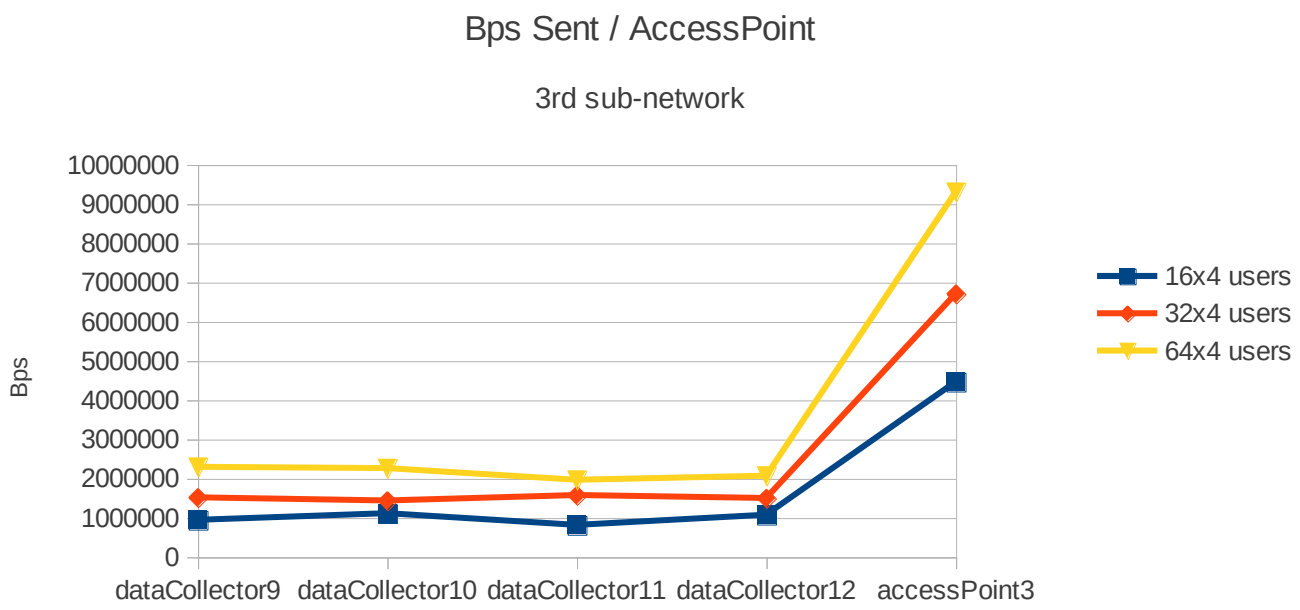
Γράφημα 8-5 Ρυθμός λήψης δεδομένων / σημείο πρόσβασης (υποδίκτυο 3)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων ρυθμού αποστολής δεδομένων ανά σημείο πρόσβασης:

(Bps)	***16x4 users***	***32x4 users***	***64x4 users***
dataCollector9	943125.5901209	1516423.5451758	2296372.8378315
dataCollector10	1112276.1318299	1436024.9674327	2260614.8958326
dataCollector11	814320.6822122	1575069.130527	1965158.8067205
dataCollector12	1073347.5658834	1498848.9897396	2067863.0230903
accessPoint3	4464079.4731985	6709647.6094124	9304262.8015451

Πίνακας 8-6 Ρυθμός αποστολής δεδομένων / σημείο πρόσβασης (υποδίκτυο 3)

Επίσης, παρουσιάζεται το γράφημα του ρυθμού αποστολής δεδομένων ανά σημείο πρόσβασης:



Γράφημα 8-6 Ρυθμός αποστολής δεδομένων / σημείο πρόσβασης (υποδίκτυο 3)

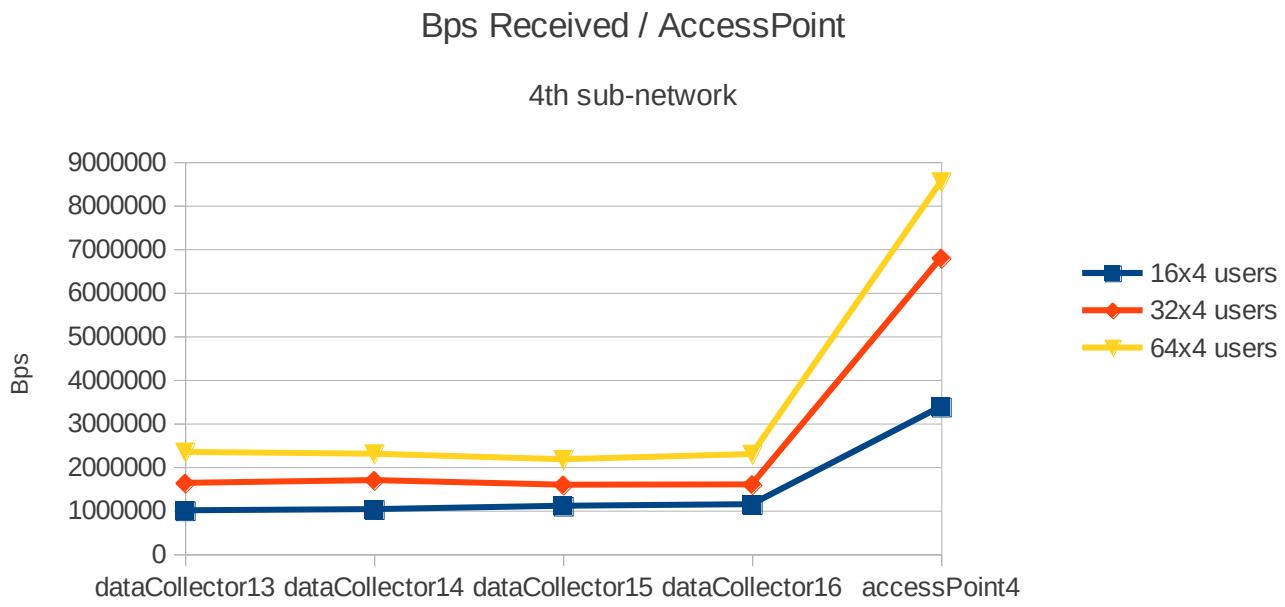
4η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων ρυθμού λήψης δεδομένων ανά σημείο πρόσβασης:

(Bps)	***16x4 users***	***32x4 users***	***64x4 users***
dataCollector13	998519.23652795	1627935.4647642	2339698.2624397
dataCollector14	1025847.7927563	1692033.0983354	2296949.3723794
dataCollector15	1104421.7252497	1585822.5589678	2171144.8406769
dataCollector16	1140537.4888397	1593479.1600191	2289342.9563548
accessPoint4	3378452.43036097	6790347.5231541	8540479.5924621

Πίνακας 8-7 Ρυθμός λήψης δεδομένων / σημείο πρόσβασης (υποδίκτυο 4)

Επίσης, παρουσιάζεται το γράφημα του ρυθμού λήψης δεδομένων ανά σημείο πρόσβασης:



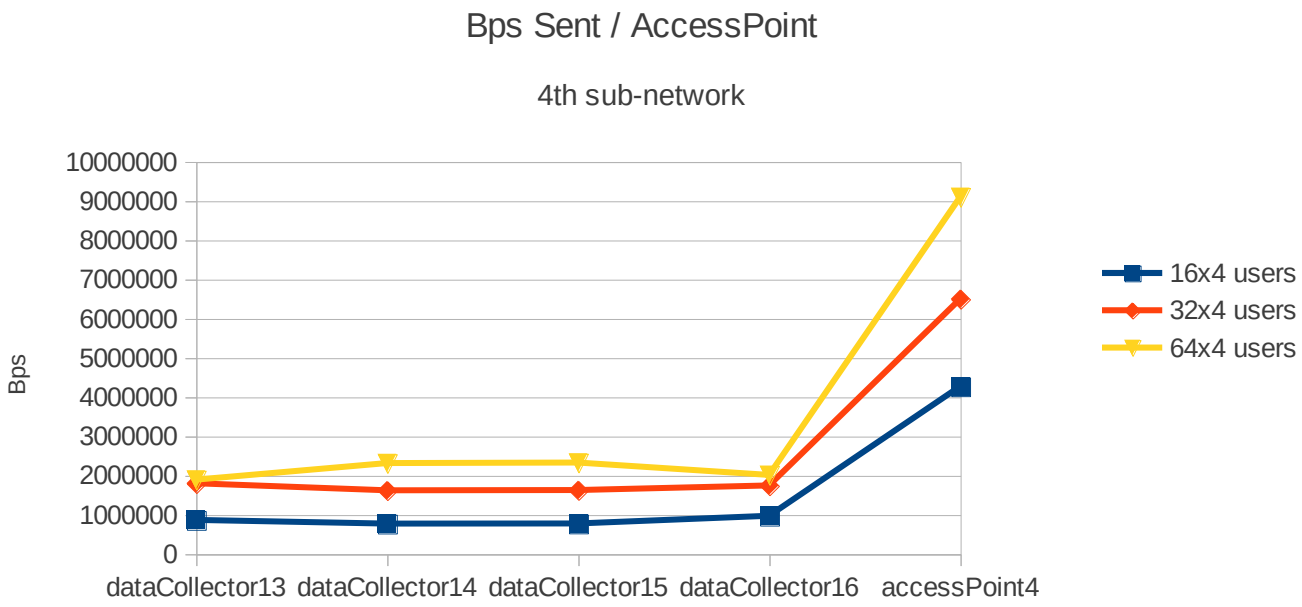
Γράφημα 8-7 Ρυθμός λήψης δεδομένων / σημείο πρόσβασης (υποδίκτυο 4)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων ρυθμού αποστολής δεδομένων ανά σημείο πρόσβασης:

(Bps)	***16x4 users***	***32x4 users***	***64x4 users***
dataCollector13	863359.65662884	1799812.7182471	1890296.2490055
dataCollector14	769378.24456085	1620355.6643921	2312551.5385823
dataCollector15	774043.31513576	1625573.8438771	2325902.2333752
dataCollector16	971671.21403552	1744605.2966378	2011729.5714991
accessPoint4	4269326.24337365	6499270.2820865	9097135.4318508

Πίνακας 8-8 Ρυθμός αποστολής δεδομένων / σημείο πρόσβασης (υποδίκτυο 4)

Επίσης, παρουσιάζεται το γράφημα του ρυθμού αποστολής δεδομένων ανά σημείο πρόσβασης:



Γράφημα 8-8 Ρυθμός αποστολής δεδομένων / σημείο πρόσβασης (υποδίκτυο 4)

Παρατηρείται ότι και στα 4 υποδίκτυα-γειτονιές, ο ρυθμός λήψης / αποστολής δεδομένων ανά σημείο πρόσβασης είναι περίπου ίδιος.

Επίσης, σε κάθε υποδίκτυο, τα κεντρικά σημεία πρόσβασης παρουσιάζουν σχεδόν τετραπλάσιο ρυθμό λήψης / αποστολής δεδομένων σε σύγκριση με τους συλλέκτες δεδομένων του υποδικτύου. Αυτό θεωρείται φυσιολογικό, αφού το κεντρικό σημείο πρόσβασης δέχεται τις πληροφορίες και τα δεδομένα των 4 συλλεκτών δεδομένων της γειτονιάς. Αξίζει να σημειωθεί πως η εισερχόμενη πληροφορία στους συλλέκτες δεδομένων προέρχεται επιπλέον από τους χρήστες VideoStream που κατεβάζουν βίντεο από χρήστες της ίδιας υπο-γειτονιάς. Για αυτό και το άθροισμα της πληροφορίας των 4 συλλεκτών δεδομένων είναι μεγαλύτερο αυτού του κεντρικού σημείου πρόσβασης.

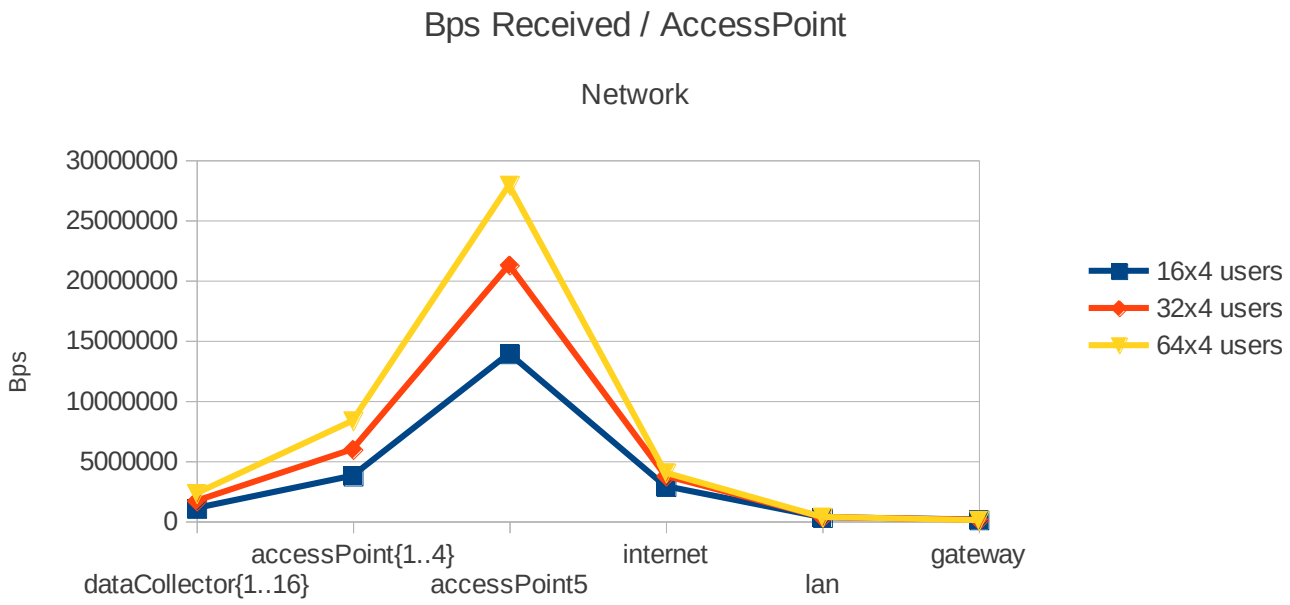
Τέλος, αυξάνοντας τους αριθμούς των χρηστών, διπλασιάζοντας και τετραπλασιάζοντας αυτούς, παρατηρούμε φυσιολογικά σχεδόν ανάλογη αύξηση της εισερχόμενης / εξερχόμενης πληροφορίας στα εμπλεκόμενα σημεία πρόσβασης. Αξίζει να σημειωθεί πως οι πληροφορίες των χρηστών δημιουργούνται ανά τυχαία χρονικά διαστήματα. Παράλληλα, καθώς αυξάνεται ο αριθμός των χρηστών, οι πληροφορίες που αναγκάζονται να περιμένουν στην ουρά των κεντρικών σημείων πρόσβασης συνεχώς αυξάνονται και καθυστερεί ο χρόνος παράδοσής τους. Για αυτό και ο ρυθμός εισερχόμενης / εξερχόμενης πληροφορίας στα σημεία πρόσβασης είναι μικρότερος του διπλάσιου όταν διπλασιάζονται οι χρήστες και μικρότερος του τετραπλάσιου όταν τετραπλασιάζονται οι χρήστες.

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων ρυθμού λήψης δεδομένων ανά σημείο πρόσβασης:

(Bps)	***16x4 users***	***32x4 users***	***64x4 users***
dataCollector{1..16}	1074063.8664835	1679667.6556372	2294518.50059158
accessPoint{1..4}	3763495.0862709	5963032.0727196	8331422.1520351
accessPoint5	13920869.262466	21273403.083625	27902404.9160933
internet	2897502.6941031	3750296.6357558	4019281.5341971
lan	319559.20104996	324075.39958283	337609.24458397
gateway	127122.77316612	111620.18721256	72151.618670456

Πίνακας 8-9 Ρυθμός λήψης δεδομένων / σημείο πρόσβασης (δίκτυο)

Επίσης, παρουσιάζεται το γράφημα του ρυθμού λήψης δεδομένων ανά σημείο πρόσβασης:



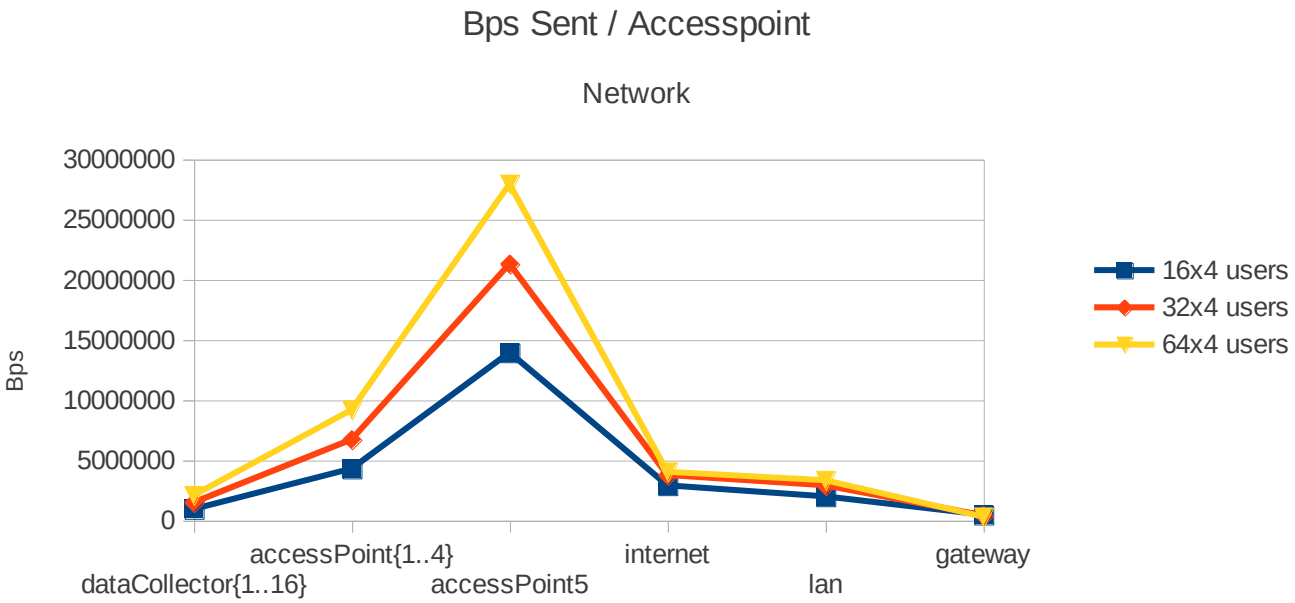
Γράφημα 8-9 Ρυθμός λήψης δεδομένων / σημείο πρόσβασης (δίκτυο)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων ρυθμού αποστολής δεδομένων ανά σημείο πρόσβασης:

(Bps)	***16x4 users***	***32x4 users***	***64x4 users***
dataCollector{1..16}	940873.77156773	1490758.0181799	2082855.53800878
accessPoint{1..4}	4296255.4659341	6718670.6225489	9178074.0023663
accessPoint5	13946802.084191	21302033.736845	27939304.1938301
internet	2906767.235198	3760976.1968767	4032268.22822315
lan	1990158.467292	2909386.2650825	3329653.414672
gateway	469312.39317513	415353.00687766	292771.28345594

Πίνακας 8-10 Ρυθμός αποστολής δεδομένων / σημείο πρόσβασης (δίκτυο)

Επίσης, παρουσιάζεται το γράφημα του ρυθμού αποστολής δεδομένων ανά σημείο πρόσβασης:



Γράφημα 8-10 Ρυθμός αποστολής δεδομένων / σημείο πρόσβασης (δίκτυο)

Καταρχάς, στα 2 παραπάνω γράφηματα εισήχθη ο μέσος όρος ρυθμού εισερχόμενης / εξερχόμενης πληροφορίας σε κάθε συλλέκτη δεδομένων και κεντρικού σημείου πρόσβασης γειτονιάς.

Κατά δεύτερον, παρατηρείται ότι το κεντρικό σημείο πρόσβασης της πόλης παρουσιάζει αρκετά υψηλό ρυθμό εισερχόμενης / εξερχόμενης πληροφορίας, για

αυτό αποτελεί και το μοναδικό σημείο πρόσβασης με δυνατότητα ρυθμού επεξεργασίας δεδομένων 100 Mbps (όλα τα άλλα σημεία πρόσβασης έχουν δυνατότητα ρυθμού επεξεργασίας δεδομένων 10 Mbps). Εξάλλου, αποτελεί και το μοναδικό κόμβο διασύνδεσης των υποδικτύων-γειτονιών μεταξύ τους καθώς και με το κέντρο ελέγχου και τους απομακρυσμένους εξυπηρετητές του Διαδικτύου.

Τέλος, φαίνεται ότι η εισερχόμενη / εξερχόμενη πληροφορία στον κόμβο διαδικτύου, χωρίζεται στην πληροφορία από / προς τους απομακρυσμένους εξυπηρετητές διαδικτύου και στην πληροφορία από / προς το κέντρο ελέγχου. Το μέγεθος της πληροφορίας που αφορά την επικοινωνία μεταξύ του κέντρου ελέγχου και των έξυπνων μετρητών, όπως και μεταξύ των χρηστών και των απομακρυσμένων εξυπηρετητών http, είναι κατά πολύ μικρότερο του μεγέθους πληροφορίας που έχουν οι συνεργατικές υπηρεσίες peer-to-peer για video-downloading. Επίσης, οι έξυπνοι μετρητές απασχολούν το δίκτυο επικοινωνιών για ελάχιστο χρονικό διάστημα κάθε 30 δευτερόλεπτα, ενώ οι υπηρεσίες βίντεο απασχολούν το δίκτυο για μεγαλύτερο χρονικό διάστημα και σε τυχαίες συχνές χρονικές στιγμές.

8.4.2. Ποσοστό χρησιμοποίησης (utilization) ανά σημείο πρόσβασης

Τα σημεία πρόσβασης που λαμβάνουν μέρος σε κάθε υποδίκτυο είναι οι 4 συλλέκτες δεδομένων (DataCollectors{1..16}) και το κεντρικό σημείο πρόσβασης της γειτονιάς (AccessPoint{1..4}).

Το ποσοστό χρησιμοποίησης κάθε κόμβου-σημείου πρόσβασης προκύπτει από το λόγο του αθροίσματος ρυθμού εισερχόμενης και εξερχόμενης πληροφορίας στον κόμβο προς τη μέγιστη δυνατότητα ρυθμού επεξεργασίας αυτού του κόμβου. Επειδή τα σημεία πρόσβασης της προσομοίωσης διασυνδέονται με γραμμές Ethernet full duplex, διαιρώ τον παραπάνω λόγο με το 2.

Τέλος, γίνεται χρήση των προηγούμενων αντιστοίχων αποτελεσμάτων.

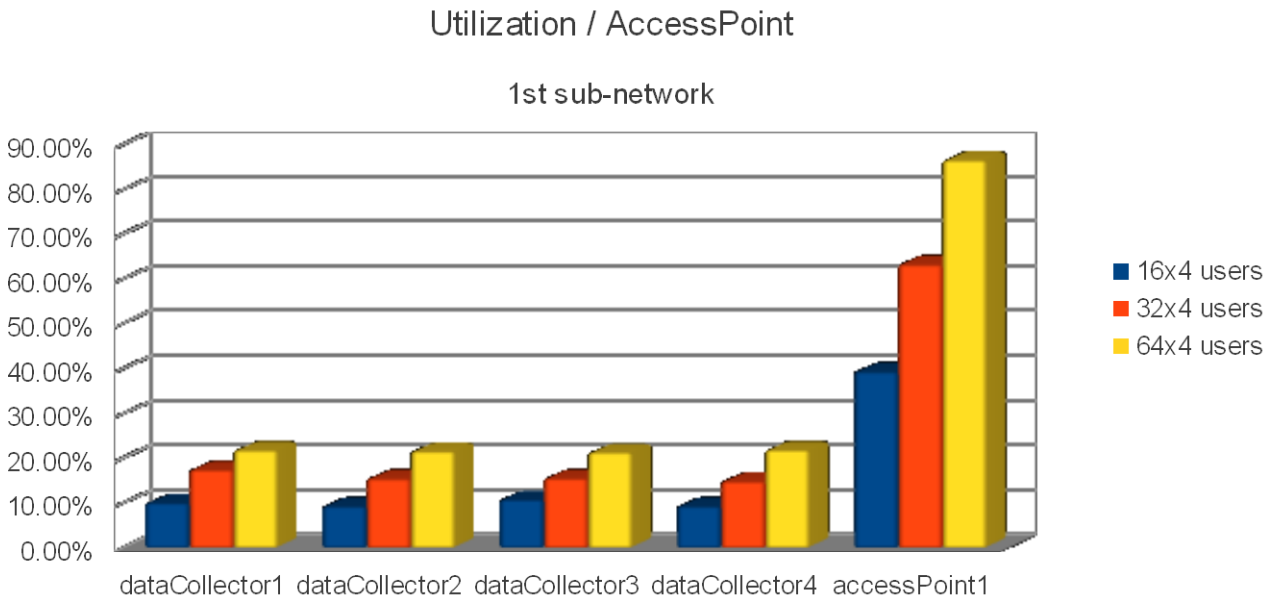
1*η γειτονιά-υποδίκτυο*

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων του ποσοστού χρησιμοποίησης ανά σημείο πρόσβασης:

	16x4 users	***32x4 users***	***64x4 users***
dataCollector1	9.98%	17.43%	21.79%
dataCollector2	9.28%	15.43%	21.58%
dataCollector3	10.78%	15.54%	21.31%
dataCollector4	9.31%	14.86%	21.83%
accessPoint1	39.34%	63.27%	86.50%

Πίνακας 8-11 Ποσοστό χρησιμοποίησης / σημείο πρόσβασης (υποδίκτυο 1)

Επίσης, παρουσιάζεται το γράφημα του ποσοστού χρησιμοποίησης ανά σημείο πρόσβασης:



Γράφημα 8-11 Ποσοστό χρησιμοποίησης / σημείο πρόσβασης (υποδίκτυο 1)

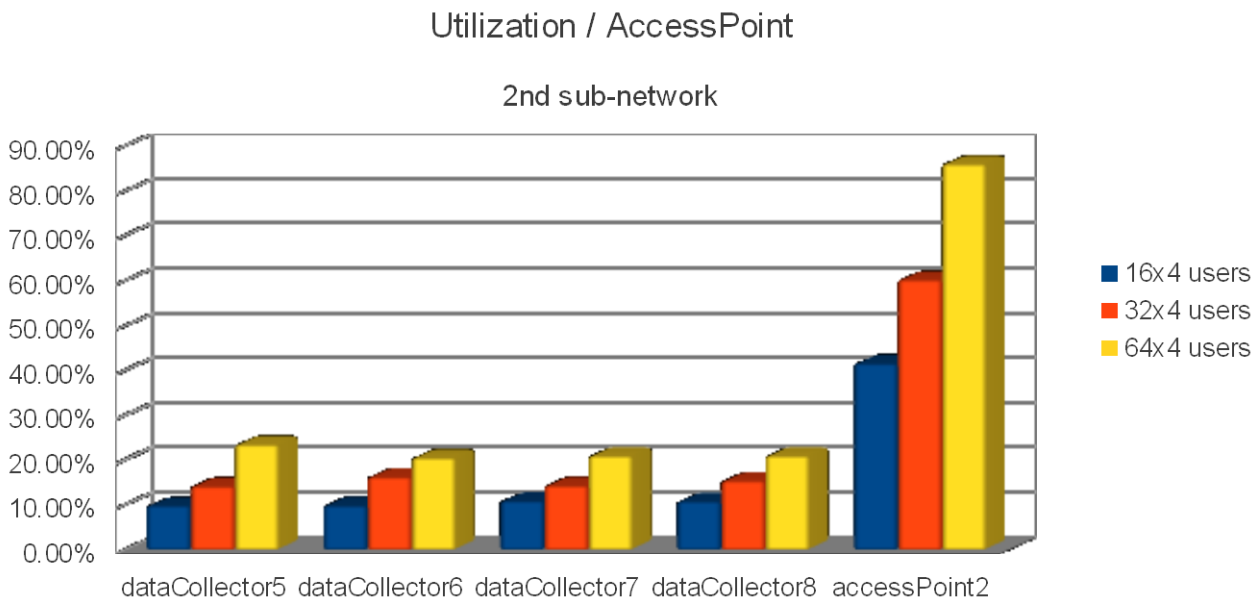
2η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων του ποσοστού χρησιμοποίησης ανά σημείο πρόσβασης:

	16x4 users	***32x4 users***	***64x4 users***
dataCollector5	9.86%	14.22%	23.49%
dataCollector6	9.93%	16.26%	20.54%
dataCollector7	10.92%	14.35%	21.00%
dataCollector8	10.86%	15.41%	21.00%
accessPoint2	41.58%	60.24%	86.03%

Πίνακας 8-12 Ποσοστό χρησιμοποίησης / σημείο πρόσβασης (υποδίκτυο 2)

Επίσης, παρουσιάζεται το γράφημα του ποσοστού χρησιμοποίησης ανά σημείο πρόσβασης:



Γράφημα 8-12 Ποσοστό χρησιμοποίησης / σημείο πρόσβασης (υποδίκτυο 2)

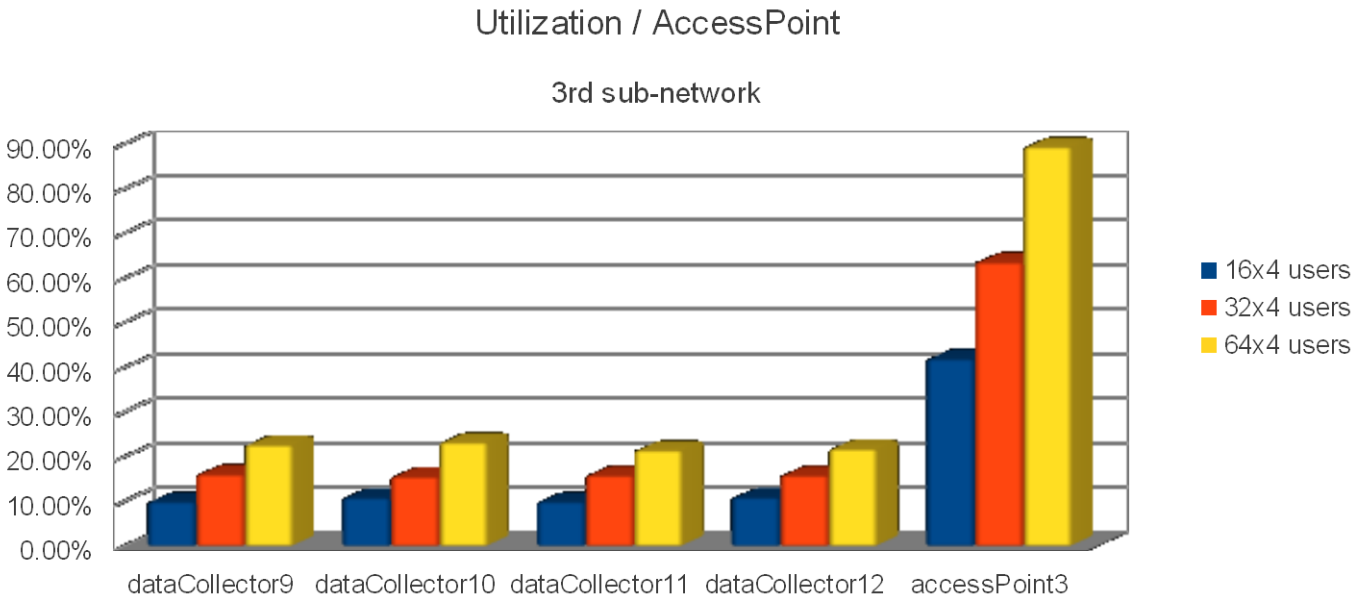
3η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων του ποσοστού χρησιμοποίησης ανά σημείο πρόσβασης:

	16x4 users	***32x4 users***	***64x4 users***
dataCollector9	10.06%	16.17%	22.76%
dataCollector10	10.94%	15.67%	23.33%
dataCollector11	10.05%	15.96%	21.56%
dataCollector12	10.98%	15.89%	21.82%
accessPoint3	42.04%	63.68%	89.47%

Πίνακας 8-13 Ποσοστό χρησιμοποίησης / σημείο πρόσβασης (υποδίκτυο 3)

Επίσης, παρουσιάζεται το γράφημα του ποσοστού χρησιμοποίησης ανά σημείο πρόσβασης:



Γράφημα 8-13 Ποσοστό χρησιμοποίησης / σημείο πρόσβασης (υποδίκτυο 3)

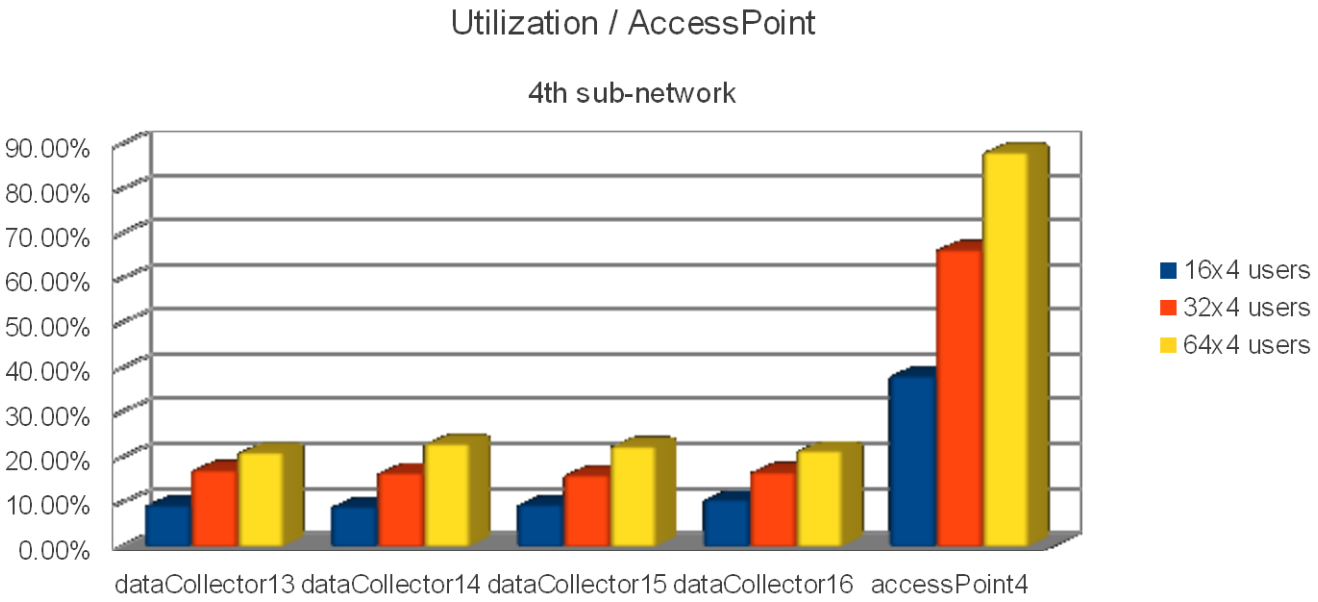
4η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων του ποσοστού χρησιμοποίησης ανά σημείο πρόσβασης:

	16x4 users	***32x4 users***	***64x4 users***
dataCollector13	9.31%	17.14%	21.15%
dataCollector14	8.98%	16.56%	23.05%
dataCollector15	9.39%	16.06%	22.49%
dataCollector16	10.56%	16.69%	21.51%
accessPoint4	38.24%	66.45%	88.19%

Πίνακας 8-14 Ποσοστό χρησιμοποίησης / σημείο πρόσβασης (υποδίκτυο 4)

Επίσης, παρουσιάζεται το γράφημα του ποσοστού χρησιμοποίησης ανά σημείο πρόσβασης:



Γράφημα 8-14 Ποσοστό χρησιμοποίησης / σημείο πρόσβασης (υποδίκτυο 4)

Παρατηρείται ότι και στα 4 υποδίκτυα-γειτονιές, το ποσοστό χρησιμοποίησης ανά σημείο πρόσβασης είναι περίπου ίδιο.

Επίσης, σε κάθε υποδίκτυο, τα κεντρικά σημεία πρόσβασης παρουσιάζουν σχεδόν τετραπλάσιο ποσοστό χρησιμοποίησης σε σύγκριση με τους συλλέκτες δεδομένων του υποδικτύου. Αυτό θεωρείται φυσιολογικό, αφού το κεντρικό σημείο πρόσβασης δέχεται τις πληροφορίες και τα δεδομένα των 4 συλλεκτών δεδομένων της γειτονιάς. Αξίζει να σημειωθεί πως η πληροφορία στους συλλέκτες δεδομένων προέρχεται επιπλέον από τους χρήστες VideoStream που κατεβάζουν βίντεο από χρήστες της ίδιας υπο-γειτονιάς. Για αυτό και το άθροισμα του ποσοστού χρησιμοποίησης των 4 συλλεκτών δεδομένων είναι μεγαλύτερο αυτού του κεντρικού σημείου πρόσβασης.

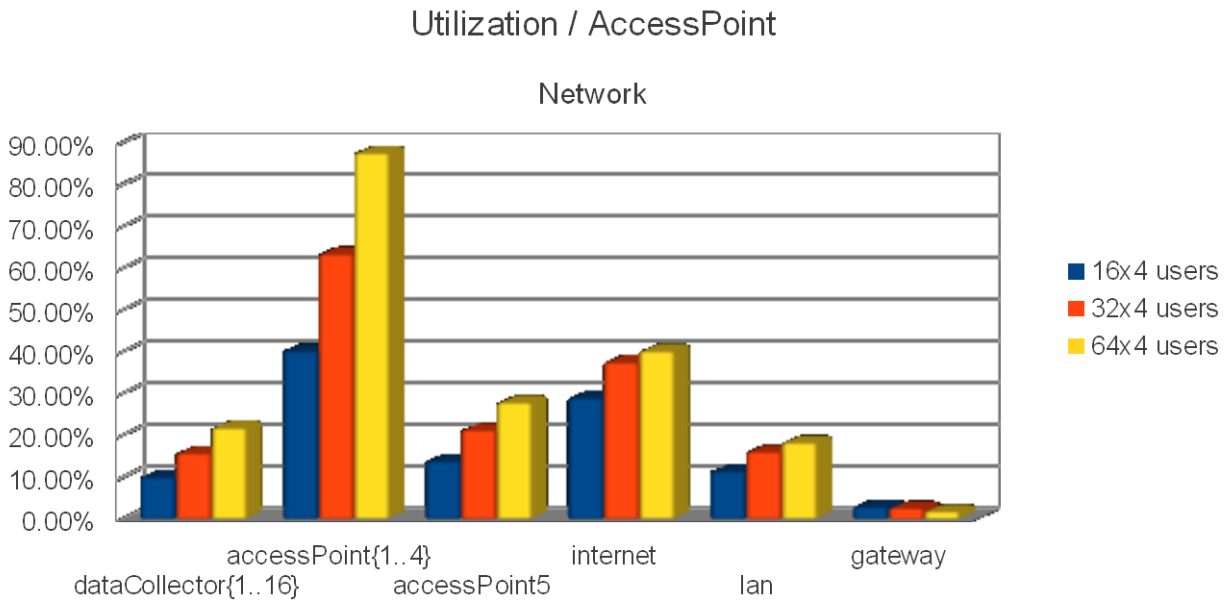
Τέλος, αυξάνοντας τους αριθμούς των χρηστών, διπλασιάζοντας και τετραπλασιάζοντας αυτούς, παρατηρούμε φυσιολογικά σχεδόν ανάλογη αύξηση του ποσοστού χρησιμοποίησης στα εμπλεκόμενα σημεία πρόσβασης. Αξίζει να σημειωθεί πως οι πληροφορίες των χρηστών δημιουργούνται ανά τυχαία χρονικά διαστήματα. Παράλληλα, καθώς αυξάνεται ο αριθμός των χρηστών, οι πληροφορίες που αναγκάζονται να περιμένουν στην ουρά των κεντρικών σημείων πρόσβασης συνεχώς αυξάνονται και καθυστερεί ο χρόνος παράδοσής τους. Για αυτό και το ποσοστό χρησιμοποίησης στα σημεία πρόσβασης είναι μικρότερο του διπλάσιου όταν διπλασιάζονται οι χρήστες και μικρότερο του τετραπλάσιου όταν τετραπλασιάζονται οι χρήστες.

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων του ποσοστού χρησιμοποίησης ανά σημείο πρόσβασης:

	16x4 users	***32x4 users***	***64x4 users***
dataCollector{1..16}	10.07%	15.85%	21.89%
accessPoint{1..4}	40.30%	63.41%	87.55%
accessPoint5	13.93%	21.29%	27.92%
internet	29.02%	37.56%	40.26%
lan	11.55%	16.17%	18.34%
gateway	2.98%	2.63%	1.82%

Πίνακας 8-15 Ποσοστό χρησιμοποίησης / σημείο πρόσβασης (δίκτυο)

Επίσης, παρουσιάζεται το γράφημα του ποσοστού χρησιμοποίησης ανά σημείο πρόσβασης:



Γράφημα 8-15 Ποσοστό χρησιμοποίησης / σημείο πρόσβασης (δίκτυο)

Παρατηρείται ότι το κεντρικό σημείο πρόσβασης κάθε γειτονιάς-υποδικτύου πλησιάζει τα όριά του στο σενάριο των 64x4 χρηστών.

Επίσης, διαπιστώνεται ότι το κεντρικό σημείο πρόσβασης της πόλης, που είναι το μοναδικό σημείο πρόσβασης με δυνατότητα ρυθμού επεξεργασίας δεδομένων 100 Mbps, έχει τη δυνατότητα επέκτασης και διασύνδεσης και άλλων παρόμοιων γειτονιών στο σημείο αυτό πρόσβασης.

Τέλος, φαίνεται η ελάχιστη χρησιμοποίηση του σημείου πρόσβασης του κέντρου ελέγχου, το οποίο σημαίνει ότι οι πληροφορίες του, που αφορούν τους καταναλωτές και ιδιοκτήτες των έξυπνων μετρητών, δεν υπερφορτώνουν το δίκτυο επικοινωνιών με τη λειτουργία τους. Εκμεταλλευόμενοι αυτό το γεγονός μελλοντικά, μπορούν να αυξηθούν οι ποσότητες πληροφορίας που ανταλλάσσονται μεταξύ πελατών-κέντρου ελέγχου που θα ωφελούν τη βέλτιστη διαχείριση ενέργειας και σχέσης μεταξύ τους.

8.4.3. Ποσότητα εισερχόμενων / εξερχόμενων δεδομένων ανά έξυπνο μετρητή

Τα στοιχεία που λαμβάνουν μέρος σε κάθε υποδίκτυο είναι οι 16 σταθεροί σε αριθμό και κινητικότητα έξυπνοι μετρητές (SmartMeters{1..64}).

Τα δεδομένα που μπορεί να αποδεχτεί / αποστείλει ένας έξυπνος μετρητής είναι:

- Η πληροφορία για οικονομική διαχείριση της ενέργειας κατανάλωσης από το κέντρο ελέγχου, μεγέθους 15000 Bytes. Οι μετρήσεις κατανάλωσης ενέργειας κατανάλωσης κάθε νοικοκυριού, μεγέθους 3000 Bytes.
- Η ενημέρωση λογισμικού ή επιδιόρθωση άλλων τεχνικών προβλημάτων του έξυπνου μετρητή από τους παρόχους τεχνικής βοήθειας του κέντρου ελέγχου, μεγέθους 1000 Bytes. Η αποστολή μηνύματος λάθους, μεγέθους 50 Bytes.
- Η διαρκής επίθεση που δέχεται από κακόβουλους χρήστες, με σκοπό να του απαγορεύσουν την παροχή υπηρεσιών προς τους ιδιοκτήτες και καταναλωτές και το κέντρο ελέγχου και κατάληψης αυτών για αρκετό χρονικό διάστημα, μεγέθους 100 Bytes. Η απόκριση προς τους άγνωστους επιτιθέμενους και τις ψεύτικες αναζητήσεις τους, μεγέθους 10 Bytes.

1*η γειτονιά-υποδίκτυο*

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων ανά έξυπνο μετρητή:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
smartMeter1	60000	45000	30000
smartMeter2	60000	60000	45000
smartMeter3	800	600	800
smartMeter4	45000	45000	30000
smartMeter5	45000	45000	30000
smartMeter6	60000	45000	30000
smartMeter7	60000	60000	30000
smartMeter8	45000	45000	45000
smartMeter9	61000	46000	31000
smartMeter10	60000	60000	30000
smartMeter11	800	800	800
smartMeter12	45000	45000	30000
smartMeter13	45000	45000	30000
smartMeter14	60000	45000	45000
smartMeter15	60000	60000	45000
smartMeter16	60000	45000	45000

Πίνακας 8-16 Εισερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 1)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων ανά έξυπνο μετρητή:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
smartMeter1	12000	9000	6000
smartMeter2	12000	12000	9000
smartMeter3	80	60	80
smartMeter4	9000	9000	6000
smartMeter5	9000	9000	6000
smartMeter6	12000	9000	6000
smartMeter7	12000	12000	6000
smartMeter8	9000	9000	9000
smartMeter9	12050	9050	6050
smartMeter10	12000	12000	6000
smartMeter11	80	80	80
smartMeter12	9000	9000	6000
smartMeter13	9000	9000	6000
smartMeter14	12000	9000	9000
smartMeter15	12000	12000	9000
smartMeter16	12000	9000	9000

Πίνακας 8-17 Εξερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 1)

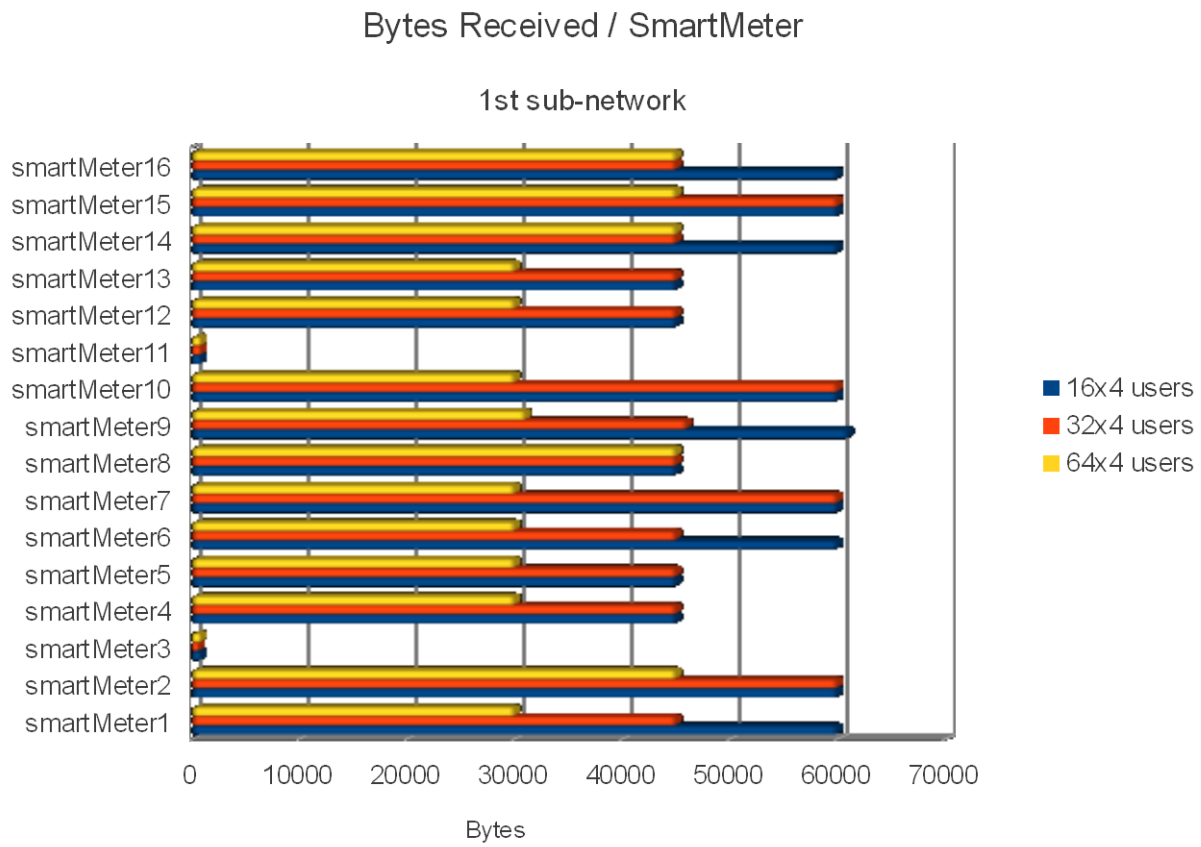
Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι έξυπνοι μετρητές της γειτονιάς είχαν από 2 έως 4 λήψεις δεδομένων από το κέντρο ελέγχου.

Ωστόσο, δυο έξυπνοι μετρητές (3 και 11) δέχθηκαν επίθεση και δεν τους επιτράπηκε καμία ανταλλαγή πληροφορίας με το κέντρο ελέγχου.

Επίσης, ένας έξυπνος μετρητής (9) παρουσίασε τεχνικό πρόβλημα και δέχτηκε την τεχνική βοήθεια του κέντρου ελέγχου.

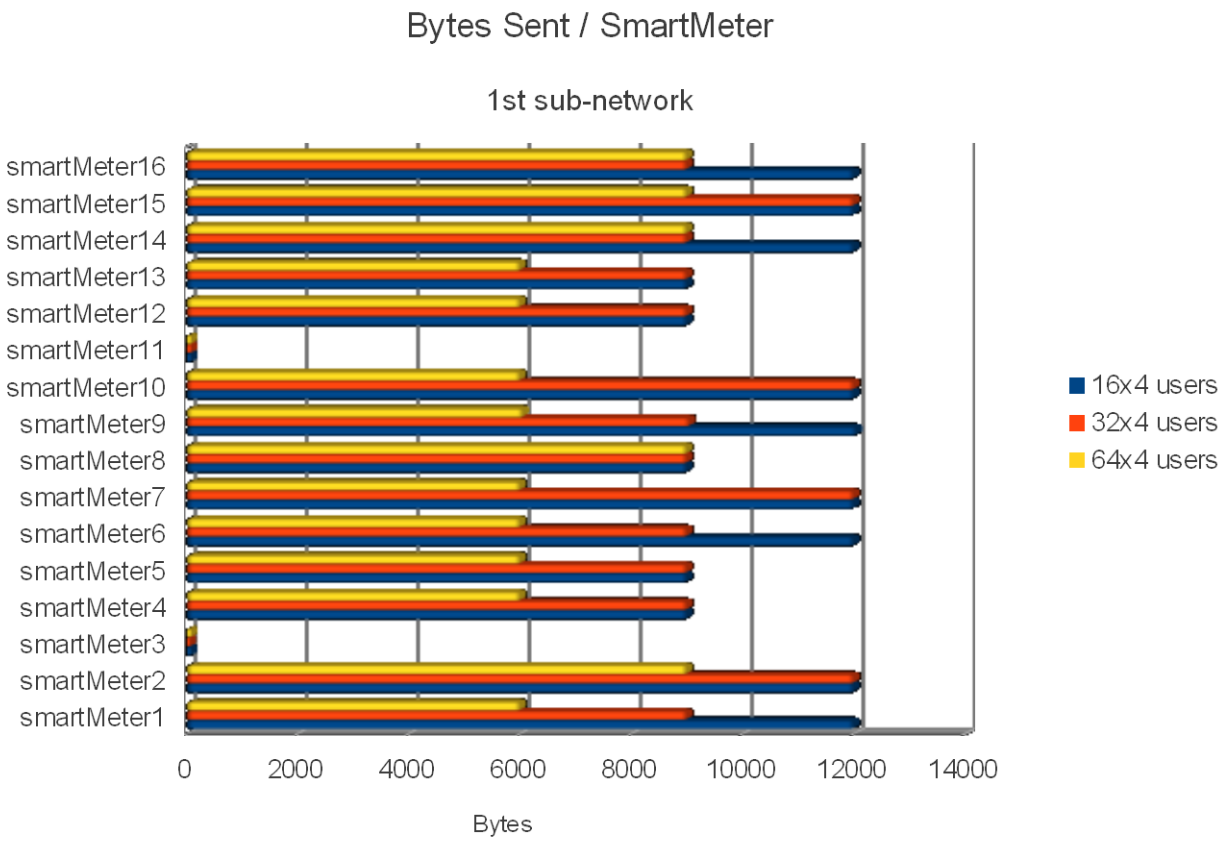
Τέλος, διαπιστώνεται ότι, καθώς αυξάνουν οι χρήστες, μειώνεται η ποσότητα δεδομένων που εισέρχεται στους μετρητές από το κέντρο ελέγχου. Αυτό οφείλεται στο γεγονός ότι, αν δεν καρποφορήσει η επιτυχής αναζήτηση του έξυπνου μετρητή την προκαθορισμένη χρονική στιγμή (π.χ. λόγω συμφόρησης δικτύου), τότε αναζητείται εκ νέου στην επόμενη προκαθορισμένη χρονική στιγμή (μετά από 30 δευτερόλεπτα).

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων ανά έξυπνο μετρητή:



Γράφημα 8-16 Εισερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 1)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων ανά έξυπνο μετρητή:



Γράφημα 8-17 Εξερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 1)

2η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων ανά έξυπνο μετρητή:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
smartMeter17	45000	45000	30000
smartMeter18	800	800	700
smartMeter19	60000	45000	30000
smartMeter20	60000	45000	30000
smartMeter21	45000	45000	45000
smartMeter22	60000	45000	30000
smartMeter23	60000	45000	30000
smartMeter24	61000	46000	31000
smartMeter25	45000	45000	45000
smartMeter26	800	800	700
smartMeter27	60000	45000	45000
smartMeter28	45000	45000	30000
smartMeter29	45000	45000	30000
smartMeter30	60000	60000	45000
smartMeter31	60000	45000	45000
smartMeter32	60000	60000	45000

Πίνακας 8-18 Εισερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 2)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων ανά έξυπνο μετρητή:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
smartMeter17	9000	9000	6000
smartMeter18	80	80	70
smartMeter19	12000	9000	6000
smartMeter20	12000	9000	6000
smartMeter21	9000	9000	9000
smartMeter22	12000	9000	6000
smartMeter23	12000	9000	6000
smartMeter24	12050	9050	6050
smartMeter25	9000	9000	9000
smartMeter26	80	80	70
smartMeter27	12000	9000	9000
smartMeter28	9000	9000	6000
smartMeter29	9000	9000	6000
smartMeter30	12000	12000	9000
smartMeter31	12000	9000	9000
smartMeter32	12000	12000	9000

Πίνακας 8-19 Εξερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 2)

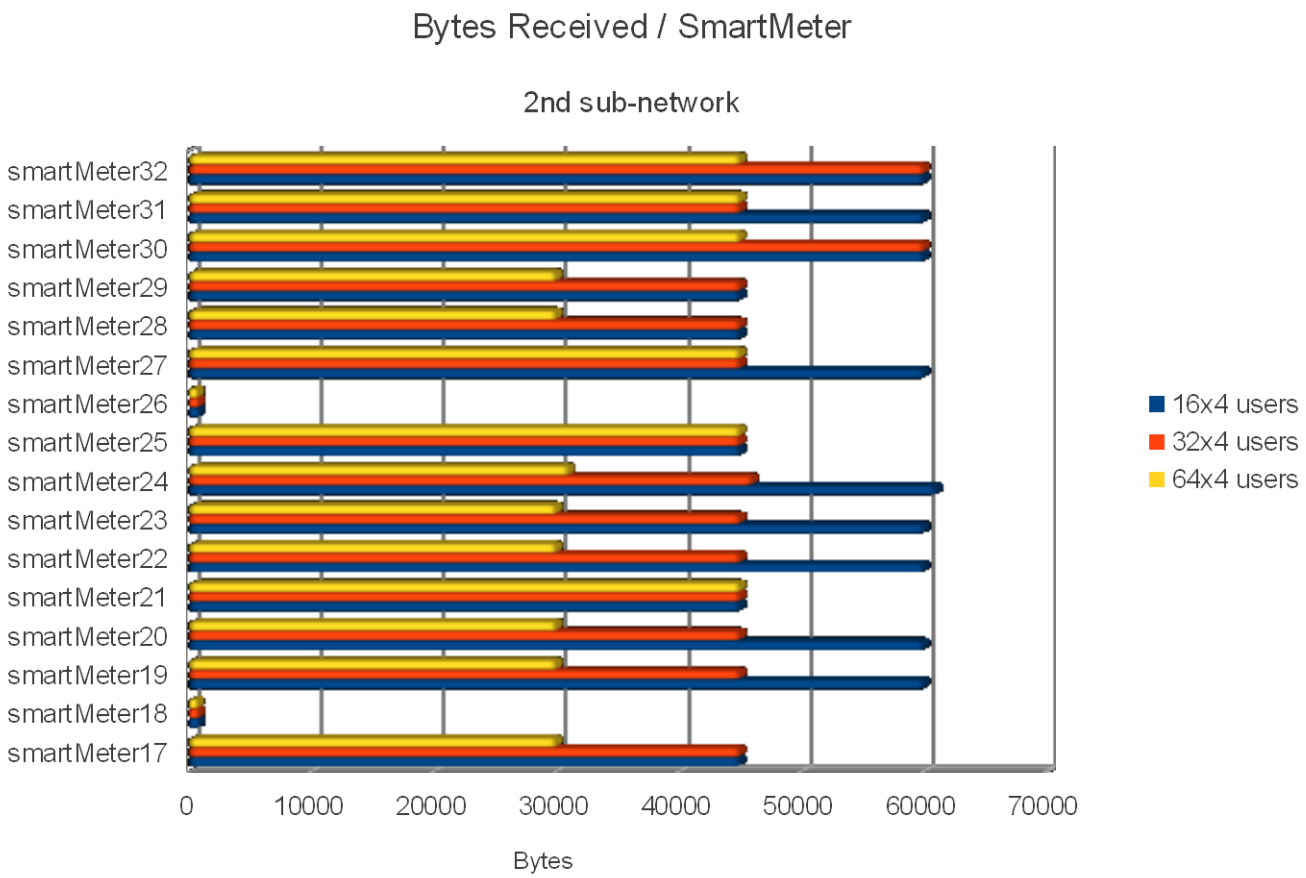
Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι έξυπνοι μετρητές της γειτονιάς είχαν από 2 έως 4 λήψεις δεδομένων από το κέντρο ελέγχου.

Ωστόσο, δυο έξυπνοι μετρητές (18 και 26) δέχθηκαν επίθεση και δεν τους επιτράπηκε καμία ανταλλαγή πληροφορίας με το κέντρο ελέγχου.

Επίσης, ένας έξυπνος μετρητής (24) παρουσίασε τεχνικό πρόβλημα και δέχτηκε την τεχνική βοήθεια του κέντρου ελέγχου.

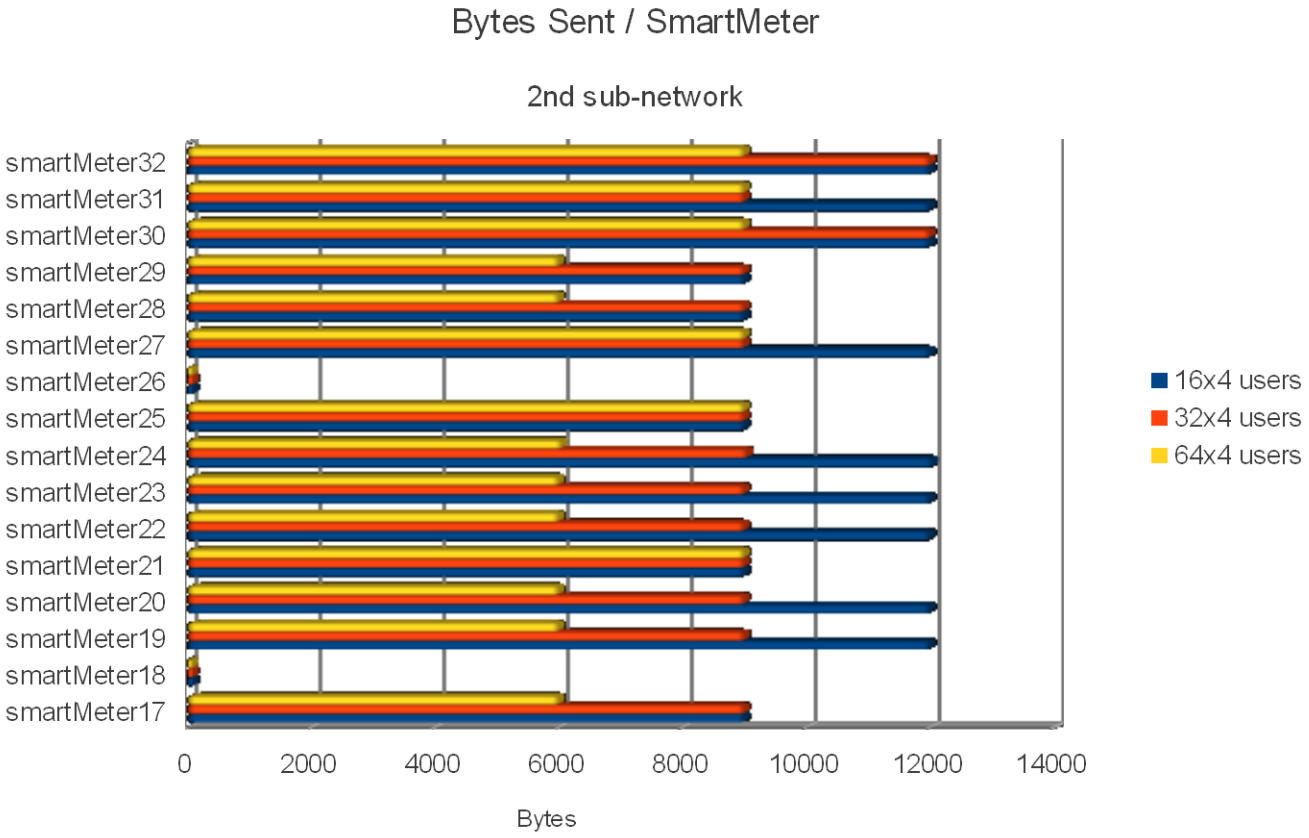
Τέλος, διαπιστώνεται ότι, καθώς αυξάνουν οι χρήστες, μειώνεται η ποσότητα δεδομένων που εισέρχεται στους μετρητές από το κέντρο ελέγχου. Αυτό οφείλεται στο γεγονός ότι, αν δεν καρποφορήσει η επιτυχής αναζήτηση του έξυπνου μετρητή την προκαθορισμένη χρονική στιγμή (π.χ. λόγω συμφόρησης δικτύου), τότε αναζητείται εκ νέου στην επόμενη προκαθορισμένη χρονική στιγμή (μετά από 30 δευτερόλεπτα).

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων ανά έξυπνο μετρητή:



Γράφημα 8-18 Εισερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 2)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων ανά έξυπνο μετρητή:



Γράφημα 8-19 Εξερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 2)

3η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων ανά έξυπνο μετρητή:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
smartMeter33	60000	60000	30000
smartMeter34	800	600	800
smartMeter35	60000	60000	30000
smartMeter36	60000	45000	30000
smartMeter37	60000	45000	30000
smartMeter38	45000	45000	30000
smartMeter39	60000	60000	45000
smartMeter40	61000	46000	31000
smartMeter41	60000	45000	30000
smartMeter42	60000	45000	45000
smartMeter43	60000	45000	45000
smartMeter44	800	800	600
smartMeter45	45000	45000	45000
smartMeter46	60000	45000	30000
smartMeter47	60000	60000	45000
smartMeter48	60000	45000	45000

Πίνακας 8-20 Εισερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 3)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων ανά έξυπνο μετρητή:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
smartMeter33	12000	12000	6000
smartMeter34	80	60	80
smartMeter35	12000	12000	6000
smartMeter36	12000	9000	6000
smartMeter37	12000	9000	6000
smartMeter38	9000	9000	6000
smartMeter39	12000	12000	9000
smartMeter40	12050	9050	6050
smartMeter41	12000	9000	6000
smartMeter42	12000	9000	9000
smartMeter43	12000	9000	9000
smartMeter44	80	80	60
smartMeter45	9000	9000	9000
smartMeter46	12000	9000	6000
smartMeter47	12000	12000	9000
smartMeter48	12000	9000	9000

Πίνακας 8-21 Εξερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 3)

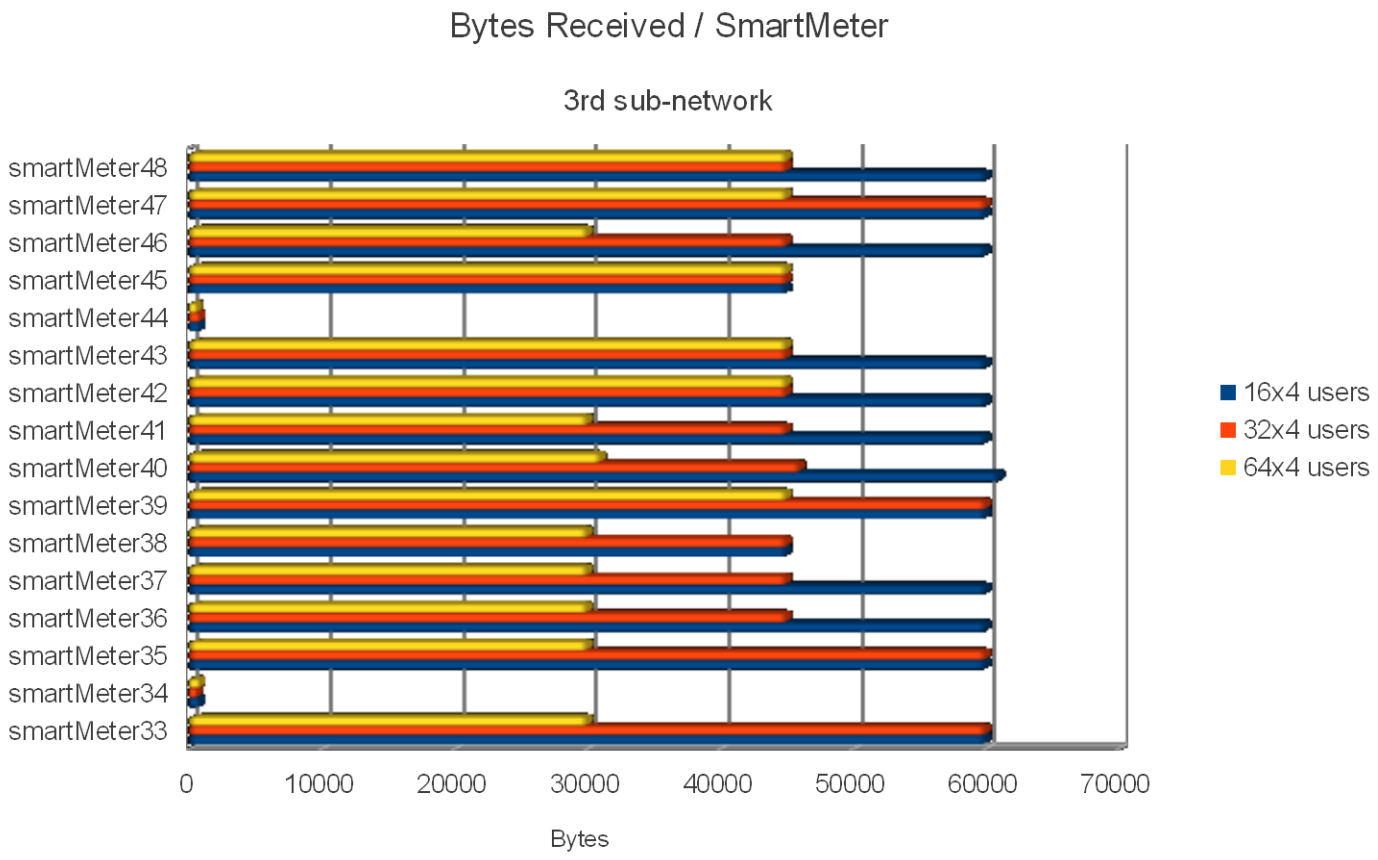
Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι έξυπνοι μετρητές της γειτονιάς είχαν από 2 έως 4 λήψεις δεδομένων από το κέντρο ελέγχου.

Ωστόσο, δυο έξυπνοι μετρητές (34 και 44) δέχθηκαν επίθεση και δεν τους επιτράπηκε καμία ανταλλαγή πληροφορίας με το κέντρο ελέγχου.

Επίσης, ένας έξυπνος μετρητής (40) παρουσίασε τεχνικό πρόβλημα και δέχτηκε την τεχνική βοήθεια του κέντρου ελέγχου.

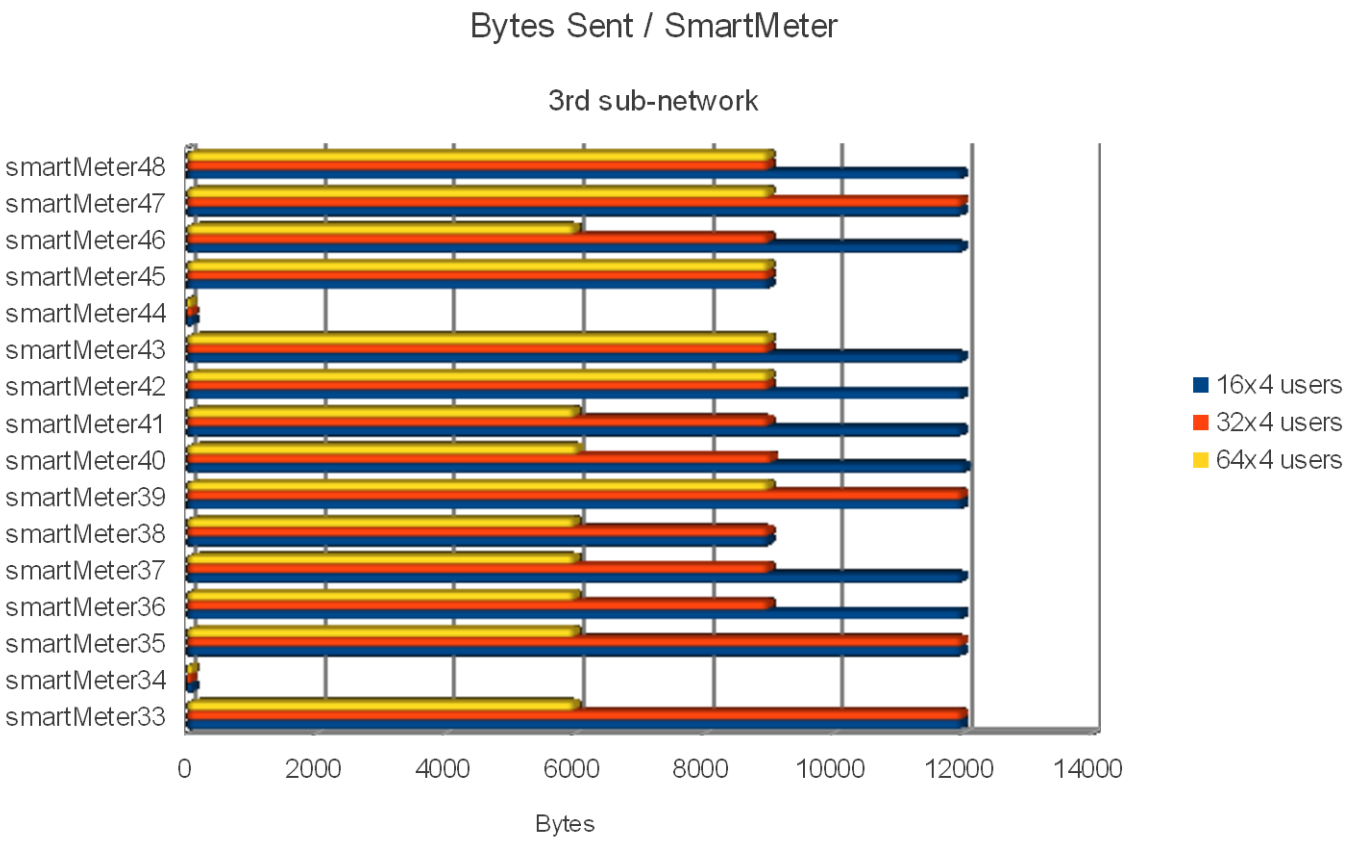
Τέλος, διαπιστώνεται ότι, καθώς αυξάνουν οι χρήστες, μειώνεται η ποσότητα δεδομένων που εισέρχεται στους μετρητές από το κέντρο ελέγχου. Αυτό οφείλεται στο γεγονός ότι, αν δεν καρποφορήσει η επιτυχής αναζήτηση του έξυπνου μετρητή την προκαθορισμένη χρονική στιγμή (π.χ. λόγω συμφόρησης δικτύου), τότε αναζητείται εκ νέου στην επόμενη προκαθορισμένη χρονική στιγμή (μετά από 30 δευτερόλεπτα).

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων ανά έξυπνο μετρητή:



Γράφημα 8-20 Εισερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 3)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων ανά έξυπνο μετρητή:



Γράφημα 8-21 Εξερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 3)

4η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων ανά έξυπνο μετρητή:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
smartMeter49	45000	45000	30000
smartMeter50	60000	45000	45000
smartMeter51	60000	60000	45000
smartMeter52	60000	45000	45000
smartMeter53	60000	45000	30000
smartMeter54	60000	60000	45000
smartMeter55	800	800	600
smartMeter56	60000	45000	30000
smartMeter57	61000	61000	46000
smartMeter58	60000	45000	45000
smartMeter59	60000	45000	30000
smartMeter60	800	600	500
smartMeter61	60000	45000	30000
smartMeter62	45000	45000	45000
smartMeter63	60000	45000	30000
smartMeter64	45000	45000	30000

Πίνακας 8-22 Εισερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 4)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων ανά έξυπνο μετρητή:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
smartMeter49	9000	9000	6000
smartMeter50	12000	9000	9000
smartMeter51	12000	12000	9000
smartMeter52	12000	9000	9000
smartMeter53	12000	9000	6000
smartMeter54	12000	12000	9000
smartMeter55	80	80	60
smartMeter56	12000	9000	6000
smartMeter57	12050	12050	9050
smartMeter58	12000	9000	9000
smartMeter59	12000	9000	6000
smartMeter60	80	60	50
smartMeter61	12000	9000	6000
smartMeter62	9000	9000	9000
smartMeter63	12000	9000	6000
smartMeter64	9000	9000	6000

Πίνακας 8-23 Εξερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 4)

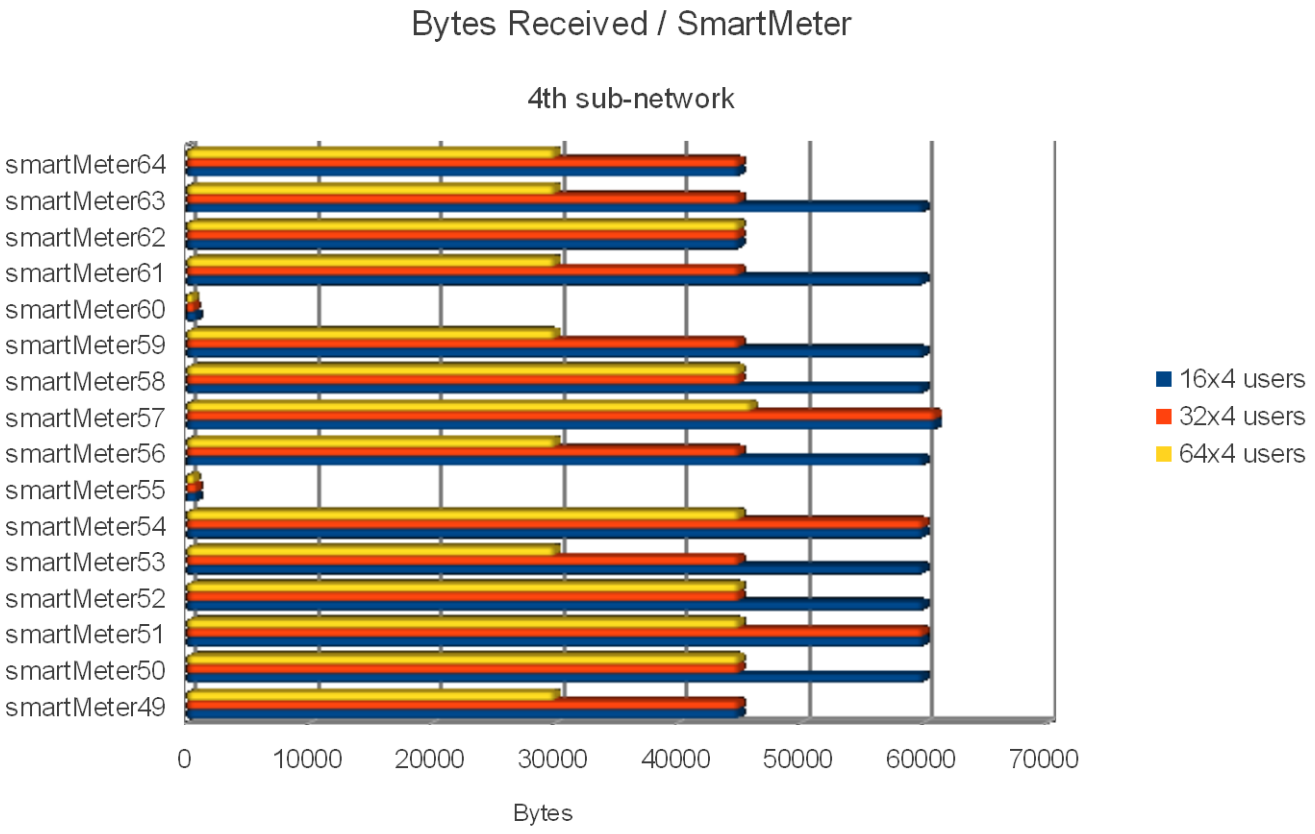
Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι έξυπνοι μετρητές της γειτονιάς είχαν από 2 έως 4 λήψεις δεδομένων από το κέντρο ελέγχου.

Ωστόσο, δυο έξυπνοι μετρητές (55 και 60) δέχθηκαν επίθεση και δεν τους επιτράπηκε καμία ανταλλαγή πληροφορίας με το κέντρο ελέγχου.

Επίσης, ένας έξυπνος μετρητής (57) παρουσίασε τεχνικό πρόβλημα και δέχτηκε την τεχνική βοήθεια του κέντρου ελέγχου.

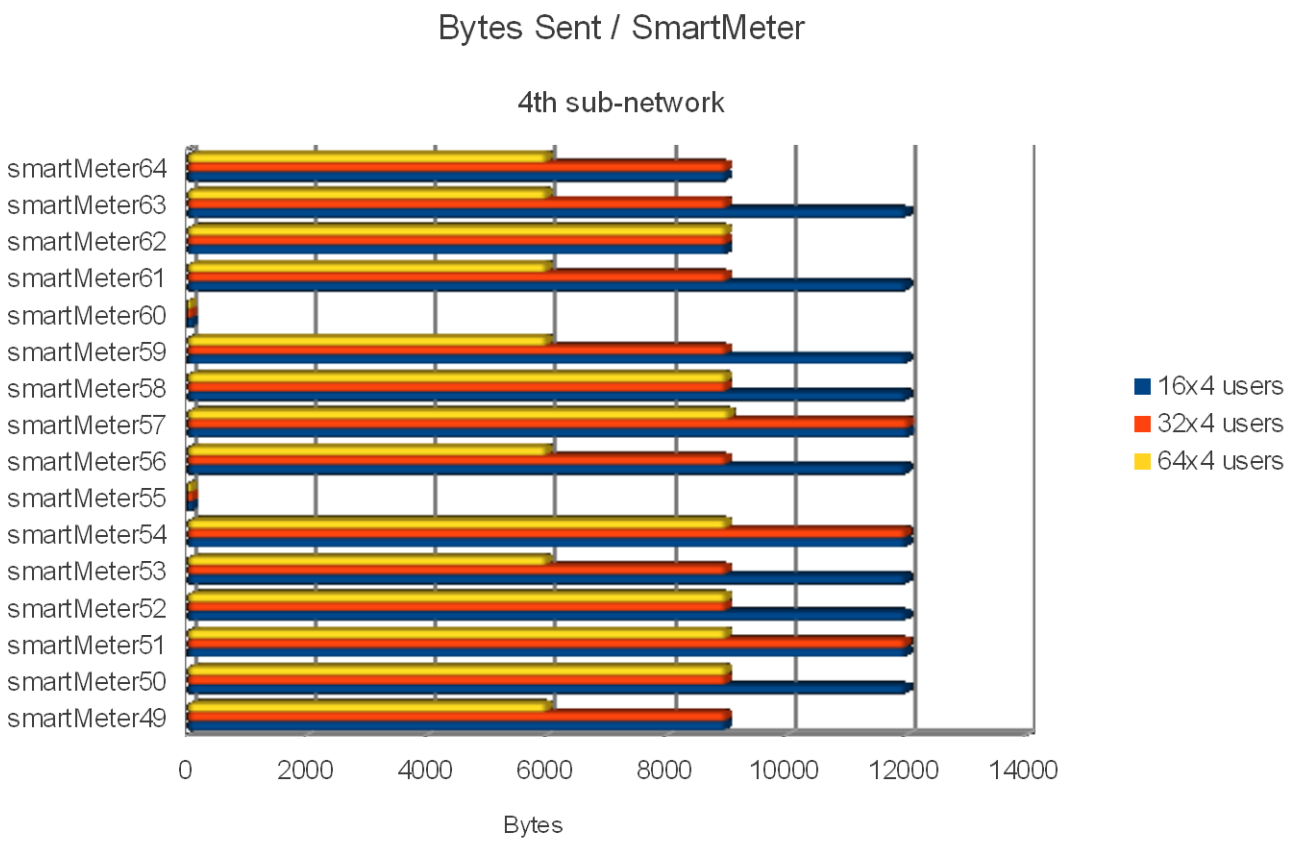
Τέλος, διαπιστώνεται ότι, καθώς αυξάνουν οι χρήστες, μειώνεται η ποσότητα δεδομένων που εισέρχεται στους μετρητές από το κέντρο ελέγχου. Αυτό οφείλεται στο γεγονός ότι, αν δεν καρποφορήσει η επιτυχής αναζήτηση του έξυπνου μετρητή την προκαθορισμένη χρονική στιγμή (π.χ. λόγω συμφόρησης δικτύου), τότε αναζητείται εκ νέου στην επόμενη προκαθορισμένη χρονική στιγμή (μετά από 30 δευτερόλεπτα).

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων ανά έξυπνο μετρητή:



Γράφημα 8-22 Εισερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 4)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων ανά έξυπνο μετρητή:



Γράφημα 8-23 Εξερχόμενα δεδομένα / έξυπνο μετρητή (υποδίκτυο 4)

8.4.4. *Ποσότητα εισερχόμενων / εξερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη*

Τα στοιχεία που λαμβάνουν μέρος σε κάθε υποδίκτυο είναι οι 16 κινούμενοι χρήστες, ο αριθμός των οποίων διπλασιάζεται και τετραπλασιάζεται σύμφωνα με τα αντίστοιχα σενάρια (Users{1..64}).

Τα δεδομένα HTTP που μπορεί να αποδεχτεί / αποστείλει ένας κινούμενος χρήστης είναι μια απόκριση HTTP, μεγέθους 30000 Bytes, και μια αίτηση HTTP, μεγέθους 5000 Bytes, αντίστοιχα. Η ανταλλαγή αυτή πληροφοριών γίνεται μεταξύ των χρηστών και απομακρυσμένων εξυπηρετητών HTTP, όταν οι χρήστες επιθυμούν να περιηγηθούν στο διαδίκτυο.

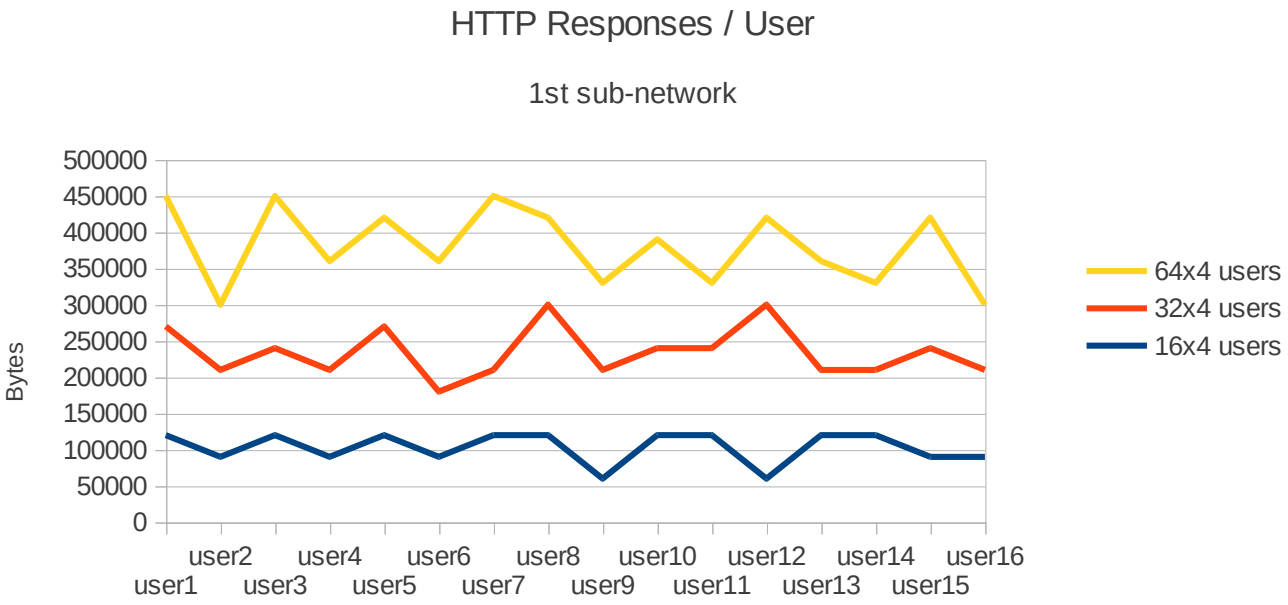
1*η γειτονιά-υποδίκτυο*

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user1	120000	150000	180000
user2	90000	120000	90000
user3	120000	120000	210000
user4	90000	120000	150000
user5	120000	150000	150000
user6	90000	90000	180000
user7	120000	90000	240000
user8	120000	180000	120000
user9	60000	150000	120000
user10	120000	120000	150000
user11	120000	120000	90000
user12	60000	240000	120000
user13	120000	90000	150000
user14	120000	90000	120000
user15	90000	150000	180000
user16	90000	120000	90000

Πίνακας 8-24 Εισερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 1)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:



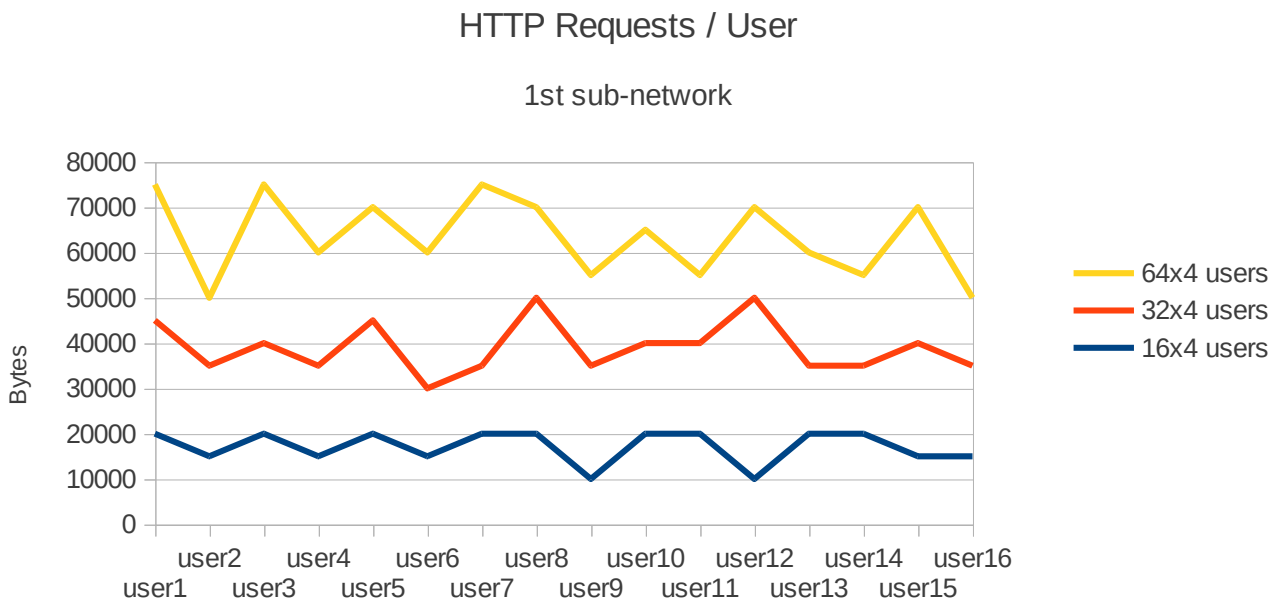
Γράφημα 8-24 Εισερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 1)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user1	20000	25000	30000
user2	15000	20000	15000
user3	20000	20000	35000
user4	15000	20000	25000
user5	20000	25000	25000
user6	15000	15000	30000
user7	20000	15000	40000
user8	20000	30000	20000
user9	10000	25000	20000
user10	20000	20000	25000
user11	20000	20000	15000
user12	10000	40000	20000
user13	20000	15000	25000
user14	20000	15000	20000
user15	15000	25000	30000
user16	15000	20000	15000

Πίνακας 8-25 Εξερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 1)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:



Γράφημα 8-25 Εξερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 1)

Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι κινούμενοι χρήστες της γειτονιάς είχαν από 3 έως 8 ανταλλαγές δεδομένων HTTP με τον απομακρυσμένο εξυπηρετητή HTTP.

Ακόμη, διαπιστώνεται ότι, καθώς αυξάνουν οι χρήστες, η ποσότητα δεδομένων που ανταλλάσσεται δεν αυξάνεται αναλογικά της αύξησης των χρηστων στην εφαρμογή των διαφορετικών σεναρίων. Για αυτό και παρατηρείται μεγαλύτερη διακύμανση στην ποσότητα δεδομένων ανταλλαγής στο σενάριο των 64x4 χρηστών. Αυτό οφείλεται στο γεγονός ότι, αν δεν καρποφορήσει η επιτυχής αναζήτηση του απομακρυσμένου εξυπηρετητή την επιθυμητή χρονική στιγμή (π.χ. λόγω συμφόρησης δικτύου), τότε αναζητάται εκ νέου μετά από 30 δευτερόλεπτα, που αποτελεί έναν εκτιμώμενο απαιτούμενο χρόνο για να αποσυμφορηθεί το δίκτυο.

Τέλος, φαίνεται ότι δεν γίνονται ανταλλαγές δεδομένων HTTP μεταξύ των χρηστών, αφού κάθε εξερχόμενη πληροφορία διαθέτει την ανάλογη και αναμενόμενη εισερχόμενη πληροφορία ως απόκριση. Οι μοναδικοί εξυπηρετητές HTTP του δικτύου προσομοίωσης είναι οι server1 και server2.

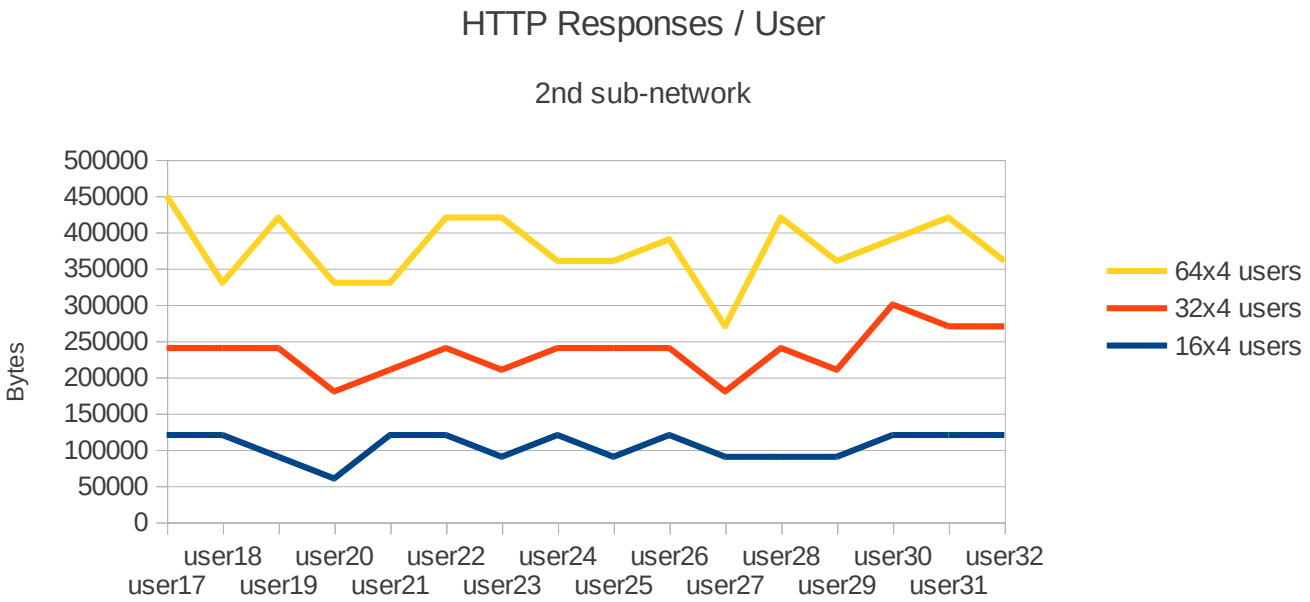
2*η γειτονιά-υποδίκτυο*

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user17	120000	120000	210000
user18	120000	120000	90000
user19	90000	150000	180000
user20	60000	120000	150000
user21	120000	90000	120000
user22	120000	120000	180000
user23	90000	120000	210000
user24	120000	120000	120000
user25	90000	150000	120000
user26	120000	120000	150000
user27	90000	90000	90000
user28	90000	150000	180000
user29	90000	120000	150000
user30	120000	180000	90000
user31	120000	150000	150000
user32	120000	150000	90000

Πίνακας 8-26 Εισερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 2)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:



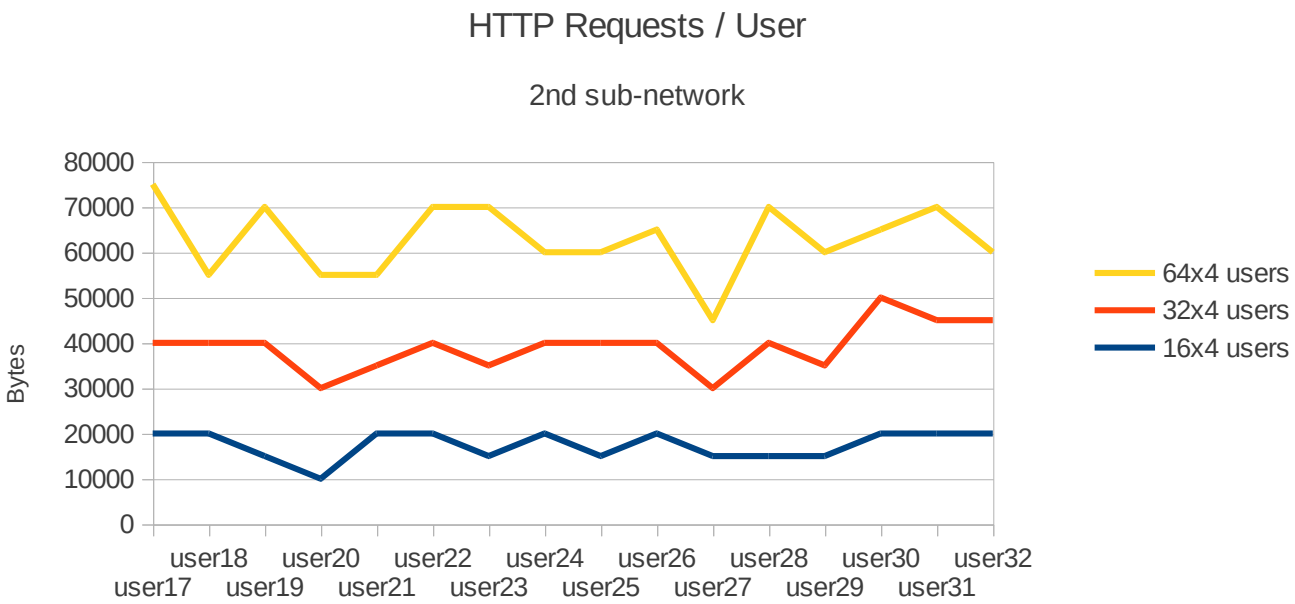
Γράφημα 8-26 Εισερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 2)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user17	20000	20000	35000
user18	20000	20000	15000
user19	15000	25000	30000
user20	10000	20000	25000
user21	20000	15000	20000
user22	20000	20000	30000
user23	15000	20000	35000
user24	20000	20000	20000
user25	15000	25000	20000
user26	20000	20000	25000
user27	15000	15000	15000
user28	15000	25000	30000
user29	15000	20000	25000
user30	20000	30000	15000
user31	20000	25000	25000
user32	20000	25000	15000

Πίνακας 8-27 Εξερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 2)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:



Γράφημα 8-27 Εξερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 2)

Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι κινούμενοι χρήστες της γειτονιάς είχαν από 3 έως 7 ανταλλαγές δεδομένων HTTP με τον απομακρυσμένο εξυπηρετητή HTTP.

Ακόμη, διαπιστώνεται ότι, καθώς αυξάνουν οι χρήστες, η ποσότητα δεδομένων που ανταλλάσσεται δεν αυξάνεται αναλογικά της αύξησης των χρηστων στην εφαρμογή των διαφορετικών σεναρίων. Για αυτό και παρατηρείται μεγαλύτερη διακύμανση στην ποσότητα δεδομένων ανταλλαγής στο σενάριο των 64x4 χρηστών. Αυτό οφείλεται στο γεγονός ότι, αν δεν καρποφορήσει η επιτυχής αναζήτηση του απομακρυσμένου εξυπηρετητή την επιθυμητή χρονική στιγμή (π.χ. λόγω συμφόρησης δικτύου), τότε αναζητάται εκ νέου μετά από 30 δευτερόλεπτα, που αποτελεί έναν εκτιμώμενο απαιτούμενο χρόνο για να αποσυμφορηθεί το δίκτυο.

Τέλος, φαίνεται ότι δεν γίνονται ανταλλαγές δεδομένων HTTP μεταξύ των χρηστών, αφού κάθε εξερχόμενη πληροφορία διαθέτει την ανάλογη και αναμενόμενη εισερχόμενη πληροφορία ως απόκριση. Οι μοναδικοί εξυπηρετητές HTTP του δικτύου προσομοίωσης είναι οι server1 και server2.

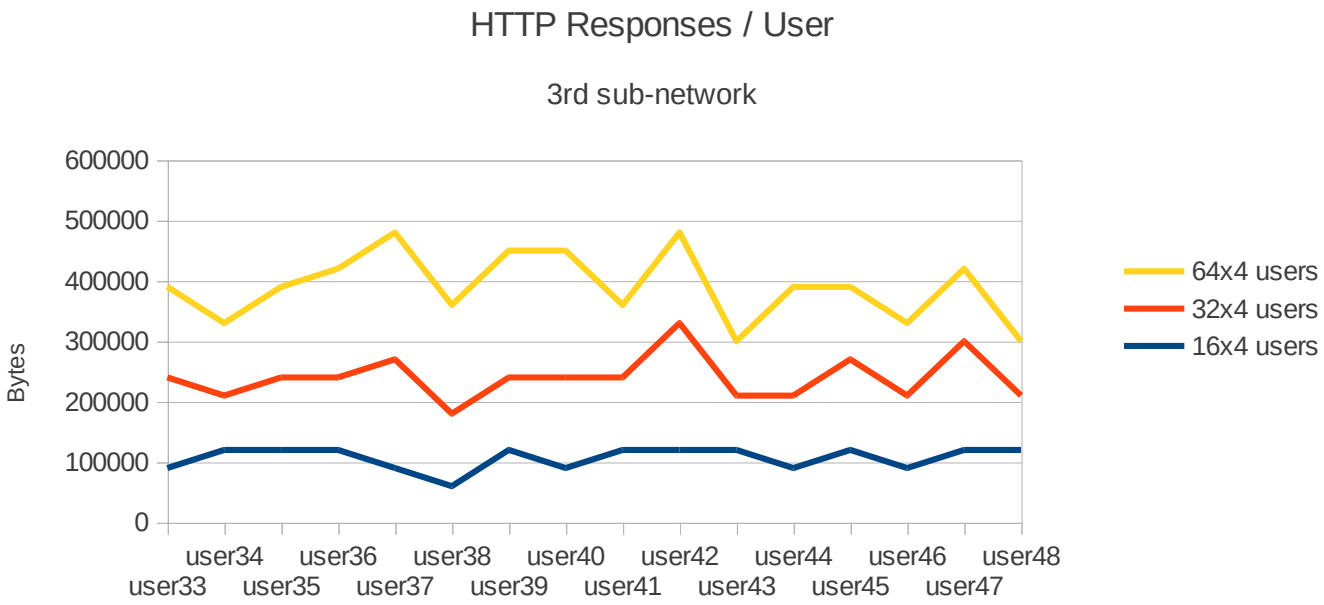
3*η γειτονιά-υποδίκτυο*

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user33	90000	150000	150000
user34	120000	90000	120000
user35	120000	120000	150000
user36	120000	120000	180000
user37	90000	180000	210000
user38	60000	120000	180000
user39	120000	120000	210000
user40	90000	150000	210000
user41	120000	120000	120000
user42	120000	210000	150000
user43	120000	90000	90000
user44	90000	120000	180000
user45	120000	150000	120000
user46	90000	120000	120000
user47	120000	180000	120000
user48	120000	90000	90000

Πίνακας 8-28 Εισερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 3)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:



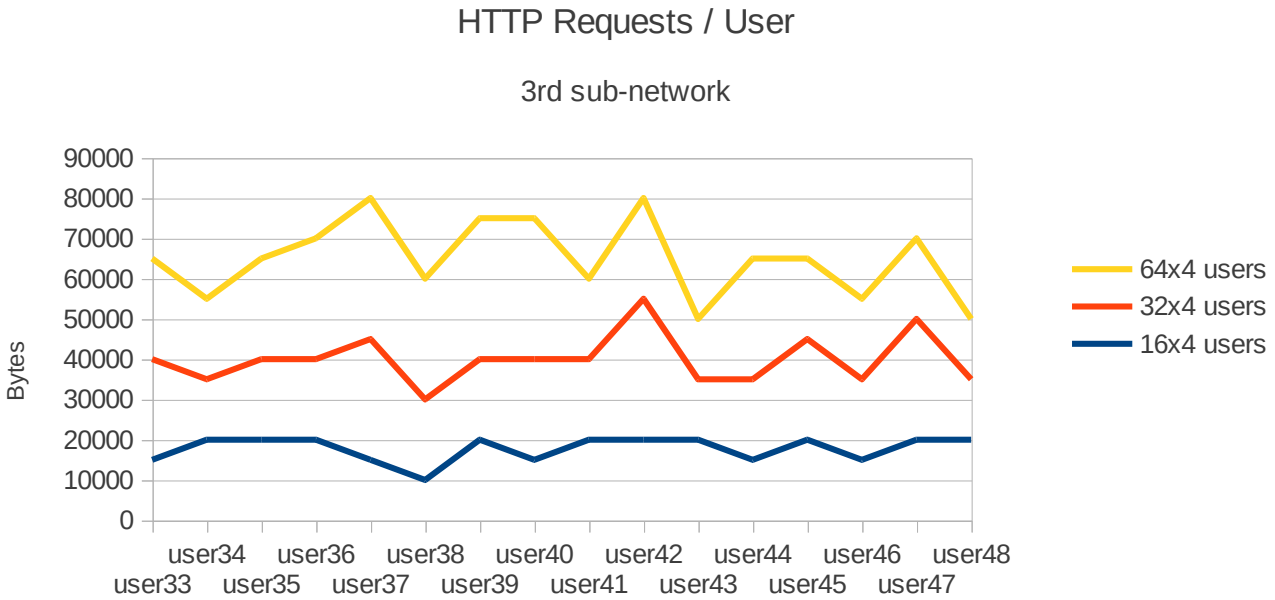
Γράφημα 8-28 Εισερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 3)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user33	15000	25000	25000
user34	20000	15000	20000
user35	20000	20000	25000
user36	20000	20000	30000
user37	15000	30000	35000
user38	10000	20000	30000
user39	20000	20000	35000
user40	15000	25000	35000
user41	20000	20000	20000
user42	20000	35000	25000
user43	20000	15000	15000
user44	15000	20000	30000
user45	20000	25000	20000
user46	15000	20000	20000
user47	20000	30000	20000
user48	20000	15000	15000

Πίνακας 8-29 Εξερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 3)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:



Γράφημα 8-29 Εξερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 3)

Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι κινούμενοι χρήστες της γειτονιάς είχαν από 3 έως 7 ανταλλαγές δεδομένων HTTP με τον απομακρυσμένο εξυπηρετητή HTTP.

Ακόμη, διαπιστώνεται ότι, καθώς αυξάνουν οι χρήστες, η ποσότητα δεδομένων που ανταλλάσσεται δεν αυξάνεται αναλογικά της αύξησης των χρηστων στην εφαρμογή των διαφορετικών σεναρίων. Για αυτό και παρατηρείται μεγαλύτερη διακύμανση στην ποσότητα δεδομένων ανταλλαγής στο σενάριο των 64x4 χρηστών. Αυτό οφείλεται στο γεγονός ότι, αν δεν καρποφορήσει η επιτυχής αναζήτηση του απομακρυσμένου εξυπηρετητή την επιθυμητή χρονική στιγμή (π.χ. λόγω συμφόρησης δικτύου), τότε αναζητάται εκ νέου μετά από 30 δευτερόλεπτα, που αποτελεί έναν εκτιμώμενο απαιτούμενο χρόνο για να αποσυμφορηθεί το δίκτυο.

Τέλος, φαίνεται ότι δεν γίνονται ανταλλαγές δεδομένων HTTP μεταξύ των χρηστών, αφού κάθε εξερχόμενη πληροφορία διαθέτει την ανάλογη και αναμενόμενη εισερχόμενη πληροφορία ως απόκριση. Οι μοναδικοί εξυπηρετητές HTTP του δικτύου προσομοίωσης είναι οι server1 και server2.

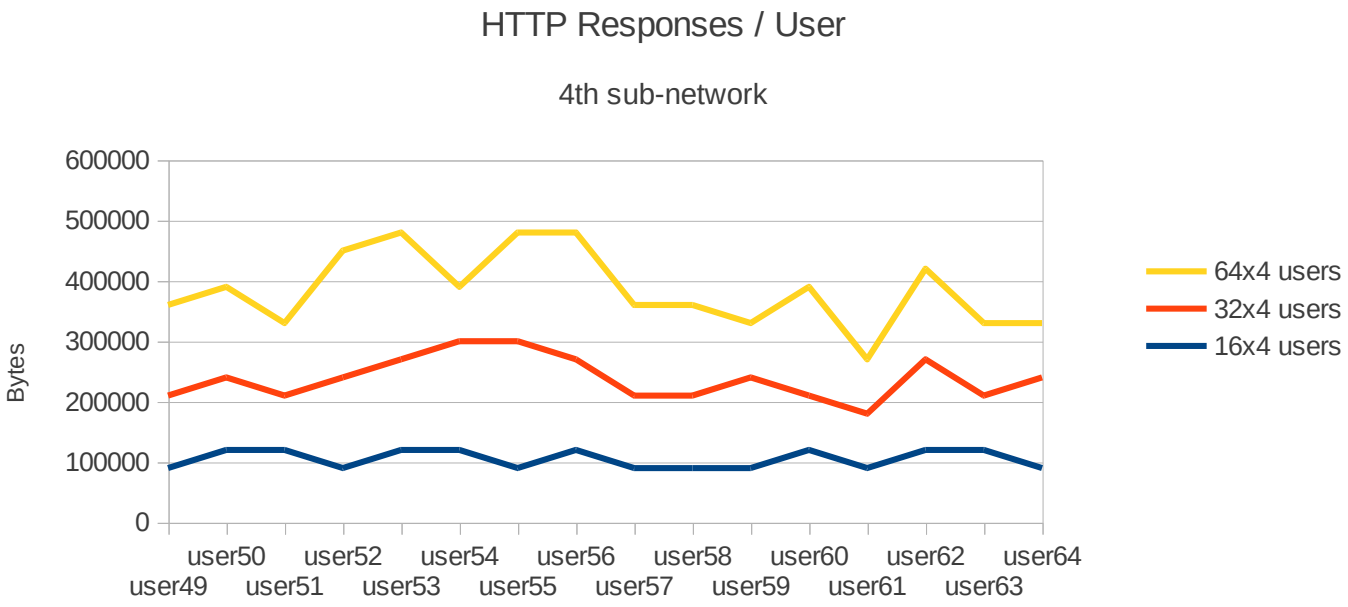
4η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user49	90000	120000	150000
user50	120000	120000	150000
user51	120000	90000	120000
user52	90000	150000	210000
user53	120000	150000	210000
user54	120000	180000	90000
user55	90000	210000	180000
user56	120000	150000	210000
user57	90000	120000	150000
user58	90000	120000	150000
user59	90000	150000	90000
user60	120000	90000	180000
user61	90000	90000	90000
user62	120000	150000	150000
user63	120000	90000	120000
user64	90000	150000	90000

Πίνακας 8-30 Εισερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 4)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:



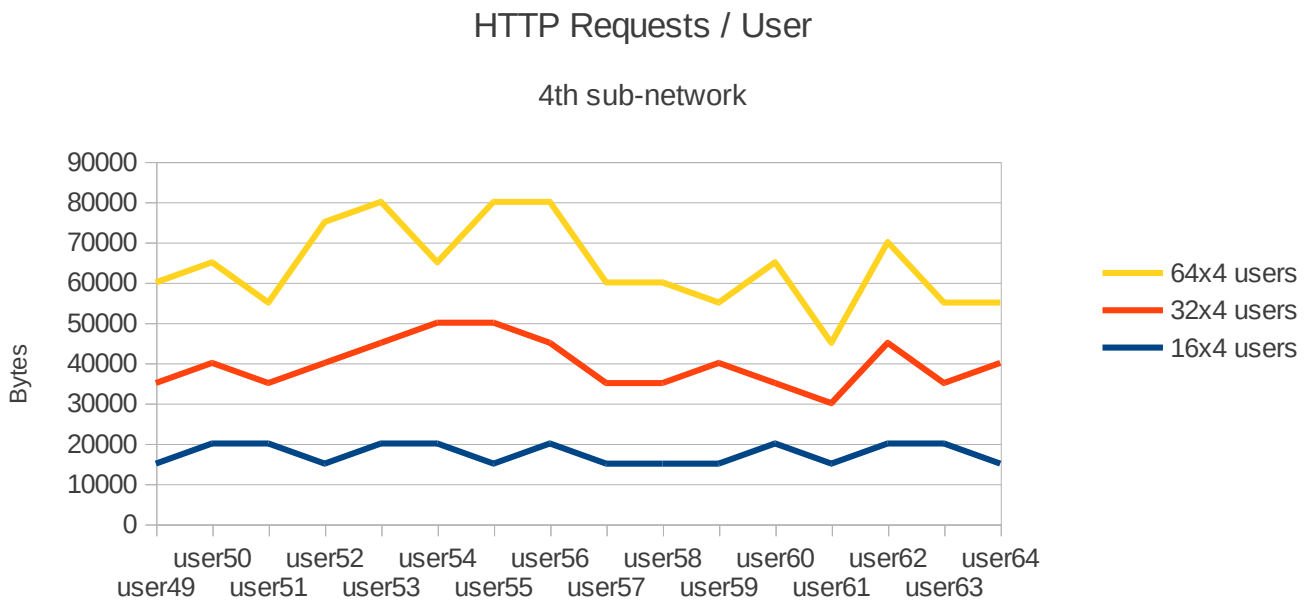
Γράφημα 8-30 Εισερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 4)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user49	15000	20000	25000
user50	20000	20000	25000
user51	20000	15000	20000
user52	15000	25000	35000
user53	20000	25000	35000
user54	20000	30000	15000
user55	15000	35000	30000
user56	20000	25000	35000
user57	15000	20000	25000
user58	15000	20000	25000
user59	15000	25000	15000
user60	20000	15000	30000
user61	15000	15000	15000
user62	20000	25000	25000
user63	20000	15000	20000
user64	15000	25000	15000

Πίνακας 8-31 Εξερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 4)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων HTTP ανά κινούμενο χρήστη:



Γράφημα 8-31 Εξερχόμενα δεδομένα HTTP / χρήστη (υποδίκτυο 4)

Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι κινούμενοι χρήστες της γειτονιάς είχαν από 3 έως 7 ανταλλαγές δεδομένων HTTP με τον απομακρυσμένο εξυπηρετητή HTTP.

Ακόμη, διαπιστώνεται ότι, καθώς αυξάνουν οι χρήστες, η ποσότητα δεδομένων που ανταλλάσσεται δεν αυξάνεται αναλογικά της αύξησης των χρηστων στην εφαρμογή των διαφορετικών σεναρίων. Για αυτό και παρατηρείται μεγαλύτερη διακύμανση στην ποσότητα δεδομένων ανταλλαγής στο σενάριο των 64x4 χρηστών. Αυτό οφείλεται στο γεγονός ότι, αν δεν καρποφορήσει η επιτυχής αναζήτηση του απομακρυσμένου εξυπηρετητή την επιθυμητή χρονική στιγμή (π.χ. λόγω συμφόρησης δικτύου), τότε αναζητάται εκ νέου μετά από 30 δευτερόλεπτα, που αποτελεί έναν εκτιμώμενο απαιτούμενο χρόνο για να αποσυμφορηθεί το δίκτυο.

Τέλος, φαίνεται ότι δεν γίνονται ανταλλαγές δεδομένων HTTP μεταξύ των χρηστών, αφού κάθε εξερχόμενη πληροφορία διαθέτει την ανάλογη και αναμενόμενη εισερχόμενη πληροφορία ως απόκριση. Οι μοναδικοί εξυπηρετητές HTTP του δικτύου προσομοίωσης είναι οι server1 και server2.

8.4.5. Ποσότητα εισερχόμενων / εξερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη

Τα στοιχεία που λαμβάνουν μέρος σε κάθε υποδίκτυο είναι οι 16 κινούμενοι χρήστες, ο αριθμός των οποίων διπλασιάζεται και τετραπλασιάζεται σύμφωνα με τα αντίστοιχα σενάρια (Users{1..64}).

Τα δεδομένα VideoStream που μπορεί να αποδεχτεί / αποστείλει ένας κινούμενος χρήστης είναι μια απόκριση / αίτηση VideoStream, μεγέθους βίντεο 200000 Bytes σε 4 πακέτα των 50000 Bytes. Η ανταλλαγή αυτή πληροφοριών γίνεται μεταξύ των χρηστών και απομακρυσμένων εξυπηρετητών VideoStream αλλά και μόνο μεταξύ των χρηστών, όταν οι χρήστες επιθυμούν να κατεβάσουν ένα βίντεο ή να συνδιαλεχτούν μεταξύ τους με παράλληλη εφαρμογή VideoStream από ένα ή περισσότερους χρήστες.

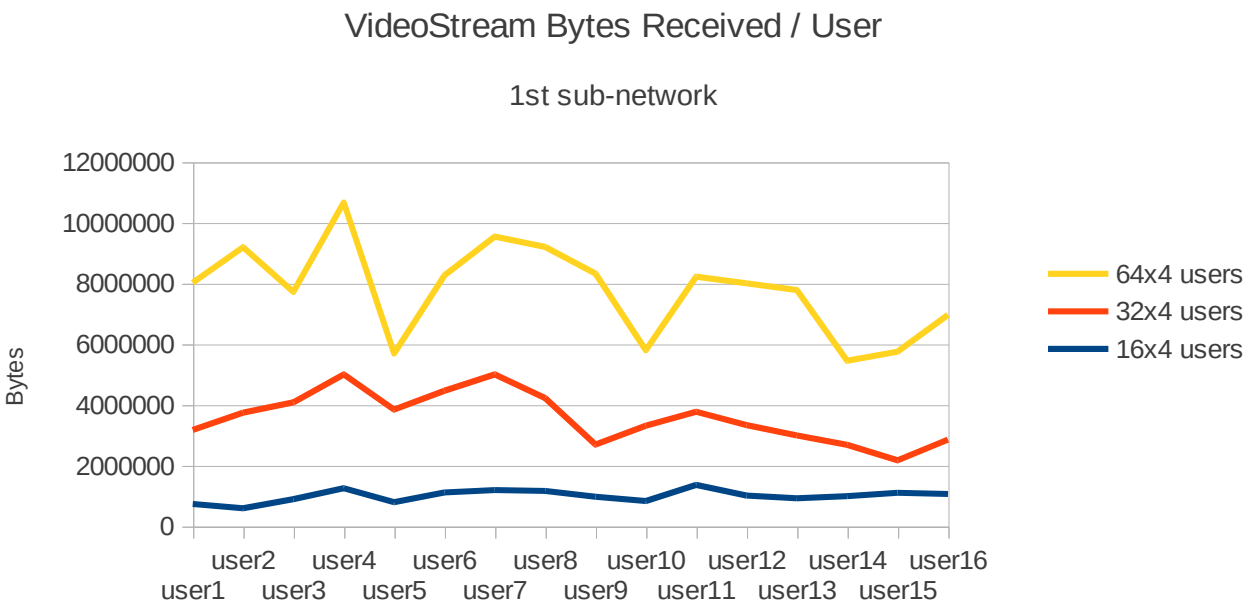
1*η γειτονιά-υποδίκτυο*

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user1	730000	2440000	4850000
user2	590000	3150000	5450000
user3	890000	3190000	3640000
user4	1250000	3750000	5660000
user5	790000	3050000	1850000
user6	1110000	3350000	3800000
user7	1190000	3810000	4540000
user8	1160000	3060000	4980000
user9	970000	1720000	5630000
user10	830000	2480000	2490000
user11	1360000	2410000	4450000
user12	1010000	2320000	4670000
user13	920000	2070000	4790000
user14	990000	1690000	2770000
user15	1100000	1070000	3580000
user16	1060000	1790000	4110000

Πίνακας 8-32 Εισερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 1)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:



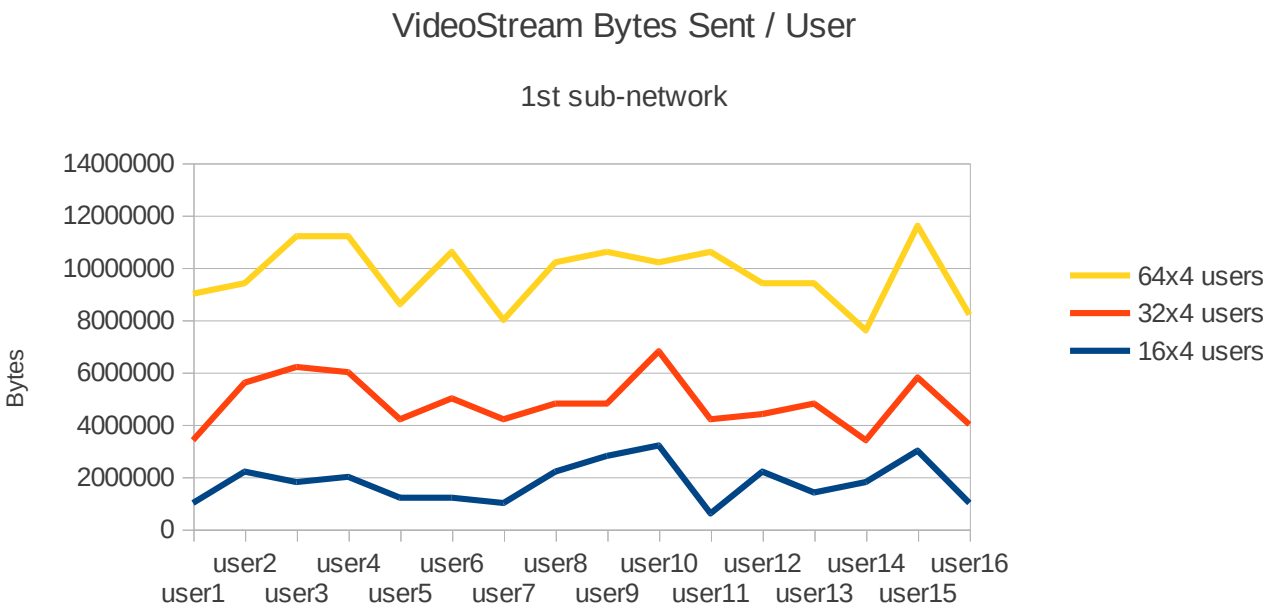
Γράφημα 8-32 Εισερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 1)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user1	1000000	2400000	5600000
user2	2200000	3400000	3800000
user3	1800000	4400000	5000000
user4	2000000	4000000	5200000
user5	1200000	3000000	4400000
user6	1200000	3800000	5600000
user7	1000000	3200000	3800000
user8	2200000	2600000	5400000
user9	2800000	2000000	5800000
user10	3200000	3600000	3400000
user11	600000	3600000	6400000
user12	2200000	2200000	5000000
user13	1400000	3400000	4600000
user14	1800000	1600000	4200000
user15	3000000	2800000	5800000
user16	1000000	3000000	4200000

Πίνακας 8-33 Εξερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 1)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:



Γράφημα 8-33 Εξερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 1)

Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι κινούμενοι χρήστες της γειτονιάς είχαν από 3 έως 29 αναζητήσεις δεδομένων VideoStream είτε στον απομακρυσμένο εξυπηρετητή VideoStream είτε σε άλλον κινούμενο χρήστη.

Ακόμη, διαπιστώνεται μεγαλύτερη διακύμανση στην ποσότητα εισερχόμενων δεδομένων στο σενάριο των 64x4 χρηστών. Αυτό οφείλεται στο γεγονός ότι, λόγω μεγαλύτερης συμφόρησης δικτύου, δεν έχουν φθάσει όλα τα πακέτα βίντεο στον προορισμό τους, αν και έχουν δημιουργηθεί εξαρχής στον αντίστοιχο εξυπηρετητή.

Επίσης, παρατηρείται ιδιαίτερη διακύμανση στην ποσότητα εξερχόμενων δεδομένων και στα 3 διαφορετικά σενάρια αριθμού χρηστών. Αυτό οφείλεται στο γεγονός ότι, η επιλογή των εξυπηρετητών γίνεται κατά τυχαίο τρόπο, με αποτέλεσμα κάποιοι χρήστες να παρουσιάζουν μεγαλύτερη ή μικρότερη προτίμηση από καοιους άλλους.

Τέλος, φαίνεται ότι γίνονται ανταλλαγές δεδομένων VideoStream μεταξύ των χρηστών, αφού υπάρχει εξερχόμενη πληροφορία από τους χρήστες προς εξυπηρέτηση άλλων χρηστών. Αυτό σημαίνει ότι ευνοούνται οι συνεργατικές υπηρεσίες μεταξύ των χρηστών και δεν απαιτείται ολοκληρωτικά η χρήση του απομακρυσμένου εξυπηρετητή.

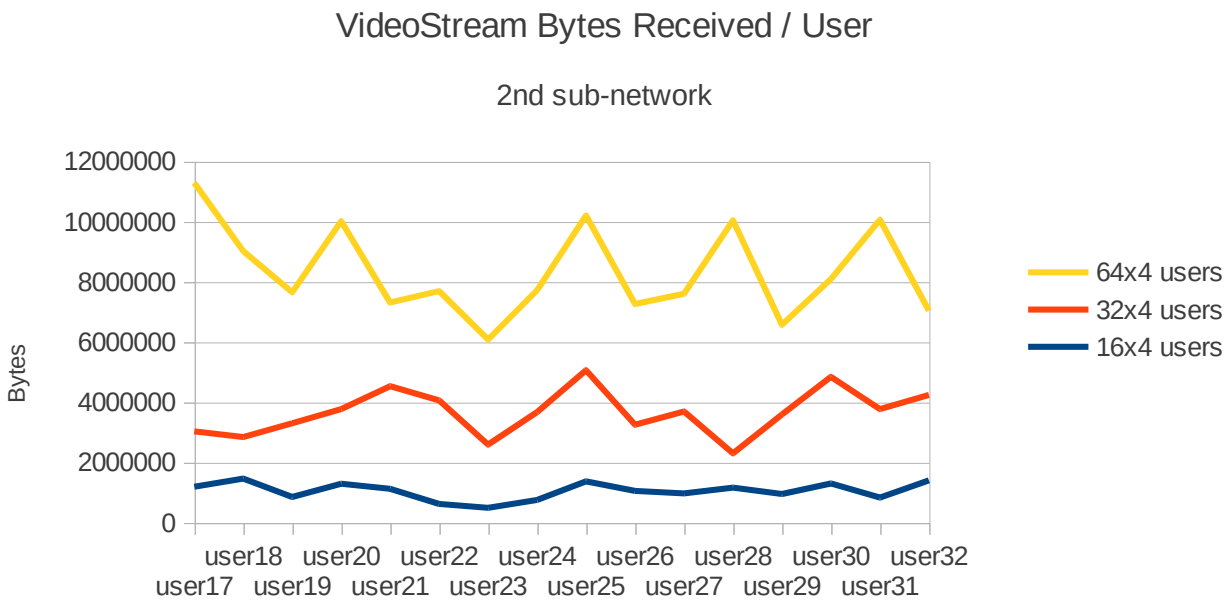
2*η γειτονιά-υποδίκτυο*

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user17	1190000	1840000	8260000
user18	1460000	1380000	6180000
user19	850000	2450000	4350000
user20	1290000	2480000	6240000
user21	1120000	3410000	2780000
user22	620000	3440000	3630000
user23	490000	2100000	3490000
user24	750000	2920000	4050000
user25	1370000	3690000	5140000
user26	1050000	2200000	4010000
user27	970000	2720000	3910000
user28	1160000	1140000	7740000
user29	950000	2640000	2980000
user30	1300000	3540000	3250000
user31	830000	2940000	6290000
user32	1400000	2840000	2800000

Πίνακας 8-34 Εισερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 2)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:



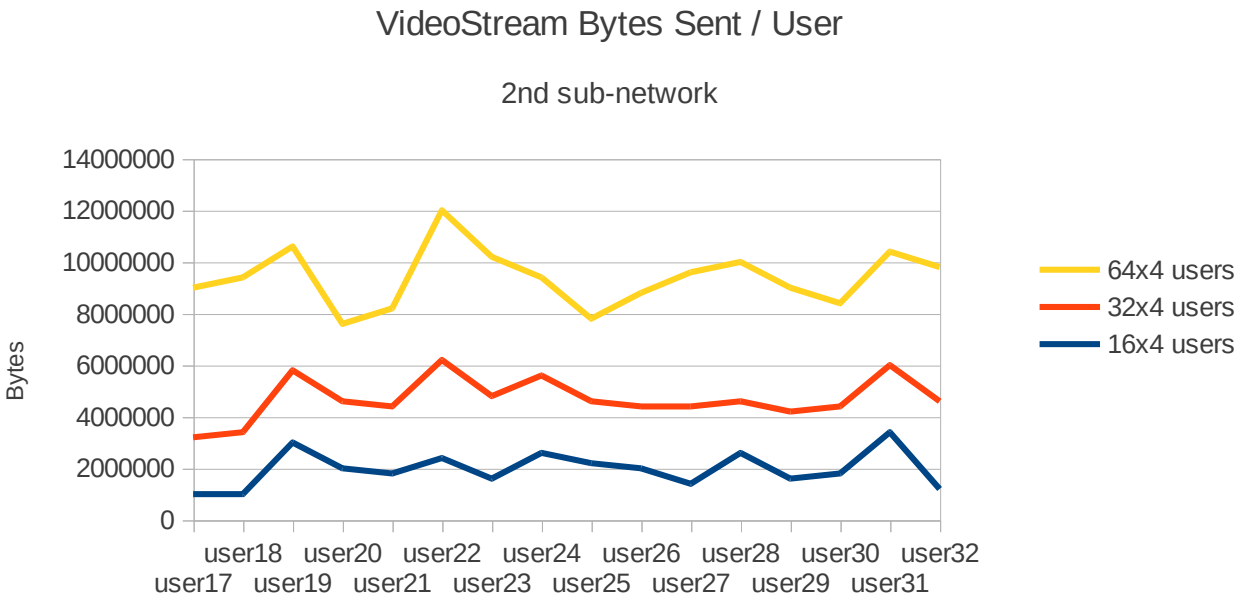
Γράφημα 8-34 Εισερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 2)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user17	1000000	2200000	5800000
user18	1000000	2400000	6000000
user19	3000000	2800000	4800000
user20	2000000	2600000	3000000
user21	1800000	2600000	3800000
user22	2400000	3800000	5800000
user23	1600000	3200000	5400000
user24	2600000	3000000	3800000
user25	2200000	2400000	3200000
user26	2000000	2400000	4400000
user27	1400000	3000000	5200000
user28	2600000	2000000	5400000
user29	1600000	2600000	4800000
user30	1800000	2600000	4000000
user31	3400000	2600000	4400000
user32	1200000	3400000	5200000

Πίνακας 8-35 Εξερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 2)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:



Γράφημα 8-35 Εξερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 2)

Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι κινούμενοι χρήστες της γειτονιάς είχαν από 5 έως 30 αναζητήσεις δεδομένων VideoStream είτε στον απομακρυσμένο εξυπηρετητή VideoStream είτε σε άλλον κινούμενο χρήστη.

Ακόμη, διαπιστώνεται μεγαλύτερη διακύμανση στην ποσότητα εισερχόμενων δεδομένων στο σενάριο των 64x4 χρηστών. Αυτό οφείλεται στο γεγονός ότι, λόγω μεγαλύτερης συμφόρησης δικτύου, δεν έχουν φθάσει όλα τα πακέτα βίντεο στον προορισμό τους, αν και έχουν δημιουργηθεί εξαρχής στον αντίστοιχο εξυπηρετητή.

Επίσης, παρατηρείται ιδιαίτερη διακύμανση στην ποσότητα εξερχόμενων δεδομένων και στα 3 διαφορετικά σενάρια αριθμού χρηστών. Αυτό οφείλεται στο γεγονός ότι, η επιλογή των εξυπηρετητών γίνεται κατά τυχαίο τρόπο, με αποτέλεσμα κάποιοι χρήστες να παρουσιάζουν μεγαλύτερη ή μικρότερη προτίμηση από καοιους άλλους.

Τέλος, φαίνεται ότι γίνονται ανταλλαγές δεδομένων VideoStream μεταξύ των χρηστών, αφού υπάρχει εξερχόμενη πληροφορία από τους χρήστες προς εξυπηρέτηση άλλων χρηστών. Αυτό σημαίνει ότι ευνοούνται οι συνεργατικές υπηρεσίες μεταξύ των χρηστών και δεν απαιτείται ολοκληρωτικά η χρήση του απομακρυσμένου εξυπηρετητή.

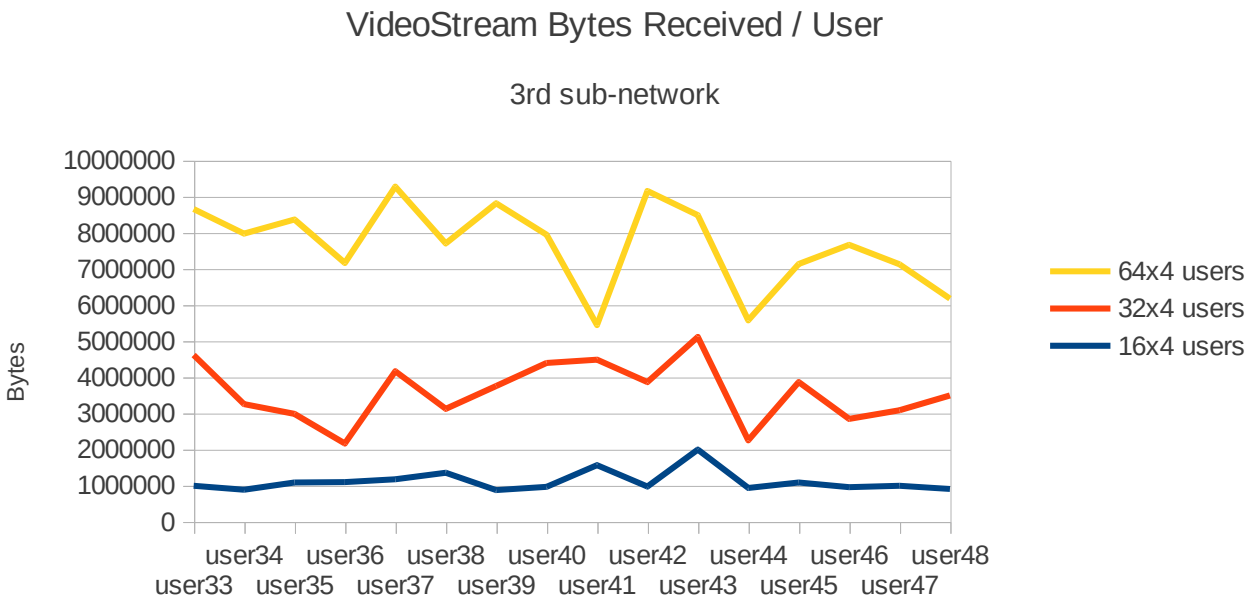
3*η γειτονιά-υποδίκτυο*

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user33	990000	3620000	4040000
user34	880000	2370000	4720000
user35	1080000	1900000	5380000
user36	1090000	1070000	5000000
user37	1170000	2990000	5110000
user38	1350000	1770000	4580000
user39	870000	2880000	5060000
user40	960000	3430000	3550000
user41	1560000	2920000	960000
user42	970000	2890000	5290000
user43	1990000	3120000	3370000
user44	930000	1320000	3320000
user45	1080000	2780000	3270000
user46	950000	1890000	4820000
user47	990000	2090000	4040000
user48	900000	2590000	2680000

Πίνακας 8-36 Εισερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 3)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:



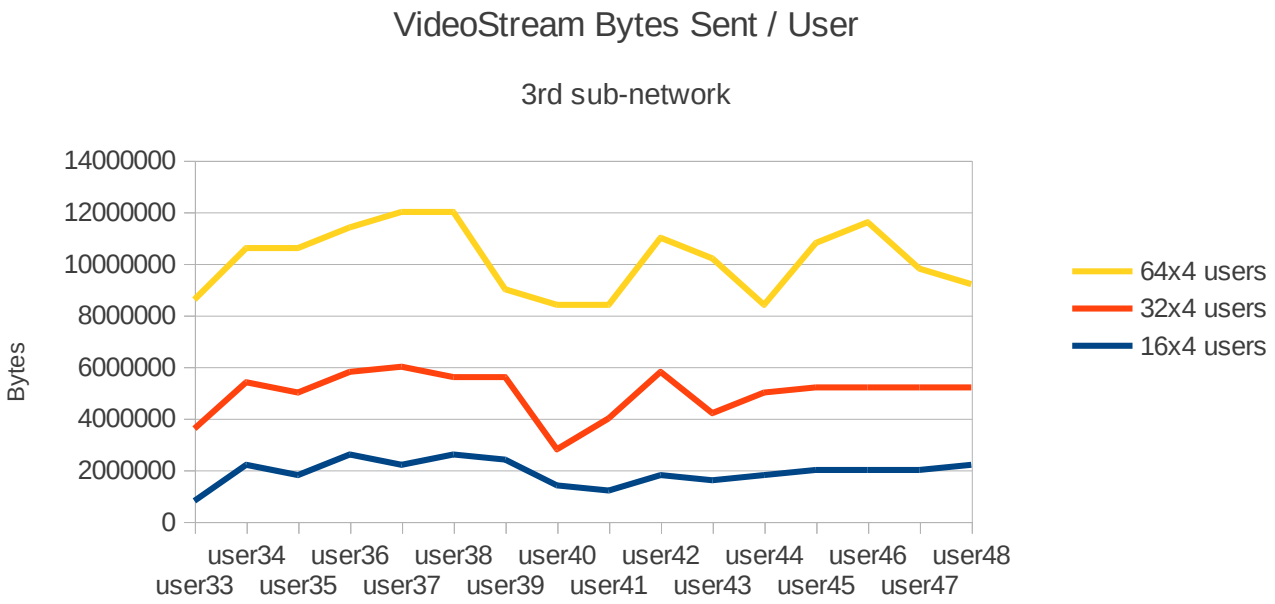
Γράφημα 8-36 Εισερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 3)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user33	800000	2800000	5000000
user34	2200000	3200000	5200000
user35	1800000	3200000	5600000
user36	2600000	3200000	5600000
user37	2200000	3800000	6000000
user38	2600000	3000000	6400000
user39	2400000	3200000	3400000
user40	1400000	1400000	5600000
user41	1200000	2800000	4400000
user42	1800000	4000000	5200000
user43	1600000	2600000	6000000
user44	1800000	3200000	3400000
user45	2000000	3200000	5600000
user46	2000000	3200000	6400000
user47	2000000	3200000	4600000
user48	2200000	3000000	4000000

Πίνακας 8-37 Εξερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 3)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:



Γράφημα 8-37 Εξερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 3)

Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι κινούμενοι χρήστες της γειτονιάς είχαν από 4 έως 32 αναζητήσεις δεδομένων VideoStream είτε στον απομακρυσμένο εξυπηρετητή VideoStream είτε σε άλλον κινούμενο χρήστη.

Ακόμη, διαπιστώνεται μεγαλύτερη διακύμανση στην ποσότητα εισερχόμενων δεδομένων στο σενάριο των 64x4 χρηστών. Αυτό οφείλεται στο γεγονός ότι, λόγω μεγαλύτερης συμφόρησης δικτύου, δεν έχουν φθάσει όλα τα πακέτα βίντεο στον προορισμό τους, αν και έχουν δημιουργηθεί εξαρχής στον αντίστοιχο εξυπηρετητή.

Επίσης, παρατηρείται ιδιαίτερη διακύμανση στην ποσότητα εξερχόμενων δεδομένων και στα 3 διαφορετικά σενάρια αριθμού χρηστών. Αυτό οφείλεται στο γεγονός ότι, η επιλογή των εξυπηρετητών γίνεται κατά τυχαίο τρόπο, με αποτέλεσμα κάποιοι χρήστες να παρουσιάζουν μεγαλύτερη ή μικρότερη προτίμηση από καοιους άλλους.

Τέλος, φαίνεται ότι γίνονται ανταλλαγές δεδομένων VideoStream μεταξύ των χρηστών, αφού υπάρχει εξερχόμενη πληροφορία από τους χρήστες προς εξυπηρέτηση άλλων χρηστών. Αυτό σημαίνει ότι ευνοούνται οι συνεργατικές υπηρεσίες μεταξύ των χρηστών και δεν απαιτείται ολοκληρωτικά η χρήση του απομακρυσμένου εξυπηρετητή.

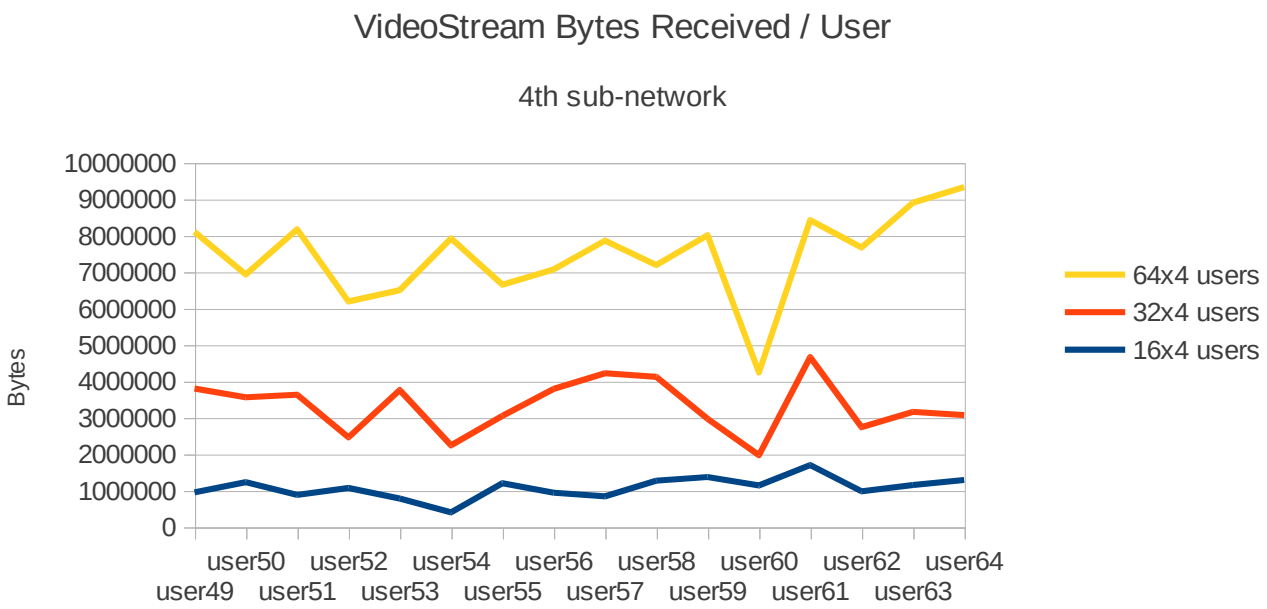
4η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εισερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user49	950000	2850000	4300000
user50	1230000	2330000	3370000
user51	880000	2750000	4540000
user52	1070000	1390000	3730000
user53	780000	2980000	2740000
user54	400000	1840000	5680000
user55	1200000	1850000	3600000
user56	940000	2850000	3280000
user57	840000	3380000	3640000
user58	1270000	2850000	3070000
user59	1370000	1600000	5040000
user60	1140000	830000	2270000
user61	1700000	2960000	3760000
user62	980000	1760000	4930000
user63	1150000	2010000	5740000
user64	1290000	1780000	6260000

Πίνακας 8-38 Εισερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 4)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εισερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:



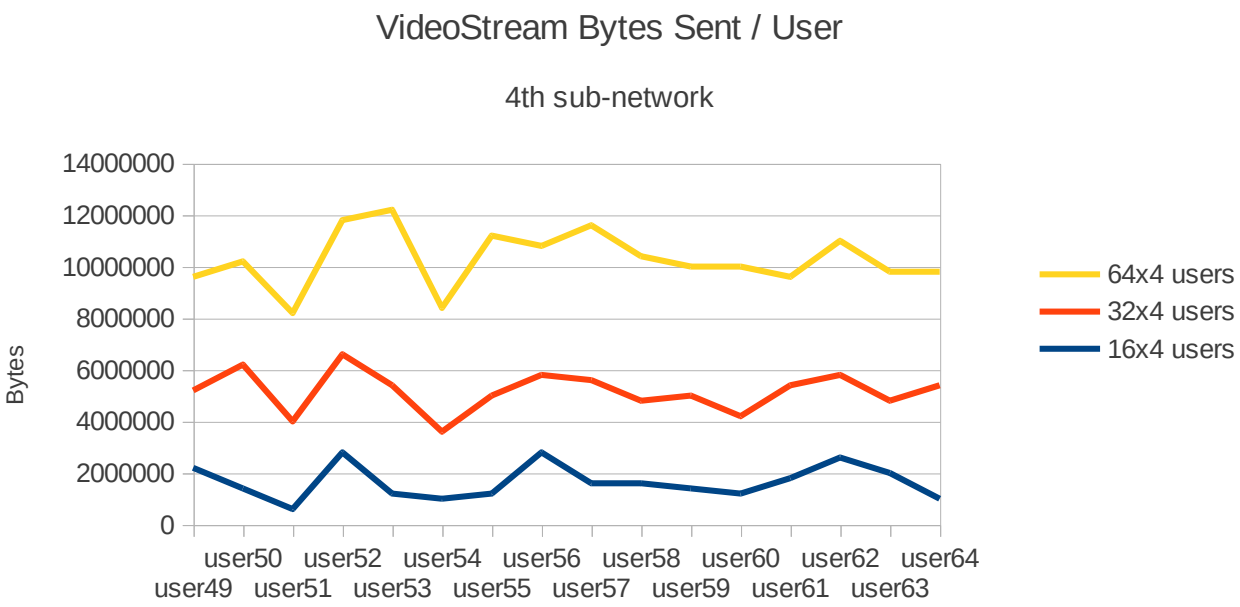
Γράφημα 8-38 Εισερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 4)

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της ποσότητας εξερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:

(Bytes)	***16x4 users***	***32x4 users***	***64x4 users***
user49	2200000	3000000	4400000
user50	1400000	4800000	4000000
user51	600000	3400000	4200000
user52	2800000	3800000	5200000
user53	1200000	4200000	6800000
user54	1000000	2600000	4800000
user55	1200000	3800000	6200000
user56	2800000	3000000	5000000
user57	1600000	4000000	6000000
user58	1600000	3200000	5600000
user59	1400000	3600000	5000000
user60	1200000	3000000	5800000
user61	1800000	3600000	4200000
user62	2600000	3200000	5200000
user63	2000000	2800000	5000000
user64	1000000	4400000	4400000

Πίνακας 8-39 Εξερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 4)

Επίσης, παρουσιάζεται το γράφημα της ποσότητας εξερχόμενων δεδομένων VideoStream ανά κινούμενο χρήστη:



Γράφημα 8-39 Εξερχόμενα δεδομένα VideoStream / χρήστη (υποδίκτυο 4)

Παρατηρείται ότι, στο διάστημα των 100 δευτερολέπτων που διήρκησε η προσομοίωση, οι κινούμενοι χρήστες της γειτονιάς είχαν από 3 έως 34 αναζητήσεις δεδομένων VideoStream είτε στον απομακρυσμένο εξυπηρετητή VideoStream είτε σε άλλον κινούμενο χρήστη.

Ακόμη, διαπιστώνεται μεγαλύτερη διακύμανση στην ποσότητα εισερχόμενων δεδομένων στο σενάριο των 64x4 χρηστών. Αυτό οφείλεται στο γεγονός ότι, λόγω μεγαλύτερης συμφόρησης δικτύου, δεν έχουν φθάσει όλα τα πακέτα βίντεο στον προορισμό τους, αν και έχουν δημιουργηθεί εξαρχής στον αντίστοιχο εξυπηρετητή.

Επίσης, παρατηρείται ιδιαίτερη διακύμανση στην ποσότητα εξερχόμενων δεδομένων και στα 3 διαφορετικά σενάρια αριθμού χρηστών. Αυτό οφείλεται στο γεγονός ότι, η επιλογή των εξυπηρετητών γίνεται κατά τυχαίο τρόπο, με αποτέλεσμα κάποιοι χρήστες να παρουσιάζουν μεγαλύτερη ή μικρότερη προτίμηση από καοιους άλλους.

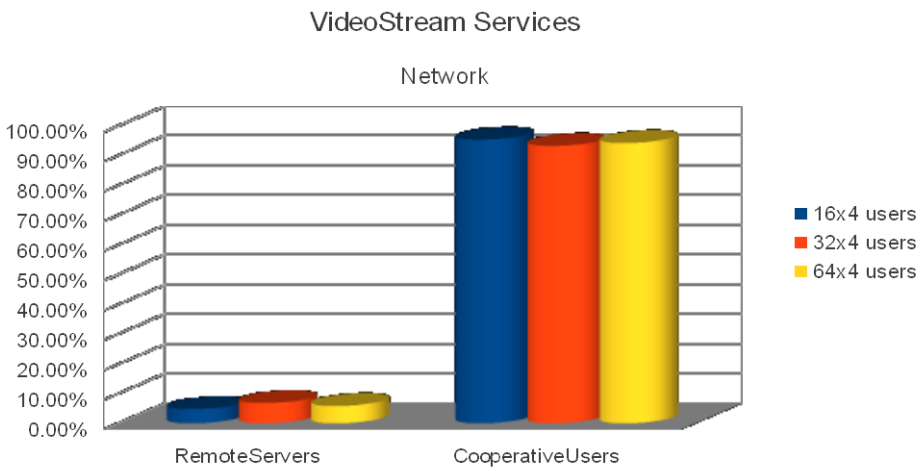
Τέλος, φαίνεται ότι γίνονται ανταλλαγές δεδομένων VideoStream μεταξύ των χρηστών, αφού υπάρχει εξερχόμενη πληροφορία από τους χρήστες προς εξυπηρέτηση άλλων χρηστών. Αυτό σημαίνει ότι ευνοούνται οι συνεργατικές υπηρεσίες μεταξύ των χρηστών και δεν απαιτείται ολοκληρωτικά η χρήση του απομακρυσμένου εξυπηρετητή.

Αξίζει να σημειωθεί πως το μεγαλύτερο μέρος των δεδομένων VideoStream ανταλλάσσεται μόνο μεταξύ των χρηστών παρά μεταξύ των χρηστών και των απομακρυσμένων εξυπηρετητών. Αντίθετα, οι αιτήσεις HTTP εξυπηρετούνται ολοκληρωτικά και μοναδικά από απομακρυσμένους εξυπηρετητές.

Παρακάτω παρουσιάζονται ο πίνακας και το γράφημα που δείχνουν ποια στοιχεία εξυπηρέτησαν τις αιτήσεις για VideoStream και σε τι βαθμό στο σύνολο των αιτήσεων και εξυπηρετήσεων.

	16x4 users	32x4 users	64x4 users
RemoteServers	4.72%	6.78%	5.82%
CooperativeUsers	95.28%	93.22%	94.18%

Πίνακας 8-40 Ποσοστό εξυπηρέτησης αιτήσεων VideoStream / στοιχείο



Γράφημα 8-40 Ποσοστό εξυπηρέτησης αιτήσεων VideoStream / στοιχείο

8.4.6. Μέση καθυστέρηση άφιξης πακέτων VideoStream ανά κινούμενο χρήστη

Τα στοιχεία που λαμβάνουν μέρος σε κάθε υποδίκτυο είναι οι 16 κινούμενοι χρήστες, ο αριθμός των οποίων διπλασιάζεται και τετραπλασιάζεται σύμφωνα με τα αντίστοιχα σενάρια (Users{1..64}).

Τα δεδομένα VideoStream που μπορεί να αποδεχτεί / αποστείλει ένας κινούμενος χρήστης είναι μια απόκριση / αίτηση VideoStream, μεγέθους βίντεο 200000 Bytes σε 4 πακέτα των 50000 Bytes. Η ανταλλαγή αυτή πληροφοριών γίνεται μεταξύ των χρηστών και απομακρυσμένων εξυπηρετητών VideoStream αλλά και μόνο μεταξύ των χρηστών, όταν οι χρήστες επιθυμούν να κατεβάσουν ένα βίντεο ή να συνδιαλεχτούν μεταξύ τους με παράλληλη εφαρμογή VideoStream από ένα ή περισσότερους χρήστες.

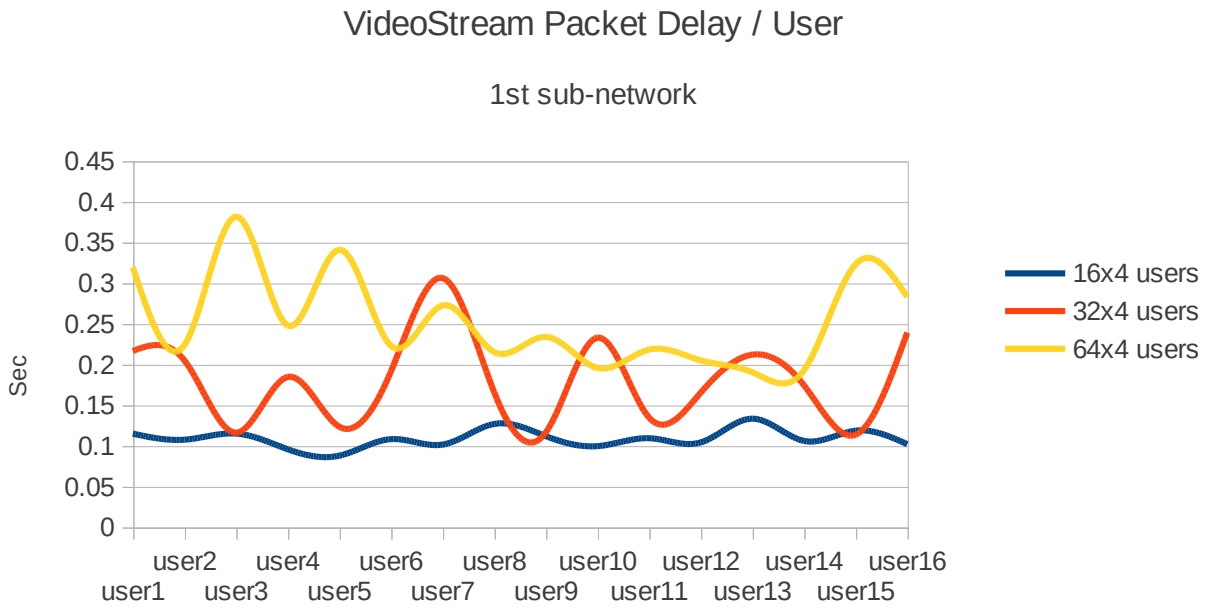
1*η γειτονιά-υποδίκτυο*

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της μέσης καθυστέρησης άφιξης πακέτων VideoStream ανά κινούμενο χρήστη:

(sec)	***16x4 users***	***32x4 users***	***64x4 users***
user1	0.1147066501	0.2164466332	0.3192122993
user2	0.1073683714	0.2047753283	0.2236472464
user3	0.1149249453	0.115806052	0.3816028727
user4	0.0956127147	0.1845776676	0.2476113316
user5	0.0877575127	0.1231860796	0.3408860691
user6	0.1080814024	0.1912747451	0.2226302186
user7	0.1013678197	0.3060987958	0.2724734595
user8	0.1267294416	0.1654354313	0.2149470429
user9	0.1117392231	0.1162724521	0.2337404709
user10	0.0994549301	0.2328046789	0.1954536995
user11	0.1092207325	0.1344297269	0.2180965333
user12	0.1040411953	0.1651817468	0.2048167045
user13	0.133211668	0.2119019593	0.1902664768
user14	0.1058683517	0.1742964227	0.1926583948
user15	0.1184644898	0.1134189708	0.3230382194
user16	0.1018371628	0.2389708565	0.2828162327

Πίνακας 8-41 Καθυστέρηση πακέτων VideoStream / χρήστη (υποδίκτυο 1)

Επίσης, παρουσιάζεται το γράφημα της μέσης καθυστέρησης άφιξης πακέτων VideoStream ανά κινούμενο χρήστη:



Γράφημα 8-41 Καθυστέρηση πακέτων VideoStream / χρήστη (υποδίκτυο 1)

Καταρχάς, παρατηρείται μια αύξηση στη μέση καθυστέρηση άφιξης πακέτων καθώς αυξάνονται οι κινούμενοι χρήστες στην εφαρμογή των 3 διαφορετικών σεναρίων. Αυτό θεωρείται λογικό και οφείλεται στο γεγονός ότι ενω τα πακέτα έχουν δημιουργηθεί στον εξυπηρετητή σε ελάχιστο χρονικό διάστημα (έναρξη χρόνου καθυστέρησης), λόγω αυξανόμενης συμφόρησης του δικτύου, αργούν να φθάσουν στον προορισμό τους.

Κατά δεύτερον, παρατηρείται ιδιαίτερη διακύμανση στη μέση καθυστέρηση άφιξης πακέτων στο 2ο και 3ο σενάριο αριθμού χρηστών. Αυτό οφείλεται και πάλι στο γεγονός της σταδιακής αύξησης της συμφόρησης του δικτύου.

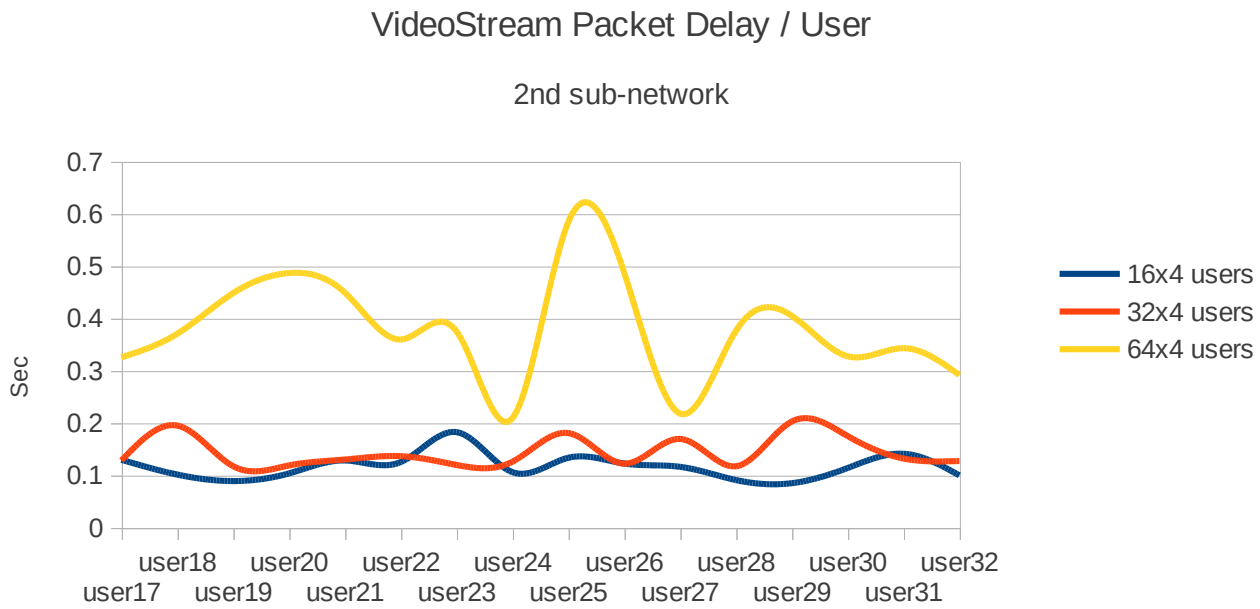
2η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της μέσης καθυστέρησης άφιξης πακέτων VideoStream ανά κινούμενο χρήστη:

(sec)	***16x4 users***	***32x4 users***	***64x4 users***
user17	0.1295990828	0.1281738885	0.3253716096
user18	0.1012254566	0.1950428474	0.3705002945
user19	0.0888930661	0.1172829617	0.4482197447
user20	0.1034995209	0.1187122644	0.4866190177
user21	0.1282535123	0.1300302845	0.4491397462
user22	0.125198383	0.1364878615	0.3594024103
user23	0.1824058687	0.1196254858	0.3750025497
user24	0.1058517076	0.1258949472	0.2090205769
user25	0.1333936171	0.1807173539	0.5843106609
user26	0.1224037338	0.1220551669	0.4873590946
user27	0.1160870544	0.1694719556	0.2176979466
user28	0.090789157	0.1170742127	0.3761260014
user29	0.0847908897	0.2028268879	0.4048440064
user30	0.1138465642	0.1748672835	0.3273259097
user31	0.1410825615	0.1318932879	0.3429309583
user32	0.0997614382	0.1271778546	0.2916360293

Πίνακας 8-42 Καθυστέρηση πακέτων VideoStream / χρήστη (υποδίκτυο 2)

Επίσης, παρουσιάζεται το γράφημα της μέσης καθυστέρησης άφιξης πακέτων VideoStream ανά κινούμενο χρήστη:



Γράφημα 8-42 Καθυστέρηση πακέτων VideoStream / χρήστη (υποδίκτυο 2)

Καταρχάς, παρατηρείται μια αύξηση στη μέση καθυστέρηση άφιξης πακέτων καθώς αυξάνονται οι κινούμενοι χρήστες στην εφαρμογή των 3 διαφορετικών σεναρίων, αν και τα 2 πρώτα σενάρια εκδηλώνουν παρόμοια συμεριφορά. Αυτό θεωρείται λογικό και οφείλεται στο γεγονός ότι ενω τα πακέτα έχουν δημιουργηθεί στον εξυπηρετητή σε ελάχιστο χρονικό διάστημα (έναρξη χρόνου καθυστέρησης), λόγω αυξανόμενης συμφόρησης του δικτύου, αργούν να φθάσουν στον προορισμό τους.

Κατά δεύτερον, παρατηρείται ιδιαίτερη διακύμανση στη μέση καθυστέρηση άφιξης πακέτων στο 3ο σενάριο αριθμού χρηστών. Αυτό οφείλεται και πάλι στο γεγονός της σταδιακής αύξησης της συμφόρησης του δικτύου.

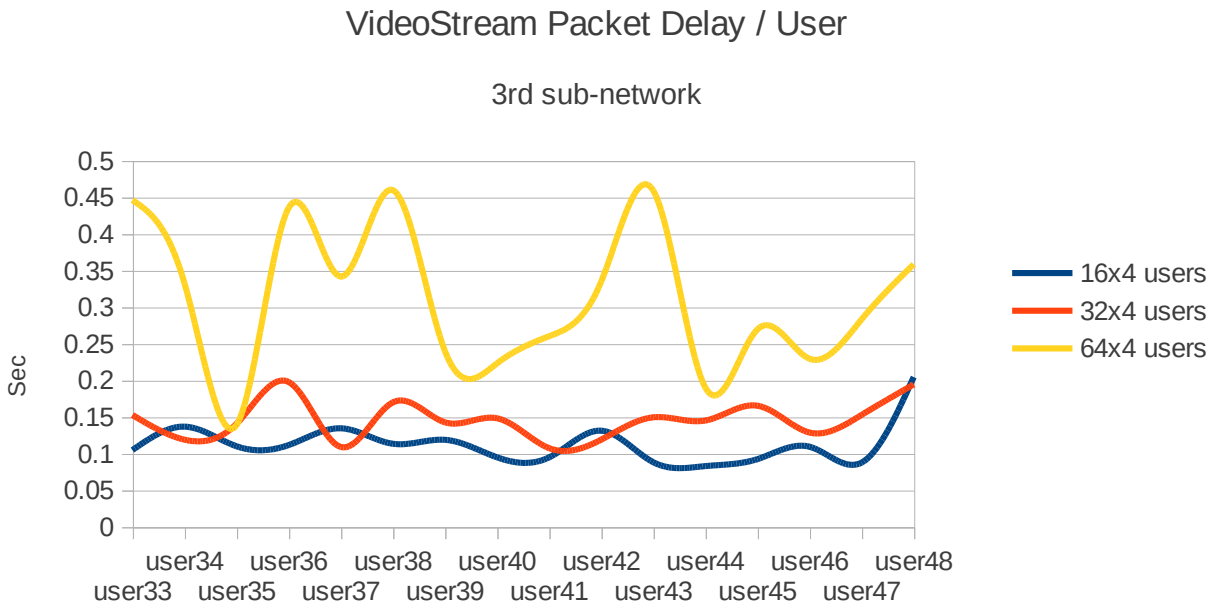
3*η γειτονιά-υποδίκτυο*

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της μέσης καθυστέρησης άφιξης πακέτων VideoStream ανά κινούμενο χρήστη:

(sec)	***16x4 users***	***32x4 users***	***64x4 users***
user33	0.1046385536	0.1525812779	0.4460717856
user34	0.1366938814	0.1188759189	0.3324136656
user35	0.109857171	0.1406325001	0.1389280597
user36	0.1115418711	0.1976810156	0.4355763635
user37	0.1344509054	0.1089104532	0.3414989301
user38	0.1132843757	0.1698175007	0.45974992
user39	0.1187198404	0.1425744103	0.2399259769
user40	0.0948015372	0.1481551619	0.2231209476
user41	0.0946846124	0.1073008868	0.2601154775
user42	0.1312100081	0.1188641474	0.334632187
user43	0.0881269761	0.1494682809	0.4591569902
user44	0.0827895002	0.1450248595	0.189904335
user45	0.0923074062	0.1653030231	0.2695942974
user46	0.1092841569	0.1286416735	0.2293692355
user47	0.0875434916	0.1526586332	0.2831155899
user48	0.2043997545	0.1942470519	0.358307444

Πίνακας 8-43 Καθυστέρηση πακέτων VideoStream / χρήστη (υποδίκτυο 3)

Επίσης, παρουσιάζεται το γράφημα της μέσης καθυστέρησης άφιξης πακέτων VideoStream ανά κινούμενο χρήστη:



Γράφημα 8-43 Καθυστέρηση πακέτων VideoStream / χρήστη (υποδίκτυο 3)

Καταρχάς, παρατηρείται μια αύξηση στη μέση καθυστέρηση άφιξης πακέτων καθώς αυξάνονται οι κινούμενοι χρήστες στην εφαρμογή των 3 διαφορετικών σεναρίων, αν και τα 2 πρώτα σενάρια εκδηλώνουν παρόμοια συμεριφορά. Αυτό θεωρείται λογικό και οφείλεται στο γεγονός ότι ενω τα πακέτα έχουν δημιουργηθεί στον εξυπηρετητή σε ελάχιστο χρονικό διάστημα (έναρξη χρόνου καθυστέρησης), λόγω αυξανόμενης συμφόρησης του δικτύου, αργούν να φθάσουν στον προορισμό τους.

Κατά δεύτερον, παρατηρείται ιδιαίτερη διακύμανση στη μέση καθυστέρηση άφιξης πακέτων στο 3ο σενάριο αριθμού χρηστών. Αυτό οφείλεται και πάλι στο γεγονός της σταδιακής αύξησης της συμφόρησης του δικτύου.

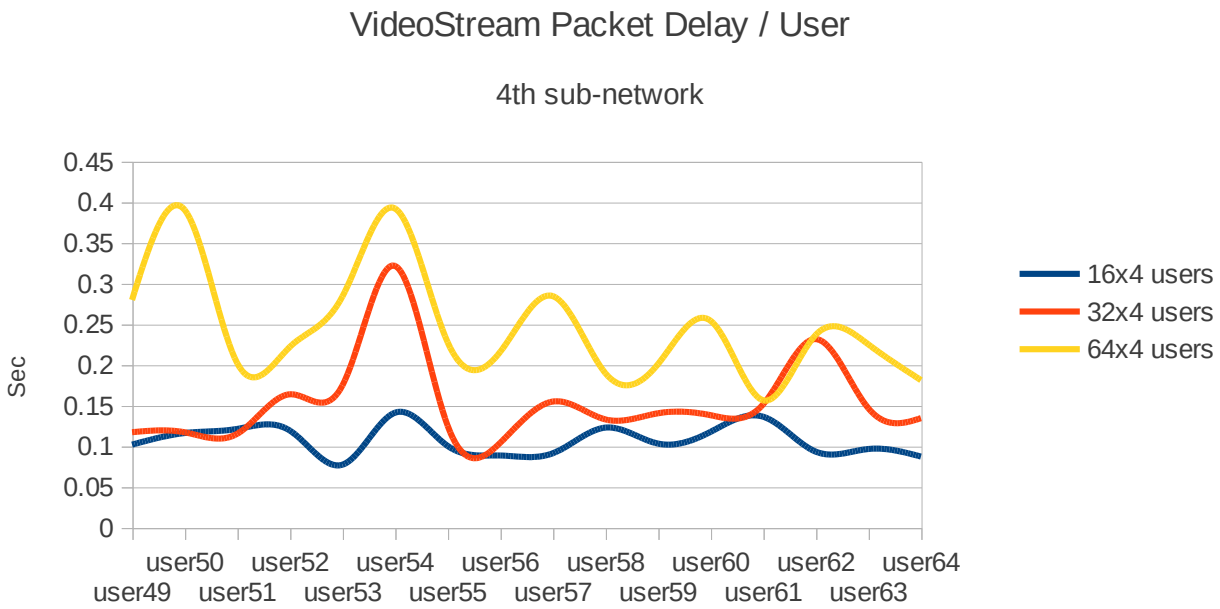
4η γειτονιά-υποδίκτυο

Παρακάτω, παρουσιάζεται ο πίνακας μετρήσεων της μέσης καθυστέρησης άφιξης πακέτων VideoStream ανά κινούμενο χρήστη:

(sec)	***16x4 users***	***32x4 users***	***64x4 users***
user49	0.1018387684	0.1171193799	0.279587631
user50	0.1161132889	0.1170505452	0.3905032291
user51	0.1211523203	0.1151802144	0.2019795109
user52	0.11919675	0.163765224	0.2219706233
user53	0.0771662664	0.17454812	0.2839350553
user54	0.1411649932	0.3216459329	0.392170248
user55	0.1002587034	0.1251837059	0.2277378595
user56	0.0885412658	0.1041373628	0.2158893509
user57	0.0912507467	0.1548393616	0.2843952592
user58	0.1227856781	0.132835878	0.1896415419
user59	0.1031463215	0.1404267258	0.2008206659
user60	0.1176109263	0.1380319195	0.2541712047
user61	0.1361921917	0.151484994	0.1562277375
user62	0.0932079096	0.2316403658	0.2368705749
user63	0.096550617	0.1464797305	0.2250056833
user64	0.0871892931	0.1344312306	0.1811188752

Πίνακας 8-44 Καθυστέρηση πακέτων VideoStream / χρήστη (υποδίκτυο 4)

Επίσης, παρουσιάζεται το γράφημα της μέσης καθυστέρησης άφιξης πακέτων VideoStream ανά κινούμενο χρήστη:



Γράφημα 8-44 Καθυστέρηση πακέτων VideoStream / χρήστη (υποδίκτυο 4)

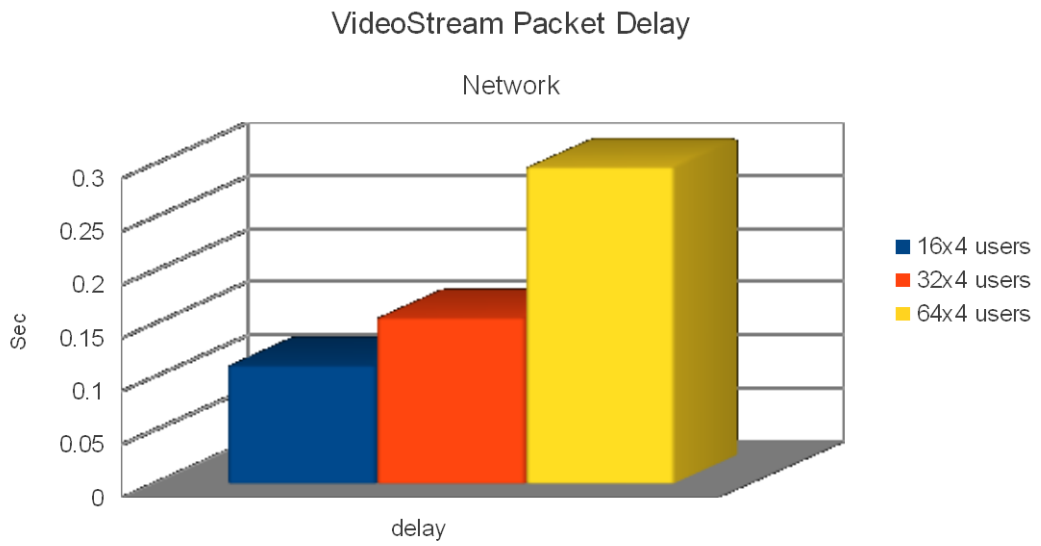
Καταρχάς, παρατηρείται μια αύξηση στη μέση καθυστέρηση άφιξης πακέτων καθώς αυξάνονται οι κινούμενοι χρήστες στην εφαρμογή των 3 διαφορετικών σεναρίων. Αυτό θεωρείται λογικό και οφείλεται στο γεγονός ότι ενω τα πακέτα έχουν δημιουργηθεί στον εξυπηρετητή σε ελάχιστο χρονικό διάστημα (έναρξη χρόνου καθυστέρησης), λόγω αυξανόμενης συμφόρησης του δικτύου, αργούν να φθάσουν στον προορισμό τους.

Κατά δεύτερον, παρατηρείται ιδιαίτερη διακύμανση στη μέση καθυστέρηση άφιξης πακέτων στο 2ο και 3ο σενάριο αριθμού χρηστών. Αυτό οφείλεται και πάλι στο γεγονός της σταδιακής αύξησης της συμφόρησης του δικτύου.

Τέλος, υπολογίζεται η μέση καθυστέρηση που έχει ένα πακέτο VideoStream στο δίκτυο. Παρακάτω παρουσιάζονται ο σχετικός πίνακας και το σχετικό γράφημα για τα 3 διαφορετικά σενάρια.

(sec)	16x4 users	32x4 users	64x4 users
delay	0.1114870048	0.1562773371	0.2978579701

Πίνακας 8-45 Μέση καθυστέρηση πακέτων VideoStream (δίκτυο)



Γράφημα 8-45 Μέση καθυστέρηση πακέτων VideoStream (δίκτυο)

9. Συμπεράσματα

Το βασικό σενάριο λειτουργίας του έξυπνου δικτύου, που περιγράφηκε στη διαδικασία της προσομοίωσης, ανταποκρίνεται με ικανοποιητικό βαθμό στις πραγματικές συνθήκες λειτουργίας του μελλοντικού έξυπνου δικτύου, σύμφωνα με τη βιβλιογραφική έρευνα που προηγήθηκε.

Καταρχάς, διαπιστώνεται ότι η ποσότητα και η συχνότητα ανταλλαγής δεδομένων μεταξύ του εκάστοτε έξυπνου μετρητή και του τοπικού κέντρου ελέγχου είναι μηδαμινές σε σύγκριση με τα δεδομένα που εκπέμπει και λαμβάνει ένας κινούμενος χρήστης του Διαδικτύου. Αυτό σημαίνει ότι το ποσοστό χρησιμοποίησης ή αξιοποίησης ενός σημείου πρόσβασης, και κατ' επέκταση του δικτύου επικοινωνιών, εξαρτάται κατά κύριο λόγο από τον διαρκώς μεταβαλλόμενο αριθμό των χρηστών και όχι από το σταθερό (ή ίσως χαμηλά αυξητικό) αριθμό εγκατεστημένων έξυπνων μετρητών. Φυσικά, στην παραπάνω διαπίστωση οδήγησαν οι παραδοχές ότι οι έξυπνοι μετρητές εκτελούν μετρήσεις κατανάλωσης κάθε 30 sec (όπως προτείνεται στη βιβλιογραφική έρευνα) και ότι τα δεδομένα που ανταλλάσσουν με το κέντρο ελέγχου είναι περίπου ίδιας ποσότητας με τα δεδομένα που ανταλλάσσει ένας χρήστης http με έναν εξυπηρετητή http. Επίσης έγιναν οι παραδοχές ότι ένας χρήστης http ή VideoStream αναζητά εξυπηρέτηση από τον αντίστοιχο εξυπηρετητή κάθε 8 έως 12 sec, ενώ κάθε φορά στέλνουν και λαμβάνουν την ίδια ποσότητα δεδομένων. Ακόμη, έγινε η παραδοχή ότι οι περισσότεροι κόμβοι έχουν τη δυνατότητα μέγιστου ρυθμού επεξεργασίας δεδομένων 10 Mbps. Οι παραπάνω παραδοχές μπορούν να μεταβληθούν κατάλληλα και να αποτελέσουν αντικείμενο έρευνας και μελέτης για μελλοντικές εργασίες, με σκοπό να ανταποκριθούν όσο το δυνατόν καλύτερα στις πραγματικές συνθήκες λειτουργίας.

Κατά δεύτερον, συμπεραίνεται ότι οι επιθέσεις Άρνησης Υπηρεσιών (DoS: Denial of Service) που εξαπολύουν οι κακόβουλοι επιτιθέμενοι κρίνονται επιτυχημένες. Αυτό συμβαίνει διότι οι έξυπνοι μετρητές, που έχουν καταληφθεί, δεν ανταποκρίνονται για μεγάλο χρονικό διάστημα στις ευθύνες τους, δηλαδή στην αποστολή μετρήσεων κατανάλωσης προς το κέντρο ελέγχου. Ένα παρόμοιο γεγονός, σε πραγματικές συνθήκες, θα μπορούσε να αποτελέσει αιτία για λανθασμένους υπολογισμούς του κέντρου ελέγχου ενάντια στη βέλτιστη κατανομή ισχύος και εξοικονόμησης ενέργειας, για εκτύπωση λανθασμένων λογαριασμών και τιμολόγησης ενέργειας πραγματικού χρόνου, ή ακόμα και για πολύωρες διακοπές ρεύματος σε περίπτωση τεχνικής βλάβης. Φυσικά, στο παραπάνω συμπέρασμα οδήγησε η παραδοχή ότι ο έξυπνος μετρητής έχει τη δυνατότητα μόνο τεσσάρων παράλληλων συνδέσεων tcp. Ο περιορισμένος αριθμός συνδέσεων ανταποκρίνεται σε πραγματικές συνθήκες, αλλά ο αριθμός 4 είναι υποτίθεται μικρός. Ωστόσο, δεν πρέπει να παραμελείται το γεγονός ότι ένας έξυπνος μετρητής αποτελεί ασύρματο στοιχείο περιορισμένων πόρων και δυνατοτήτων (περιορισμένη ενέργεια, υπολογιστική ισχύ και μνήμη). Η παραπάνω παραδοχή και τα απαιτούμενα trade-off που είναι ανάγκη να υλοποιηθούν, μπορούν να αποτελέσουν αντικείμενο έρευνας και μελέτης για μελλοντικές εργασίες, με σκοπό να ανταποκριθούν όσο το δυνατόν καλύτερα στις πραγματικές συνθήκες λειτουργίας.

Τέλος, παρατηρείται ότι οι συνεργατικές υπηρεσίες αφορούν μόνο τις συνεργασίες μεταξύ των κινούμενων χρηστών και ειδικότερα τη διαδικασία επιλογής ενός

εξυπηρετητή για κατέβασμα ενός βίντεο (video downloading, peer-to-peer cooperation). Έγιναν οι παραδοχές ότι οι κινούμενοι χρήστες http αναζητούν μόνο απομακρυσμένους εξυπηρετητές http του Διαδικτύου, ενώ οι κινούμενοι χρήστες VideoStream επιλέγουν με τυχαίο τρόπο μεταξύ των διαφόρων κινούμενων χρηστών της μικρής πόλης και των απομακρυσμένων εξυπηρετητών VideoStream του Διαδικτύου. Ωστόσο, η επιλογή αυτή ίσως ήταν ρεαλιστικότερο να μην ήταν εντελώς τυχαία, αλλά να περιλαμβάνει και κάποιου είδους κριτήρια για την επιλεκτική εξυπηρέτηση VideoStream, όπως ποιότητα υπηρεσιών, αξιοπιστία, ασφάλεια. Επίσης οι συνεργατικές υπηρεσίες θα μπορούσαν να αφορούν όχι μόνο τους κινούμενους χρήστες αλλά και τους έξυπνους μετρητές. Για παράδειγμα, σε περίπτωση αδυναμίας ενός έξυπνου μετρητή να μεταδώσει τις μετρήσεις του απευθείας στο συλλέκτη δεδομένων, τότε θα έχει τη δυνατότητα να μεσολαβήσει ένας διαφορετικός κοντινός έξυπνος μετρητής, να παραλάβει τις μετρήσεις και να τις προωθήσει αυτός στο συλλέκτη δεδομένων, ενώ στην απόκριση του κέντρου ελέγχου να τηρηθεί η αντίστροφη διαδικασία μεσολάβησης και συνεργασίας. Οι παραπάνω παραδοχές και ιδέες μπορούν να μεταβληθούν και να επεκταθούν κατάλληλα, και φυσικά να αποτελέσουν αντικείμενο έρευνας και μελέτης για μελλοντικές εργασίες, με σκοπό να ανταποκριθούν όσο το δυνατόν καλύτερα στις πραγματικές συνθήκες λειτουργίας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Chee-Wooi Ten, Junho Hong, and Chen-Ching Liu, "Anomaly Detection for Cybersecurity of the Substations", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[2] Le Xie, Yilin Mo, and Bruno Sinopoli, "Integrity Data Attacks in Power Market Operations", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[3] Meikang Qiu, Wenzhong Gao, Min Chen, Jian-Wei Niu, Lei Zhang, "Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[4] Adam Hahn, and Manimaran Govindarasu, "Cyber Attack Exposure Evaluation Framework for the Smart Grid", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[5] Yunfei Wang, Iraj Rahimi Pordanjani, and Wilsun Xu, "An Event-Driven Demand Response Scheme for Power System Security Enhancement", *IEEE Transactions on Smart Grid*, vol. 2, no. 1, March 2011

[6] Amir-Hamed Mohsenian-Rad, and Alberto Leon-Garcia, "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[7] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C. Green II, and Mansoor Alam, "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[8] Yanling Yuan, Zuyi Li, and Kui Ren, "Modeling Load Redistribution Attacks in Power Systems", *IEEE Transactions on Smart Grid*, vol. 2, no. 2, June 2011

[9] Dong Wei, Yan Lu, Mohsen Jafari, Paul M. Skare, and Kenneth Rohde, "Protecting Smart Grid Automation Systems Against Cyberattacks", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[10] Hairong Qi, Xiaorui Wang, Leon M. Tolbert, Fangxing Li, Fang Z. Peng, Peng Ning, and Massoud Amin, "A Resilient Real-Time System Design for a Secure and Reconfigurable Power Grid", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[11] Dapeng Wu, and Chi Zhou, "Fault-Tolerant and Scalable Key Management for Smart Grid", *IEEE Transactions on Smart Grid*, vol. 2, no. 2, June 2011

[12] Biplab Sikdar, and Joe H. Chow, "Defending Synchrophasor Data Networks Against Traffic Analysis Attacks", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[13] Georgios Kalogridis, Rafael Cepeda, Stojan Z. Denic, Tim Lewis, and Costas Efthymiou, "ElecPrivacy: Evaluating the Privacy Protection of Electricity Management Algorithms", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[14] Andrea Bartoli, Juan Hernández-Serrano, Miguel Soriano, Mischa Dohler, Apostolos Kountouris, and Dominique Barthel, "Secure Lossless Aggregation Over Fading and Shadowing Channels for Smart Grid M2M Networks", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[15] Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori and Ramjee Prasad, "Behavioural Modelling of WSN MAC Layer Security Attacks: A Sequential UML Approach", *Center for TeleInFrastruktur, Aalborg University, Journal of Cyber Security and Mobility*, 65–82, 2012

[16] Technology Roadmap-Smart Grids, *International Energy Agency*, 2011

[17] Ye Yan, Yi Qian and Hamid Sharif, "A Secure and Reliable In-network Collaborative Communication Scheme for Advanced Metering Infrastructure in Smart Grid", *IEEE WCNC 2011-Network*

[18] Javier Lopez, "Security & Privacy in WSN", *NICS Lab. University of Malaga Spain*

[19] Todd Baumeister, "Literature Review on Smart Grid Cyber Security", *Collaborative Software Development Laboratory, Department of Information and Computer Sciences, University of Hawai'i,* December 2010

[20] Jeff Naruchitparames and Mehmet Hadi Gunes, Cansin Yaman Evrenosoglu, "Secure Communications in the Smart Grid"

[21] Fangxing Li, Wei Qiao, Hongbin Sun, Hui Wan, Jianhui Wang, Yan Xia, Zhao Xu, and Pei Zhang, "Smart Transmission Grid: Vision and Framework", *IEEE Transactions on Smart Grid*, vol. 1, no. 2, September 2010

[22] Daniel E. Nordell, "Terms of Protection", *IEEE Power and Energy Magazine—Keeping the Smart Grid Safe*, vol.10, no. 1, January/February 2012

[23] Faycal Bouhafs, Michael Mackay, and Madjid Merabti, "Links to the Future", *IEEE Power and Energy Magazine—Keeping the Smart Grid Safe*, vol.10, no. 1, January/February 2012

[24] S. Massoud Amin and Anthony M. Giacomoni, "Smart Grid—Safe, Secure, Self-Healing", *IEEE Power and Energy Magazine—Keeping the Smart Grid Safe*, vol.10, no. 1, January/February 2012

[25] Chen-Ching Liu, Alexandru Stefanov, Junho Hong, and Patrick Panciatici, "Intruders in the Grid", *IEEE Power and Energy Magazine—Keeping the Smart Grid Safe*, vol.10, no. 1, January/February 2012

[26] Γ. Πάγκαλος, Ι. Μαυρίδης, "ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ", 2002

[27] Weihua Zhuang and Muhammad Ismail, "Cooperation in Wireless Communication Networks", *IEEE Wireless Communications*, April 2012

[28] Rong Yu, Yan Zhang, Liu Yi and Shemgli Xie, Lingyang Song, Mohsen Guizani, "Secondary Users Cooperation in Cognitive Radio Netwoks: Balancing Ssensing Accuracy and Efficiency", *IEEE Wireless Communications*, April 2012

[29] Dejun Yang, Xi Fang, and Guoliang Xue, "Game Theory in Cooperative Communications", *IEEE Wireless Communications*, April 2012

[30] Quansheng Guan, F. Richard Yu, Shengming Jiang, Victor C. M. Leung, Hamid Mehrvar, "Topology Control in Mobile Ad Hoc Networks With Cooperative Communications", *IEEE Wireless Communications*, April 2012

[31] Rong Yu, Yan Zhang and Stein Gjessing, Chau Yuen, Shengli Xie, Mohsen Guizani, "Cognitive-Radio-Based Hierarchical Communications Infrastructure for Smart Grid", *IEEE Network*, September/October 2011

[32] ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ Έξυπνα ηλεκτρικά δίκτυα: από την καινοτομία στην αξιοποίηση, {SEC(2011) 463 τελικό}

[33] Carlos Queiroz, Abdun Mahmood, and Zahir Tari, "SCADASim—A Framework for Building SCADA Simulations", *IEEE Transactions on Smart Grid*, vol. 2, no. 4, December 2011

[34] Christoph P. Mayer, Thomas Gamer, "Integrating real world applications into OMNeT++", *Universitat Karlsruhe (TH), TELEMATICS TECHNICAL REPORTS*, February 2008

[35] Andrew Davis, *Gabor Karsai*, Himanshu Neema, Annarita Giani, *Rohan Chabukswar*,"TRUST for SCADA: A Simulation-based Experimental Platform"

[36] Andras Varga, Rudolf Hornig, "AN OVERVIEW OF THE OMNeT++ SIMULATION ENVIRONMENT"

[37] Thomas Gamer, Michael Scharf, "Realistic Simulation Environments for IP-based Networks", March 2008

[38] Ιστοσελίδα αναζήτησης λειτουργικού συστήματος Ubuntu: http://www.ubuntu.com/, ημερομηνία τελευταίας επίσκεψης: 19/3/2012

[39] Ιστοσελίδα αναζήτησης συστήματος προσομοίωσης Omnet++: http://www.omnetpp.org/, ημερομηνία τελευταίας επίσκεψης: 20/3/1012

[40] Ιστοσελίδα αναζήτησης INET Framework: http://inet.omnetpp.org, ημερομηνία τελευταίας επίσκεψης: 21/3/2012

[41] Ιστοσελίδα αναζήτησης SCADA-Sim: https://github.com/caxqueiroz/scadasim, ημερομηνία τελευταίας επίσκεψης: 21/3/2012

ΠΑΡΑΡΤΗΜΑ

SCADA-Sim
Οδηγός Εγκατάστασης

1. Εισαγωγή

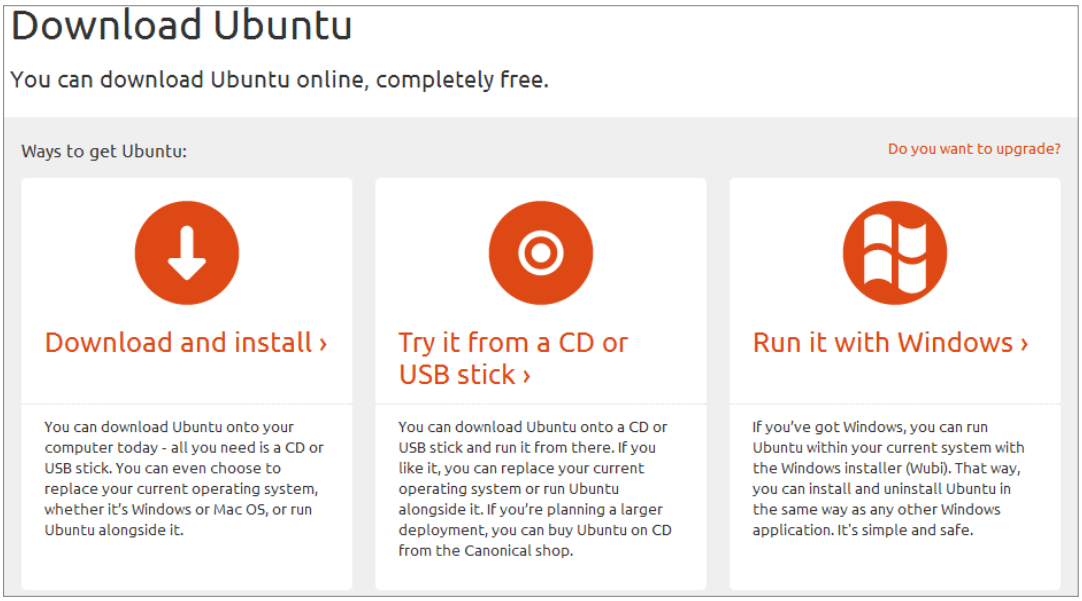
Παρακάτω περιγράφεται ο τρόπος με τον οποίο μπορεί κάποιος να εγκαταστήσει τον Προσομοιωτή Συστημάτων SCADA (*SCADA-Sim*) στον υπολογιστή του.

2. Λειτουργικό Σύστημα

Το *SCADA-Sim* υποστηρίζεται, προς το παρόν, μόνο από το λειτουργικό σύστημα Unix. Εν προκειμένω, έγινε χρήση της έκδοσης Linux/Ubuntu 11.10 .

Αν χρησιμοποιείται διαφορετικό λειτουργικό σύστημα, τότε από την ιστοσελίδα http://www.ubuntu.com/ δίνεται η δυνατότητα:

- Είτε να κατεβάσουμε και να εγκαταστήσουμε τα Ubuntu στον υπολογιστή μας, αντικαθιστώντας πλήρως το υπάρχον λειτουργικό μας σύστημα
- Είτε, σε περίπτωση που χρησιμοποιούνται Windows, να κατεβάσουμε και να εγκαταστήσουμε τα Ubuntu στο υπάρχον λειτουργικό μας σύστημα, τρέχοντας αυτά σαν μια εφαρμογή των Windows (Wubi).



Εικόνα Π-1 Επιλογές εγκατάστασης Ubuntu

3. Εγκατάσταση OMNeT++

Το OMNeT++ αποτελεί μια επεκτάσιμη, συναρμολογούμενη βιβλιοθήκη στοιχείων βασισμένων σε C++, σχεδιασμένη κυρίως για την κατασκευή και δημιουργία προσομοιώσεων δικτύων.

3.1. Εγκατάσταση προαπαιτούμενων πακέτων (prerequisite packages)

Το OMNeT++ απαιτεί την εγκατάσταση διαφόρων πακέτων στον υπολογιστή. Αυτά τα πακέτα περιλαμβάνουν τον C++ compiler (gcc), Java runtime και διάφορες άλλες βιβλιοθήκες (libraries) και προγράμματα.

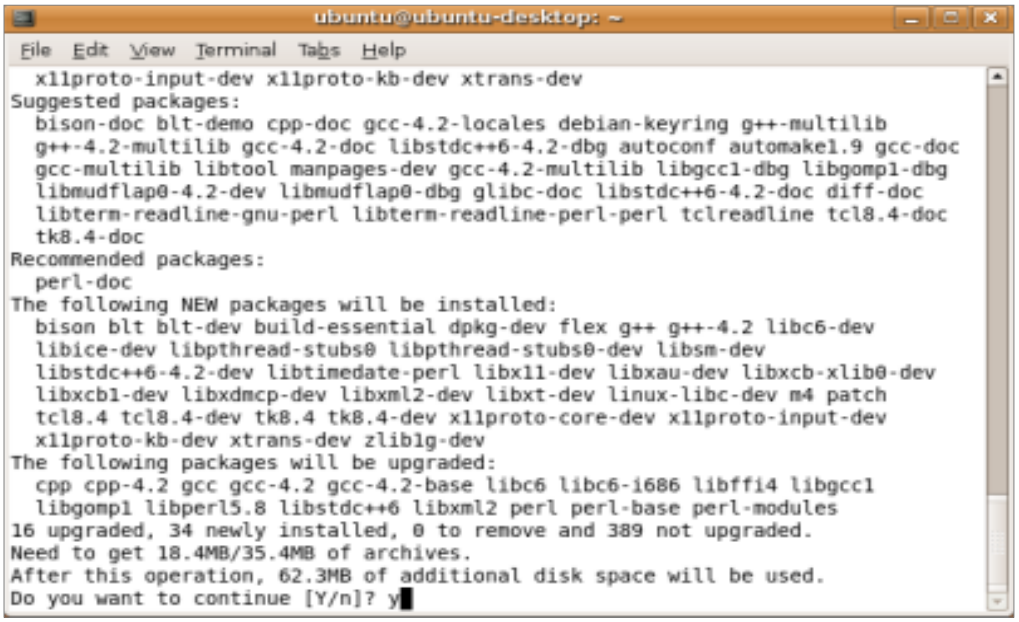
- Ανοίγουμε το τερματικό (terminal)
- Ανανεώνουμε τη βάση δεδομένων των διαθέσιμων πακέτων, εισάγοντας την εντολή:

$ sudo apt-get update

- Εγκαθιστούμε τα απαιτούμενα πακέτα, εισάγοντας την εντολή:

$ sudo apt-get install build-essential gcc g++ bison flex perl \ tcl-dev tk-dev blt libxml2-dev zlib1g-dev openjdk-6-jre \ doxygen graphviz openmpi-bin libopenmpi-dev libpcap-dev

Στις ερωτήσεις επιβεβαίωσης (Θέλετε να συνεχίσετε?[N/O]), απαντήστε N.



Εικόνα Π-2 Εγκατάσταση απαιτούμενων πακέτων

3.2. Κατέβασμα και ξεπακετάρισμα (downloading and unpacking)

- Κατεβάζουμε το OMNeT++ από την ιστοσελίδα http://www.omnetpp.org/. Επιβεβαιώνουμε ότι επιλέξαμε να κατεβάσουμε το αρχείο omnetpp-4.2.2-src.tgz (το 4.2.2 απλά αποτελεί την τελευταίο release).
- Αντιγράφουμε το παραπάνω αρχείο στο φάκελο όπου θέλουμε να το εγκαταστήσουμε.
- Ανοίγουμε το τερματικό, μεταφερόμαστε στον επιθυμητό φάκελο ($ cd …) και αποσυμπιέζουμε το αρχείο εκτελώντας την ακόλουθη εντολή:
  $ tar xvfz omnetpp-4.2.2-src.tgz

Με αυτό τον τρόπο θα δημιουργηθεί ένας υποφάκελος omnetpp-4.2.2 με τα αρχεία του OMNeT++ μέσα σε αυτόν.

3.3. Μεταβλητές περιβάλλοντος (environment variables)

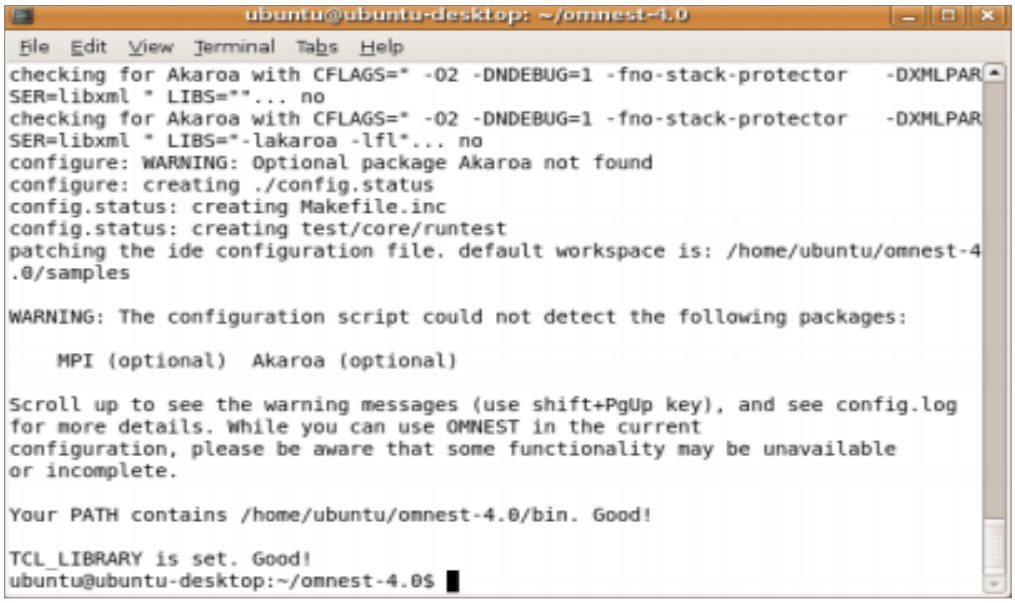
- Για να ρυθμίσουμε μόνιμα τις μεταβλητές περιβάλλοντος, μεταφερόμαστε στον επιθυμητό φάκελο ($ cd …) και εκτελούμε την εντολή: $ gedit ~/.bashrc

Με αυτό τον τρόπο, μπορούμε να τροποποιήσουμε το αρχείο .bashrc που ανοίγει σε text editor.

- Προσθέτουμε την ακόλουθη γραμμή στο τέλος του αρχείου και αποθηκεύουμε:
  export PATH=$PATH:$HOME/omnetpp-4.2.2/bin
- Τέλος, απαιτείται να κλείσουμε και να ανοίξουμε ξανά το τερματικό έτσι ώστε να επιδράσουν οι αλλαγές.

3.4. Διαμόρφωση και χτίσιμο του OMNeT++ (configuring and building)

- Μεταφερόμαστε στην κορυφή του φακέλου του OMNeT++ χρησιμοποιώντας την εντολή: $ cd omnetpp-4.2.2
- Εκτελούμε: $ ./configure
  Με αυτό τον τρόπο, εντοπίζεται το εγκατεστημένο λογισμικό και διαμορφώνεται το σύστημά μας. Τα αποτελέσματα εγγράφονται στο φάκελο Makefile.inc, ο οποίος θα διαβαστεί από τα makefiles κατά τη διάρκεια του χτισίματος.

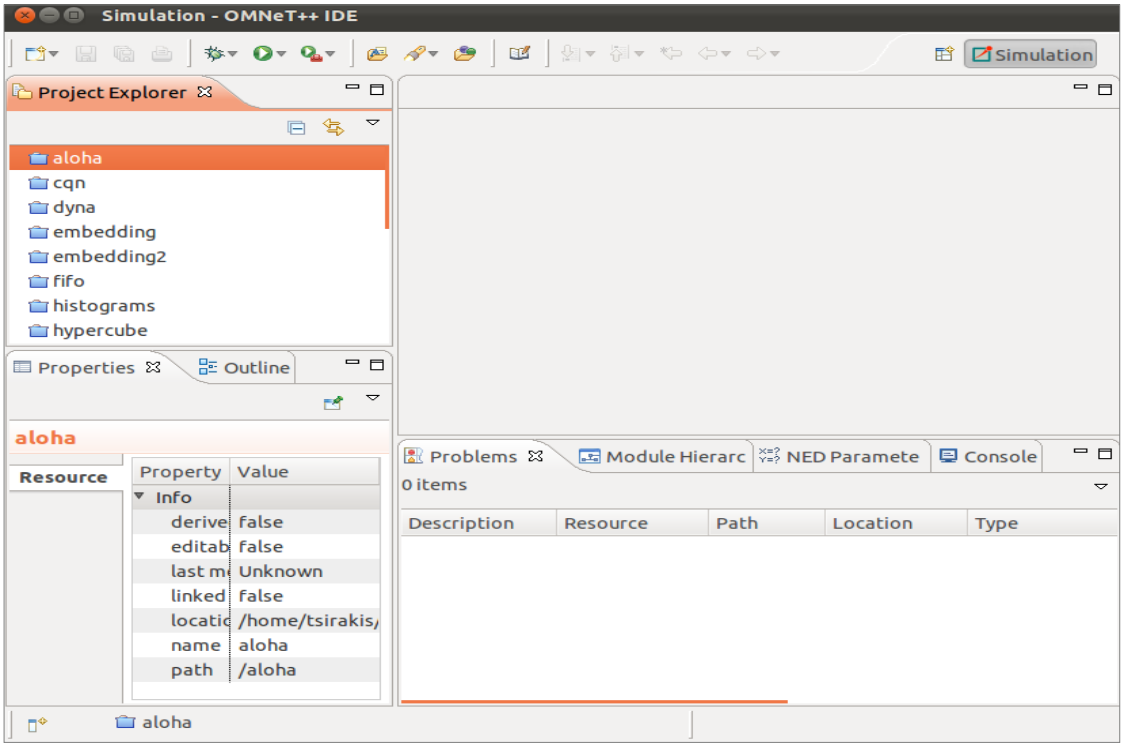


Εικόνα Π-3 Διαμόρφωση OMNeT++

- Όταν τελειώσει η εντολή ./configure, μπορούμε να κάνουμε compile το OMNeT++, εισάγοντας την εντολή:
  $ make

Εικόνα Π-4 Χτίσιμο OMNeT++

- Ανοίγουμε το περιβάλλον προσομοίωσης OMNeT++, εισάγοντας στο τερματικό την εντολή: $ omnetpp



Εικόνα Π-5 Περιβάλλον OMNeT++

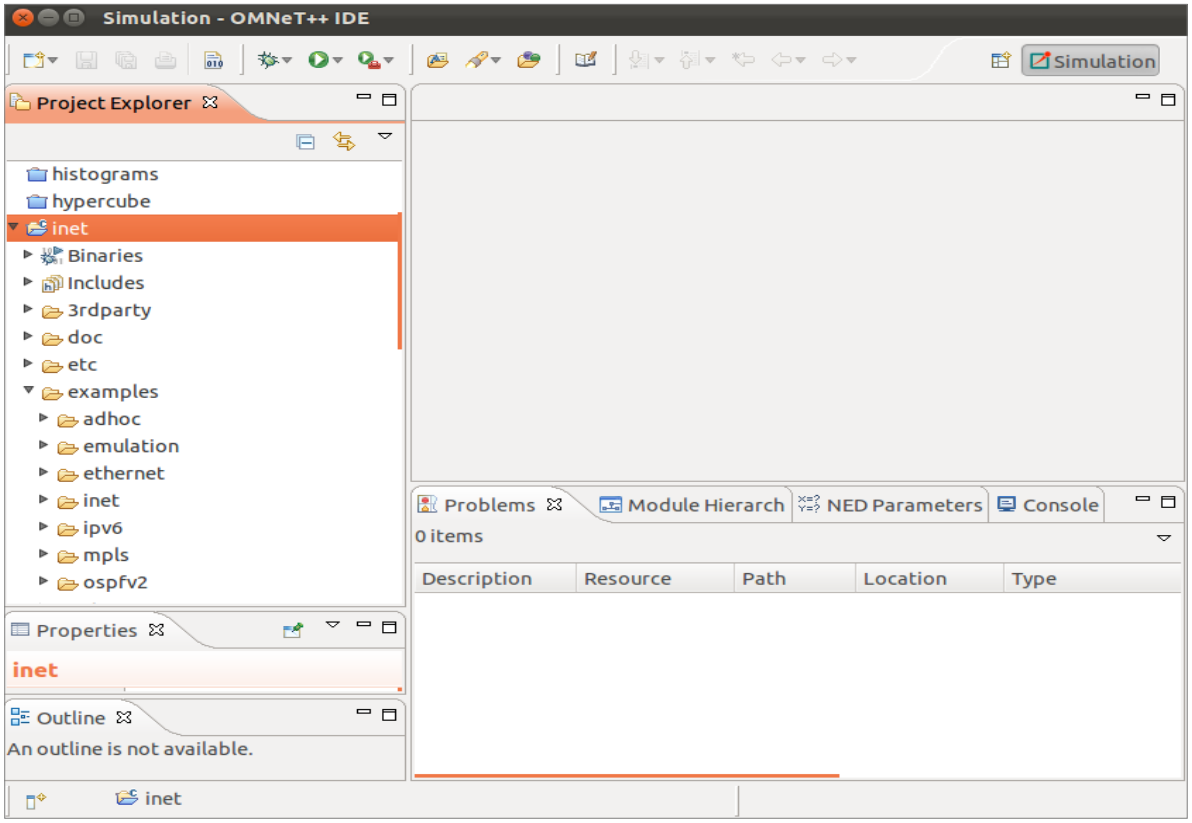
4. Εγκατάσταση INET Framework στο OMNeT++

4.1. Τι είναι το INET Framework

Το INET Framework περιέχει IPv4, IPv6, TCP, SCTP, UDP πρωτόκολλα και διάφορα μοντέλα εφαρμογών τους. Τα μοντέλα του στρώματος ζεύξεων δεδομένων είναι PPP, Ethernet και 802.11. Επίσης, υποστηρίζονται κινητές και ασύρματες προσομοιώσεις.

4.2. Εγκατάσταση INET Framework

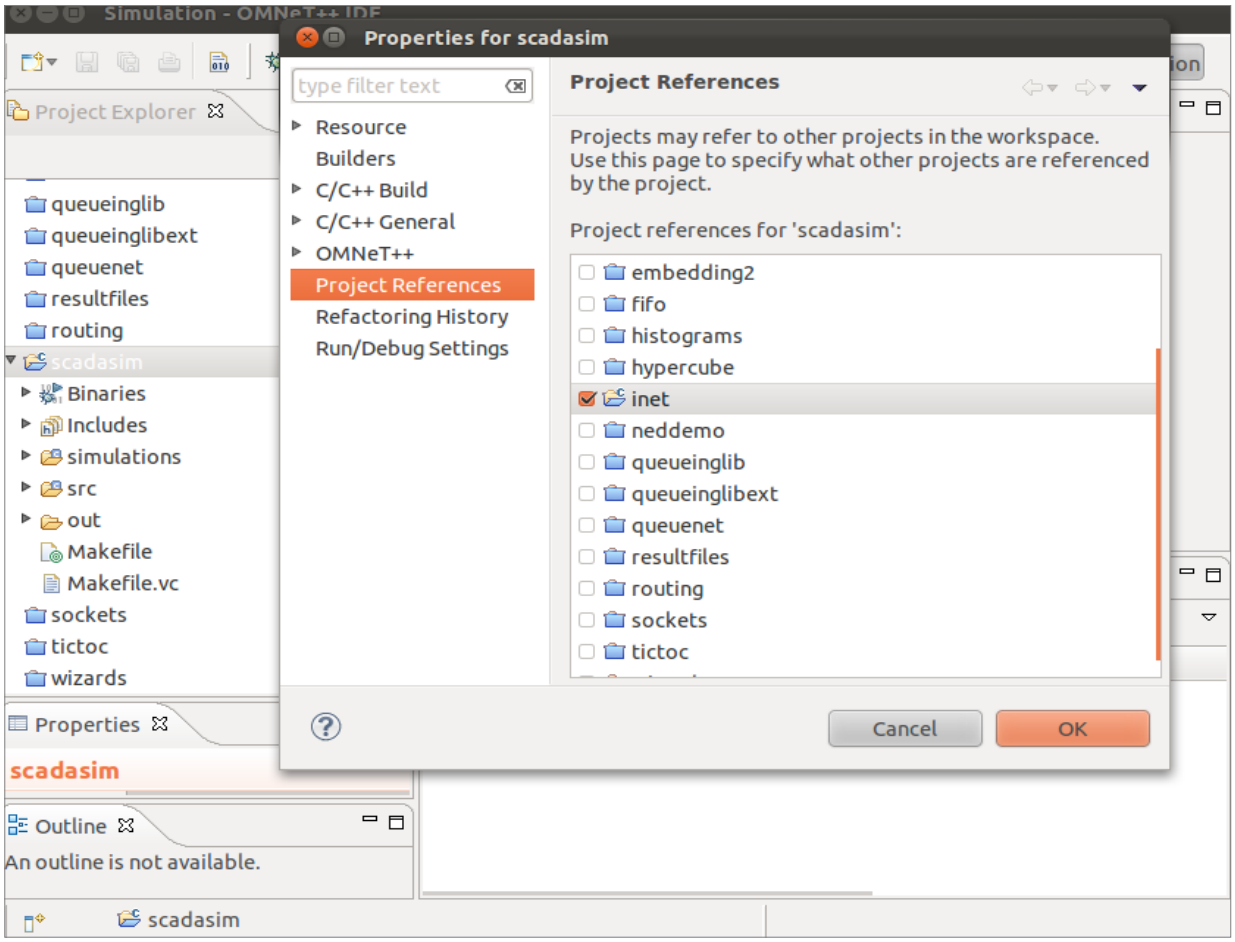
- Κατεβάζουμε την επιθυμητή έκδοση INET Framework, που αντιστοιχεί στην έκδοση OMNeT++ που ήδη έχουμε, από την ιστοσελίδα http://inet.omnetpp.org. Αποσυμπιέζουμε το αρχείο, όπως προηγουμένως.
- Στο περιβάλλον OMNeT++, επιλέγουμε *File* > *Import...* > *General* > *Existing Project into Workspace*. Εισάγουμε τη διαδρομή του **inet** φακέλου, που μόλις κατεβάσαμε, στο κενό *Select root directory*. Στη συνέχεια *Select All* και *Finish*.
- Το project **inet** θα εμφανιστεί αριστερά μαζί με τα άλλα αρχικά παραδείγματα του OMNeT++.
- *Δεξί κλικ στο project* ***inet*** > *Build Project*.



Εικόνα Π-6 INET Framework

5. Εγκατάσταση SCADASim στο OMNeT++

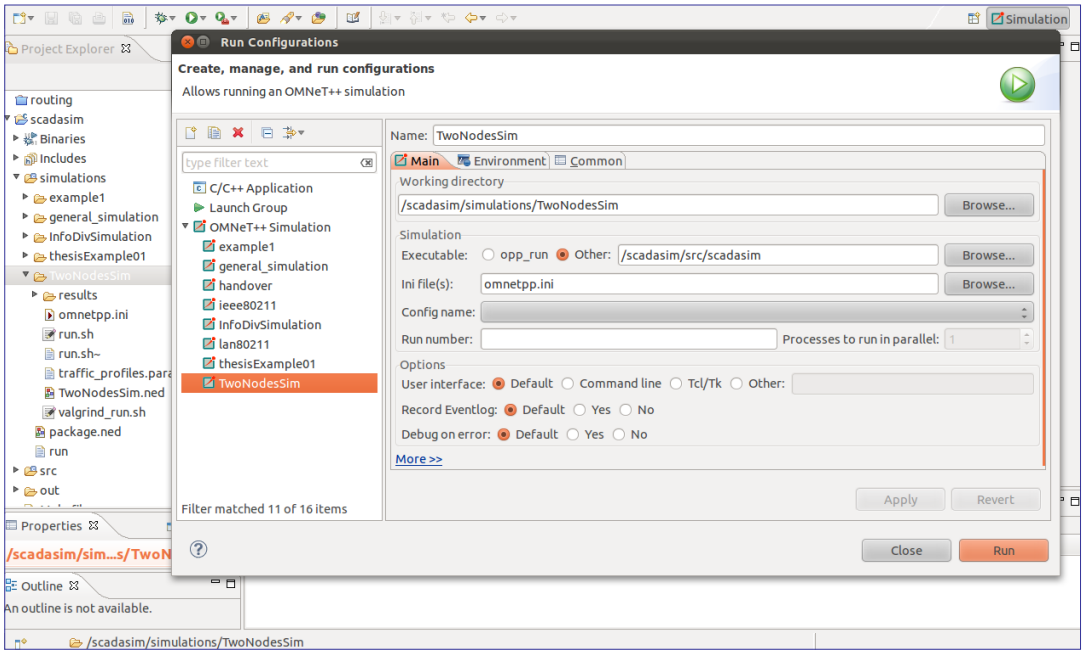
- Κατεβάζουμε το SCADASim από την ιστοσελίδα https://github.com/caxqueiroz/scadasim και αποσυμπιέζουμε το φάκελο.
- Ο συγκεκριμένος φάκελος δεν περιέχει κάποιο *.project* αρχείο. Έτσι, δεν μπορούμε να ακολουθήσουμε την ίδια διαδικασία όπως προηγουμένως (**inet** φακέλου) για την εισαγωγή του στο OMNeT++.Για αυτό το λόγο, δημιουργούμε ένα νέο κενό project.
- Στο περιβάλλον OMNeT++, επιλέγουμε *File* > *New* > *OMNet Project...* και το ονομάζουμε **scadasim**.
- Κάνουμε copy-paste τους φακέλους *source* και *simulations* του κατεβασμένου φακέλου στο νεοδημιουργηθέν project **scadasim**.
- Η βιβλιοθήκη του **scadasim** εξαρτάται από τη βιβλιοθήκη του **inet**. Έτσι, *Δεξί κλικ στο project* ***scadasim***> *Properties* > *Project References* και επιλέγουμε το **inet**.
- Τέλος, *Δεξί κλικ στο project* ***scadasim*** > *Build Project*.



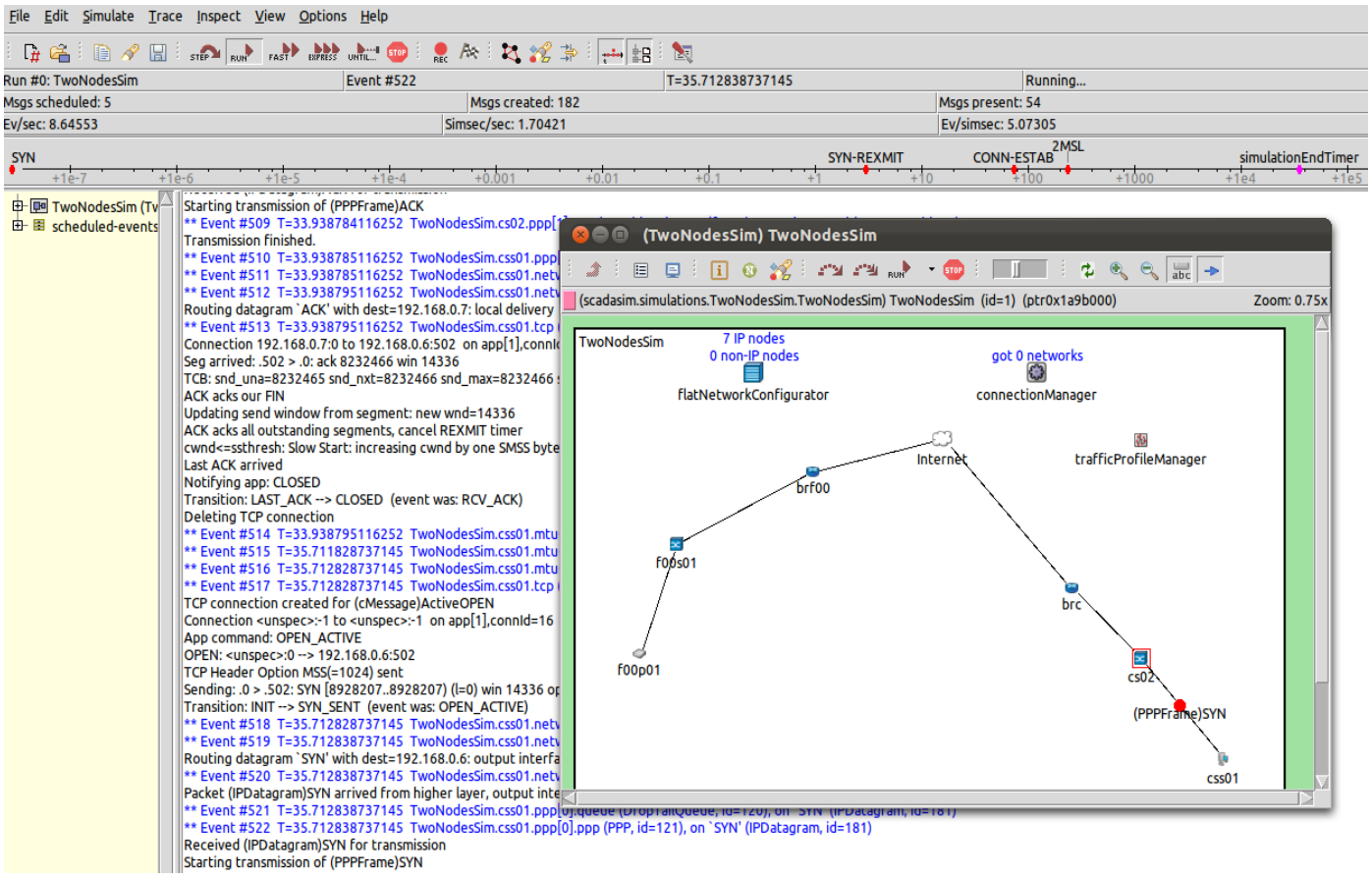
Εικόνα Π-7 Εξάρτηση του scadasim από το inet

6. Εκτέλεση προσομοιώσεων δειγμάτων

- Έστω ότι επιθυμούμε να εκτελέσουμε την προσομοίωση παράδειγμα που ονομάζεται *TwoNodesSim*.
- Επιλέγουμε το συγκεκριμένο φάκελο. Έπειτα, *Run* > *Run Configurations...* και διπλό κλικ στο OMNeT++ Simulations.
- Επιλέγουμε τα χαρακτηριστικά της προσομοίωσης και στη συνέχεια *Apply* > *Run*.



Εικόνα Π-8 Run Configurations



Εικόνα Π-9 Simulation: TwoNodesSim