ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΥΠΟΛΟΓΙΣΤΙΚΟ ΣΥΣΤΗΜΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΑΠΕΙΛΩΝ ΓΙΑ ΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ ΜΕ ΧΡΗΣΗ ΤΟΥ NETFLOW

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΣΠΗΛΙΟΣ ΕΥΜΟΡΦΟΣ

Επιβλέπων : Θεοδώρα Βαρβαρίγου
Καθηγήτρια Ε.Μ.Π.

Αθήνα, Οκτώβριος 2018

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΥΠΟΛΟΓΙΣΤΙΚΟ ΣΥΣΤΗΜΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΑΠΕΙΛΩΝ ΓΙΑ ΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ ΜΕ ΧΡΗΣΗ ΤΟΥ NETFLOW

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΣΠΗΛΙΟΣ ΕΥΜΟΡΦΟΣ

Επιβλέπων : Θεοδώρα Βαρβαρίγου
Καθηγήτρια Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 31η Οκτωβρίου 2018.

……	……..	……...
Θεοδώρα Βαρβαρίγου	Συμεών Παπαβασιλείου	Ιωάννα Ρουσσάκη
Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π	Καθηγήτρια Ε.Μ.Π.

Αθήνα, Οκτώβριος 2018

. . . . . .

Εύμορφος Σπήλιος

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

Περίληψη

Το ενδιαφέρον για κάθε είδος τέχνης έχει κατεξοχήν διττή φύση. Η μία πτυχή του είναι πάντα το αισθητικό ενδιαφέρον, δηλαδή το κατά πόσο το έργο που παρουσιάζεται είναι pleasing στις αισθήσεις του εκάστοτε individual. Η δεύτερη πτυχή είναι αυτή του κλινικού ενδιαφέροντος, δηλαδή του ενδιαφέροντος που έχει να κάνει με το methodology και την τεχνοτροπία που ο καλλιτέχνης χρησιμοποίησε για να αποτυπώσει νοήματα και σκέψεις, πχ γιατί στη Μόνα Λίζα ο Ντα βίντσι επέλεξε την τεχνοτροπία sfumato και όχι προοπτική σε γωνία και ούτω καθεξής.

Το δικό μου προσωπικό ambition ήταν πάντα ότι αυτή η λογική μελέτης (αυτή η δυική φύση ενδιαφέροντος) μπορεί να υιοθετηθεί από το μέσο άνθρωπο και για την επιστήμη και την τεχνολογία. Δηλαδή να μπορεί κάποιος που είναι επιστήμων να εκτιμήσει τα concepts μίας επιστημονικής σύλληψης γιατί κατανοεί τα specific principals των οποίων το interaction παράγει τη νέα αυτή δομή γνώσης(κλινικό ενδιαφέρον), αλλά παράλληλα να μπορεί κάποιος που δεν είναι αρκούντως καταρτισμένος να εκτιμήσει μία νέα ιδέα από αισθητικής πλευράς, δηλαδή να μπορεί να συλλάβει σε αφηρημένη μορφή το περί τίνος πρόκειται και να λάβει την ευχαρίστηση της αντίληψης σε abstract level του πως αυτή η ιδέα αλλάζει τη ζωή όλων και μαζί και τη δική του(αισθητικό ενδιαφέρον).

Με αυτή τη λογική χτίστηκε και η παρούσα διπλωματική. Το πρώτο κομμάτι απευθύνεται σε οποιονδήποτε, καταρτισμένο ή μη, να κατανοήσει επαρκώς τις βασικές αρχές της νέας πραγματικότητας του Διαδικτύου των Πραγμάτων και πως αυτές αλλάζουν τη ζωή μας. Το δεύτερο κομμάτι απευθύνεται περισσότερο στο κλινικό ενδιαφέρον του αναγνώστη με την περιγραφή μίας μεθόδου adaptive sampling και της δικαιολόγησης του γιατί αυτή είναι προτιμητέα για ένα οικοσύστημα IoT από άλλες αντίστοιχες μεθόδους.

Λέξεις κλειδιά

Διαδίκτυο των Πραγμάτων, IoT, NetFlow, δίκτυο, sampling,

Abstract

The interest in every kind of art has a predominantly dual nature. The first aspect of it is always the aesthetic interest, that is, the extent to which the work presented is pleasing to everyone's senses. The second aspect is that of clinical interest, that is, interest in the methodology and technology that the artist used to capture meanings and thoughts, for example what is the inherent reason why Da Vinci chose the sfumato style and not a perspective at an angle to create the Mona Lisa and so on

My own personal ambition has always been that this logic of study (this dual nature of interest) can be adopted by the average person and for science and technology. That is, it is possible for one who is a scientist to appreciate the concepts of a scientific idea because they understand the specific principals whose interaction produces this new knowledge structure (clinical interest), but at the same time that someone who is not sufficiently qualified can appreciate a new idea from an aesthetic standpoint, that is to be able to capture in abstract form what it is about and to receive the pleasure of perception on abstract level of how this idea changes the life of everyone and their own (aesthetic interest)

With this logic the present diploma was built. The first piece is addressed to anyone, trained or not, to understand the basic principles of the new reality of the Internet of Things and how they change our lives. The second part focuses more on the clinical interest of the reader by describing an adaptive sampling method and justifying why this is preferable for an IoT ecosystem by other similar methods

Key words

Internet of Things, IoT, NetFlow, network, sampling

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο του προπτυχιακού προγράμματος σπουδών της Σχολής Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου. Μέσω αυτής είχα τη δυνατότητα να διευρύνω τις γνώσεις μου πάνω στο Διαδίκτυο των πραγμάτων καθώς και πιο specific έννοιες που έχουν να κάνουν με το πώς πραγματοποιείται η δειγματοληψία σε ένα IoT οικοσύστημα. Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου Πρωτονοτάριο Εμμανουήλ, για την δυνατότητα που μου προσέφερε να εργαστώ πάνω στον τομέα του διαδικτύου των πραγμάτων, καθώς και για τις πολύτιμες συμβουλές του καθόλη τη διάρκεια των μαθημάτων και της εκπόνησης της διπλωματικής μου εργασίας, καθώς επίσης και για την επιρροή που ασκεί καθημερινά στο πως βλέπω το όλο context του τι σημαίνει να είσαι ηλεκτρολόγος μηχανικός. Παράλληλα θα ήθελα να ευχαριστήσω τους Θεοδώρα Βαρβαρίγου,Καθηγήτρια Ε.Μ.Π, Συμεών Παπαβασιλείου, Καθηγητή Ε.Μ.Π και Ιωάννα Ρουσσάκη, Καθηγήτρια Ε.Μ.Π, που με τίμησαν με την παρουσία τους στην επιτροπή εξέτασης της διπλωματικής εργασίας. Θα ήθελα να ευχαριστήσω ξεχωριστά και τον κ. Νικόλαο Μπάκαλο, Ε.ΔΙ.Π Ε.Μ.Π. για την πολύτιμη βοήθεια του στην εκπόνηση της συγκεκριμένης εργασίας. Ξεχωριστή μνεία θα ήθελα να κάνω στη σημαντική βοήθεια και στήριξη που έλαβα από το φίλο και συνεργάτη μου Γιώργο Βλαχοδημητρόπουλο και τον ευχαριστώ θερμά για αυτό. Τέλος θέλω να ευχαριστήσω με όλη μου την καρδιά τον πατέρα μου Παναγιώτη Εύμορφο για τη στήριξη και καθοδήγησή του σε όλη τη διάρκεια της ακαδημαικής μου πορείας, από το δημοτικό μέχρι σήμερα, καθώς επίσης τη μητέρα μου, Βασιλική Καραμάμη, για την αγάπη και τη βοήθειά της σε κάθε έκφανση της μέχρι τώρα ζωής μου.

Σπήλιος Εύμορφος,

Αθήνα, 30η Οκτωβρίου 2018

Πίνακας περιεχομένων

1 Internet of Things

1.1 Γενική επισκόπηση

Βλέπουμε την αυγή μιας νέας εποχής του Ίντερνετ των πραγμάτων (Internet of Things), επίσης γνωστή ως Διαδίκτυο των Αντικειμένων).Σε γενικές γραμμές, το IoT αναφέρεται στη δικτυωμένη διασύνδεση καθημερινών αντικειμένων, τα οποία είναι συχνά εξοπλισμένα με πανταχού παρούσα νοημοσύνη. Το Διαδίκτυο των Πραγμάτων θα αυξήσει την πανταχού παρούσα ζωή του Διαδικτύου με την ενσωμάτωση κάθε αντικειμένου για αλληλεπίδραση μέσω ενσωματωμένων συστημάτων, γεγονός που οδηγεί σε ένα εξαιρετικά κατανεμημένο δίκτυο συσκευών που επικοινωνούν με ανθρώπους καθώς και άλλες συσκευές. Χάρη στην ταχεία πρόοδο των βασικών τεχνολογιών, το IoT ανοίγει τεράστιες ευκαιρίες για μεγάλο αριθμό νέων εφαρμογών που υπόσχονται να βελτιώσουν την ποιότητα της ζωής μας. Τα τελευταία χρόνια, το IoT κέρδισε μεγάλη προσοχή από ερευνητές και επαγγελματίες από όλο τον κόσμο

Πριν την αναλυτικότερη παρουσίασή του, κρίνεται σκόπιμο να ξεκαθαρίσουμε ότι ενώ ορισμένοι εξισώνουν τη νέα αυτή τεχνολογία με την επικοινωνία μηχανής με μηχανή (M2M), μια τέτοια ταύτιση δεν είναι σωστή

Η επικοινωνία μεταξύ συσκευών ορίζεται ως οι τεχνολογίες που επιτρέπουν σε μηχανές, τυπικά (μικρούς) υπολογιστικούς αισθητήρες που εκτελούν ειδικά καθήκοντα (ευφυΐα), να επικοινωνούν ή να αναμεταδίδουν πληροφορίες που απαιτούνται, συνήθως μέσω απλών πρωτοκόλλων αλλά πιο πρόσφατα πάνω από το Πρωτόκολλο Διαδικτύου (IP) μέσω ασύρματης ή ενσύρματης επικοινωνίας, ακόμα και μέσω Υπηρεσίας Σύντομου Μηνύματος (SMS).

Αφορά την αλληλεπίδραση με τα αντικείμενα γύρω μας, ακόμη και με στατικά μη-έξυπνα αντικείμενα και την αύξηση τέτοιων αλληλεπιδράσεων σε πλαίσια που παρέχονται από τη γεωγραφική θέση, το χρόνο και ούτω καθεξής. Ακόμα και μη-ευφυείς/μη-συνδεδεμένες συσκευές μπορούν να ενταχθούν στο IoT μέσω π.χ. ενός έξυπνου τηλεφώνου που λειτουργεί ως πύλη για το Διαδίκτυο. Έχει να κάνει, για παράδειγμα, με την αλληλεπίδραση μέσω barcode (γραμμικού κώδικα) με το βιβλίο που διαβάζουμε, μέσω NFC (Near Field Communication –Επικοινωνία κοντινού πεδίου) με μια αφίσα, ή με μια διαφήμιση σε εφημερίδα μέσω μικρού κώδικα. Έτσι, η M2M τεχνολογία δεν συνιστά το Διαδίκτυο των Πραγμάτων, αλλά είναι υποσύνολό του. (Ευφροσύνη Θ. Ζώτου, 2012)

Το IoT είναι ένας όρος ομπρέλα με πολλές περιπτώσεις χρήσης, τεχνολογίες, πρότυπα και εφαρμογές. Επιπλέον, αποτελεί μέρος μιας μεγαλύτερης πραγματικότητας με ακόμα περισσότερες τεχνολογίες. Τα πράγματα και τα δεδομένα είναι το σημείο εκκίνησης και η ουσία του τι επιτρέπει και σημαίνει το IoT. Οι συσκευές και τα περιουσιακά στοιχεία του Διαδικτύου είναι εξοπλισμένα με ηλεκτρονικά μέσα, όπως αισθητήρες και ενεργοποιητές, ηλεκτρονικά στοιχεία συνδεσιμότητας / επικοινωνίας και λογισμικό για τη συλλογή, το φιλτράρισμα και την ανταλλαγή δεδομένων για τον εαυτό τους, την κατάσταση και το περιβάλλον τους

Η σύνδεση των «πραγμάτων» του IoT και η χρήση των δεδομένων του IoT επιτρέπουν διάφορες βελτιώσεις και καινοτομίες στη ζωή των καταναλωτών, των επιχειρήσεων, της υγειονομικής περίθαλψης, της κινητικότητας, των πόλεων και της κοινωνίας. Οι δυνητικοί στόχοι της Διασύνδεσης Διαδικτύου συχνά κατατάσσονται σε περιπτώσεις χρήσης IoT. Παραδείγματα: παρακολούθηση της υγείας, παρακολούθηση περιουσιακών στοιχείων, παρακολούθηση του περιβάλλοντος, πρόβλεψη συντήρησης και οικιακή αυτοματοποίηση (I-scoop.eu, 2018)

Υπάρχουν εκατοντάδες περιπτώσεις χρήσης IoT, ανάλογα με τη βιομηχανία και / ή τον τύπο της εφαρμογής. Ορισμένες υποθέσεις χρήσης IoT υπάρχουν σε διάφορες βιομηχανίες, άλλες είναι πιο κάθετες. Ένα παράδειγμα: η παρακολούθηση στοιχείων ενεργητικού είναι μια υπόθεση γενικής χρήσης. Θα μπορούσε να είναι μια εφαρμογή καταναλωτών για να μάθετε πού είναι το κατοικίδιο ζώο ή το skateboard σας. Αλλά θα μπορούσε επίσης να σημαίνει την παρακολούθηση εμπορευματοκιβωτίων σε ένα τεράστιο φορτηγό πλοίο. Η ίδια βασική αρχή, ένας κόσμος διαφορετικός όσον αφορά τις τεχνολογίες και το πλαίσιο της γενικότερης χρήσης τους.

Το IoT αποτελεί ουσιαστικό οδηγό για την καινοτομία που βασίζεται στον πελάτη, τη βελτιστοποίηση των δεδομένων και τον αυτοματισμό, τον ψηφιακό μετασχηματισμό, το R&D και τις εντελώς νέες εφαρμογές, τα επιχειρηματικά μοντέλα και τις ροές εσόδων σε όλους τους τομείς

Το Διαδίκτυο των πραγμάτων είναι το λογικό επόμενο βήμα στην εξέλιξη του Διαδικτύου και αποτελεί συνέχεια των δικτύων και τεχνολογιών M2M (μηχανή-μηχανή), που βασίζεται και επεκτείνει τις τεχνολογίες του M2M, των κινητών τεχνολογιών, της RFID και άλλων

Οι προβλέψεις δείχνουν ότι το σύμπαν του Ίντερνετ των Αντικειμένων θα έχει 20 έως 30 δισεκατομμύρια συνδεδεμένες συσκευές μέχρι το 2020. Το IoT εκτείνεται πέρα από αυτές τις ρίζες ενώ τις περιβάλλει και γίνεται όλο και πιο δημοφιλές λόγω πολλών παραγόντων, συμπεριλαμβανομένου του χαμηλότερου κόστους αισθητήρων και τεχνολογιών των δικτύων (I-scoop.eu, 2018)

Το Διαδίκτυο των πραγμάτων συγκεντρώνει βιομηχανίες και επιχειρηματικούς τομείς, ενώνοντας την τεχνολογία της πληροφορικής και την επιχειρησιακή τεχνολογία (IT και OT) και συμβάλλοντας στον βιομηχανικό μετασχηματισμό (Industry 4.0) και ένα κύμα χρήσης περιπτώσεων σε αυτό που ονομάζεται Βιομηχανική Διασύνδεση και είναι το μεγαλύτερο τμήμα του Διαδικτύου εφαρμογών και επενδύσεων. Οι κυριότεροι τομείς των επενδύσεων στο Διαδίκτυο των πραγμάτων (βιομηχανίες και περιπτώσεις χρήσης) περιλαμβάνουν τις μεταποιητικές δραστηριότητες, τις μεταφορές, τις τεχνολογίες έξυπνων δικτύων, τα έξυπνα κτίρια.

1.2 Κατανόηση του Internet of Things

Για να κατανοήσει κανείς τα οφέλη, την αξία, το περιβάλλον και ακόμη και τις τεχνολογίες του IoT, είναι σημαντικό να δει παραδείγματα σε διάφορες εφαρμογές και βιομηχανίες.

Παρόλο που το IoT προσεγγίζεται συχνά σαν να ήταν ένα «πράγμα» ως τέτοιο, πρέπει να κατανοήσουμε τις διαφορές από την άποψη των εφαρμογών σε τομείς όπως το βιομηχανικό διαδίκτυο των πραγμάτων, το Διαδίκτυο των καταναλωτών των πραγμάτων. (Al-Fuqaha et al., 2015)

Η χρήση του Ίντερνετ των πραγμάτων συμβαίνει με διαφορετικές ταχύτητες. Οι επενδύσεις διαδικτύου στον τομέα της μεταποιητικής βιομηχανίας, για παράδειγμα, είναι πολύ υψηλότερες από ό, τι σε κάθε άλλη κάθετη βιομηχανία και στον χώρο του Διαδικτύου των καταναλωτών (Consumer Internet of Things)

Αυτό είναι έτοιμο να αλλάξει μέχρι το 2020, αν και σε παγκόσμιο επίπεδο η παραγωγή θα εξακολουθήσει να αντιπροσωπεύει την πλειονότητα των δαπανών για το διαδίκτυο (υλικό, λογισμικό, υπηρεσίες και συνδεσιμότητα)

Η μεταποιητική βιομηχανία, μαζί με τις μεταφορές και τις επιχειρήσεις κοινής ωφέλειας, είναι οι τρεις κύριοι επενδυτικοί τομείς του διαδικτύου και αποτελούν μέρος του βιομηχανικού διαδικτύου των πραγμάτων(Industrial Internet of Things)

1.3 Οι απαρχές του IoT σα νέα τεχνολογική οντότητα

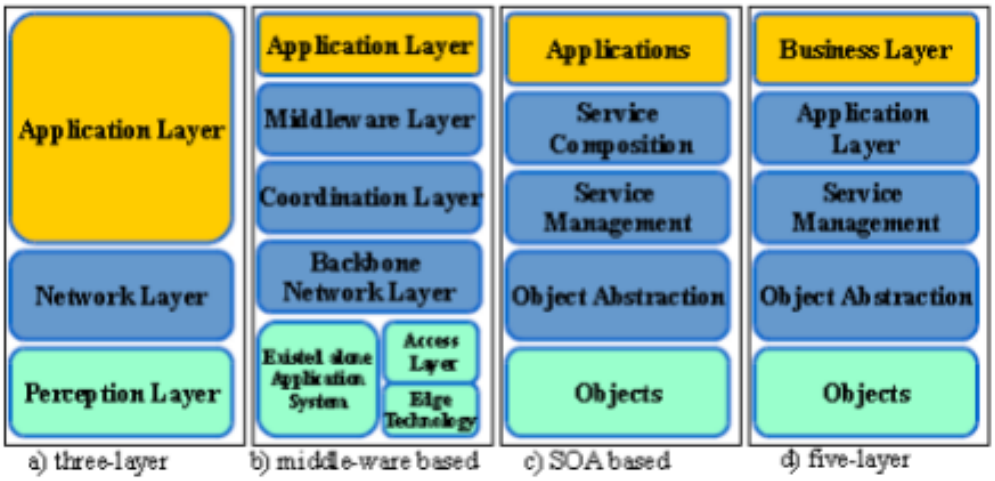
Η ιδέα του Διαδικτύου των πραγμάτων πηγαίνει πίσω αρκετό καιρό. Ξεκίνησε στο τέλος της προηγούμενης χιλιετίας, όπου η RFID τεχνολογία υπήρξε βασική εξέλιξη προς το Διαδίκτυο των πραγμάτων και ο όρος Internet των πραγμάτων έχει σχεδιαστεί σε ένα πλαίσιο RFID (και NFC), όπου χρησιμοποιήθηκε RFID για την παρακολούθηση αντικειμένων σε διάφορες λειτουργίες, όπως η διαχείριση της αλυσίδας εφοδιασμού και τα logistics (I-scoop.eu, 2018)

Οι ρίζες και η προέλευση του Ίντερνετ των πραγμάτων ξεπερνούν ακριβώς την τεχνολογία RFID. Όπως για παράδειγμα τα δίκτυα μηχανής-μηχανής (M2M) ή τα ATM (αυτόματη ταμειακή μηχανή ή ταμειακές μηχανές), τα οποία συνδέονται με διατραπεζικά δίκτυα, ακριβώς όπως το σημείο των τερματικών πώλησης όπου γίνεται η πληρωμή με τις κάρτες ATM. Οι λύσεις M2M για ATM υπήρξαν για μεγάλο χρονικό διάστημα, όπως και η RFID. Αυτές οι παλαιότερες μορφές δικτύων, συνδεδεμένων συσκευών και δεδομένων προέρχονται από το Διαδίκτυο των Πράξεων. Ωστόσο, δεν είναι το Διαδίκτυο των πραγμάτων με την τωρινή του ανεπτυγμένη μορφή.

1.4 Το γενικό framework του architecture του IoT

Το IoT θα πρέπει να είναι σε θέση να παρέχει επικοινωνία σε δισεκατομμύρια ή τρισεκατομμύρια ετερόκλητα αντικείμενα μέσω του Διαδικτύου. Έτσι υπάρχει μια κρίσιμη ανάγκη για ευέλικτη πολύ επίπεδη αρχιτεκτονική. Ο συνεχώς αυξανόμενος αριθμός προτεινόμενων αρχιτεκτονικών ακόμα δεν συγκλίνει σε ένα μοντέλο αναφοράς. Εν τω μεταξύ, υπάρχουν ορισμένα έργα όπως IoT-A, το οποίο προσπαθεί να σχεδιάσει μια κοινή αρχιτεκτονική που να βασίζεται στην ανάλυση των αναγκών των ερευνητών και της βιομηχανίας.

Από το “pool” των προτεινόμενων μοντέλων, το βασικό μοντέλο αρχιτεκτονικής είναι αυτό των τριών επιπέδων (3-layer), αποτελούμενο από τα στρώματα εφαρμογής, δικτύου και αντίληψης. Ωστόσο, στην πρόσφατη βιβλιογραφία, κάποια άλλα μοντέλα έχουν προταθεί που προσθέτουν μια πιο αφηρημένη IoT αρχιτεκτονική.



Η αρχιτεκτονική του IoT [13]

Objects/Perception Layer: Το πρώτο στρώμα, τα Αντικείμενα (συσκευές) ή στρώμα Αντίληψης, αντιπροσωπεύει τους φυσικούς αισθητήρες του IoT, που στοχεύουν στη συλλογή και επεξεργασία πληροφοριών. Αυτό το στρώμα περιλαμβάνει αισθητήρες και ενεργοποιητές, οι οποίοι εκτελούν διάφορες λειτουργίες, όπως η υποβολή ερωτημάτων θέσεως, θερμοκρασίας, βάρους, κίνησης, δόνησης, επιτάχυνσης, υγρασίας, κ.τ.λ. Τυποποιημένοι μηχανισμοί plug-and-play πρέπει να χρησιμοποιούνται από αυτό το επίπεδο για να ρυθμίζονται τα ετερόκλητα αντικείμενα. Το στρώμα Αντίληψης ψηφιοποιεί και μεταφέρει δεδομένα στο Object Abstraction layer μέσω ασφαλών καναλιών.

Object Abstraction layer: Το Object Abstraction layer μεταφέρει τα δεδομένα που παράγονται από το στρώμα Αντίληψης ή Αντικειμένων στο στρώμα Διαχείρισης Υπηρεσιών –Service Management μέσω ασφαλών καναλιών. Τα δεδομένα μπορούν να μεταφερθούν μέσω διαφόρων τεχνολογιών όπως RFID, 3G, GSM, UMTS, Wi-Fi, Bluetooth Low Energy, infrared, ZigBee κ.α. Επιπλέον, άλλες λειτουργίες όπως το cloud computing και οι διαδικασίες διαχείρισης δεδομένων είναι χειρίσιμες σε αυτό το στρώμα.

Service Management Layer: Το στρώμα Διαχείρισης ή Middleware συνδυάζει μια υπηρεσία με τον αιτούντα αυτής, βάση διεύθυνσης ή ονόματος. Αυτό το στρώμα ενεργοποιεί τους IoT προγραμματιστές εφαρμογών να δουλέψουν με ετερογενή αντικείμενα χωρίς να λαμβάνουν υπόψη μια συγκεκριμένη πλατφόρμα υλικών. Επιπλέον, αυτό το στρώμα επεξεργάζεται τα ληφθέντα δεδομένα, παίρνει αποφάσεις και παραδίδει τις απαιτούμενες υπηρεσίες μέσω πρωτοκόλλων ενσύρματων δικτύων.

Application Layer: Το στρώμα Εφαρμογής παρέχει τις υπηρεσίες που ζητούν οι πελάτες. Για παράδειγμα, το στρώμα αυτό μπορεί να παρέχει μετρήσεις θερμοκρασίας και υγρασίας αέρα στον πελάτη που ρωτά για αυτά τα δεδομένα. Η σημασία αυτού του στρώματος για το IoT είναι ότι έχει τη δυνατότητα να παρέχει έξυπνες υπηρεσίες υψηλής ποιότητας για την κάλυψη των αναγκών των πελατών. Το στρώμα Εφαρμογής

καλύπτει πολλές κάθετες αγορές όπως το έξυπνο σπίτι, κτήριο, μεταφορές, Βιομηχανικοί Αυτοματισμοί και την έξυπνη υγειονομική περίθαλψη.

Business Layer: Το Επιχειρησιακό στρώμα (management) διαχειρίζεται τις συνολικές IoT δραστηριότητες και υπηρεσίες του συστήματος. Οι ευθύνες αυτού του επιπέδου είναι να οικοδομήσει ένα επιχειρηματικό μοντέλο, γραφικές παραστάσεις, διαγράμματα ροής κ.λ.π., βάσει των ληφθέντων δεδομένων από το στρώμα Εφαρμογής. Επίσης, αναλύει, σχεδιάζει, υλοποιεί, αξιολογεί, παρακολουθεί, αναπτύσσει συσχετιζόμενα IoT στοιχεία και υποστηρίζει τη διαδικασία λήψης αποφάσεων, με βάση την ανάλυση μεγάλου όγκου δεδομένων (Big Data). Επιπλέον, αυτό το στρώμα συγκρίνει το αποτέλεσμα του κάθε επιπέδου με το αναμενόμενο αποτέλεσμα για την βελτίωση των υπηρεσιών και τη διατήρηση του απόρρητου των χρηστών. (Al-Fuqaha et al., 2015)

Οι αρχιτεκτονικές που δανείζονται τα στρώματα και τις έννοιες τους από στοίβες δικτύου (όπως το μοντέλο των τριών επιπέδων), δεν ανταποκρίνονται σε πραγματικά IoT περιβάλλοντα, δεδομένου ότι, π.χ., το στρώμα «δικτύου» δεν καλύπτει όλες τις υποκείμενες τεχνολογίες οι οποίες μεταφέρουν δεδομένα σε μια IoT πλατφόρμα. Επιπλέον, αυτά τα μοντέλα έχουν σχεδιαστεί για συγκεκριμένους τύπους μέσων επικοινωνίας όπως το WSNs. Το πιο σημαντικό είναι ότι τα στρώματα θα "τρέχουν" σε συσκευές περιορισμένων πόρων. Για το λόγο αυτό, δεν είναι αποδεκτό ένα στρώμα σαν το Service Composition-Σύσταση Υπηρεσίας στην SoA (Service oriented Architecture) αρχιτεκτονική, να καταλαμβάνει ένα μεγάλο κλάσμα του χρόνου και της ενέργειας της συσκευής για να επικοινωνήσει με άλλες συσκευές και να ενσωματώσει τις απαραίτητες υπηρεσίες.

Στο μοντέλο των πέντε στρωμάτων, το στρώμα Εφαρμογών είναι η διασύνδεση με την οποία οι τελικοί χρήστες μπορούν να αλληλεπιδράσουν με μια συσκευή και να θέτουν ερωτήματα. Παρέχει επίσης μια διεπαφή στο στρώμα Επιχειρήσεων, όπου υψηλού επιπέδου ανάλυση και αναφορές μπορούν να παραχθούν. Οι μηχανισμοί ελέγχου της πρόσβασης στα δεδομένα σε επίπεδο Εφαρμογής, γίνεται επίσης σε αυτό το στρώμα. Λαμβάνοντας υπόψη όλα τα παραπάνω από την μια πλευρά και την απλότητα της αρχιτεκτονικής από την άλλη, το μοντέλο των πέντε-στρωμάτων είναι το πιο εφαρμόσιμο για τις IoT εφαρμογές.

Πρέπει να σημειωθεί, ωστόσο, πως επί του παρόντος, δεν υπάρχει κάποια ευρέως αποδεκτή αρχιτεκτονική του Διαδικτύου των Πραγμάτων. Αρκετά άρθρα προτείνουν διάφορες εννοιολογικές αρχιτεκτονικές σχεδίασης, ενώ άλλα προτείνουν κριτήρια για την αξιολόγηση των προτεινόμενων αρχιτεκτονικών, καθώς και μια εννοιολογική αρχιτεκτονική που να ανταποκρίνεται στις απαιτήσεις των έξυπνων αντικειμένων.

1.5 Τεχνολογία RFID

Στη δεκαετία του '90, τεχνολογίες όπως η RFID, οι αισθητήρες και μερικές ασύρματες καινοτομίες οδήγησαν σε διάφορες εφαρμογές στη σύνδεση συσκευών και "πραγμάτων"

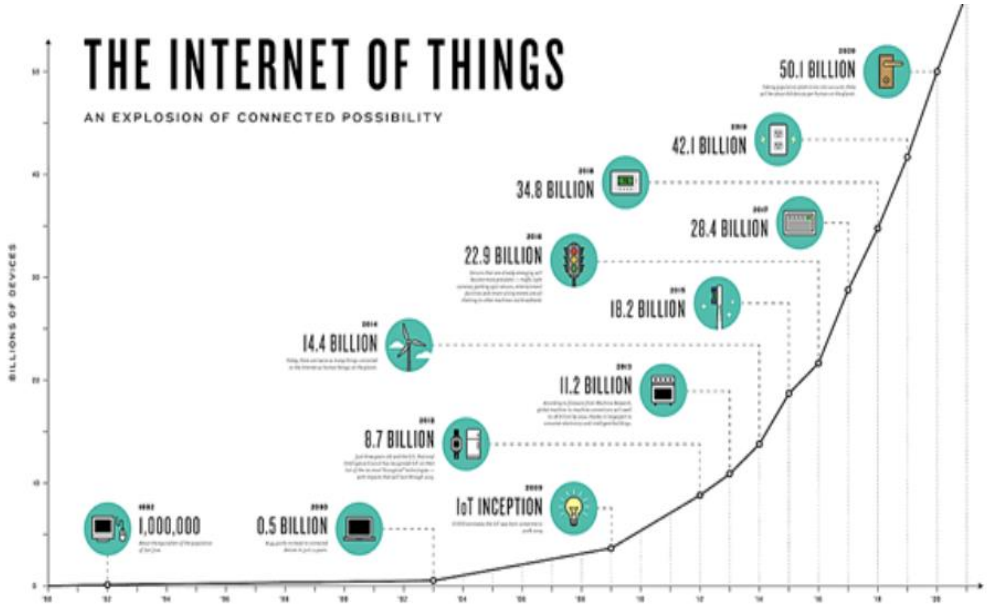
Οι περισσότερες πραγματικές εφαρμογές RFID σε εκείνες τις ημέρες συνέβησαν στην εφοδιαστική, τις αποθήκες και την αλυσίδα εφοδιασμού γενικά. Ωστόσο, υπήρξαν πολλές προκλήσεις και εμπόδια για να ξεπεραστούν, όπως εξηγήθηκε κατά το τέλος του 1999 σε μια λευκή βίβλο από έναν Βέλγο ειδικό του RFID που είχε ως στόχο τη βιομηχανία εφοδιαστικής (κυρίως αποθήκευση και βιομηχανική εφοδιαστική, καθώς η RFID εξακολουθεί να είναι δαπανηρή) (I-scoop.eu, 2018)

Σταδιακά, η χρήση της τεχνολογίας RFID (και μαζί με αυτήν, πολλές τεχνολογίες ασύρματης επικοινωνίας κοντά στην περιοχή) έγινε δημοφιλής σε περιοχές πέραν της εφοδιαστικής και της διαχείρισης της εφοδιαστικής αλυσίδας: από τις δημόσιες συγκοινωνίες, την ταυτοποίηση (από κατοικίδια σε ανθρώπους) συλλογή , έλεγχος πρόσβασης και έλεγχος ταυτότητας, παρακολούθηση της κυκλοφορίας, λιανική πώληση και καινοτόμες μορφές εξωτερικής διαφήμισης. Αυτή η αυξανόμενη χρήση οφείλεται, μεταξύ άλλων, στην μείωση του κόστους των ετικετών RFID, στην αύξηση της τυποποίησης και της NFC

1.6 Το πέρασμα από την τεχνολογία RFID σε M2M δίκτυα

Η δυνατότητα επισήμανσης, παρακολούθησης, σύνδεσης και "ανάγνωσης" και ανάλυσης δεδομένων από αντικείμενα πήγε χέρι-χέρι με αυτό που θα γίνει γνωστό ως το Διαδίκτυο των Πραγμάτων γύρω στις αρχές αυτής της Χιλιετίας

Ήταν προφανές ότι η σύνδεση των τύπων των "πραγμάτων" και των εφαρμογών - όπως ήταν φανερό στην τεχνολογία RFID με το Διαδίκτυο θα άλλαζε πολύ. Μπορεί να μην είναι τόσο προφανές, αλλά οι έννοιες των συνδεδεμένων ψυγείων, που ενημερώνουν για την ανάγκη αγοράς συγκεκριμένων αγαθων , την έννοια των γνωστών ως έξυπνων πόλεων και το όραμα μιας εντυπωσιακής εμπειρίας αγορών (χωρίς σάρωση με γραμμικό κώδικα και αξιοποίηση έξυπνων πληροφοριών σε πραγματικό χρόνο που λαμβάνονται μέσω συνδεδεμένων συσκευών και αγαθών) επιστρέφουν από τότε που υπήρχε ακόμη ο όρος Ίντερνετ των πραγμάτων



1.7 Ορισμός του IoT σε ευρύτερο πλαίσιο (intuitive)

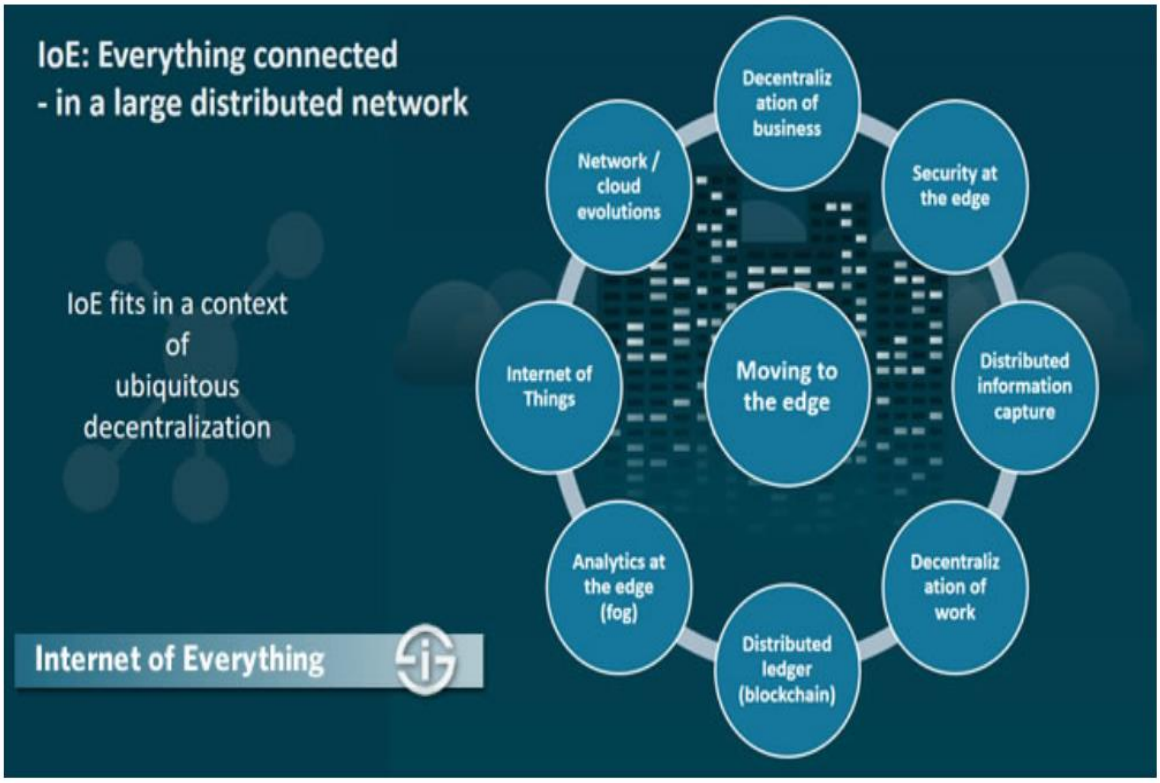
Το Διαδίκτυο των πραγμάτων είναι η διασυνδεδεμένη σφαίρα των φυσικών συσκευών με το Διαδίκτυο και άλλα δίκτυα μέσω διευθύνσεων IP με μοναδική αναγνώριση, όπου τα δεδομένα συλλέγονται και μεταδίδονται μέσω ενσωματωμένων αισθητήρων, ηλεκτρονικών συστημάτων και λογισμικού

Οι φυσικές συσκευές είτε έχουν σχεδιαστεί για το Διαδίκτυο των πραγμάτων είτε είναι περιουσιακά στοιχεία, συμπεριλαμβανομένων των ζωντανών όντων, τα οποία είναι εξοπλισμένα με την ανίχνευση δεδομένων και τη μετάδοση ηλεκτρονικών. Πέρα από αυτήν την διάσταση του τελικού σημείου με συσκευές, αισθητήρες, ενεργοποιητές και συστήματα επικοινωνίας, το Ίντερνετ των πραγμάτων χρησιμοποιείται επίσης για να περιγράψει τι γίνεται πραγματικά με τα δεδομένα που αποκτώνται από τα συνδεδεμένα πράγματα (Perera et al., 2014)

ο Ίντερνετ των πραγμάτων είναι ένας γενικός όρος και, όπως αναφέρθηκε, γίνεται συχνά διάκριση μεταξύ του Διαδικτύου των Καταναλωτών των Πραγμάτων (CIoT) και του Βιομηχανικού Διαδικτύου των Πραγμάτων (IIoT).

το CIoT και το IIoT καλύπτουν πολλές περιπτώσεις χρήσης και εφαρμογές, καθώς και, επομένως, και οι ομπρέλες. Επιπλέον, υπάρχουν αλληλεπικαλύψεις μεταξύ των δύο.

Το Διαδίκτυο των Πραγμάτων δεν είναι πράγμα. Τα δεδομένα που αποκτώνται υποβάλλονται σε επεξεργασία ή αποστέλλονται σε συσκευές, στις περισσότερες περιπτώσεις ταξιδεύουν στο Διαδίκτυο, σε σταθερές γραμμές, σε οικοσυστήματα νέφους (cloud ecosystems) ή μέσω τεχνολογιών ασύρματης συνδεσιμότητας που αναπτύσσονται για συγκεκριμένες εφαρμογές του Διαδικτύου



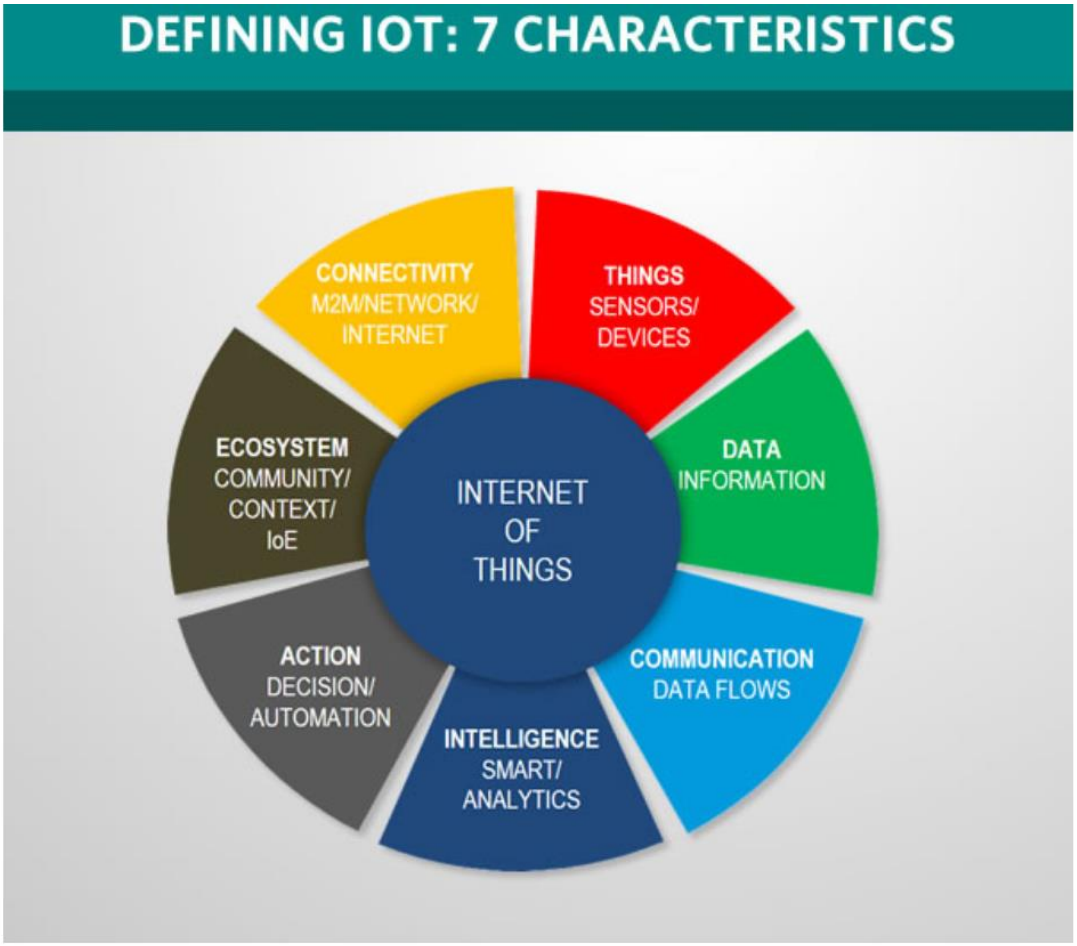
Η γεφύρωση της ψηφιακής, φυσικής και ανθρώπινης σφαίρας μέσω δικτύων, συνδεδεμένων διαδικασιών και δεδομένων, που μετατράπηκαν σε γνώση και δράση, αποτελεί ουσιαστική πτυχή αυτής της εξίσωσης. Τα τελευταία χρόνια, η εστίαση στο Διαδίκτυο των Πράξεων έχει μετατοπιστεί από την καθαρή πλευρά της σύνδεσης των συσκευών και της συλλογής δεδομένων σε αυτή της διασύνδεσης των συσκευών, των δεδομένων, των επιχειρηματικών στόχων, των ανθρώπων και των διαδικασιών

1.8 Γενικά χαρακτηριστικά του IoT

- Συνδεσιμότητα: Όλοι οι ορισμοί του IoT περιλαμβάνουν τη συνδεσιμότητα και την πτυχή του δικτύου: ένα δίκτυο πραγμάτων, συσκευών, αισθητήρων, αντικειμένων ή / και περιουσιακών στοιχείων, ανάλογα με την πηγή. Είναι αρκετά σαφές ότι μια διάσταση των δικτύων και της σύνδεσης πρέπει να είναι παρούσα σε κάθε αξιοπρεπή ορισμό του IoT. Υπάρχουν πολλά πρωτόκολλα και πρότυπα δικτύου, τόσο ασύρματα όσο και σταθερά. Στα περισσότερα έργα IoT της πραγματικής ζωής είναι ένας συνδυασμός. Συνδεσιμότητα συμβαίνει σε όλα τα επίπεδα: σε πολύ κοντινό εύρος (π.χ. μεταξύ συσκευών), πιο μακριά (π.χ. μεταξύ συσκευών και σύννεφο) ή σε πολύ μεγάλες αποστάσεις. Τα πρότυπα σύνδεσης είναι επίσης διαφορετικά, ανάλογα με την απαιτούμενη ισχύ και τους όγκους των δεδομένων IoT που μεταδίδονται, προσθέτοντας το ευρύ φάσμα προτύπων και λύσεων. Συνδεσιμότητα με την έννοια των συνδεδεμένων συσκευών είναι η αρχή, τα συνδεδεμένα δεδομένα είναι εκεί όπου αρχίζει η αξία του εγχειρήματος.
- Τα αντικείμενα στο Διαδίκτυο των Αντικειμένων. Τα περιουσιακά στοιχεία, συσκευές, φυσικά αντικείμενα, αισθητήρες, οτιδήποτε συνδέεται με τον

φυσικό κόσμο, τις συσκευές, τα τελικά σημεία. Είναι όλοι οι όροι για να περιγράψουμε τι είναι ουσιαστικό μέρος ενός δικτύου πραγμάτων. Μερικοί προσθέτουν λέξεις όπως έξυπνες ή ευφυείς στις συσκευές. Αν υποτεθεί ότι περιέχουν τεχνολογία που τους παρέχει μια πρόσθετη δυνατότητα να παράγουν έργο: τη μέτρηση της θερμοκρασίας ή της υγρασίας, τη λήψη δεδομένων θέσης, την ανίχνευση κίνησης ή τη λήψη οποιασδήποτε άλλης μορφής δράσης και περιβάλλοντος που μπορεί να καταγραφεί και να μετατραπεί σε δεδομένα. Εκεί εμφανίζεται η διαχείριση συσκευών IoT: τη διαμόρφωση και τη συνολική διαχείριση των συσκευών IoT. Η διαχείριση συσκευών IoT μπορεί να είναι απλή (π.χ. σε εφαρμογές καταναλωτών) και να γίνεται χρησιμοποιώντας πλατφόρμες cloud με χαρακτηριστικά διαχείρισης συσκευών IoT ή ιδιόκτητες λύσεις προμηθευτών. Μπορεί επίσης να είναι περίπλοκο. Καθώς οι πλατφόρμες IoT γίνονται όλο και πιο σημαντικές, η διαχείριση συσκευών IoT γίνεται σε αυτό το επίπεδο καθώς η διαχείριση συσκευών είναι ένα από τα βασικά συστατικά μιας τέτοιας πλατφόρμας. Άλλα στοιχεία μιας πλατφόρμας IoT περιλαμβάνουν τη διαχείριση δεδομένων IoT, τον έλεγχο πρόσβασης και την ενεργοποίηση εφαρμογής (ανάπτυξης).

- Δεδομένα.Αυτό είναι μέρος αυτής της ευφυούς ιδέας. Μπορεί να οριστεί το Διαδίκτυο των Πραγμάτων, περιγράφοντας απλώς όλα τα χαρακτηριστικά ("τι είναι"), αλλά πρέπει επίσης να εξετάσετε το σκοπό του ("γιατί"). Τα δεδομένα είναι ένα κρίσιμο μέρος αυτής της εξίσωσης, αν και είναι μόνο ένα πρώτο βήμα, δεδομένου ότι τα δεδομένα αυτά δεν αρκούν. Ωστόσο, δεν υπάρχει Διαδίκτυο των Πράξεων χωρίς (μεγάλα) δεδομένα.
- Επικοινωνία.Τα δεδομένα που συλλέγησαν έχουν αξία, αλλά σίγουρα δεν έχουν νόημα αν δεν χρησιμοποιηθούν για ένα σκοπό και μετατραπούν σε νόημα, γνώσεις, νοημοσύνη και ενέργειες. Τα δεδομένα που συλλέγονται και γίνονται αντιληπτά από τις συσκευές του Διαδικτύου πρέπει να ανακοινώνονται προκειμένου να αρχίσουν να μετατρέπονται σε πληροφορίες που μπορούν να ενεργοποιηθούν, πόσο μάλλον η γνώση, οι γνώσεις, η σοφία ή οι ενέργειες
- Αυτοματοποίηση. Υπάρχει πάντα ένας βαθμός αυτοματοποίησης, ανεξάρτητα από το πεδίο εφαρμογής του έργου ή από τον τύπο της εφαρμογής Internet of Things. Στην πραγματικότητα, οι περισσότερες εφαρμογές IoT αφορούν ουσιαστικά την αυτοματοποίηση. Και αυτό συχνά έρχεται με κόστος και οφέλη. Βιομηχανικός αυτοματισμός, αυτοματοποίηση επιχειρηματικών διαδικασιών ή αυτόματη ενημέρωση λογισμικού (I-scoop.eu, 2018)



Defining the Internet of Things using 7 characteristics

1.9 Ραγδαία αύξηση του IoT

Είναι ασφαλές να λεχθεί ότι, παρά το γεγονός ότι γίνεται κουβέντα για το Διαδίκτυο των Πραγμάτων για μεγάλο χρονικό διάστημα και το γεγονός ότι το IoT σε πολλές βιομηχανίες είναι πραγματικότητα, όλο το concept είναι πολύ πρώιμο. Παρόλο που αναμένεται ότι, ως όρος και έννοια, το Διαδίκτυο των Πραγμάτων θα εξαφανιστεί και θα γίνει απλώς μέρος μίας νέας πραγματικότητας, ακόμα δεν έχουμε φτάσει εκεί. Π.

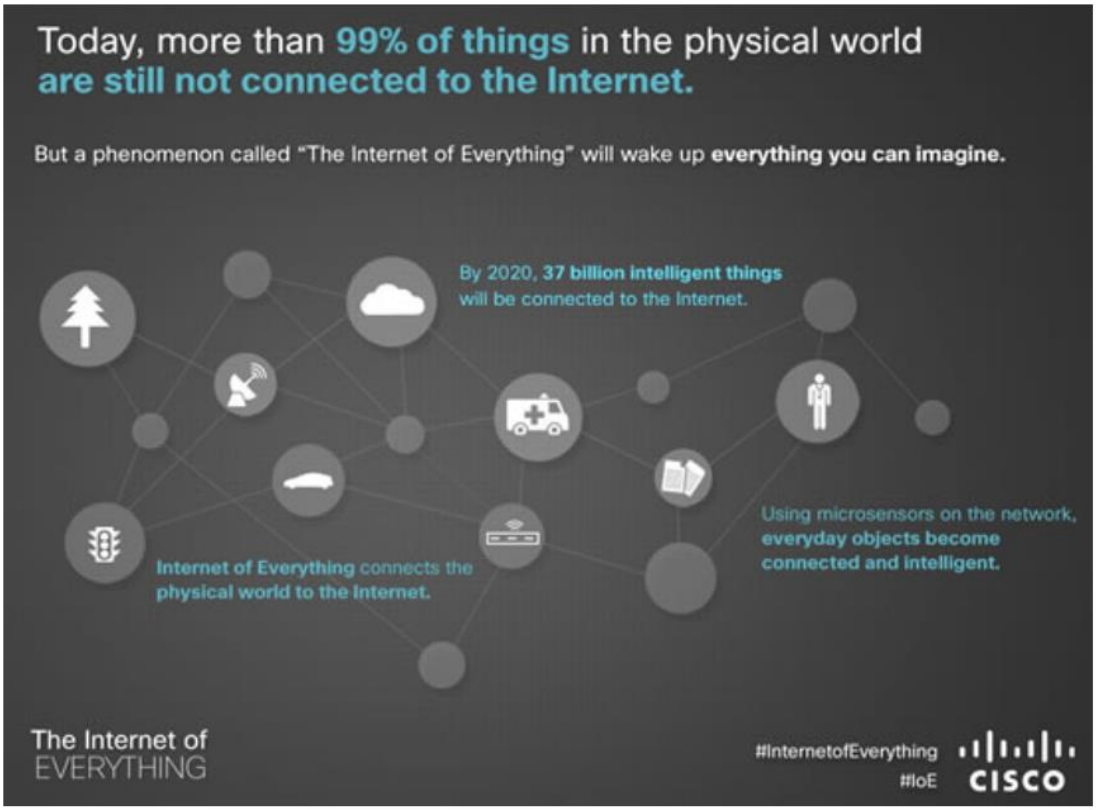
Με την εκθετική αύξηση, έρχεται η ανάπτυξη σε πολλούς άλλους τομείς όπως η κυκλοφορία, η αποθήκευση, η χωρητικότητα επεξεργασίας, οι όγκοι δεδομένων, οι δυνατότητες δικτύου.

Το Διαδίκτυο των πραγμάτων υπάρχει σε πολλές βιομηχανίες, εφαρμογές και περιβάλλοντα. Ορισμένα έργα βρίσκονται ακόμα στο πιλοτικό στάδιο ενώ άλλα αποτελούν τη ραχοκοκαλιά σημαντικών διαδικασιών, λειτουργιών και καινοτομιών. Με άλλα λόγια: το Διαδίκτυο των πραγμάτων είναι σίγουρα εδώ αλλά ο βαθμός στον οποίο αλλάζει τους τρόπους που ζούμε, εργαζόμαστε και ασκούμε τις επιχειρήσεις εξαρτάται από το εκάστοτε πλαίσιο. (I-scoop.eu, 2018)

Οι ακριβείς προβλέψεις σχετικά με το μέγεθος και την εξέλιξη του τοπίου στο Ίντερνετ των πραγμάτων τείνουν να επικεντρώνονται στον αριθμό συσκευών και άλλων «πραγμάτων» που συνδέονται, καθώς επίσης και στην εντυπωσιακή αύξηση αυτού του όγκου συσκευών IoT με δυνατότητα IP και τα δεδομένα που παράγουν.

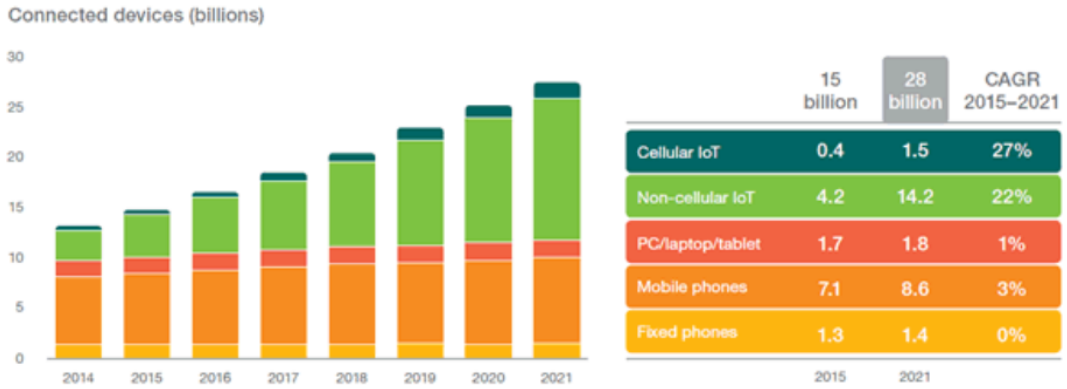
Φαίνεται ότι το Διαδίκτυο των πραγμάτων δεν είναι ακόμα πουθενά. Ωστόσο, στην πραγματικότητα είναι ήδη μεγαλύτερο από ό, τι πολλοί πιστεύουν και χρησιμοποιείται σε πολύ περισσότερες εφαρμογές από αυτές που συνήθως αναφέρονται στα mainstream media.

Ταυτόχρονα, είναι αλήθεια ότι η αύξηση των συνδεδεμένων συσκευών είναι συγκλονιστική και επιταχυνόμενη. Περίπου κάθε μία ώρα πραγματοποιούνται περίπου ένα εκατομμύριο νέες συνδέσεις και συνδέονται με το Διαδίκτυο περίπου 5 έως 6 δισεκατομμύρια διαφορετικά στοιχεία. Μέχρι το 2020, η Cisco αναμένει ότι θα υπάρχουν 20 δισεκατομμύρια συσκευές στο Διαδίκτυο των πραγμάτων. Οι εκτιμήσεις για το 2030 αυξήθηκαν κατά 50 δισεκατομμύρια συσκευές και κάποιες προβλέψεις είναι ακόμη πιο αισιόδοξες, δηλώνοντας ότι μέχρι το 2025 θα φτάσουν τα 100 δισεκατομμύρια συσκευές.



Σύμφωνα με την Έκθεση Κινητικότητας της Ericsson το 2016, θα υπάρχουν περίπου 28 δισεκατομμύρια συνδεδεμένες συσκευές μέχρι το 2021. Η έκθεση αναμένει ότι το Διαδίκτυο των πραγμάτων θα ξεπεράσει τα κινητά τηλέφωνα ως τη μεγαλύτερη

κατηγορία συνδεδεμένων συσκευών με 16 δις συνδεδεμένες συσκευές που είναι συσκευές IoT (από τις προβλεπόμενες συνολικά 28 δισ. ευρώ, τα οποία περιλαμβάνουν για παράδειγμα smartphones, όπως αναφέρθηκε στο άρθρο μας για κινητά και κινητικότητα.

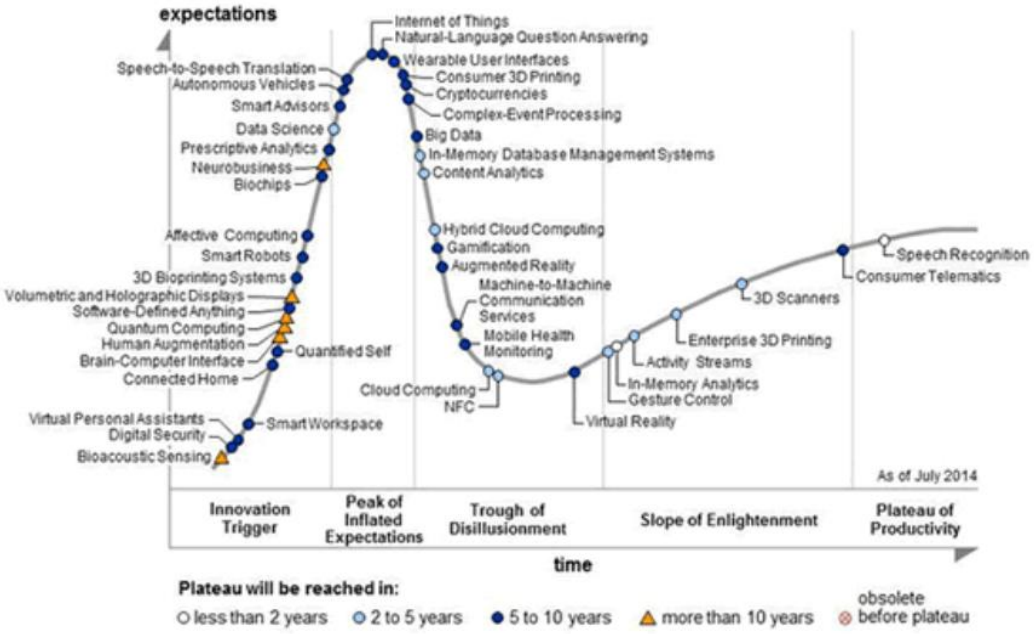


	15 billion	28 billion	CAGR 2015–2021
Cellular IoT	0.4	1.5	27%
Non-cellular IoT	4.2	14.2	22%
PC/laptop/tablet	1.7	1.8	1%
Mobile phones	7.1	8.6	3%
Fixed phones	1.3	1.4	0%
	2015	2021	

Λοιπόν, πρώτα απ 'όλα το Διαδίκτυο των πραγμάτων σήμερα είναι αποτελεσματικά προωθημένο (αλλά ταυτόχρονα πολύ πραγματικό). Ο τελευταίος κύκλος Hype για τις αναδυόμενες τεχνολογίες του Gartner δείχνει ότι το Διαδίκτυο των πραγμάτων βρίσκεται στην κορυφή των διογκωμένων προσδοκιών (ενώ το NFC φθίνει σημαντικά)

Υπάρχουν πολλοί λόγοι για την αυξανόμενη προσοχή για το Διαδίκτυο των πραγμάτων. Ενώ συχνά υπάρχουν αναφορές σχετικά με το μειωμένο κόστος αποθήκευσης, επεξεργασίας και υλικού.. Υπάρχει σίγουρα μια κοινωνική αλλά παράλληλα και ανθρώπινη διάσταση με πολύ ισχυρό το στοιχείο της κατανάλωσης.

Ένας παράγοντας που συνέβαλε επίσης πολύ στην άνοδο του Διαδικτύου των Πραγμάτων, σίγουρα σε ένα πλαίσιο του βιομηχανικού Διαδικτύου των πραγμάτων και των έξυπνων κτιρίων είναι η σύγκλιση του IT τομέα με τον OT οι οποίοι θεωρητικά είναι ασύμβατοι.



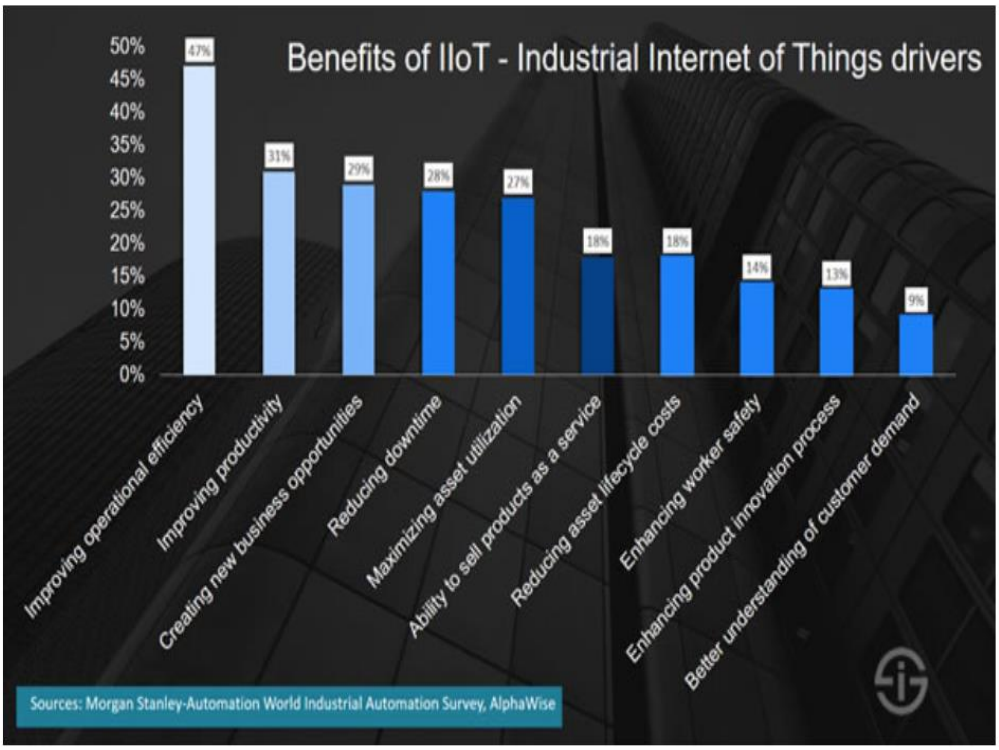
1.10 Industrial Internet of Things

Το Βιομηχανικό Ίντερνετ των πραγμάτων ορίζεται από την Κοινοπραξία Βιομηχανικού Διαδικτύου ως «μηχανές, υπολογιστές και άτομα που επιτρέπουν ευφυείς βιομηχανικές επιχειρήσεις χρησιμοποιώντας προηγμένες αναλύσεις δεδομένων για μετασχηματιστικά επιχειρησιακά αποτελέσματα»

Τυπικές περιπτώσεις χρήσης του Βιομηχανικού Διαδικτύου των πραγμάτων περιλαμβάνουν έξυπνες λύσεις αστραπής και έξυπνης κυκλοφορίας σε έξυπνες πόλεις, έξυπνες εφαρμογές μηχανών, εφαρμογές βιομηχανικού ελέγχου, περιπτώσεις χρήσης σε εργοστάσια, παρακολούθηση κατάστασης, περιπτώσεις χρήσης στη γεωργία, εφαρμογές έξυπνων δικτύων και εφαρμογές διυλιστηρίων πετρελαίου

Έτσι, ακόμα και αν ο όρος δεν είναι τόσο ένας όρμος ομπρέλα όσο το Ίντερνετ των πραγμάτων, καλύπτει ακόμα πολλές πιθανές εφαρμογές και περιπτώσεις χρήσης (Perera et al., 2014)

Πολλοί οργανισμοί εξετάζουν τις εφαρμογές IIoT και πολλοί έχουν ήδη ξεκινήσει, σίγουρα σε αγορές, όπως η βιομηχανία ή το πετρέλαιο και το φυσικό αέριο. Αλλά άλλοι εξακολουθούν να περιμένουν ή έχουν ακόμα ένα βαθμό αβεβαιότητας.



Είναι σημαντικό να κατανοήσει κανείς ότι το Βιομηχανικό Διαδίκτυο των Πράξεων δεν είναι μόνο για την εξοικονόμηση κόστους και τη βελτιστοποίηση της αποτελεσματικότητας. Οι εταιρείες έχουν επίσης τη δυνατότητα να πραγματοποιήσουν σημαντικούς μετασχηματισμούς και να βρουν νέες ευκαιρίες χάρη στο ΠΠ

1.11 Consumer Internet of Things

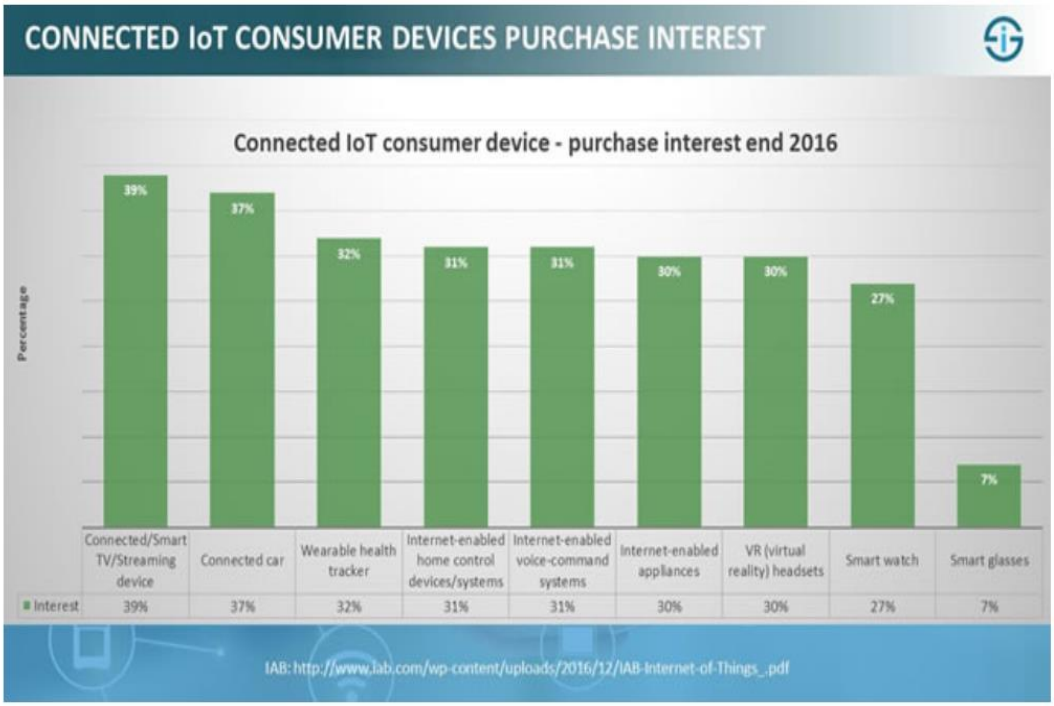
Πριν από μία πενταετία, οι καταναλωτές σπάνια είχαν μία εικόνα του τι σημαίνει το Διαδίκτυο των πραγμάτων στην ιδιωτική τους ζωή. Σήμερα, όλο και περισσότερο: όχι μόνο επειδή ενδιαφέρονται για την τεχνολογία, αλλά κυρίως επειδή μια σειρά από νέες εφαρμογές και συνδεδεμένες συσκευές έχει κατακλείσει την αγορά.

Αυτές οι συσκευές και οι δυνατότητες που επιτρέπουν παίρνουν μεγάλη προσοχή σε σχεδόν κάθε μέσο που καλύπτει την τεχνολογία. Φορητά και έξυπνα ρολόγια, συνδεδεμένες και έξυπνες οικιακές εφαρμογές με το Nest της Google να είναι δημοφιλές, αλλά σίγουρα όχι το μόνο (Καλύβας Βασίλειος)

Ενώ το επίκεντρο του βιομηχανικού διαδικτύου των πραγμάτων είναι περισσότερο για τα οφέλη των εφαρμογών, το Διαδίκτυο για τα καταναλωτικά αγαθά είναι περισσότερο για νέες και εμβαθυντικές εμπειρίες με κέντρο τον ίδιο τον πελάτη.

Αναμένεται ότι η αγορά θα αρχίσει πραγματικά να αναδύεται από τα τέλη του 2018, όταν το Διαδίκτυο για τα αγαθά των καταναλωτών θα αναπτυχθεί γρήγορα σε διάφορους τύπους συσκευών και εφαρμογών και όταν οι κατασκευαστές είναι σε θέση να αντιμετωπίσουν τις διάφορες προκλήσεις

Όπως αναφέρθηκε, το Διαδίκτυο για τα καταναλωτικά πράγματα είναι συνήθως για έξυπνες φορητές συσκευές και έξυπνες οικιακές συσκευές, αλλά και για έξυπνες τηλεοράσεις, κινητά τηλέφωνα για εφαρμογές καταναλωτών και ένα ευρύ φάσμα συσκευών με συνδεσιμότητα του Internet of Things.

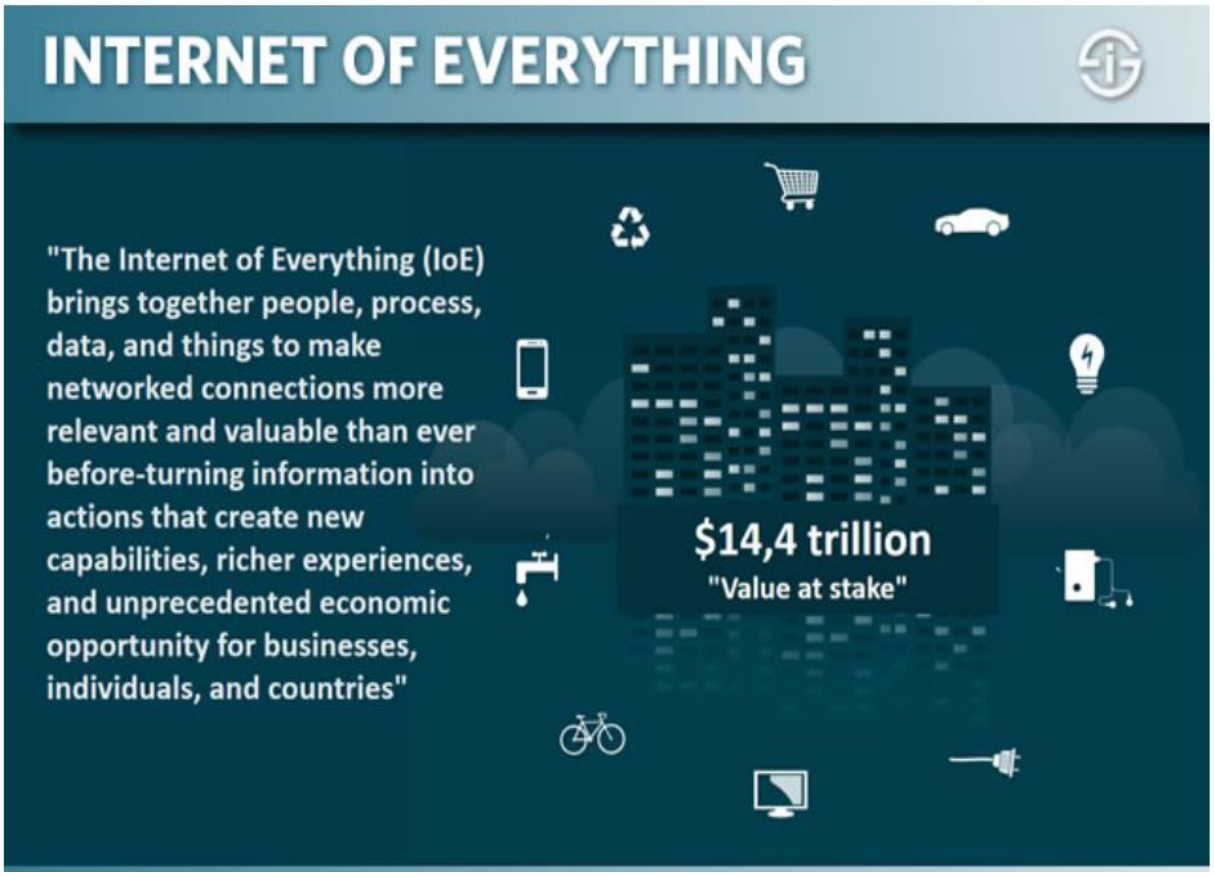


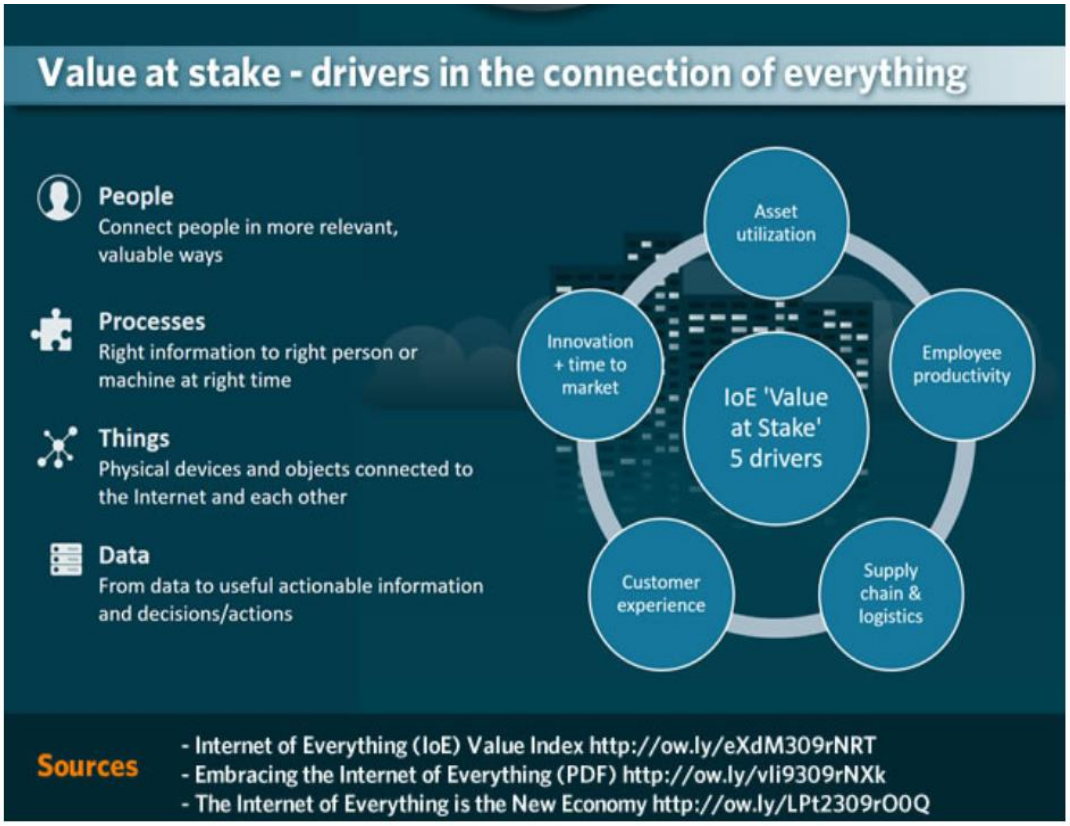
1.12 Internet of Everything

Το Internet of Everything είναι ένας όρος που δημιουργήθηκε από τη Cisco αλλά χρησιμοποιείται και από άλλες εταιρείες

Το Διαδίκτυο των πραγμάτων επικεντρώνεται πάρα πολύ στα πράγματα και, όπως αναφέρθηκε, χρησιμοποιείται επίσης ευρέως. Γι 'αυτό ορισμένοι άρχισαν να κάνουν διάκριση μεταξύ του ακριβώς αναφερθέντος Διαδικτύου των πραγμάτων των καταναλωτών και του βιομηχανικού διαδικτύου των πραγμάτων. (I-scoop.eu, 2018)

Η Cisco και άλλοι προτιμούν να χρησιμοποιούν το όρο Internet Everything, εν μέρει λόγω του θέματος του ορολογικού θέματος, εν μέρει λόγω της εστίασης στα πράγματα και εν μέρει για να δώσουν ένα πλαίσιο στις απόψεις και τις προσφορές τους. Αλλά δεν είναι μόνο μάρκετινγκ. Το Internet of Everything ή αλλιώς IoE απεικονίζει βασικές πτυχές του IoT, δηλαδή ανθρώπους, δεδομένα, πράγματα και διαδικασίες. με άλλα λόγια: τι κάνει μια επιχείρηση. Επιπλέον, η κλασική απεικόνιση του Internet of Everything δημιούργησε σαφές, για παράδειγμα, τι είναι το M2M.


INTERNET OF EVERYTHING
"The Internet of Everything (IoE) brings together people, process, data, and things to make networked connections more relevant and valuable than ever before-turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries"
$14,4 trillion
"Value at stake"

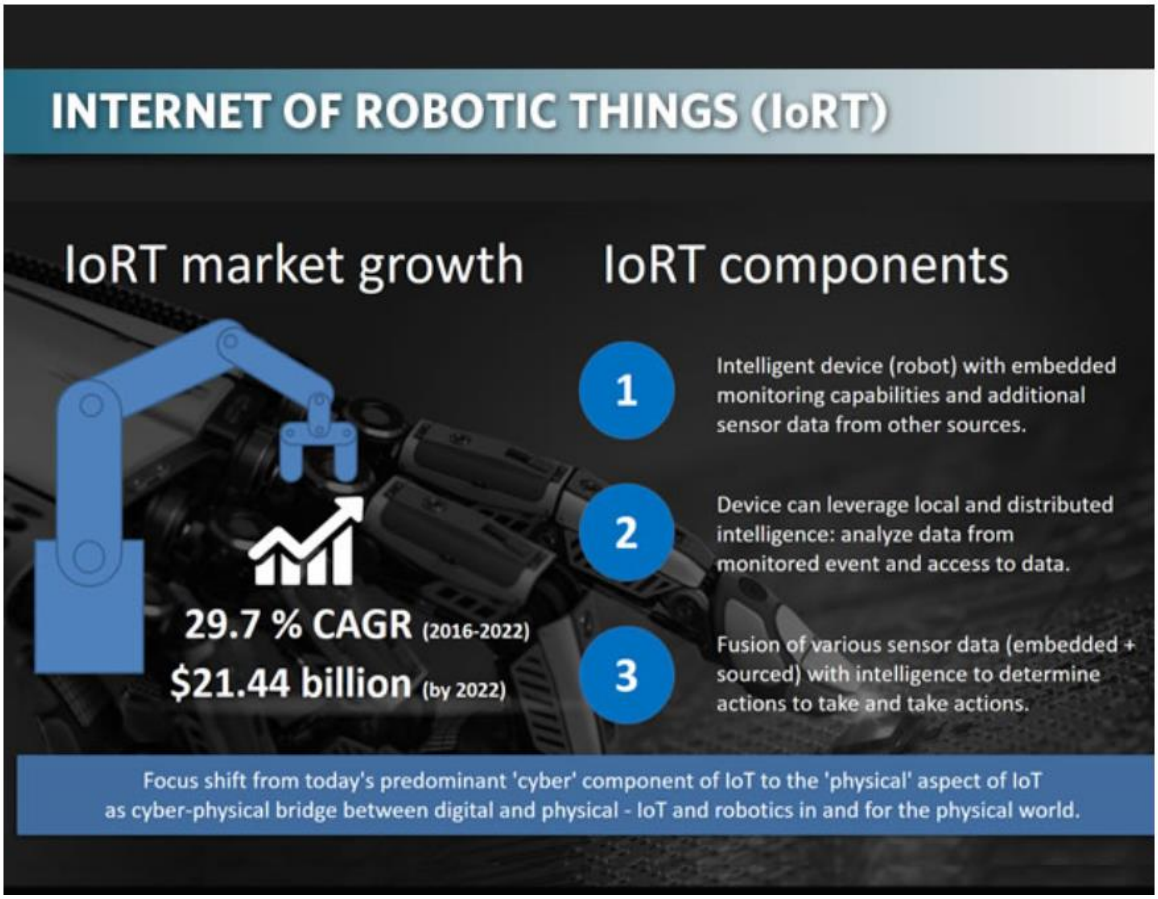

Value at stake - drivers in the connection of everything
People
Connect people in more relevant, valuable ways
Processes
Right information to right person or machine at right time
Things
Physical devices and objects connected to the Internet and each other
Data
From data to useful actionable information and decisions/actions
Asset utilization
Employee productivity
Supply chain & logistics
Customer experience
Innovation + time to market
IoE 'Value at Stake' 5 drivers
Sources
- Internet of Everything (IoE) Value Index http://ow.ly/eXdM309rNRT
- Embracing the Internet of Everything (PDF) http://ow.ly/vli9309rNXk
- The Internet of Everything is the New Economy http://ow.ly/LPt2309rO0Q

1.13 The Internet of Robotic Things (IoRT)

Ένα από τα κύρια χαρακτηριστικά του Διαδικτύου των Πραγμάτων είναι ότι μπορεί να δημιουργήσει ισχυρότερες γέφυρες μεταξύ φυσικών και ψηφιακών κόσμων. Αυτό εν γένει είναι φανερό σε όλες τις περιπτώσεις χρήσης του Διαδικτύου και στο Βιομηχανικό Διαδίκτυο των Πράξεων, σε αυτά τα concepts που αποτελούν τα λεγόμενα και ως Cyber Physical Systems.

Ωστόσο, στην πλειονότητα των περιπτώσεων, η εστίαση επικεντρώνεται κατά κύριο λόγο στο τμήμα «cyber», όπου τα δεδομένα από τους αισθητήρες χρησιμοποιούνται κυρίως για να επιτύχουν ένα συγκεκριμένο αποτέλεσμα με ανθρώπινη παρέμβαση και με επίκεντρο την ανάλυση δεδομένων και τις πλατφόρμες «κυβερνοχώρου». Ο τρόπος με τον οποίο συμβαίνει, όπως η ABI Research, που έρχεται με την ιδέα της IoRT αποτελεί ουσιαστικά τη μετουσίωση της ιδέας πως πολλές εφαρμογές και επιχειρηματικά μοντέλα βασίζονται σε κάποια παθητική αλληλεπίδραση. (I-scoop.eu, 2018)

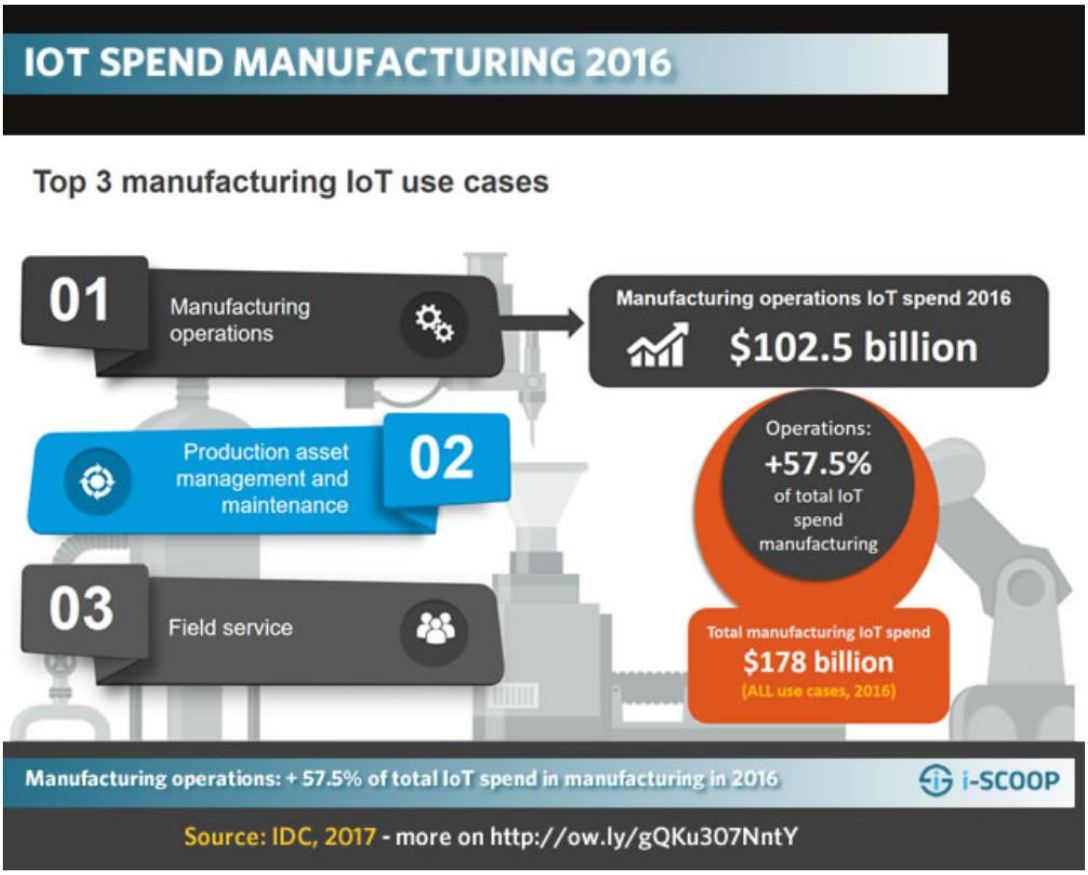
Η αγορά Διαδικτύου Ρομποτικών Πραγμάτων αναμένεται να αποτιμηθεί στα 21,44 δισ. Δολάρια μέχρι το 2022. Με την προσθήκη ρομποτικής στην εξίσωση και μετατρέποντας τις συσκευές σε πραγματικά έξυπνες με ενσωματωμένες δυνατότητες παρακολούθησης, δυνατότητας προσθήκης δεδομένων αισθητήρων από άλλες πηγές, τοπικής και κατανεμημένης νοημοσύνης και σύντηξης δεδομένων και ευφυΐας, μπορεί να παραχθεί μια συσκευή που μπορεί να ελέγχει και να χειρίζεται αντικείμενα στον φυσικό κόσμο.



1.14 Internet of Things in manufacturing

Δεδομένης της προέλευσης του Διαδικτύου των Πραγμάτων, των αρχών της RFID τεχνολογίας και των πιο χαρακτηριστικών περιπτώσεων χρήσης, ο τομέας της κατασκευαστικής αποτελεί το πιο γόνιμο περιβάλλον ανάπτυξης.

Στη μεταποιητική βιομηχανία δαπανήθηκαν 178 δισεκατομμύρια δολάρια το 2016, το οποίο είναι περισσότερο από διπλάσιο από τη δεύτερη μεγαλύτερη αγορά σε δαπάνες, τις μεταφορές.
Σε μια πρόβλεψη του Μαΐου του 2015 σχετικά με την παγκόσμια ανάπτυξη της αγοράς Internet of Things, η IDC προέβλεψε ότι η αγορά των διαδικτυακών πραγμάτων στις μεταποιητικές επιχειρήσεις θα φτάσει τα 98,8 δισεκατομμύρια δολάρια το 2018.



Σύμφωνα με έκθεση της PwC του Φεβρουαρίου 2015, η πλειοψηφία των αμερικανών κατασκευαστών έχει αναπτύξει συσκευές για τη συλλογή, ανάλυση,μέτρηση και επεξεργασία δεδομένων. Σύμφωνα με την εν λόγω έρευνα, το 34,6% των ερωτηθέντων είχε ήδη εφαρμόσει συσκευές και αισθητήρες για να συλλέξει αυτά τα δεδομένα και άλλα 9,6% σχεδίαζαν να υλοποιήσουν συσκευές του Διαδικτύου των Πραγμάτων εντός ενός έτους. έτος. Μόνο το 24% όλων των ερωτηθέντων από την αμερικανική μεταποιητική βιομηχανία δήλωσε ότι δεν είχαν σχέδια να εφαρμόσουν συσκευές για τη συλλογή, ανάλυση και επεξεργασία δεδομένων

Caterpilar

Η εταιρία μηχανημάτων και εξοπλισμού **Caterpilar** δημοσίευσε συνεργασία με την Uptake, η οποία είναι μία εταιρία για analytics, με στόχο να βοηθήσει τους πελάτες της πρώτης να έχουν μεγαλύτερη επίγνωση για την κατάσταση των μηχανημάτων τους, να μπορούν δηλαδή να τα παρακολουθούν και να οργανώνουν τον στόλο τους όσο το δυνατόν πιο αποδοτικά. Η εταιρία υποστηρίζει ότι οι πελάτες χρησιμοποιούν την τεχνολογία αυτή για να επιβλέπουν τους στόλους των μηχανημάτων καθώς και ανιχνεύουν τα επίπεδα καυσίμου σε κάθε μηχανή. Βέβαια, υποστηρίζεται ότι η συνεργασία αυτή στοχεύει να ανεβάσει τις υπηρεσίες της Caterpillar στο επόμενο επίπεδο.

Doug Oberhelman, CEO of Caterpillar ισχυρίζεται ότι με την εφαρμογή των νέων τεχνολογιών που φέρνει το IoT δίνεται μία νέα προοπτική στους πελάτες καθώς πλέον ξεφεύγουν από τη λογική ‘repair after failure’ και πλέον έχουν τη δυνατότητα του ‘repair before failure’. Αποτέλεσμα αυτού είναι η μεγιστοποίηση του κέρδους των πελατών μέσω της καλύτερης διαχείρισης του στόλου των μηχανημάτων τους.

(Today's Motor Vehicles, 2018)

Airbus

Η Airbus, μία από τις πιο ισχυρές εταιρίες που ασχολούνται με την κατασκευή και συντήρηση αεροσκαφών χρησιμοποιεί τις τεχνολογίες του IoT σε μεγάλο βαθμό. Όχι μόνο εισάγει τις καινούριες τεχνολογίες του IoT στα προιόντα της (αεροπλάνα) αλλά και στα εργαλεία που χρησιμοποιούν οι εργάτες κατά την παραγωγική διαδικασία.

Για την Airbus, το εργοστάσιο του μέλλοντος περιλαμβάνει έναν εργάτη ο οποίος με τη χρήση ενός tablet ή smart glasses μπορεί να οργανώσει μία συγκεκριμένη εργασία και μετά να τη μεταδόσει σε ένα ρομποτικό εργαλείο το οποίο θα εκτελέσει την εργασία με επιτυχία. Συμφωνα με τον Jean-Bernard Hentz, head of PLM R&T & Innovation at Airbus ICT, με το να συνδέεις τους ανθρώπους και τα εργαλεία που χρησιμοποιούν σε μία πλατφόρμα IoT, όχι μόνο επιταχύνει την παραγωγή αλλά και αυξάνει και την αξιοπιστία.

(Drinkwater, 2018)

Siemens

Οι Γερμανοί πάντα ήταν στην πρώτη γραμμή σε ότι αφορά την καινοτομία στην παραγωγή, άρα γιατί θα αποτελούσε είδηση ότι χρησιμοποιούν ήδη τις τεχνολογίες του IoT? Σε ένα εργοστάσιο στο Amberg, το γερμανικό πάθος για τεχνολογική καινοτομία είναι προσωποποιημένο, όχι με αυτό που κάνουν αλλά με το πώς το κάνουν.

Τα αυτοκίνητα του μέλλοντος θα είναι ασφαλέστερα και για τους επιβάτες αλλά και για τους πεζούς και θα προσφέρουν ασφαλιστικές υπηρεσίες όπως pay-as-you-go insurance δηλαδή, τα ασφάλιστρα θα υπολογίζονται ανάλογα με τον τρόπο που οδηγεί ο κάθε οδηγός. Συνολικά, τα έξυπνα αυτοκίνητα θα προσφέρουν μία πιο συναρπαστική

εμπειρία οδήγησης. Η Hewlett Packard συμβάλλει στην ταχύτερη άφιξη του έξυπνου αυτοκινήτου μέσω του συνδυασμού των τεχνολογιών που προσφέρει.

Στις δύο δεκαετίες πριν λανσαριστεί η τεχνολογία OnStar σε συνεργασία μεταξύ General Motors (GM), Hughes Electronics, και EDS, η ιδέα του έξυπνου αυτοκινήτου που θα είναι συνδεδεμένο σε ένα δίκτυο και θα ανταλλάσει πληροφορίες ήταν εξαιρετικά αμφιλεγόμενη. Πέρα από την κεντρική ιδέα του συνδεδεμένου αυτοκινήτου με πρόσβαση στο internet, ανοίγουν και νέες αγορές, όπως Vehicle-to-Infrastructure(V2I), Vehicle-to-Vehicle(V2V), Vehicle-to-Cloud(V2C), Vehicle-to-Pedestrian(V2P), and Vehicle-to-Everything(V2X).

Μία πρόσφατη έρευνα που διεξήχθει από το κεντρικό τμήμα έρευνας της αυτοκινητοβιομηχανίας τόνισε ότι ένα μέσο αυτοκίνητο τώρα περιέχει 60 μικροεπεξεργαστές και πάνω από 10 εκατομμύρια γραμμές κώδικα ενώ οι αντίστοιχες γραμμές κώδικα για ένα αεροπλάνο τύπου Boeing Dreamliner airplane περιορίζονται στο μισό. Τα αυτοκίνητα έχουν αρχίσει να γίνονται ολοένα και πιο έξυπνα και μέχρι το τέλος του 2018, ένα στα πέντε αυτοκίνητα θα έχει γνώση για την κατάστασή του και θα είναι ικανό να μοιράζεται πληροφορίες σχετικά με την μηχανική του κατάσταση, την τοποθεσία του καθώς και να ενημερώνει για την κατάσταση του χώρου στον οποίο βρίσκεται. Η ικανότητα του αυτοκινήτου να αυτοπροσδιορίζεται σε πραγματικό χρόνο μαζί με την ανάγκη να είναι συνεχώς ενεργό, απαιτεί αξιόπιστη σύνδεση στο διαδίκτυο καθώς και λύσεις τύπου Internet of Things.

Η ευρεία χρήση του 4G LTE αλλά και η επερχόμενη τεχνολογία των 5G δικτύων θα αυξήσουν περαιτέρω τις δυνατότητες των έξυπνων αυτοκινήτων και θα διευκολύνουν γρηγορότερη ταχύτητα μετάδοσης και μεγαλύτερο όγκο δεδομένων. Η εταιρίες επικοινωνιών μπορούν εύκολα να παρέχουν μια τέτοιου είδους σύνδεση στο διαδίκτυο ενώ ταυτόχρονα χρειάζεται και η συμβολή ενός ακόμα εταίρου που θα δίνει λύσεις μέσω της τεχνολογίας του Internet of Things για να ικανοποιεί τις ανάγκες της αυτοβιομηχανίας.

Smartphone εφαρμογές που υποστηρίζονται από τους QR κώδικες και ετικέτες NFC παρέχουν ενδιαφέρουσες και χρήσιμες τουριστικές πληροφορίες σε όλη την πόλη. Οι πληροφορίες θα μπορούσαν να περιλαμβάνουν μουσεία, πινακοθήκες, βιβλιοθήκες, τουριστικά αξιοθέατα, γραφεία τουρισμού, τα μνημεία, τα καταστήματα, λεωφορεία, ταξί, κήπους, κλπ

Δύο «έξυπνες» εφαρμογές στάθμευσης και φωτισμού θα εγκατασταθούν στην Χαλκίδα, την πρώτη πόλη στην Ελλάδα, υποστηριζόμενα από μία ενιαία πλατφόρμα έξυπνης πόλης. Οι δυο εφαρμογές αυτές, θα συμβάλλουν στην αποσυμφόρηση της κυκλοφορίας και στη μείωση κατανάλωσης ενέργειας στην πόλη της Χαλκίδας. Σύμφωνα με ανακοίνωση του Ομίλου ΟΤΕ, σε ότι αφορά την εφαρμογή "Smart Parking" στο πλαίσιο του έργου θα εγκατασταθούν, σε κεντρικό σημείο της Χαλκίδας, ειδικοί αισθητήρες έξυπνης στάθμευσης, οι οποίοι μέσω εφαρμογής στο κινητό, που αναπτύχθηκε από την OTS, θα ενημερώνουν τους οδηγούς που βρίσκονται ελεύθερες θέσεις στάθμευσης και πως θα φτάσουν εκεί.

Το Τελ Αβίβ αντιμετωπίζει τη κίνηση στους πιο πολυσύχναστους δρόμους, εξασφαλίζοντας μία λωρίδα κυκλοφορίας για λεωφορεία και ταξί, επιτρέποντας όμως στους ανυπόμονους οδηγούς ή σ' αυτούς με τις βαθιές τσέπες να χρησιμοποιούν την ορισθείσα λωρίδα, με το ανάλογο αντίτιμο. Αισθητήρες στην άσφαλτο παίρνουν τον αριθμό της πινακίδας του αυτοκινήτου και χρεώνεται αυτόματα στην πιστωτική κάρτα του ιδιοκτήτη ένα ποσό, που ποικίλλει ανάλογα με το πόση κυκλοφοριακή συμφόρηση παρουσιάζει ο δρόμος.

Το Έξυπνο δίκτυο (Smart Grid) ενσωματώνει δυνατότητες επικοινωνίας με τα δίκτυα κοινής ωφέλειας (π.χ. ηλεκτρική ενέργεια, φυσικό αέριο, νερό) και τις υποδομές, για την αυτοματοποίηση της παρακολούθησης και του ελέγχου. Βασικές εφαρμογές έξυπνων δικτύων είναι οι έξυπνοι μετρητές, η αυτοματοποίηση του δικτύου διανομής, η ανταπόκριση στην ζήτηση, η διάγνωση εξοπλισμού καθώς και η παρακολούθηση και ο έλεγχος της κατάστασης του δικτύου ευρείας περιοχής. Το έξυπνο δίκτυο μπορεί ανά πάσα στιγμή να γνωρίζει τις μεταβλητές της κατάστασής του, να βελτιώνει τον εντοπισμό, την απόκριση ακόμα και την πρόβλεψη σφαλμάτων και καταστροφών, μειώνοντας έτσι τις απώλειες που προκαλούνται από αυτά και τους χρόνους διακοπών παροχής ενέργειας.

(Geng Wu et al., 2011) Τα κύρια σενάρια εφαρμογής του IoT στα έξυπνα δίκτυα είναι:

- (Ευφροσύνη Θ. Ζώτου, 2012) Στον τομέα της παραγωγής ενέργειας, το IoT μπορεί να χρησιμοποιηθεί για την παρακολούθηση της μονάδας, των κατανεμημένων σταθμών ηλεκτροπαραγωγής, της περιοχής των σταθμών παραγωγής, των ρύπων και των εκπομπών αερίων, της ενεργειακής κατανάλωσης, του υλικού του άνθρακα, της αιολικής μονάδας παραγωγής, των φωτοβολταϊκών σταθμών παραγωγής, της παραγωγής ηλεκτρικής ενέργειας από βιομάζα, της αποθήκευσης ενέργειας, της διασύνδεσης ηλεκτρικής ενέργειας κτλ.

- Το IoT επίσης χρησιμοποιείται ευρέως για την παρακολούθηση των γραμμών μεταφοράς, την προστασία των πύργων, τους έξυπνους υποσταθμούς, την αυτοματοποίηση της διανομής, την παρακολούθηση της κατάστασης διανομής και για τη διαχείριση της λειτουργίας και του εξοπλισμού.

- Το IoT χρησιμοποιείται κυρίως για τους έξυπνους μετρητές και τη μέτρηση κατανάλωσης ενέργειας, τη σύγκλιση του πολύ-δικτύου, τα ηλεκτρικά οχήματα και τη φόρτισή τους, την παρακολούθηση και διαχείριση της ενεργειακής απόδοσης και για τη διαχείριση ζήτησης, η οποία αποτελεί σημαντική εξοικονόμηση στην κατανάλωση πόρων όταν η παροχή ταιριάζει δυναμικά με τη ζήτηση.

1.15 Internet of Things και νομοθεσία

Υπάρχουν πραγματικά εκατοντάδες τρόποι με τους οποίους οι κυβερνήσεις αξιοποιούν και μπορούν να αξιοποιήσουν το Διαδίκτυο των Πράξεων για να βελτιώσουν την εμπειρία των πολιτών, να πραγματοποιήσουν εξοικονόμηση κόστους και να δημιουργήσουν νέες ροές εσόδων

Το τελευταίο concept είναι πολύ σημαντικό, καθώς πολλά έργα του IoT έχουν αντίκτυπο στη χρηματοδότηση των πόλεων. Ένα απλό παράδειγμα: εάν υπάρχει μια τέλεια έξυπνη λύση στάθμευσης σε μια πόλη, χάνονται έσοδα για όλους τους προφανείς λόγους. Έτσι, δεν είναι μόνο ζήτημα τεχνολογιών, αλλά και εύρεσης δημιουργικών τρόπων για να μετατραπεί η ενισχυμένη εμπειρία των πολιτών και των υπηρεσιών των πολιτών σε μια παγκόσμια πραγματικότητα που είναι επωφελής για όλους.

Αυτό απαιτεί χρόνο, προγραμματισμό και, όπως γίνεται εύκολα κατανοητό, δεδομένης της πολυπλοκότητας των κυβερνητικών οικοσυστημάτων, αναγκαία καθίσταται η ευθυγράμμιση και ο συντονισμός.

Σε ορισμένες χώρες και σε υπερεθνικά επίπεδα λαμβάνονται πρωτοβουλίες και προβλέπεται χρηματοδότηση σε μια σειρά «έξυπνων» πρωτοβουλιών όπου συχνά πόλεις και κυβερνητικές υπηρεσίες μπορούν να επωφεληθούν από το πεδίο εφαρμογής των έργων εντός καθορισμένης περιοχής και από μια ατζέντα με σαφή στόχο . Ταυτόχρονα, οι κυβερνήσεις δραστηριοποιούνται όλο και περισσότερο στον τομέα του Διαδικτύου των Πραγμάτων,. Για παράδειγμα, το συνδεδεμένο αυτοκίνητο του μέλλοντος. Είναι αρκετά σαφές ότι οι κυβερνήσεις θα ασχοληθούν πολύ με αυτό. Για να δοθεί μία συνολική εικόνα, σε ορισμένες χώρες, οι κανονισμοί κυκλοφορίας είναι ήδη ένα πλήρες χάος λόγω της άφιξης γρήγορων ηλεκτρικών ποδηλάτων. Μπορεί να φανταστεί κανείς εύκολα τι θα συμβεί όταν τα οχήματα είναι συνδεδεμένα και «έξυπνα».

1.16 Το integration του Internet of Things σε facilities

Το Διαδίκτυο των πραγμάτων διαδραματίζει σημαντικό ρόλο στη διαχείριση εγκαταστάσεων, μεταξύ των οποίων περιλαμβάνονται τα κέντρα δεδομένων και τα έξυπνα κτίρια

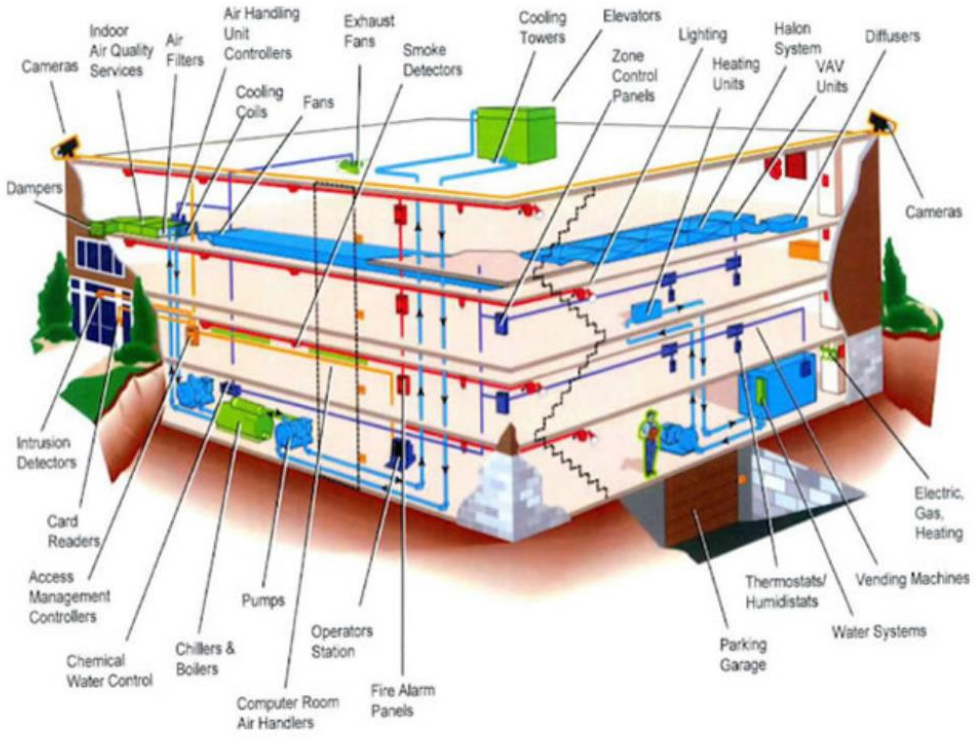
Η ενσωμάτωση της πληροφορικής (IT) και της τεχνολογίας πληροφοριών (OT) διαδραματίζει σημαντικό ρόλο από αυτή την άποψη, όπως συνέβη και στην ταχεία άνοδο του βιομηχανικού διαδικτύου των πραγμάτων. Χάρη στο Ίντερνετ των πραγμάτων και σε αυτή τη σύγκλιση τεχνολογιών πληροφοριών και επικοινωνιών, οι διευθυντές εγκαταστάσεων και οι επαγγελματίες στον τομέα των κατασκευών μπορούν να υλοποιήσουν διάφορους στόχους. Αυτά εξαρτώνται από τη φύση και το εύρος της εγκατάστασης.

Τα έξυπνα κτίρια είναι μεταξύ των ταχύτερα αναπτυσσόμενων διαδικτυακών use cases μέχρι το 2020. Επιπλέον, οι έρευνες δείχνουν ότι η συλλογή δεδομένων από κτίρια και άλλες δομές, όπως ο κλιματισμός, είναι ήδη υψηλή. Τέλος, η αγορά και οι εξελίξεις του BMS (Building Management System) επηρεάζονται έντονα από το Διαδίκτυο των πραγμάτων. Σύμφωνα με έρευνα, το Διαδίκτυο των πραγμάτων είναι ένας από τους κυριότερους παράγοντες τόσο στις δαπάνες όσο και στις εξελίξεις στην

αγορά BMS, η οποία προβλέπεται να αυξηθεί σε CAGR 16,7% μεταξύ 2017 και 2023 σύμφωνα με μία από τις πολλές μελέτες σχετικά με την αγορά BMS.

Η αξιοποίηση των στοιχείων από τα περιουσιακά στοιχεία του IoT που υποστηρίζει τη λειτουργία, μαζί με τις νέες πλατφόρμες του Διαδικτύου, οδηγούν σε δυνατότητες και οφέλη σε τομείς διαχείρισης κτιρίων όπως:

- Ευφυέστερα συστήματα ασφάλειας κτιρίων
- Ευφυέστερη θέρμανση, εξαερισμό και κλιματισμό (Heating, Ventilation και air-conditioning, HVAC)
- Ασφαλέστεροι και πιο υγιείς χώροι εργασίας και κτίρια
- Βελτιστοποίηση της υπηρεσίας εξυπηρέτησης
- Μείωση κόστους και μείωση της κατανάλωσης ενέργειας και νερού
- Καλύτερος σχεδιασμός, λειτουργική αποτελεσματικότητα και ενισχυμένη κατανομή πόρων
- Προγνωστική συντήρηση και προγραμματισμός συντήρησης εγκαταστάσεων
- Έλεγχος, διαμόρφωση και ρύθμιση του εξοπλισμού εγκατάστασης
- Διαχείριση κτιρίων και αυτοματισμοί κτιρίων
- Ενεργειακή απόδοση
- Φως και έλεγχος χώρου, άνεση



Έξυπνο πάρκινγκ

Παρακολούθηση σε πραγματικό χρόνο της διαθεσιμότητας χώρων στάθμευσης στην πόλη, επιτρέποντας έτσι στους κατοίκους να εντοπίζουν και να δεσμεύουν την πλησιέστερη διαθέσιμη θέση παρκινγκ. Μερικά από τα οφέλη είναι, η μείωση της κυκλοφοριακής συμφόρησης και η αύξηση των εσόδων από την δυναμική τιμολόγηση του πάρκινγκ.

Διαχείριση σκουπιδιών

Ανίχνευση του επιπέδου των σκουπιδιών για τη βελτιστοποίηση των δρομολογίων συλλογής των απορριμμάτων. Κάδοι απορριμμάτων και ανακύκλωσης με ετικέτες RFID, επιτρέπουν στο προσωπικό υγιεινής, να δουν πότε άδειασε τελευταία φορά ο κάδος. Ίσως ένα πρόγραμμα "Pay as you Throw" να μειώσει τα σκουπίδια και να εντείνει τις προσπάθειες της ανακύκλωσης.

Έξυπνο σύστημα μεταφορών

Έξυπνοι δρόμοι και αυτοκινητόδρομοι με προειδοποιητικά μηνύματα και εκτροπές ανάλογα με κλιματολογικές συνθήκες και απροσδόκητα γεγονότα όπως ατυχήματα ή κυκλοφοριακή συμφόρηση. Φανάρια με ενσωματωμένους αισθητήρες βίντεο, που μπορούν να προσαρμόσουν τα πράσινα και τα κόκκινα, ανάλογα με το που είναι τα αυτοκίνητα και την ώρα της ημέρας, μειώνοντας έτσι την κυκλοφοριακή συμφόρηση και την αιθαλομίχλη, δεδομένου ότι τα οχήματα στο ρελαντί στα κόκκινα φανάρια καίνε έως και 17% από τα καύσιμα που καταναλώνονται σε αστικές περιοχές, Σαν αποτέλεσμα θα έχουμε λιγότερη κατανάλωση καυσίμων, άρα και μείωση της ατμοσφαιρικής ρύπανσης.

Έξυπνος τουρισμός

Smartphone εφαρμογές που υποστηρίζονται από τους QR κώδικες και ετικέτες NFC παρέχουν ενδιαφέρουσες και χρήσιμες τουριστικές πληροφορίες σε όλη την πόλη. Οι πληροφορίες θα μπορούσαν να περιλαμβάνουν μουσεία, πινακοθήκες, βιβλιοθήκες, τουριστικά αξιοθέατα, γραφεία τουρισμού, τα μνημεία, τα καταστήματα, λεωφορεία, ταξί, κήπους, κλπ

Δύο «έξυπνες» εφαρμογές στάθμευσης και φωτισμού θα εγκατασταθούν στην Χαλκίδα, την πρώτη πόλη στην Ελλάδα, υποστηριζόμενα από μία ενιαία πλατφόρμα έξυπνης πόλης. Οι δυο εφαρμογές αυτές, θα συμβάλλουν στην αποσυμφόρηση της κυκλοφορίας και στη μείωση κατανάλωσης ενέργειας στην πόλη της Χαλκίδας. Σύμφωνα με ανακοίνωση του Ομίλου ΟΤΕ, σε ότι αφορά την εφαρμογή "Smart Parking" στο πλαίσιο του έργου θα εγκατασταθούν, σε κεντρικό σημείο της Χαλκίδας, ειδικοί αισθητήρες έξυπνης στάθμευσης, οι οποίοι μέσω εφαρμογής στο κινητό, που αναπτύχθηκε από την OTS, θα ενημερώνουν τους οδηγούς που βρίσκονται ελεύθερες θέσεις στάθμευσης και πως θα φτάσουν εκεί.

(Νέα, κατάλογος για Αλληλέγγυα, Κοινωνική Οικονομία enallaktikos.gr, 2018)

Το Τελ Αβίβ αντιμετωπίζει τη κίνηση στους πιο πολυσύχναστους δρόμους, εξασφαλίζοντας μία λωρίδα κυκλοφορίας για λεωφορεία και ταξί, επιτρέποντας όμως

στους ανυπόμονους οδηγούς ή σ' αυτούς με τις βαθιές τσέπες να χρησιμοποιούν την ορισθείσα λωρίδα, με το ανάλογο αντίτιμο. Αισθητήρες στην άσφαλτο παίρνουν τον αριθμό της πινακίδας του αυτοκινήτου και χρεώνεται αυτόματα στην πιστωτική κάρτα του ιδιοκτήτη ένα ποσό, που ποικίλλει ανάλογα με το πόση κυκλοφοριακή συμφόρηση παρουσιάζει ο δρόμος.

Μεταξύ των έξυπνων συστημάτων καταμέτρησης πρώτος έρχεται ο μετρητής κατανάλωσης ηλεκτρικής ενέργειας. Εκτός από το να καταγράφει πόσες kWh έχουν καταναλωθεί από την ηλεκτρική εγκατάσταση, θα πρέπει να μπορεί να δίδει και άλλες πληροφορίες όπως οι δυνατότητες άμεσης τηλεανάγνωσης της κατανάλωσης αλλά και δημιουργίας στατιστικών χρήσης και αξιοποίησής τους από το εσωτερικό του κτιρίου. Η πλέον ενδιαφέρουσα δυνατότητα που δίδεται στον καταναλωτή είναι το να μπορεί να ελέγχει κάθε στιγμή την κατανάλωσή του, άρα και το κόστος της ενέργειας που καταναλώνει από το εσωτερικό της κατοικίας του. Οι πληροφορίες αυτές μπορούν να μεταδίδονται από το μετρητή προς την κατοικία είτε μέσω του δικτύου (της παροχής) ή ασύρματα με την τεχνική KNX-RF. Ο καταναλωτής θα μπορεί (αν θέλει βέβαια) να λαμβάνει τις πληροφορίες για την ενέργεια που καταναλώνει μέσω του υπολογιστή του (με ειδικό modem) ή μέσω ενός ειδικού panel. Αντίστοιχες εξελίξεις προβλέπονται για τους μετρητές κατανάλωσης νερού και αερίου.

Με την χρήση των τεχνολογιών του έξυπνου δικτύου διευκολύνεται η ενσωμάτωση ενός μεγάλου εύρους κατανεμημένων πηγών παραγωγής, από ανανεώσιμες πηγές ενέργειας, όπως φωτοβολταϊκά και ανεμογεννήτριες, μέχρι μικρής κλίμακας συστήματα συμπαραγωγής ηλεκτρικής και θερμικής ενέργειας, καθώς και συστημάτων αποθήκευσης ενέργειας. Μέσα από τη χρήση εξελιγμένων εργαλείων μοντελοποίησης και ανάλυσης των συστημάτων, υποστήριξης αποφάσεων, πρόβλεψης καιρού και πρόβλεψης κατάστασης φορτίου μέσω μηχανικής μάθησης, η εισαγωγή των πηγών αυτών στο δίκτυο θα μπορεί να γίνει με πολύ μεγαλύτερη ευκολία σε σύγκριση με το δίκτυο του παρελθόντος.(Παντισκα Λεονάρδος,2016)

- Φωτοβολταϊκές εγκαταστάσεις: Παρακολούθηση και βελτιστοποίηση της απόδοσης στον τομέα της ηλιακής ενέργειας.
- Ανεμογεννήτριες: Παρακολούθηση και ανάλυση της ροής της ενέργειας από ανεμογεννήτριες και αμφίδρομη επικοινωνία με τους ευφυείς μετρητές των καταναλωτών για την ανάλυση καταναλωτικών προτύπων.

Στα συστήματα του έξυπνου δικτύου, ο ρόλος των καταναλωτών αλλάζει και πλέον από παθητικοί χρήστες γίνονται ενεργοί συμμετέχοντες στη διαχείριση της ενέργειάς τους. Με τη χρήση εξελιγμένου υλικού, όπως έξυπνοι μετρητές και έξυπνες συσκευές, λογισμικού και τεχνολογιών επικοινωνίας, οι καταναλωτές έχουν μια πληθώρα πληροφοριών στη διάθεσή τους, οι οποίες τους βοηθούν στο να παίρνουν αποφάσεις και κάνουν δυνατή την εφαρμογή ενεργειών, όπως η τιμολόγηση πραγματικού χρόνου και η απόκριση σε αιτήματα των εταιρειών για μείωση φορτίου στις ώρες αιχμής του δικτύου, με οικονομικά και περιβαλλοντικά οφέλη και για τις εταιρείες αλλά και για τους καταναλωτές. Ακόμα, στο έξυπνο ηλεκτρικό δίκτυο κάθε καταναλωτής μπορεί να γίνει και παραγωγός, θέτοντας απλά στην υπηρεσία του συστήματος τα δεδομένα χρήσης των οικιακών του συσκευών, δηλαδή, πότε και πόση ώρα χρησιμοποιεί πχ το πλυντήριο ρούχων, ώστε τη συγκεκριμένη στιγμή να μπορεί το δίκτυο να μειώνει τη

παροχή ρεύματος στο συγκεκριμένο σπίτι και να τη διαθέτει σε έναν άλλο χρήστη, χωρίς κάτι τέτοιο να προκαλεί δυσλειτουργίες.

1.17 Οι προεκτάσεις του IoT στον τομέα της υγείας

Το Ίντερνετ των Πραγμάτων είναι παρόν στην υγειονομική περίθαλψη σε πολλές μορφές εδώ και αρκετά χρόνια.
Με την απομακρυσμένη παρακολούθηση της υγειονομικής περίθαλψης και την παρακολούθηση και συντήρηση ιατρικών, νοσοκομειακών περιουσιακών στοιχείων ως τυπικά παραδείγματα αυτών των αρχικών αιτήσεων, το πρόσωπο του Διαδικτύου των πραγμάτων στην υγειονομική περίθαλψη αλλάζει γρήγορα (I-scoop.eu, 2018)

Ορισμένες εξελίξεις και προβλέψεις στον τομέα της υγειονομικής περίθαλψης σε αριθμούς
Οι έρευνες δείχνουν ότι έως το 2019 το 89% όλων των οργανώσεων υγειονομικής περίθαλψης θα έχει υιοθετήσει την τεχνολογία του Διαδικτύου και ότι το Ίντερνετ των πραγμάτων θα είναι απαραίτητο στις πρωτοβουλίες των πληρωτών και των παρόχων υγειονομικής περίθαλψης το 2017 και το 2018. Παράλληλα, Μεταξύ των κύριων αντιλήψεων για τα οφέλη της υγειονομικής περίθαλψης στο Διαδίκτυο στο μέλλον είναι η αύξηση της παραγωγικότητας του εργατικού δυναμικού (57%), η εξοικονόμηση κόστους (57%), η δημιουργία νέων επιχειρηματικών μοντέλων (36%) και η καλύτερη συνεργασία με συναδέλφους και ασθενείς (27%). Τα βασικά οφέλη, όπως αναφέρθηκαν τον Μάρτιο του 2017, είναι η αύξηση της καινοτομίας (80%), η προβολή σε ολόκληρο τον οργανισμό (76%) και η εξοικονόμηση κόστους (73%). Άλλες έρευνες δείχνουν ότι τα φορητά εξαρτήματα θα διαδραματίσουν βασικό ρόλο στα σχέδια υγειονομικής περίθαλψης, τα κλινικά δεδομένα της συσκευής IoT θα απελευθερώσουν τον χρόνο του ιατρού σημαντικά μέχρι το 2019 (μέχρι 30%) και θα υπάρξει ένας αυξανόμενος ρόλος για τους βιοαισθητήρες και τα ρομπότ την παράδοση προμηθειών στα νοσοκομεία μέχρι το 2019.

1.18 Internet of Things στην αυτοκινητοβιομηχανία

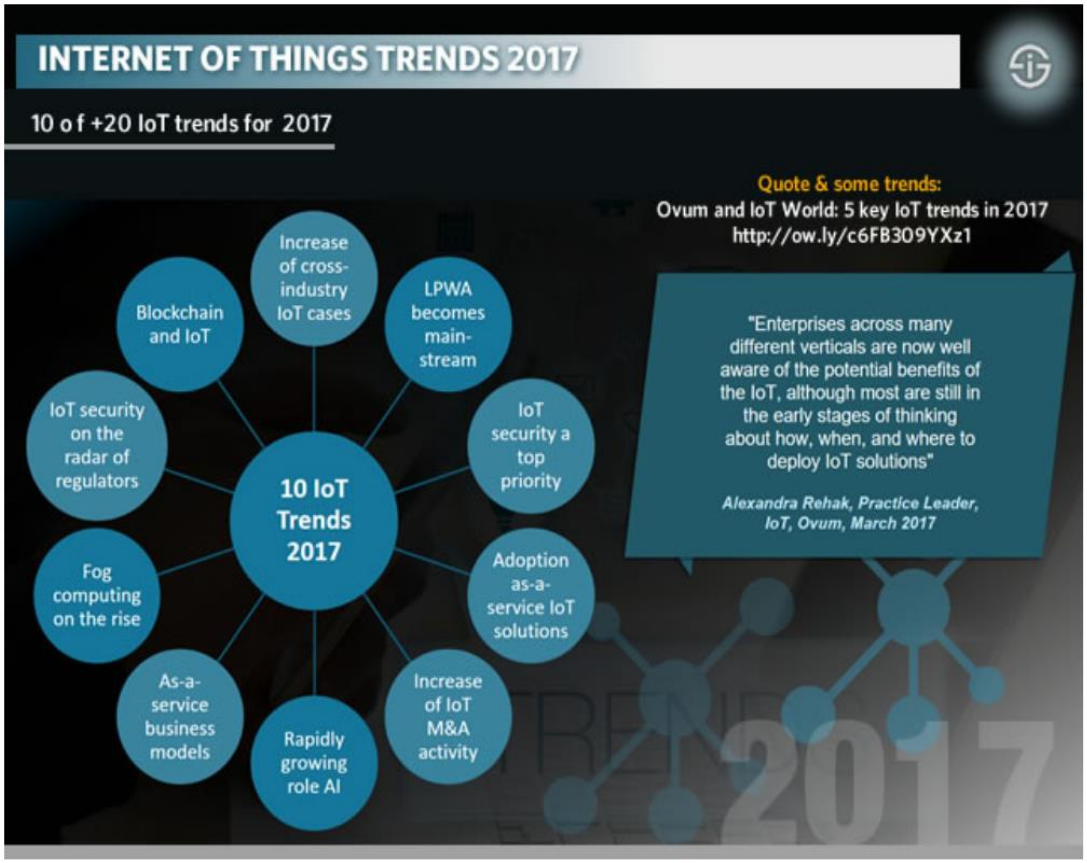
Τα συνδεδεμένα αυτοκίνητα και όλες οι άλλες εξελίξεις στην αυτοκινητοβιομηχανία οδηγούν την αγορά.
Τα συνδεδεμένα οχήματα μπορούν κάλλιστα να αποτελούν την πιο hot αγορά των ΗΠΑ συνολικά. Το συνδεδεμένο αυτοκίνητο είναι ένα από αυτά τα τυπικά παραδείγματα όπου το Διαδίκτυο για τα καταναλωτικά πράγματα και το βιομηχανικό διαδίκτυο των πραγμάτων αλληλεπικαλύπτονται

1.19 Σύγχρονες τάσεις που αφορούν το οικοσύστημα του IoT

- Τεχνολογίες LPWA
- _Η ασφάλεια και η κανονιστική συμμόρφωση αποτελούν προτεραιότητα
- Μεγαλύτερες οργανώσεις αναπτύσσουν περισσότερα μοντέλα ως υπηρεσία και ταυτόχρονα αγκαλιάζονται περισσότερες λύσεις όπως η υπηρεσία IoT

- Η σύγκλιση του blockchain με το Internet of Things είναι ένα γεγονός που θα δημιουργήσει πολλές νέες αλλαγές αλλά κάποια εγγενή ζητήματα της τεχνολογίας του blockchain πρέπει να αντιμετωπιστούν
- Η τεχνητή νοημοσύνη και τα analytics καθίστανται όλο και πιο σημαντικά στην αυξανόμενη πραγματικότητα του IoT
- Στο βιομηχανικό Διαδίκτυο, η πληροφορική και η OT ενσωμάτωση μεγαλώνει αλλά παρεμποδίζεται από τις ανησυχίες για την ασφάλεια στον κυβερνοχώρο
- Τα Wearables θα είναι ένα ταχέως αναπτυσσόμενο τμήμα, μεταξύ άλλων στην αγορά της υγειονομικής περίθαλψης και της βιομηχανίας
- Το industry 4.0 και η βιομηχανία επενδύουν τα περισσότερα στο Διαδίκτυο και προωθούν την ανάπτυξη του Διαδικτύου των ρομποτικών πραγμάτων, του cloud και της 5G

(I-scoop.eu, 2018)



1.20 5G και Internet of Things

Το 5G είναι η επόμενη γενιά κυψελοειδούς κινητικότητας μετά από 4G και έρχεται με διαφορετική αρχιτεκτονική και πολύ υψηλότερες ταχύτητες μεταφοράς δεδομένων, προσφέροντας παράλληλα το εύρος ζώνης που απαιτείται για ζωντανές ροές εικονικής πραγματικότητας και αυτόνομα οχήματα

Οι τελικές προδιαγραφές του 5G θα είναι έτοιμες μέχρι το τέλος του 2019, αλλά ήδη αρκετές μεγάλες βιομηχανικές εταιρείες IoT εξετάζουν τις δυνατότητες και την

υιοθέτηση του 5G ως το κέντρο ενός ετερογενούς περιβάλλοντος δικτύου. Το 5G δεν έχει σχεδιαστεί για IoT, έχει σχεδιαστεί για πανταχού παρούσα συνδεσιμότητα με ρυθμούς δεδομένων στην περιοχή των gigabit ανά δευτερόλεπτο

Παρόλο που αναμένεται ότι η 5G θα αρχίσει να συσπειρώνεται μόνο προς το τέλος της επόμενης δεκαετίας και στη δεκαετία μετά, υπάρχουν σχετικά πλάνα για την ενσωμάτωση σε θέματα IoT.
Σύμφωνα με την ερευνητική εταιρεία IDC, η ευρεία ενεργοποίηση των περιπτώσεων χρήσης του IoT χάρη στο 5G έως το 2021 θα οδηγήσει το 70% των μεγαλύτερων 2000 δημόσιων εταιρειών ανά την υφήλιο να ξοδέψουν 1,2 δισεκατομμύρια δολάρια για λύσεις διαχείρισης συνδεσιμότητας. Το δυναμικό της αγοράς του 5G είναι τόσο τεράστιο όσο και οι δυνατότητες που προσφέρει, επαναπροσδιορίζοντας την ίδια την έννοια της κινητικότητας και ενισχύοντας την πανταχού παρούσα συνδετικότητα του IoT
Το 5G δεν αφορά μόνο υψηλότερους ρυθμούς μεταφοράς δεδομένων, αλλά και αξιοπιστία, λανθάνουσα κατάσταση και αυτό που είναι γνωστό ως edgeless computing. (I-scoop.eu, 2018)

1.21 Security considerations για το IoT

Οι συνδεδεμένες συσκευές και το Διαδίκτυο των Πραγμάτων χρησιμοποιούνται όλο και περισσότερο για επιθέσεις μεγάλης κλίμακας.Διάφορες επιθέσεις DDoS έχουν αναφερθεί κατά τη διάρκεια του 2016, συμπεριλαμβανομένης της επίθεσης DDoS μέχρι 620 Gbps, η οποία καθιστά την ιστοσελίδα του γνωστού δημοσιογράφου ασφαλείας Bryan Krebs να είναι εκτός λειτουργίας από τα τέλη Σεπτεμβρίου 2016. Η επίθεση έτυχε πολλής προσοχής

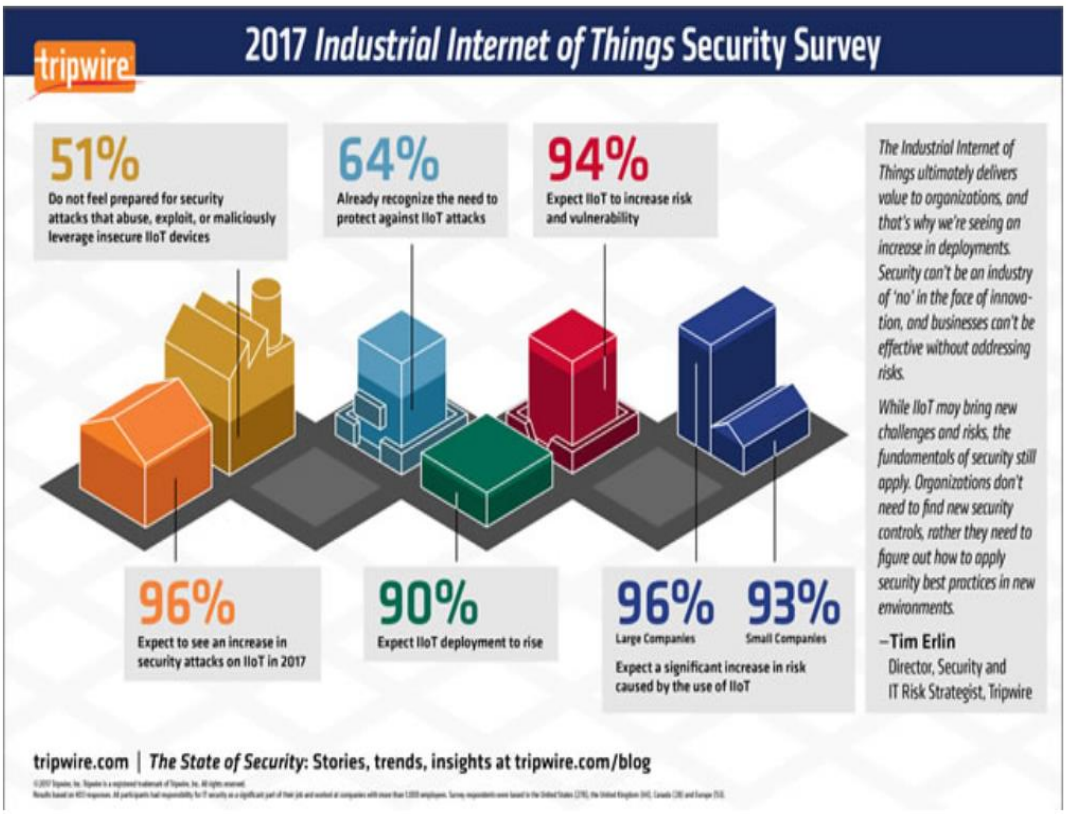
Οι φόβοι είναι υψηλοί πως σύντομα τέτοιες επιθέσεις θα καταστούν ακόμα πιο εντατικές θα γίνουν ο κανόνας. Και δεν πρόκειται μόνο για επιθέσεις DDoS. Το Ransomware μετακινείται επίσης στο Διαδίκτυο των πραγμάτων και οι εμπειρογνώμονες ασφαλείας προειδοποιούν για την κατακόρυφη επίδραση των εκμεταλλευόμενων τρωτών σημείων στη συνδεδεμένη πραγματικότητα που έχει το IoT. Εκτός από τις προκλήσεις ασφάλειας, πρέπει επίσης να αντιμετωπιστεί η συμμόρφωση και η προστασία δεδομένων(GDPR) (I-scoop.eu, 2018)

Στο Διαδίκτυο των πραγμάτων, οι αισθητήρες επικοινωνούν μεταξύ τους και μέσω των πύλων που συνδέονται με την πλατφόρμα Internet of Things, οι διάφορες εφαρμογές της εταιρείας τροφοδοτούνται και πυροδοτούνται

Κάποιες ενδεικτικές ανησυχίες είναι οι παρακάτω:

- Χαρακτηριστικά ευπάθειας στις συσκευές
- Δύσκολες ή μη υπάρχουσες διαδικασίες για την επίθεση των συσκευών IoT
- Η έλλειψη ενημέρωσης και υποστήριξης από το boardroom
- Η υπερβολική εστίαση στην εξοικονόμηση κόστους στα έργα του Διαδικτύου των Πράξεων και η μη επένδυση σε βασικούς ελέγχους ασφαλείας
- Έλλειψη τυποποίησης σε δίκτυα και Application Programming Interfaces(API)
- Παλιές συσκευές

- Εκπαίδευση και ενημέρωση των καταναλωτών
- Τυποποίηση και πρωτόκολλα



Η ασφάλεια του Διαδικτύου παίρνει τόση προσοχή τώρα που αναμένεται να έχει προσωρινό αντίκτυπο στα κέρδη παραγωγικότητας των διαδικτυακών εταιρειών καθώς ωθούνται να είναι έτοιμες να επενδύσουν πολύ περισσότερο στην ασφάλεια. Εκτός από την ασφάλεια, υπάρχει και το ζήτημα της σωματικής ασφάλειας. Ορισμένες τεχνολογίες, όπως το blockchain, εξετάζονται επίσης ως τρόποι παροχής πιο αξιόπιστου IoT. Ωστόσο, η ασφάλεια του Διαδικτύου δεν περιλαμβάνει μόνο φυσικά δεδομένα και συναλλαγές.

οι πιθανές ανησυχίες σχετικά με την ασφάλεια του κυβερνοχώρου και τη σωματική ασφάλεια που σχετίζονται με συσκευές IoT θα ασκήσουν πιέσεις στους CIO στις μεγαλύτερες εταιρείες του κόσμου για να αυξήσουν τις δαπάνες για την ασφάλεια του Διαδικτύου έως και 25%, γεγονός που εξηγεί την προσωρινή εξουδετέρωση των κερδών της παραγωγικότητας των επιχειρήσεων

Η προστασία των προσωπικών δεδομένων, με ενδεχομένως σημαντικά πρόστιμα σε περίπτωση παραβίασης και μη συμμόρφωσης, αποτελεί τον ακρογωνιαίο λίθο του Κανονισμού περί Γενικής Προστασίας Δεδομένων ή του GDPR ο κανονισμός της ΕΕ αφορά όλους τους οργανισμούς που επεξεργάζονται τα προσωπικά δεδομένα των πολιτών της ΕΕ. Είναι σημαντικό να προετοιμαστεί κανείς για τη συμμόρφωση με το GDPR εν γένει, αλλά και για το Διαδίκτυο των πραγμάτων. Επειδή με το Διαδίκτυο των πραγμάτων υπάρχει μια σειρά από τεχνολογίες, συσκευές, περιπτώσεις χρήσης,

εφαρμογές και διαδικασίες που είναι αρκετά συγκεκριμένες και κάποιες φορές παραβλέπονται.Ένα δεύτερο νομοθετικό πλαίσιο, επίσης στην ΕΕ, που θα επηρεάσει τι μπορεί και δεν μπορεί να γίνει με το Διαδίκτυο των πραγμάτων είναι ο κανονισμός για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Το κείμενο αυτό δεν είναι ακόμη τελικό, αλλά μόλις τελειοποιηθεί, θα έχει σημαντικές συνέπειες καθώς καλύπτει την προστασία της ιδιωτικής ζωής στα κανάλια ηλεκτρονικών επικοινωνιών και υπάρχει ρητή αναφορά στο Διαδίκτυο των πραγμάτων

Οι κανονιστικές αλλαγές θα οδηγήσουν επίσης στην υιοθέτηση του Ίντερνετ των πραγμάτων τόσο στις καταναλωτικές όσο και στις επιχειρηματικές / βιομηχανικές εφαρμογές, όπου τα δεδομένα, η ιδιωτικότητα και η ασφάλεια παραμένουν βασικές προκλήσεις

Μετά τη γενική επισκόπηση του IoT ακολουθεί η εξής προσέγγιση

Περιγραφή του SerIoT Task 3.6

Traffic tracing, provenance certification of SerIoT Flows and attack detection:

Within this task, effective techniques for tracing traffic flows and packet sampling such as NetFlow will be researched and developed. Metrics related to the optimum performance of an IoT infrastructure will be taken into account (based also on requirements set by the Use Cases of SerIoT – T1.2) and new approaches will be designed for paths modifications in the IoT network, satisfying security requirements of the end-users. It also focuses on an automatic policy generation to protect the IoT's networks from any internal attacks by any compromised node. This is done by forwarding the traffic collected via Netflow to traffic analyser nodes. SDN controller is enhanced to calculate the shortest path in a way to place traffic analyser on a way of each flows. Traffic analyser can submits any suspicious patterns to an IDS system for attack detection and inform the pattern to SDN controller to generate and apply policy on the network to prevent this attack automatically.

Στο πλαίσιο της επίλυσης του ζητήματος του provenance of traffic flows παρατίθεται παρακάτω μία γενικότερη επισκόπηση του NetFlow, το οποίο αποτελεί ένα εργαλείο για Network Traffic Monitoring και θα χρησιμοποιηθεί πρακτικά για να γίνει implement ένα μεγάλο μέρος του Task 3.6 για provenance of traffic flows. Παράλληλα με την παρουσίαση των γενικών χαρακτηριστικών του NetFlow, υπάρχει και ένα general troubleshooting και μία σύγκριση του NetFlow με άλλα αντίστοιχα tools.

Παράλληλα καθίσταται σαφές και από το description του SerIoT project, ένα κομμάτι του όλου εγχειρήματος είναι η υλοποίηση ενός packet sampler. Κατά συνέπεια ακολουθεί μία σύντομη comparative analysis κάποιων τεχνικών για packet sampling η οποία καταλήγει στην παρουσίαση μίας μεθόδου για adaptive sampling με consideration για traffic classification. Το traffic classification, παρότι δεν είναι κομμάτι του Task 3.6, αποτελεί κομμάτι του όλου project, καθώς θα αποτελέσει εργαλείο τόσο για το γενικότερο monitoring του SerIoT ecosystem, θα αποτελέσει και κομμάτι της διαδικασίας για το anomaly detection.

2.NetFlow

2.1 Εισαγωγή στο NetFlow

Το NetFlow είναι ένα ενσωματωμένο όργανο στο Cisco IOS Software για να χαρακτηρίσει τη λειτουργία του δικτύου. Ορατότητα στο δίκτυο είναι ένα απαραίτητο εργαλείο για τους επαγγελματίες πληροφορικής. Ως απάντηση σε νέες απαιτήσεις και πιέσεις, οι φορείς εκμετάλλευσης δικτύου θεωρούν κρίσιμο να κατανοήσουν πώς συμπεριφέρεται το δίκτυο συμπεριλαμβανομένων των εξής στοιχείων.

- Εφαρμογή και χρήση του δικτύου
- Η παραγωγικότητα του δικτύου και η αξιοποίηση των πόρων του δικτύου
- Ο αντίκτυπος των αλλαγών στο δίκτυο
- Ανωμαλία δικτύου και ευπάθειες ασφαλείας
- Μακροπρόθεσμα ζητήματα συμμόρφωσης

Το Cisco IOS NetFlow ικανοποιεί αυτές τις ανάγκες, δημιουργώντας ένα περιβάλλον όπου οι διαχειριστές διαθέτουν τα εργαλεία να καταλάβουν πότε, πού, και πώς κυκλοφορεί η ροή του δικτύου. Όταν κατανοείται η συμπεριφορά του δικτύου, η επιχειρηματική διαδικασία βελτιώνεται και είναι διαθέσιμη μια διαδρομή ελέγχου για τον τρόπο με τον οποίο χρησιμοποιείται το δίκτυο. Αυτή η αυξημένη γνώση μειώνει την ευπάθεια του δικτύου σε σχέση με την διακοπή και επιτρέπει την αποτελεσματική λειτουργία του δικτύου. Οι βελτιώσεις στη λειτουργία του δικτύου μειώνουν το κόστος και οδηγούν σε υψηλότερα έσοδα των επιχειρήσεων με την καλύτερη αξιοποίηση των υποδομών του δικτύου
(Services et al., 2018)

2.2 SNMP performance monitoring

Παραδοσιακά, οι πελάτες βασίζονταν σχεδόν αποκλειστικά στο πρωτόκολλο Simple Network Management Protocol (SNMP) για την παρακολούθηση του bandwidth. Παρόλο που το SNMP διευκολύνει το capacity planning, δεν κάνει τίποτα για να χαρακτηρίσει network applications και μοτίβα, απαραίτητα για την κατανόηση του βαθμού στον οποίο το δίκτυο υποστηρίζει την επιχείρηση. Μια πιο λεπτομερής κατανόηση για το πώς χρησιμοποιείται το εύρος ζώνης είναι εξαιρετικά σημαντική στα δίκτυα IP σήμερα. Μετρητές διασύνδεσης πακέτων και byte είναι χρήσιμοι, αλλά η κατανόηση ποιων διευθύνσεων IP είναι η πηγή και ο προορισμός του traffic και ποιες εφαρμογές δημιουργούν το traffic είναι πολύτιμη
(Services et al., 2018)

2.3 Κατανόηση του δικτύου με χρήση του NetFlow

Η ικανότητα χαρακτηρισμού του IP traffic και η κατανόηση του τρόπου και του τόπου ροής της είναι κρίσιμη για τη διαθεσιμότητα του δικτύου,
τις επιδόσεις και την αντιμετώπιση προβλημάτων. Η παρακολούθηση των IP traffic flows διευκολύνει το capacity planning και εξασφαλίζει ότι οι πόροι χρησιμοποιούνται κατάλληλα για την υποστήριξη των οργανωτικών στόχων. Βοηθά το IT να καθορίσει πού να εφαρμόσει Quality of Service (QoS), να βελτιστοποιήσει τη χρήση των πόρων και να διαδραματίσει

ζωτικό ρόλο στην ασφάλεια του δικτύου για την ανίχνευση Denial of Service (DoS) attacks, network propagated worms και άλλα ανεπιθύμητα συμβάντα στο εσωτερικό του δικτύου. (Services et al., 2018)

2.4 Σημαντικά προβλήματα που αντιμετωπίζονται συχνά από IT professionals στα οποία το NetFlow επιχειρεί να δώσει άμεσα λύση

- *Ανάλυση νέων εφαρμογών και των επιπτώσεών τους στο δίκτυο*.

Αναγνώριση νέων application network loads όπως VoIP ή remote site additions.

- *Μείωση του peak WAN traffic*

Χρήση των NetFlow statistics για μέτρηση των μεταβολών του WAN traffic από αλλαγές του application-policy. Κατανόηση του ποιος χρησιμοποιεί, κατά κύριο λόγο, το δίκτυο και ποιοι είναι οι top talkers του δικτύου.

- *Troubleshooting και εντοπισμός των pain points του δικτύου.*

Διάγνωση χαμηλής απόδοσης του δικτύου, bandwidth hogs και χρήσης του bandwidth με Command Line Interface (CLI) και χρήση διαφορετικών reporting tools

- *Ανίχνευση unauthorized WAN traffic*

Αποφυγή κοστοβόρων αναβαθμίσεων ταυτοποιώντας ποιες εφαρμογές προκαλούν congestion

- *Security και anomaly detection*

Το NetFlow μπορεί να χρησιμοποιηθεί για anomaly detection και worm diagnosis με την υποβοήθηση άλλων εργαλείων όπως το Cisco CS-Mars.

- *Επικύρωση παραμέτρων του Quality of Service (QoS)*

Επιβεβαίωση ότι το κατάλληλο bandwidth έχει αποτεθεί σε κάθε Class of Service (CoS) και παράλληλα ότι καμμία Class of Service δεν είναι over ή under-subscribed. (Manageengine.com, 2018)

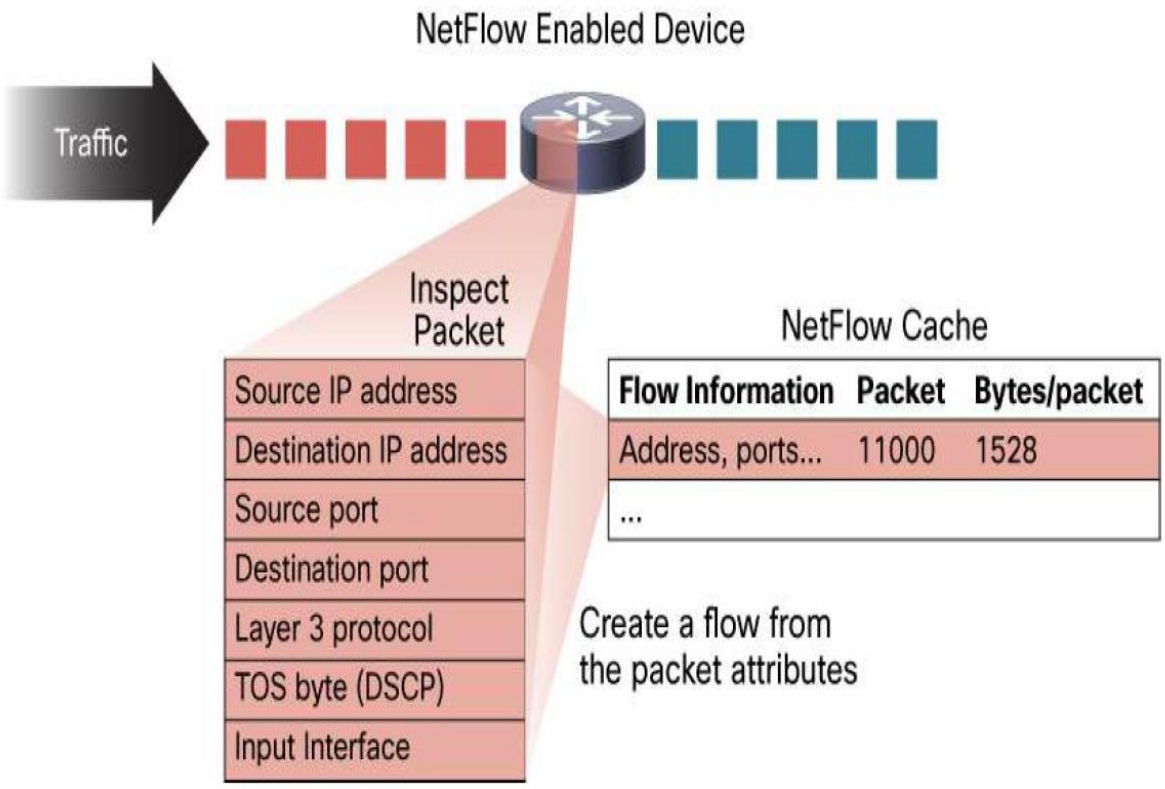
2.5 IP Flow

Κάθε πακέτο που προωθείται μέσα σε δρομολογητή ή διακόπτη εξετάζεται για ένα σύνολο χαρακτηριστικών πακέτων IP. Αυτά τα χαρακτηριστικά είναι η ταυτότητα του πακέτου IP ή το δακτυλικό αποτύπωμα του πακέτου και καθορίζει εάν το πακέτο είναι μοναδικό ή παρόμοιο με άλλα πακέτα. Παραδοσιακά ένα IP Flow αποτελεί ένα σύνολο από 5 με 7 χαρακτηριστικά των πακέτων. Πιο συγκεκριμένα:

- IP της διεύθυνσης αποστολής

- IP της διεύθυνσης προορισμού
- Source Port
- Destination Port
- Τύπος πρωτοκόλλου Layer 3
- Class of Service
- Το interface των routers και των switches

Όλα τα πακέτα με την ίδια διεύθυνση IP προέλευσης / προορισμού, θύρες προέλευσης / προορισμού, διεπαφή πρωτοκόλλου και Class of Service ομαδοποιούνται σε ένα flow και στη συνέχεια τα πακέτα και τα byte είναι ταυτισμένα. Αυτή η μεθοδολογία δακτυλικών αποτυπωμάτων ή ταυτοποίησης ενός flow μπορεί να κλιμακωθεί επειδή μια μεγάλη ποσότητα πληροφοριών δικτύου συμπυκνώνεται σε μια βάση δεδομένων με NetFlow information που ονομάζονται NetFlow cache. (Services et al., 2018)



Το information του εκάστοτε flow είναι πολύ χρήσιμο για τη συνολική κατανόηση της συμπεριφοράς του δικτύου. Η διεύθυνση προέλευσης επιτρέπει την κατανόηση του ποιος κόμβος ξεκινά το traffic. Παράλληλα η διεύθυνση προορισμού δηλώνει ποιος είναι, σε κάθε περίπτωση, ο παραλήπτης του traffic. Οι πύλες χαρακτηρίζουν την εφαρμογή που κάνει χρήση του traffic. Το Class of Service εξετάζει την προτεραιότητα του traffic. Το interface της συσκευής πως χρησιμοποιείται το

αναπτυσσόμενο traffic και τέλος τα συνολικά πακέτα και bytes δίνουν το συνολικό ποσό του traffic.

Επιπλέον πληροφορία που προστίθεται στα πακέτα του traffic

- Life timestamps τα οποία αντιλαμβάνονται τον κύκλο ζωής του flow. Χρησιμοποιούνται, κατά κύριο λόγο, για να υπολογιστούν τα packets και τα flows per second.
- Next hop IP addresses, συμπεριλαμβανομένου και του BGP routing Autonomous Systems (AS)
- Subnet mask με σκοπό να μπορεί η πηγή και ο προορισμός να υπολογίζουν prefixes
- TCP flags για να μπορούν να εξεταστούν τα εκάστοτε TCP handshakes.

(Manageengine.com, 2018)

2.6 Πρόσβαση στα δεδομένα που παράγονται από το NetFlow

Υπάρχουν δύο κύριες μέθοδοι για την πρόσβαση σε δεδομένα NetFlow: το Command Line Interface (CLI) με εντολές εμφάνισης ή χρησιμοποιώντας ένα εργαλείο αναφοράς εφαρμογών(application reporting tool). Αν ενδιαφέρεται κανείς για μια άμεση προβολή του τι συμβαίνει στο δίκτυο, το CLI μπορεί να χρησιμοποιηθεί. Το NetFlow CLI είναι πολύ χρήσιμο, εν γένει, για troubleshooting.
Η άλλη επιλογή είναι η εξαγωγή του NetFlow σε ένα reporting server ή σε αυτό που ονομάζεται "NetFlow collector". Το NetFlow collector έχει τη δουλειά της συγκέντρωσης και κατανόησης των εξαγόμενων flows και του συνδυασμού και οργάνωσής τους ώστε να παραχθούν πολύτιμες αναφορές που χρησιμοποιούνται για την ανάλυση του traffic και του security. Η εξαγωγή του NetFlow, σε αντίθεση με το SNMP polling, ωθεί
πληροφορίες περιοδικά στο NetFlow reporting collector. Σε γενικές γραμμές, η NetFlow cache γεμίζει συνεχώς με flows και λογισμικό τον router ή το switch αναζητά την cache για flows που έχουν λήξει ή έχουν τερματιστεί. Αυτά τα flows εξάγονται στο NetFlow collector server. Οι ροές τερματίζονται όταν η επικοινωνία των δύο κόμβων του δικτύου έχει τελειώσει (δηλαδή: ένα πακέτο περιέχει τη σημαία TCP FIN). Τα παρακάτω βήματα εφαρμόζονται για NetFlow data reporting:

- Το Netflow έχει διαταχθεί ώστε να τοποθετεί flows στη Netflow cache
- Το export του NetFlow στέλνει τα flows στον collector
- Η NetFlow cache αναζητείται για flows που έχουν τερματιστεί και αυτά, στη συνέχεια, εξάγονται στο NetFlow collector server
- Περίπου 30 με 50 flows συγκεντρώνονται και μεταφέρονται, σε μορφή UDP, στο NetFlow collector server.
- Το software του NetFlow collector δημιουργεί, σε real time, reports από τα λαμβανόμενα δεδομένα (Manageengine.com, 2018)

Ένα flow είναι έτοιμο για εξαγωγή όταν είναι ανενεργό για ένα συγκεκριμένο χρονικό διάστημα (δηλαδή: δεν έχουν ληφθεί νέα πακέτα για το flow αυτό) ή αν το flow είναι ενεργό και διαρκεί περισσότερο από τον ενεργό χρονοδιακόπτη (δηλαδή: μακρύ download FTP).Επίσης, το flow είναι έτοιμο για εξαγωγή όταν μια σημαία TCP υποδεικνύει ότι το flow τερματίζεται. Υπάρχουν χρονομετρητές για να προσδιοριστεί αν ένα flow είναι ανενεργό ή εάν το flow είναι long lived και η προεπιλογή για τον ανενεργό χρονοδιακόπτη ροής είναι 15 δευτερόλεπτα για τον ενεργό χρονοδιακόπτη ροής είναι 30 λεπτά. Όλοι οι χρονομετρητές για εξαγωγή είναι

διαμορφώσιμοι αλλά οι προεπιλογές χρησιμοποιούνται στις περισσότερες περιπτώσεις εκτός από το Switch Cisco Catalyst 6500 Series platform. Ο collector μπορεί να συνδυάσει flows και να συγκεντρώσει το συνολικό traffic.Για παράδειγμα,ένα FTP download που διαρκεί περισσότερο από ότι επιτάσσει ο ενεργός χρονοδιακόπτης μπορεί να σπάσει σε πολλαπλά flows και ο collector μπορεί να συνδυάσει αυτές τις ροές που δείχνουν συνολικό FTP traffic σε ένα server σε μια συγκεκριμένη ώρα της ημέρας.
(Services et al., 2018)

Ακολουθούν κάποια παραδείγματα δεδομένων που αποθηκεύονται στην cache του NetFlow.

1. Flow cache–The first unique packet creates a flow

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	162	/24	5	163	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	161	/24	180	10	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Flow Aging Timers

- Inactive Flow (15 sec is default)
- Long Flow (30 min (1800 sec) is default)
- Flow ends by RST or FIN TCP Flag

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

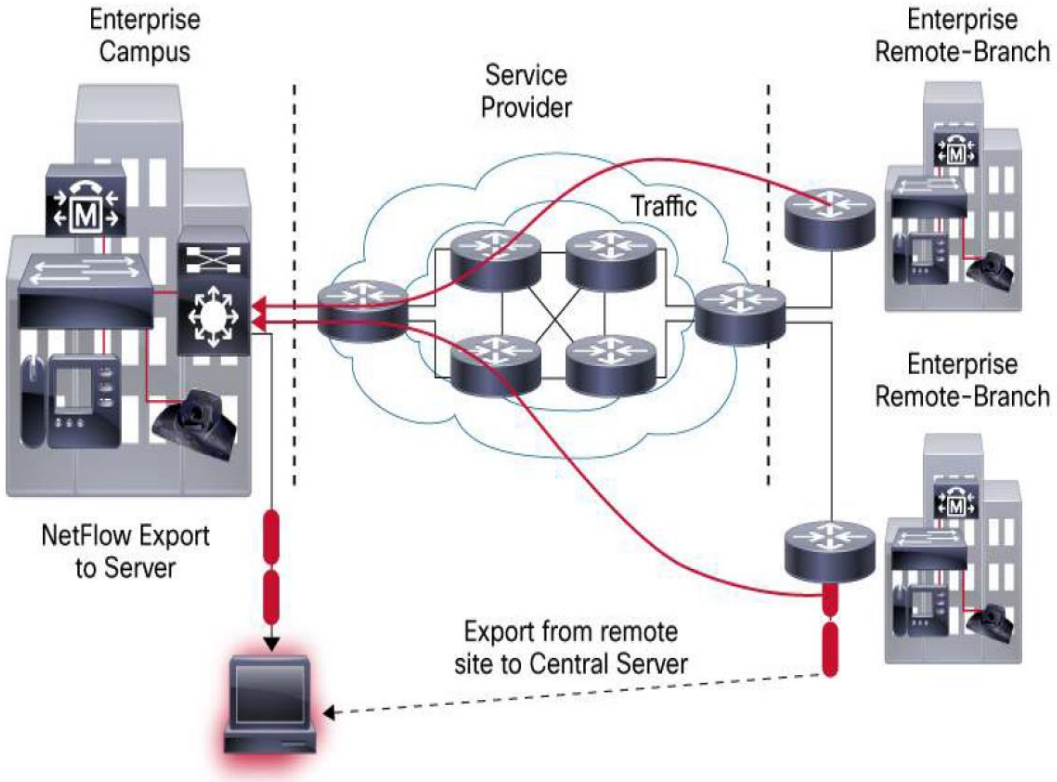
3. Flows packaged in export packet

Non-aggregated Flows–Export Version 5 or 9

4. Transport Flows to Reporting Server

2.7 Ο τρόπος με τον οποίο μπορεί το NetFlow να εισαχθεί στο δίκτυο

Το NetFlow χρησιμοποιείται συνήθως σε κεντρική τοποθεσία, επειδή χαρακτηρίζεται και διατίθεται όλη το traffic από απομακρυσμένες περιοχές μέσα στο NetFlow. Η τοποθεσία όπου αναπτύσσεται το NetFlow μπορεί να εξαρτάται από τη θέση του reporting solution και
την τοπολογία του δικτύου. Εάν ο διακομιστής συλλογής αναφορών βρίσκεται κεντρικά, τότε η υλοποίηση του NetFlow κοντά στον εξυπηρετητή συλλογής αναφορών είναι το βέλτιστο. Το NetFlow μπορεί επίσης να ενεργοποιηθεί σε απομακρυσμένες θέσεις υποκαταστημάτων κατανοώντας ότι τα δεδομένα εξαγωγής θα χρησιμοποιούν εύρος ζώνης. Περίπου το 1-5% του μετακινούμενου traffic χρησιμοποιείται για εξαγωγή στον collection server.
(Services et al., 2018)



Μόλις επιλεγεί η εφαρμογή αναφοράς, το μέγεθος του διακομιστή και ο αριθμός των διακομιστών καθορίζεται με την ομιλία με τον προμηθευτή του προϊόντος. Ορισμένα συστήματα αναφοράς παρέχουν μια αρχιτεκτονική δύο επιπέδων, όπου τοποθετούνται οι συλλέκτες
κοντά σε βασικούς ιστότοπους στο δίκτυο και συγκεντρώνουν και διαβιβάζουν τα δεδομένα σε έναν κύριο διακομιστή αναφορών. Άλλες μικρότερες διατάξεις ενδέχεται να έχουν έναν μόνο διακομιστή για αναφορά και συλλογή.

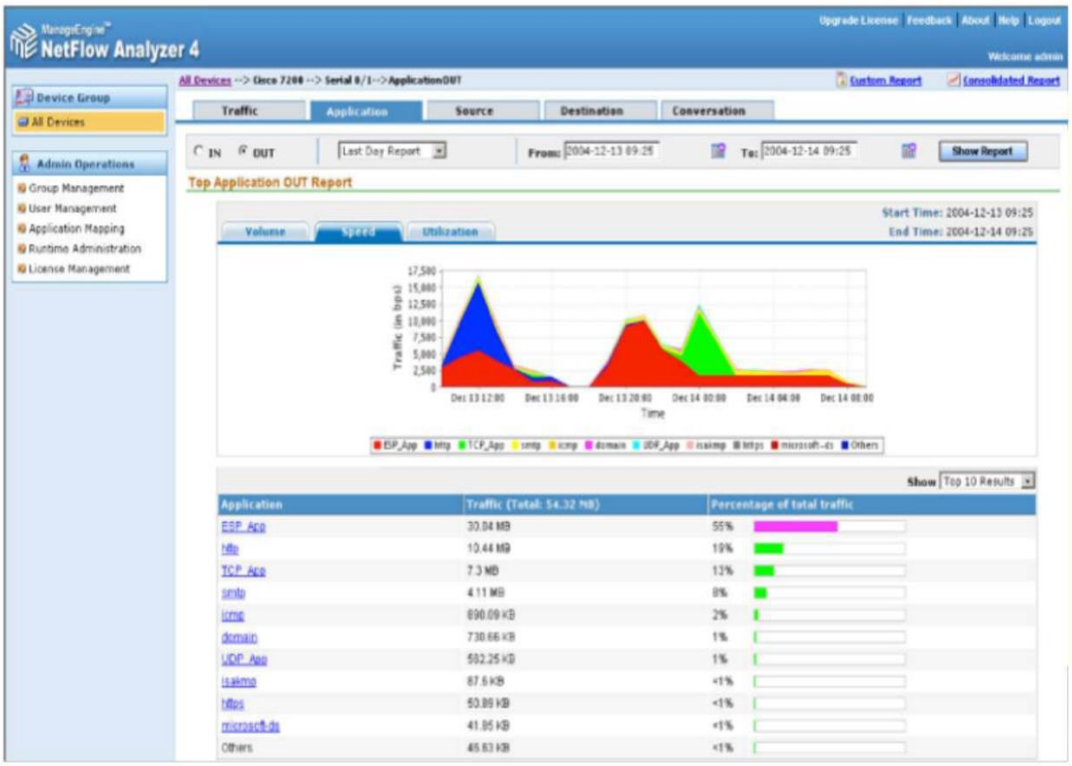
Ακολουθούν κάποιοι πίνακες με κάποια εμπορικά προιόντα του NetFlow για reporting

Product Name	Primary Use	Primary User	Operating System	Starting Price Range
Cisco NetFlow Collector	Traffic Analysis	Enterprise, Service Provider	Linux, Solaris	Medium
Cisco CS-Mars	Security Monitoring	Enterprise, SMB	Linux	Medium
AdventNet	Traffic Analysis	Enterprise, SMB	Windows	Low
Apoapsis	Traffic Analysis	Enterprise	Linux	Medium
Arbor Networks	Traffic/Security Analysis	Enterprise, Service Provider	BSD	High
Caligare	Traffic/Security Analysis	Enterprise, Service Provider	Linux	Medium
Fluke Networks	Traffic Analysis	Enterprise, SMB	Windows	Medium
Evident Software[1]	Traffic Analysis, Billing	Enterprise	Linux	High
HP[1]	Traffic Analysis	Enterprise, Service Provider	Linux, Solaris	High
IBM Aurora	Traffic Analysis/Security	Enterprise, Service Provider	Linux	Medium
IdeaData	Traffic Analysis	Enterprise	Windows/Linux	Medium
InfoVista	Traffic Analysis	Enterprise, Service Provider	Windows	High
IsarNet	Traffic Analysis	Enterprise, Service Provider	Linux	Medium

Product Name	Primary Use	Primary User	Operating System	Starting Price Range
Lancope	Traffic/Security Analysis	Enterprise, Service Provider	Linux	High
Micromuse[1]	Traffic Analysis	Enterprise, Service Provider	Solaris	High
CA NetQoS	Traffic/Security Analysis	Enterprise	Windows	High
Plixer / Scrutinizer	Traffic Analysis / Security Analysis / Billing	Enterprise / SMB/ Service Provider	Windows/Linux	Medium
Valencia Systems	Traffic Analysis	Enterprise	Windows	High
Solarwinds	Traffic Analysis	Enterprise, SMB	Windows	Low
Wired City	Traffic Analysis	Enterprise	Windows	High

Product Name	Primary Use	Comment	Operating System
CFlowd	Traffic Analysis	No longer supported	Unix
Flow-tools	Collector Device	Scalable	Unix
Flowd	Collector Device	Supports V9	BSD, Linux
FlowScan	Reporting for Flow-Tools		Unix
IPFlow	Traffic Analysis	Support V9, IPv4, IPv6, MPLS, SCTP, etc.	Linux, FreeBSD, Solaris
NetFlow Monitor	Traffic Analysis	Supports V9	Linux
NTOP	Collector Device	Supports V9	Unix
Panoptis	Security Monitoring		Unix
Stager	Reporting for Flow-Tools		Unix

Παρακάτω ακολουθεί ένα παράδειγμα ανάλυσης του traffic με χρήση δεδομένων από το NetFlow



2.8 Σύγκριση NetFlow με SNMP

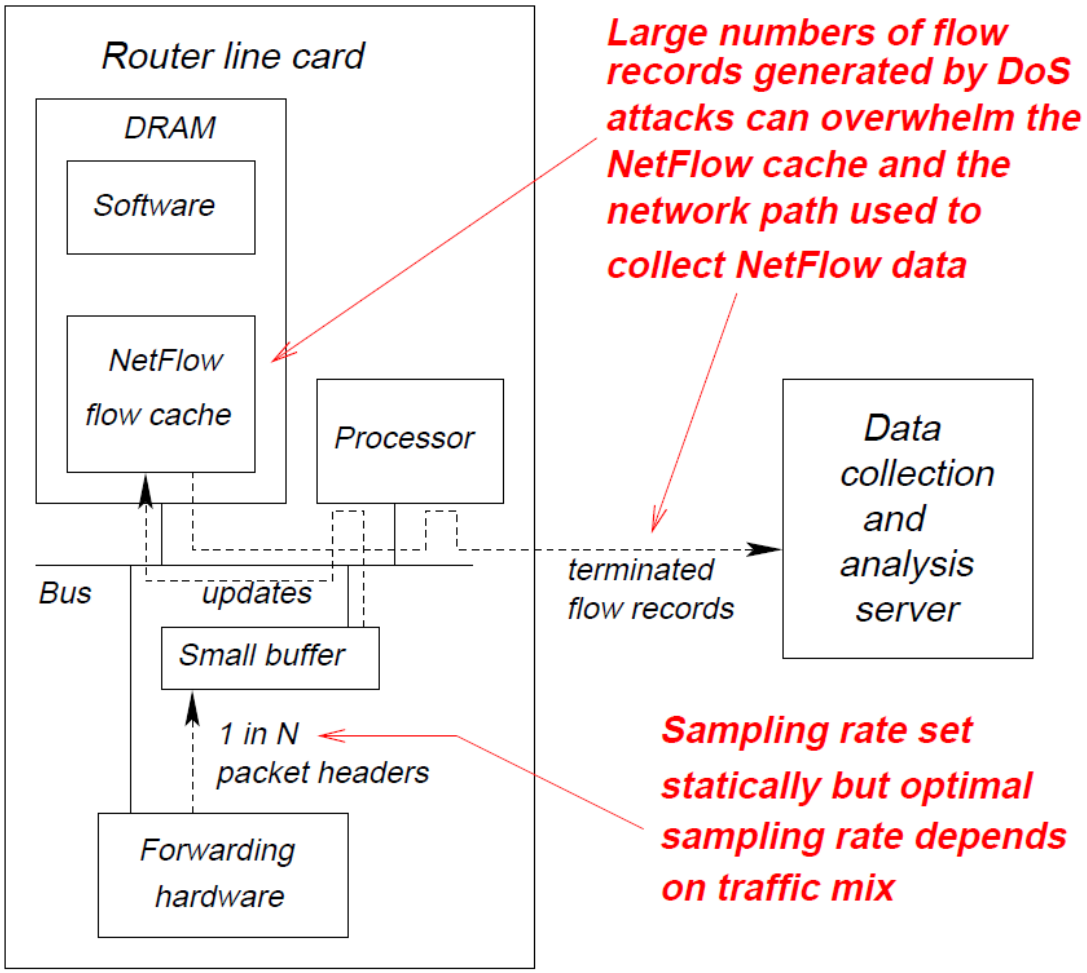
Μία κοινότυπη χρήση του NetFlow της Cisco είναι η εξαγωγή μετρήσεων bytes που να είναι application specific, του συνολικού traffic που περνά μέσα από ένα router του συνολικού δικτύου. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν για ανάλυση η εικονικοποίηση της λειτουργίας του δικτύου. Το SNMP προσφέρει τέτοια δεδομένα συνολικών bytes αλλά μόνο ανά router ή ανά interface, όμως από την άλλη το NetFlow μπορεί να παρέχει αντίστοιχα δεδομένα για ένα ευρύτερο υποσύνολο των routers του δικτύου αλλά και ανά εφαρμογή. (Services et al., 2018)
Το πρόβλημα είναι πως η λεπτομερειακότητα, σε επίπεδο χρόνου, των flows που προέρχονται από το NetFlow είναι πιο χονδροειδής από αυτή που προκύπτει από SNMP. Η διάρκεια του time step στο NetFlow μπορεί να είναι μεγαλύτερη από αυτή του SNMP και ακόμα και αν είναι σημαντικά μικρότερη το NetFlow μπορεί να ξεκινά την ανάλυση από ένα χρονικό κβάντο και να την ολοκληρώνει στο επόμενο.

Κατά συνέπεια για να παίρνονται δεδομένα σε συγκεκριμένα χρονικά διαστήματα από το NetFlow πρέπει να διανεμηθούν τα bytes. Ο χρόνος εξαγωγής του NetFlow καθορίζει το κβάντο χρόνου στο οποίο όλα τα bytes έχουν καταγραφεί. Σε συνδυασμό με τη βολικότητα αυτής της σύμβασης έρχεται και η χρησιμότητα αυτού του γεγονότος για επεξεργασία δεδομένων σε πραγματικό χρόνο. Κάθε φορά μόνο ένα κβάντο χρόνου ανανεώνεται για κάθε νέο flow και ο αριθμός αυτός αυξάνεται συνεχώς μονότονα. Προφανώς υφίσταται ένα εγγενές tradeoff ανάμεσα σε απλοικότητα και ακρίβεια. Συγκεκριμένα flows που έχουν μεγάλη διάρκεια και μεγάλο όγκο διατηρούν και μεγάλο, συνήθως, ποσοστό της συνολικής πληροφορίας του traffic. Τα συγκεκριμένα flows έχουν σε μεγάλο βαθμό πιθανότητα να συνεισφέρουν στο miscalculation των κβάντων χρόνου και αντίστοιχα να δημιουργήσουν κατεξοχήν θέματα με λάθη υπολογισμών στην ανάλυση.

2.9 Θέματα με το NetFlow

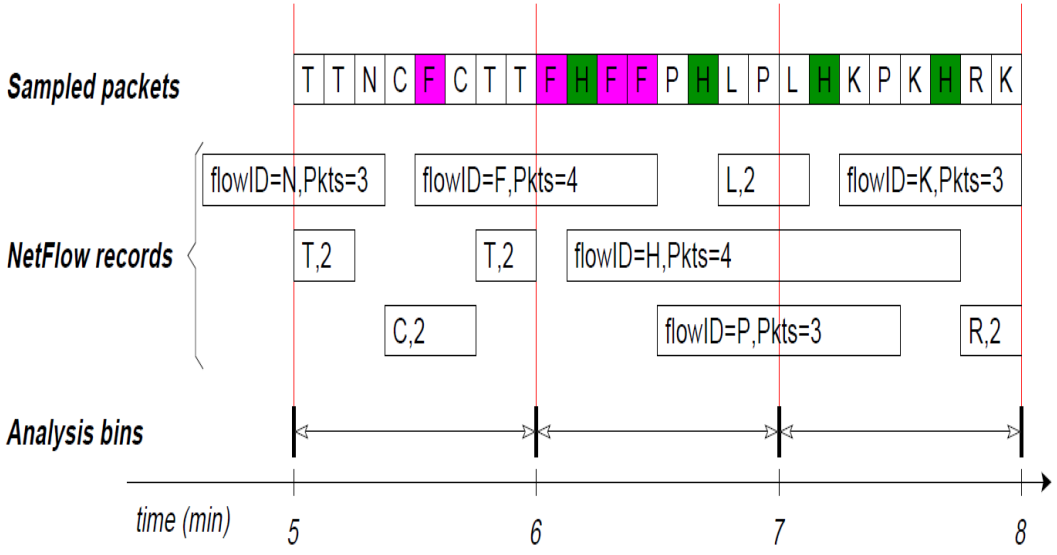
Παρόλο που χρησιμοποιείται ευρέως, το NetFlow παρουσιάζει προβλήματα

- Ο αριθμός των εγγραφών εξαρτάται σημαντικά από το traffic mix.Ένας μεγαλύτερος από τον αναμενόμενο αριθμό αρχείων μπορεί να κατακλείσει τον δρομολογητή και τη διαδρομή δικτύου στο σταθμό συλλογής.Τα σημερινά traffic mixes περιλαμβάνουν συχνά μαζική άρνηση πλημμύρας επιθέσεων υπηρεσίας ή επιθετική σάρωση των θυρών και των IPs. Αυτά δημιουργούν ένα μεγάλο αριθμό "ροών" που αποτελούνται από ένα μόνο μικρό πακέτο.Ο αριθμός των καταχωρήσεων που εξήχθησαν κάτω από αυτές τις συνθήκες είναι πολύ μεγάλος, και η κυκλοφορία που παράγουν μπορεί να προκαλέσει την πτώση των πακέτων από το δίκτυο (Duffield, Lund and Thorup, 2004). Τα λάθη από τα χαμένα πακέτα του NetFlow είναι, σε πολλές περιπτώσεις, μεγαλύτερα από τα λάθη που προκαλούνται από διαφόρων ειδών sampling που λαμβάνει χώρα στο περιβάλλον του κομματιού του συστήματος που έχει να κάνει με τις μετρήσεις.

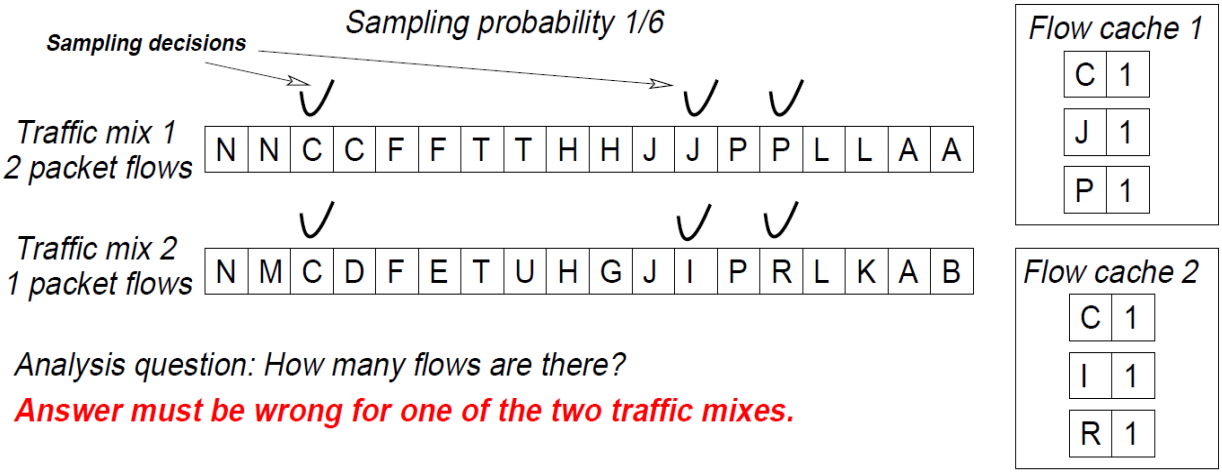


- Ο διαχειριστής του δικτύου αναγκάζεται να αλλάζει εκείνος το ρυθμό δειγματοληψίας. Το να τίθεται ξανά και ξανά ο ρυθμός δειγματοληψίας περιέχει εγγενώς ένα tradeoff. Όσο μικρότερος ρυθμός δειγματοληψίας τίθεται τόσο λιγότερα πακέτα λαμβάνονται. Αυτό μειώνει το φόρτο της μονάδας επεξεργασίας που τρέχει το NetFlow και παράλληλα λύνει και το πρόβλημα της έλλειψης χώρου στη μνήμη του router του δικτύου αλλά και στο δίκτυο που χρησιμοποιείται για την αποστολή των δημιουργούμενων records. Όμως μικρότερος ρυθμός δειγματοληψίας σημαίνει και αυτόματα περισσότερα λάθη και αβεβαιότητα όσον αφορά τις μετρήσεις και την ανάλυση του traffic. Ο ρυθμός δειγματοληψίας αποτελεί το compromise ανάμεσα σε αυτές τις δύο έννοιες λειτουργίας του δικτύου. Όταν το traffic είναι χαμηλά θέλουμε μεγάλο ρυθμό δειγματοληψίας με σκοπό τη μεγαλύτερη ακρίβεια και, αντίστοιχα, όταν το traffic είναι υψηλό και οι περισσότερες επιθέσεις είναι σε εξέλιξη ο ρυθμός δειγματοληψίας πρέπει να είναι χαμηλότερος. Κατά συνέπεια ο στατικός ρυθμός δειγματοληψίας δημιουργεί εγγενώς θέματα στη συνολική λειτουργία του δικτύου.
- Αναντιστοιχία ανάμεσα στα heuristics του τερματισμού του flow και της ανάλυσης. (Feldmann et al., 2000). Η ανάλυση του traffic στηρίζεται σε διαμερισμό του traffic σε χρονικά διαστήματα που ονομάζονται bins. Το χρονικό διάστημα κάθε bin μπορεί να κυμαίνεται από μερικά λεπτά έως μερικές μέρες και συνήθως πρέπει κανείς να εξετάζει πολλά συνεχόμενα bins στη σειρά του ίδιου μεγέθους. (Managing traffic flow to stop DOS attack,

2000)Αν τα timestamps δηλώνουν την αρχή και το τέλος κάθε record που αντιστοιχεί σε κάθε bin τότε όλα τα πακέτα μετρούνται στο πλαίσιο αυτού του bin και το υπολογιστικό βάρος είναι, εν γένει, χαμηλά. Αν όμως το flow ξεκινά μέσα σε ένα bin και τελειώνει μέσα σε άλλο τότε πρέπει να υπολογιστεί ποιο ποσό του traffic μεταφέρθηκε στο επόμενο bin. Κάτι τέτοιο πολυπλοκεύει αρκετά τον υπολογισμό και προκαλεί ανακρίβειες. Μπορεί κάλλιστα ένα flow να καταγραφεί περισσότερες από μία φορές.



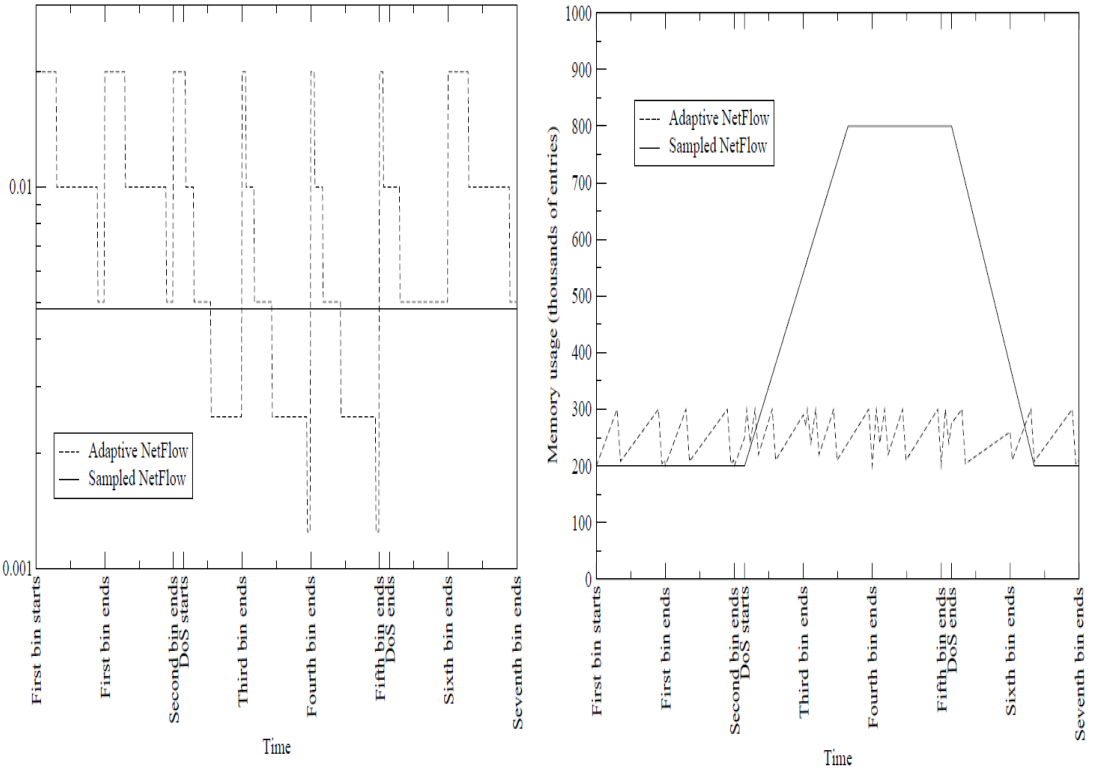
Δεν μπορεί να εκτιμηθεί, εν γένει, ο αριθμός των συνολικών flows. Ακραία αύξηση των flows είναι πολύ ισχυρή ένδειξη επιθέσεων στο δίκτυο όπως Denial of Service (DoS), scans, worms. Αυτές οι επιθέσεις είναι πολύ πιο εύκολο να γίνουν detect αν το συνολικό traffic μετριέται σε flows και όχι σε πακέτα ή bytes. (Managing traffic flow to stop DOS attack, 2000) Χωρίς τη χρήση των πρωτοκόλλων είναι πολύ δύσκολο να ανακτηθεί ο αριθμός των flows από τα δεδομένα που έχουν συλλεγεί (Chaudhuri, Motwani and Narasayya, 1998).



Το πραγματικό πρόβλημα που πρέπει να λυθεί δεν έχει να κάνει με τη μέτρηση των συνολικών flows αλλά με τη μέτρηση των flows εντός κάποιων συγκεκριμένων παραμέτρων, όπως για παράδειγμα τα flows που είναι SMTP, ή τα flows που προέρχονται από κάποια συγκεκριμένη IP που είναι ύποπτη για να παράγει spam. Το να μετρηθούν TCP flows δεν είναι τόσο δύσκολο υπό την έννοια πως υπάρχουν τα αντίστοιχα flags που υποδεικνύουν αρχή και τέλος αλλά η μέτρηση σε άλλα πρωτόκολλα UDP και ICMP είναι εξίσου σημαντικό αλλά σχετικά πιο δύσκολο στο περιβάλλον του NetFlow

2.10 Προσαρμογή του ρυθμού δειγματοληψίας

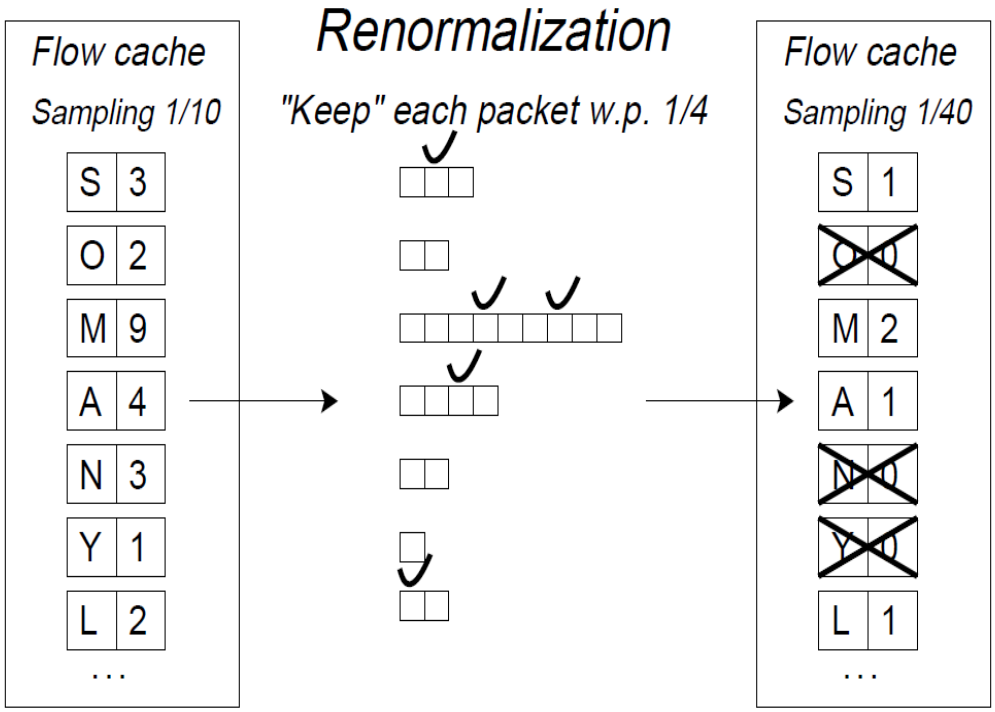
Ο εντοπισμός του βέλτιστου ρυθμού δειγματοληψίας για το NetFlow είναι δύσκολος επειδή υπάρχουν πολλοί αντικρουόμενοι παράγοντες που πρέπει να εξεταστούν. Ένας από αυτούς είναι η αποφυγή της υπερφόρτωσης του επεξεργαστή που εκτελεί
την επεξεργασία NetFlow, είτε πρόκειται για τη CPU του ίδιου του router είτε για τον επεξεργαστή σε μια κάρτα γραμμής.Οι διαχειριστές δικτύου πρέπει να χρησιμοποιούν δοκιμή και σφάλμα για να βρουν το ρυθμό δειγματοληψίας που μπορεί να υποστηρίξει ο δρομολογητής. Αντίθετα υπάρχει η λογική να καθορίζεται ο μέγιστος ρυθμός δειγματοληψίας από τον κατασκευαστή ανάλογα με το πόσος είναι ο μέγιστος ρυθμός που μπορεί να υποστηριχθεί από τον επεξεργαστή σε worst case scenarios. Η τιμή του ρυθμού δειγματοληψίας αρχικοποιείται σε αυτή την τιμή για κάθε bin. Ακόμα κι αν ξεκινήσουμε με ένα ρυθμό δειγματοληψίας αρκετά χαμηλό ώστε να μην συντρίψει τον επεξεργαστή, ο αριθμός των εγγραφών που δημιουργούνται μπορεί υπερβαίνει τη διαθέσιμη μνήμη. Με τα περισσότερα traffic mixes ο αριθμός των εισόδων κατά τις μετρήσεις ενός bin διάρκειας ενός λεπτού εφαρμόζοντας το μέγιστο ρυθμό δειγματοληψίας που ο επεξεργαστής μπορεί να υποστηρίξει ξεπερνά τις δεκάδες χιλιάδες Megabytes μνήμης που η μνήμη τυπικά διατηρεί για να αποθηκεύει τα διάφορα flows. Κατά συνέπεια, αντί να τίθεται ο ρυθμός δειγματοληψίας στατικά μπορεί αυτός να μεταβάλλεται δυναμικά μέχρι να φτάσει σε αρκετά χαμηλό επίπεδο στο οποίο η μνήμη μπορεί να αντέξει τα records από τα καταγεγραμμένα flows.



Η ανάλυση κυκλοφορίας πολλαπλασιάζει την μετρηθείσα κυκλοφορία με το αντίστροφο του ποσοστού δειγματοληψίας για την εκτίμηση της πραγματικής κίνησης, αλλά αν συνεχίσουμε να αλλάζουμε το ρυθμό δειγματοληψίας ενώ τα flow records συνεχίζουν την καταμέτρηση της κυκλοφορίας, είναι δύσκολο να καθοριστεί ποια δειγματοληψία να χρησιμοποιηθεί ως βάση για την αποζημίωση αυτή κατά τη διάρκεια της ανάλυσης. Για να αποφύγουμε αυτό το πρόβλημα, πρέπει να επαναριθμήσουμε υφιστάμενες καταχωρήσεις ροής όταν μειώσουμε το ρυθμό δειγματοληψίας. Η διαδικασία αναμόρφωσης είναι ισοδύναμη με την παύση της λειτουργίας του NetFlow και τη μετάβαση σε όλα τα αρχεία για προσαρμογή των μετρητών πακέτων και bytes για να αντικατοπτρίζουν τις τιμές που θα λάμβαναν αν είχε τεθεί σε ισχύ ο νέος δείκτης δειγματοληψίας από την αρχή του bin. Με αυτόν τον τρόπο χρειάζεται η ανάλυση της κυκλοφορίας να γνωρίζει μόνο το τελικό ποσοστό δειγματοληψίας. Η επαναρύθμιση επίσης καταργεί τις καταχωρήσεις ροής για τις οποίες δεν θα υπήρχαν πακέτα που θα είχαν δειγματοληπτηθεί με το νέο ρυθμό δειγματοληψίας. Με την απελευθέρωση καταχωρήσεων, η ανανέωση του περιεχομένου εξασφαλίζει ότι υπάρχει αρκετή μνήμη για να φιλοξενήσει τα αρχεία των νέων ροών που εμφανίζονται μέχρι το τέλος του εκάστοτε bin.

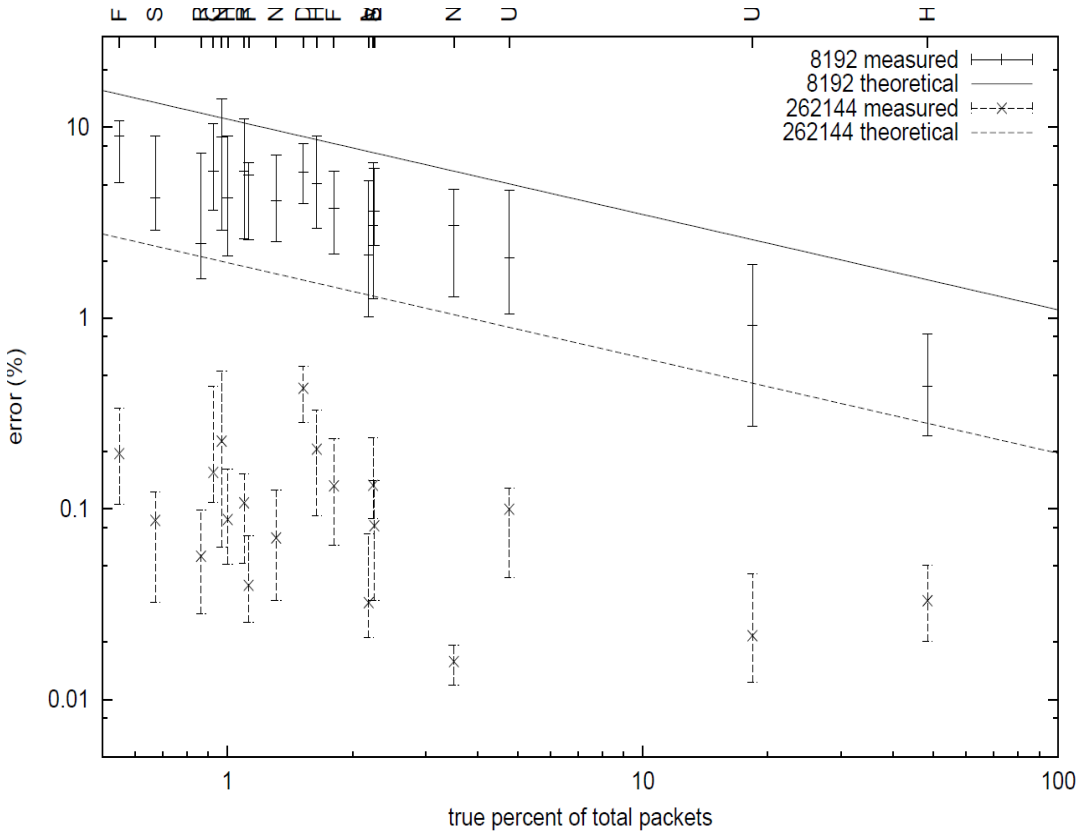
Αν ο πραγματικός ρυθμός δειγματοληψίας είναι δυναμικός, δεν μπορεί να εξασφαλιστεί ότι είναι το ίδιο για όλους τους δρομολογητές, ακόμη και για διαφορετικά χρονικά bins στον ίδιο δρομολογητή.Αυτό δεν προκαλεί προβλήματα συνδυάζοντας δεδομένα από διαφορετικά bins ή από πολλαπλές πηγές. Για παράδειγμα, συνδυάζοντας τα 60 bins ενός λεπτού για να συγκεντρώσουμε την κυκλοφορία
για ολόκληρη την ώρα, ή συνδυάζοντας την κυκλοφορία πολλών δρομολογητών

για να υπολογιστεί το traffic ενός PoP. Γιατί μπορούμε απλά να προσθέσουμε τους μετρητές από τα αρχεία ροής, αφού αυτοί έχουν διαιρεθεί με τους αντίστοιχους ρυθμούς δειγματοληψίας.



Είναι χρήσιμο να ποσοτικοποιηθεί η ακρίβεια των αποτελεσμάτων της ανάλυσης μπορεί να επιτευχθεί με την εφαρμογή ενός σταθερού αριθμού εγγραφών.

Η εκτίμηση πακέτων και bytes σε αυθαίρετα κυκλοφοριακά σύνολα αποτελεί ένα ορισμένο κλάσμα της συνολικής κυκλοφορίας. Σε αυτήν την περίπτωση το λιγότερο που μπορεί να δειχθεί είναι ότι η σχετική τυπική απόκλιση της υπόθεσης εξαρτάται μόνο από τον αριθμό των καταχωρήσεων και όχι από την ταχύτητα του συνδέσμου. Με απλά λόγια αυτό σημαίνει ότι μπορείτε να γίνουν οσεσδήποτε αλλαγές στα δεδομένα με οποιοδήποτε τρόπο, και όσο τα κλάσματα διαίρεσης των δεδομένων δεν είναι μικρότερα από ορισμένο ποσοστό του συνόλου, τα σχετικά σφάλματα των εκτιμήσεων είναι αρκετά μικρά.
Για παράδειγμα, ας πούμε ότι χρησιμοποιούμε ένα ρυθμό δειγματοληψίας που παράγει 100.000 εισροές ροής του δικτύου A και αποτελεί το 10% των συνολικών πακέτων, θα μπορέσουμε να μετρήσουμε την κυκλοφορία του με σχετική τυπική απόκλιση το πολύ 1%. Αν αυτο αντιστοιχεί στο 10% των bytes, ενώ το μέσο μέγεθος πακέτων είναι 400 bytes και το μέγιστο μέγεθος 1500, θα είμαστε σε θέση να μετράμε την κυκλοφορία του με μέση σχετική τυπική απόκλιση το πολύ 1,94%. Όλοι αυτοί οι υπολογισμοί γίνονται χωρίς να χρειάζεται να ληφθεί υπόψη

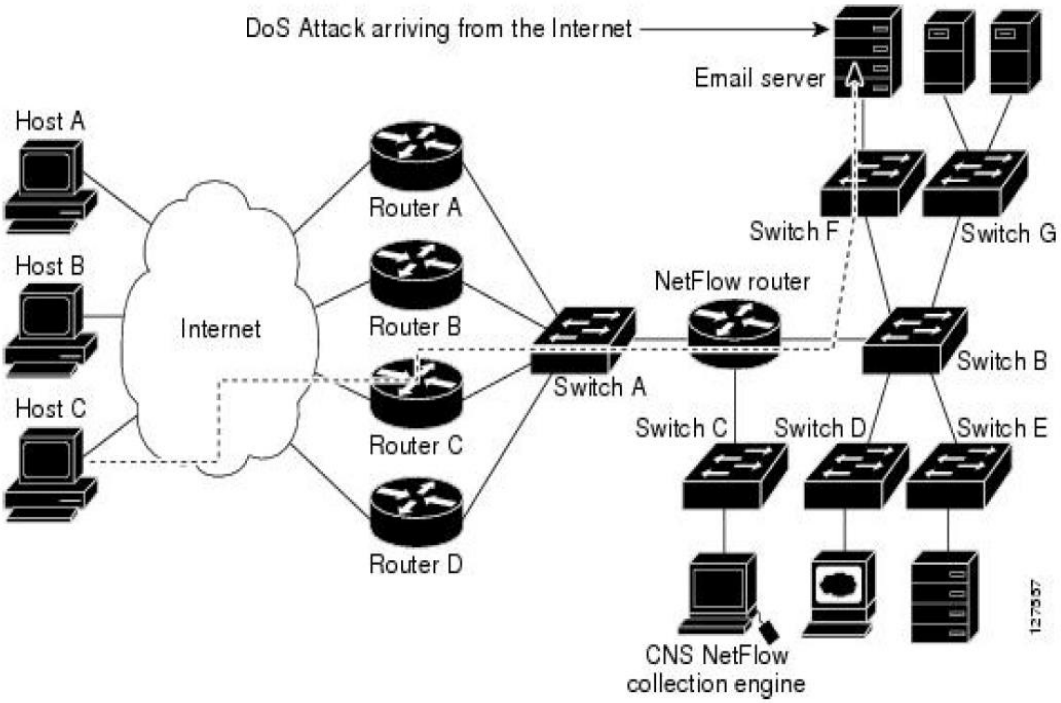


2.10 Εντοπισμός απειλών μέσω του NetFlow

NetFlow Layer 2

Τα πεδία του Layer 2 και του Layer 3, που υποστηρίζονται από το NetFlow Layer 2 feature και το Security Monitoring Exports feature, αυξάνουν το ποσό των πληροφοριών που μπορούν να εξαχθούν από το NetFlow σχετικά με την κίνηση στο δίκτυό .Αυτές οι πληροφορίες για network traffic μπορούν να χρησιμοποιηθούν για εφαρμογές όπως το traffic engineering και το usage-base billing.
Το πεδίο του layer 3, που υποστηρίζεται από το NetFlow Layer 2 και το Security Monitoring feature βελτιώνει τις δυνατότητες του NetFlow για ανίχνευση DoS επιθέσεων. Το IP header του Layer 2 βοηθά στην ανίχνευση του μονοπατιού της DoS επίθεσης μέσα στο εσωτερικό του δικτύου.
Τα Layer 2 και Layer 3 δεν είναι fields κλειδιά. Παρέχουν απλά επιπλέον πληροφορία του traffic σε κάποιο υπάρχον flow. Αλλαγές σε key fields του NetFlow, όπως το source IP address, από ένα πακέτο στο επόμενο συνιστούν τη δημιουργία διαφορετικού flow.
Οι περισσότερες επιθέσεις Denial of Service αποτελούνται από έναν attacker ο οποίος στέλνει τον ίδιο τύπο IP datagram επαναλαμβανόμενα σε μία προσπάθεια να κυριεύσει συστήματα στόχους. Σε τέτοιες περιπτώσεις, το ερχόμενο traffic έχει αρκετά κοινά χαρακτηριστικά, όπως κοινές τιμές στο datagram σε ένα η περισσότερα πεδία που μπορούν να ελεγχθούν από τα NetFlow Layer 2 και Security Monitoring Exports features.
Αυτός που προκαλεί τις επιθέσεις Denial of Service δεν μπορεί να ταυτοποιηθεί εύκολα καθώς η διεύθυνση IP της συσκευής που στέλνει το traffic είναι καλυμμένη.

Ωστόσο μπορεί, σχετικά εύκολα να εντοπιστεί ο router, στον οποίο φτάνει το traffic με χρήση του NetFlow Layer 2 και Security Monitoring Exports feature.
Αν ο router, στον οποίο φτάνει το traffic υποστηρίζει NetFlow μπορούν να χρησιμοποιηθούν τα 2 προαναφερθέντα features για να αναγνωριστεί το interface στο οποίο καταλήγει το traffic.
Ακολουθεί ένα σχεδιάγραμμα κάποιας επίθεσης σε εξέλιξη.



Μία ανάλυση των δεδομένων από το NetFlow Layer 2 και το Security Monitoring Exports feature για το σενάριο επίθεσης που διαδραματίζεται στο σχεδιάγραμμα δείχνει πως η επίθεση Denial of Service φτάνει στο router C, καθώς το MAC address upstream προέρχεται από το interface που διασυνδέει το router C με το switch A. Ταυτόχρονα είναι φανερό ότι δεν υπάρχουν routers ανάμεσα στον target host και στο router του NetFlow, καθώς το MAC address destination του Denial of Service traffic που προωθείται από το router του NetFlow στον e-mail server είναι η MAC address του ίδιου του e-mail server.
Μπορεί να βρεθεί η MAC address που ο Host C χρησιμοποιεί για να στείλει traffic στο router C διατάσσοντας το Layer 2 του Netflow , καθώς επίσης και το Monitoring Exports feature πάνω στο router C. Σε αυτήν την περίπτωση το MAC source address θα είναι από το Host C. Η MAC address του προορισμού θα είναι στο interface του router του NetFlow.
Από τη στιγμή που υπάρχει η γνώση του MAC address του Host C και του interface του router C στον οποίο φτάνει η επίθεση Denial of Service υπάρχει δυνατότητα αντιμετώπισης της επίθεσης διατάσσοντας το router C να μπλοκάρει όλο το traffic προερχόμενο από το Host C. Υπάρχει επίσης η δυνατότητα να απενεργοποιηθεί το interface. Αν ο host C μεταφέρει traffic από άλλους users πρέπει να αναδιαταχθεί το fiware ώστε να μπλοκάρει το traffic από το Host , αλλά παράλληλα να επιτρέπει το traffic από τους άλλους χρήστες να ρέει μέσα από το router C.

NetFlow Layer 3

Τα πέντε πεδία που το Layer 2 του NetFlow και το Security Monitoring Exports feature λαμβάνουν από το IP traffic του Layer 3 είναι τα ακόλουθα:

- Internet Control Message Protocol (ICMP) type and code
- ID field
- Fragment offset
- Packet length field
- Time-to-live field

Ακολουθεί παράδειγμα με κάποια Header Fields από IP Packet

Field	Description
Version	The version of the IP protocol. If this field is set to 4, it is an IPv4 datagram. If this field is set to 6, it is an IPv6 datagram. **Note** IPv4 and IPv6 headers have different structures.
IHL (Internet Header Length)	Internet Header Length is the length of the Internet header in 32-bit word format and thus points to the beginning of the data. **Note** The minimum value for the correct header length is 5.
ToS	Type of service (ToS) provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when a networking device transmits a datagram through a particular network.
Total Length	Total length is the length of the datagram, measured in octets, including Internet header and data.

Field	Description
Identification (ID)	The value in the ID field is entered by the sender. All the fragments of an IP datagram have the same value in the ID field. Subsequent IP datagrams from the same sender will have different values in the ID field. Frequently, a host receives fragmented IP datagrams from several senders concurrently. Also, frequently a host receives multiple IP datagrams from the same sender concurrently. The value in the ID field is used by the destination host to ensure that the fragments of an IP datagram are assigned to the same packet buffer during the IP datagram reassembly process. The unique value in the ID field is used to prevent the receiving host from mixing together IP datagram fragments of different IP datagrams from the same sender during the IP datagram reassembly process.
Flags	A sequence of three bits is used to set and track IP datagram fragmentation parameters. The bits are: • 001—The IP datagram can be fragmented. More fragments of the current IP datagram are in transit. • 000—The IP datagram can be fragmented. This is the last fragment of the current IP datagram. • 010—The IP datagram cannot be fragmented. This is the entire IP datagram.
Fragment Offset	This field indicates where in the datagram this fragment belongs.
TTL (Time-to-Live)	This field indicates the maximum time the datagram is allowed to remain in the Internet system. If this field contains the value 0, then the datagram must be destroyed. This field is modified in Internet header processing. The TTL is measured in units of seconds, but because every module that processes a datagram must decrease the TTL by at least 1 even if it processes the datagram in less than a second, the TTL must be thought of only as an upper bound on the time a datagram can exist. The intention is to discard undeliverable datagrams and bound the maximum datagram lifetime.
Protocol	Indicates the type of transport packet included in the data portion of the IP datagram. Common values are: • 1—ICMP • 6—TCP • 17—UDP
Header checksum	A checksum on the header only. Because some header fields, such as the TTL field, change every time an IP datagram is forwarded, this value is recomputed and verified at each point that the Internet header is processed.

Field	Description
Source IP Address	IP address of the sending station.
Destination IP Address	IP address of the destination station.
Options and Padding	The options and padding may appear in datagrams. If they do appear, they must be implemented by all IP modules (host and gateways). Options and padding are always implemented in any particular datagram; transmissions are not.

Το Layer 2 του NetFlow και το Security Monitoring Exports feature έχουν την ικανότητα να πιάσουν τις τιμές των MAC address και VLAN ID πεδίων από τα διάφορα flows. Συγκεκριμένα:

- Το MAC address πεδίο της πηγής από τα frames που λαμβάνονται από το router του NetFlow
- Το MAC address πεδίο του προορισμού από frames που μεταδίδονται από το router του NetFlow.
- Το πεδίο VLAN ID της πηγής από frames που λαμβάνονται από το router του NetFlow
- Το πεδίο VLAN ID του προορισμού από frames που μεταδίδονται από το router του NetFlow

(Duffield, Lund and Thorup, 2004)

Οι top talkers του NetFlow

Οι λειτουργίες NetFlow Top Talkers μπορούν να χρησιμοποιηθούν για λόγους παρακολούθησης της ασφάλειας ή λογιστικής για κορυφαίους συνομιλητές, καθώς και για την αντιστοίχιση και αναγνώριση σημαντικού traffic στο δίκτυο. Αυτές οι λειτουργίες είναι επίσης χρήσιμες για μια θέση δικτύου όπου η συμβατική διαδικασία εξαγωγής του NetFlow δεν είναι εφικτή. Οι λειτουργίες NetFlow Top Talkers δεν απαιτούν collector που να συγκεντρώνει πληροφορίες σχετικά με τα flows. Αντίθετα, τα δεδομένα του NetFlow εμφανίζονται στο δρομολογητή όταν τα Dynamic NetFlow top talkers CLIs εμφανίζουν την εντολή ip flow top.

Υπάρχουν δύο παρόμοιες λειτουργίες του NetFlow που χρησιμοποιούνται για έλεγχο του σημαντικότερου όγκου traffic μέσα στο δίκτυο:

NetFlow Dynamic Top Talkers CLI

Το συγκεκριμένο feature χρησιμοποιείται για να παρθεί μία εικόνα για το περισσότερο όγκο traffic στο εσωτερικό του δικτύου. Παρουσιάζει μία γενική εικόνα

του traffic συγκεντρώνοντας όλα τα flows στην cache βασιζόμενο στο πεδίο που έχει επιλεχθεί σε κάθε περίπτωση.
Το συγκεκριμένο feature δεν απαιτεί αλλαγές και διαφοροποιήσεις στη διάταξη του router. Η εντολή show ip flow top είναι η μόνη εντολή που είναι απαραίτητη για τη χρήση αυτού του feature. Αντίστοιχα όλες οι επιλογές μπορούν να παρθούν από τη χρήση αυτής της εντολής.
Όλη η πληροφορία που είναι απαραίτητη για τη χρήση τη χρήση του NetFlow Dynamic Top Talkers CLI οφείλει να είναι αποθηκευμένη στην cache. Για παράδειγμα, αν χρειάζεται να αναγνωριστεί το MAC address σε κάποια flows πρέπει αντίστοιχα να διαταχθεί η εντολή ip flow-capture mac-addresses έτσι ώστε να πιάνει τις τιμές από τα πεδία MAC address πρώτα από την κανονική ροή του traffic.

Τα flows των συνολικών top talkers μπορούν να ταξινομηθούν με κάποιο από τα ακόλουθα κριτήρια:

- Το συνολικό πεδίο των display data
- Ο αριθμός των bytes στα display data
- Ο αριθμός των flows στα display data
- Ο αριθμός των πακέτων στα display data

Μπορούν επίσης να γίνει διάταξη των flows των top talkers σε αύξουσα ή φθίνουσα σειρά.
(Feldmann et al., 2000)

2.11 Δειγματοληψία του NetFlow traffic

Το NetFlow παρέχει στατιστικά στοιχεία κυκλοφορίας με μεγάλη περιεκτικότητα ανά ροή σε δρομολογητή Cisco.Μια ροή είναι ένα μονοδιάστατο ρεύμα πακέτων που φτάνουν στο δρομολογητή στην ίδια υποπεριοχή, έχουν τις ίδιες διευθύνσεις IP πηγής και προορισμού, το ίδιο πρωτόκολλο Layer 4, τις ίδιες TCP / UDP θύρες προέλευσης και προορισμού και το ίδιο Type of Service (ToS) byte στην IP κεφαλίδα.
Ο δρομολογητής συσσωρεύει στατιστικά στοιχεία από το NetFlow σε μια προσωρινή μνήμη NetFlow cache και μπορεί να τα εξάγει σε εξωτερική συσκευή (όπως το Cisco Networking Services (CNS) NetFlow Collection Engine) για περαιτέρω επεξεργασία.
Το πλήρες NetFlow αντιπροσωπεύει το σύνολο του traffic που εισέρχεται στην υποπεριοχή στην οποία είναι ενεργοποιημένο. Αλλά σε μερικές περιπτώσεις, μπορεί να συγκεντρωθούν δεδομένα NetFlow μόνο σε ένα υποσύνολο αυτού του συνολικού traffic. Το στοιχείο Random Sampled NetFlow, όπως επίσης και το στοιχείο NetFlow Input Filters παρέχουν τρόπους να μειωθεί το εισερχόμενο traffic, ώστε να υπάρχει μόνο κομμάτι του συνολικού traffic που παρουσιάζει κάποιο ενδιαφέρον για επεξεργασία στο εσωτερικό του NetFlow. Το Random Sampled NetFlow παρέχει πληροφορίες του NetFlow για κάποιο υποσύνολο του συνολικού traffic που φθάνει σε κάποιο router της Cisco με την εξής μεθοδολογία. Επιλέγει ένα πακέτο τυχαία για κάθε n συνεχόμενα πακέτα που φτάνουν στο router. Το NetFlow Input Filters στοιχείο παρέχει τη δυνατότητα να συλλεγούν δεδομένα του NetFlow σε ένα υποσύνολο του traffic τα χαρακτηριστικά του οποίου ορίζονται ρητά από το χρήστη.

Ακολουθεί πίνακας με μία σύγκριση του NetFlow Input Filters και του Sampled NetFlow

Comparison Category	NetFlow Input Filters Feature	Random Sampled NetFlow Feature
Brief description	This feature enables you to gather NetFlow data on only a specific subset of traffic. You do this by creating filters to select flows for NetFlow processing. For example, you can select flows from a specific group of hosts. This feature also lets you select various sampling rates for selected flows.	This feature provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of n sequential packets (n is a user-configurable parameter). Packets are sampled as they arrive (before any NetFlow cache entries are made for those packets).
Main uses	You can use this feature for class-based traffic analysis and monitoring on-network or off-network traffic. This feature is also useful if you have too much traffic and you want to limit the traffic that is analyzed.	You can use this feature for traffic engineering, capacity planning, and applications where full NetFlow is not needed for an accurate view of network traffic. This feature is also useful if you have too much traffic and you want to limit the traffic that is analyzed.
Export format support	This feature is supported in the Version 5 and Version 9 NetFlow export formats.	This feature is supported in the Version 5 and Version 9 NetFlow export formats.
Cisco IOS release support	12.3(4)T.	12.3(2)T, 12.2(18)S, and 12.0(26)S.

Comparison Category	NetFlow Input Filters Feature	Random Sampled NetFlow Feature
Subinterface support	You can configure NetFlow Input Filters per subinterface as well as per physical interface. You can select more than one filter per subinterface and have all of the filters run simultaneously.	You can configure the Random Sampled NetFlow feature per subinterface as well as per physical interface. You can not run Full NetFlow and Random Sampled NetFlow concurrently on the same subinterface. You must disable full NetFlow on the subinterface before Random Sampled NetFlow will take effect. Traffic is collected only on the subinterfaces on which Random Sampled NetFlow is configured. As with full NetFlow, enabling Random Sampled NetFlow on a physical interface does not enable Random Sampled NetFlow on subinterfaces automatically--you must explicitly configure it on the subinterfaces.
Memory impact	This feature requires no additional memory. It allows you to use a smaller NetFlow cache than full NetFlow, because it significantly reduces the number of flows. This feature requires an insignificant amount of memory for each configured NetFlow filter.	This feature can create a smaller NetFlow cache than full NetFlow if by reducing the number of packets being analyzed the numbers of flows in the cache is also reduced. This feature requires an insignificant amount of memory for each configured NetFlow sampler.
Performance impact	Accounting of classified traffic saves router resources by reducing the number of flows being processed and exported. The amount of bandwidth saved depends on the usage and the class-map criteria. However, performance might degrade depending on the number and complexity of class maps configured in a policy.	Statistical traffic sampling substantially reduces consumption of router resources (especially CPU resources) while providing valuable NetFlow data. This feature substantially reduces the impact of NetFlow data export on interface traffic. For example, a sampling rate of 1 out of 100 packets reduces the export of NetFlow data by about 99% percent.

2.12 Flow Classification

Το Classification των πακέτων μπορεί να γίνει με το NetFlow Input Filters Feature με βάσει οποιοδήποτε από τα ακόλουθα: διευθύνσεις IP της πηγής και του προορισμού, Πρωτόκολλο επιπέδου 4 και αριθμούς των ports, interface, MAC address, IP Precedence, DSCP τιμή, πληροφορίες του Layer 2 και πληροφορίες Network-Based Application Recognition (NBAR). Τα πακέτα κατηγοριοποιούνται σύμφωνα με τα παραπάνω κριτήρια και πραγματοποιείται μία λογιστική ανάλυση πάνω σε αυτά τα flows
(Managing traffic flow to stop DOS attack, 2000)
Ο μηχανισμός φιλτραρίσματος χρησιμοποιεί τη διαλειτουργική μονάδα γραμμής εντολών QoS (MQC) για να ταξινομεί τις ροές. Μπορούν να δημιουργηθούν πολλαπλά φίλτρα με ταιριαστές δειγματοληπτικές ετικέτες. Για παράδειγμα, μπορεί να υποδιαιρεθεί το traffic σε πολλαπλές κατηγορίες ανάλογα με τις τιμές των Type of service (ToS) ή τα προθέματα προορισμού. Για κάθε κατηγορία μπορεί να διαταχθεί το sampling σε διαφορετικό ρυθμό χρησιμοποιώντας μεγαλύτερους ρυθμούς για μεγαλύτερη προτεραιότητα κατηγοριών του traffic και μικρότερους ρυθμούς για traffic χαμηλότερης προτεραιότητας.
Το MQC έχει πολλές πολιτικές όπως το ρυθμό εύρους ζώνης και τη διαχείριση ουρών. Αυτές οι πολιτικές εφαρμόζονται μόνο αν ένα πακέτο ταιριάζει με ένα κριτήριο σε ένα χάρτη κλάσης που εφαρμόζεται στην υποεπιφάνεια. Ένας χάρτης τάξης περιέχει ένα σύνολο των ρητρών αντιστοίχισης και οδηγίες για τον τρόπο αξιολόγησης των ρητρών και λειτουργεί ως φίλτρο για τις πολιτικές, οι οποίες εφαρμόζονται μόνο εάν το περιεχόμενο ενός πακέτου πληροί τη ρήτρα αντιστοίχισης. Τα χαρακτηριστικά φίλτρων εισόδου NetFlow προσθέτουν το NetFlow με την υποδομή MQC, πράγμα που σημαίνει ότι η λογιστική ροής γίνεται σε ένα πακέτο μόνο αν ικανοποιεί τις ρήτρες αντιστοίχισης.

Οι δύο τύποι φίλτρων είναι οι εξής

- ACL-based flow-mask filters
- Πεδία του φίλτρου όπως, IP διεύθυνση προέλευσης, IP διεύθυνση προορισμού, πύλη εφαρμογής προέλευσης, πύλη εφαρμογής προορισμού, TCP flags

Η λειτουργία δειγματοληψίας χρησιμοποιεί έναν αλγόριθμο που επιλέγει ένα υποσύνολο επισκεψιμότητας για την επεξεργασία NetFlow. Στην τυχαία λειτουργία δειγματοληψίας που χρησιμοποιεί η λειτουργία τυχαίας δειγματοληψίας NetFlow, τα εισερχόμενα πακέτα είναι τυχαία και επιλέγεται κατά μέσο όρο ένα από κάθε n διαδοχικά πακέτα . Για παράδειγμα, εάν ρυθμίζεται ο ρυθμός δειγματοληψίας σε 1 από τα 100 πακέτα, τότε το NetFlow μπορεί να δοκιμάσει το 5ο πακέτο και στη συνέχεια το 120ο, 230ο, 302ο, και ούτω καθεξής. Αυτή η διαμόρφωση δείγματος παρέχει δεδομένα NetFlow στο 1% της συνολικής επισκεψιμότητας. Η τιμή n είναι μια παράμετρος που μπορεί να διαμορφωθεί από 1 έως 65535 πακέτα
(Feldmann et al., 2000)

3. Δειγματοληψία

3.1 Εκμετάλλευση μετρήσεων από packet sampler με σκοπό το χαρακτηρισμό και την κατηγοριοποίηση του traffic

Η χρήση του packet sampler για μετρήσεις που αφορούν το traffic έχει καταστεί απαραίτητη για τους χειριστές δικτύων ώστε να διαχειριστούν τον τεράστιο όγκο δεδομένων που μεταφέρονται μέσω των σημερινών δικτύων, με τη συνδρομή των ολοένα και ταχύτερων τεχνολογιών μετάδοσης της πληροφορίας. Κατά συνέπεια πολλές λειτουργίες του δικτύου πρέπει να εκπαιδευτούν ώστε να διαχειρίζονται τέτοια δεδομένα, πιο διαθέσιμα από ότι παλιά, αλλά λιγότερο, ίσως, πλούσια σε πληροφορία.
Ακόμα και αν η επιτυχία του Internet, ως παγκόσμια πλατφόρμα επικοινωνίας οφείλεται σε τεράστιο βαθμό στην αποκεντροποιημένη και ανοικτή αρχιτεκτονική του, οι αλλαγές στις τεχνολογίες επικοινωνίας έχουν παίξει αντίστοιχα μεγάλο ρόλο υποστηρίζοντας νέες γενιές από εφαρμογές κατεξοχήν bandwidth-intensive. Ως συνέπεια αυτής της συνεχώς αυξανόμενης ταχύτητας μετάδοσης πληροφοριών, οι χειριστές των δικτύων πρέπει να αντιμετωπίσουν συνεχώς αυξανόμενο traffic, και επομένως, τεράστιο αριθμό από μετρήσεις των οποίων η διαδικασία συλλογής, αποθήκευσης και επεξεργασίας αποτελεί σημαντική πρόκληση. Επομένως η διαδικασία του packet sampling είναι αρκετά σημαντική για την αποτελεσματική παθητική συλλογή μετρήσεων του δικτύου, ειδικά στον κορμό του δικτύου, με σκοπό τη μείωση του όγκου των δεδομένων σε μέγεθος σχετικώς διαχειρίσιμο. Φυσικώς μία τέτοια μείωση έρχεται με το κόστος της γενικής απώλειας ακρίβειας των δεδομένων και πολλές ερευνητικές εργασίες επικεντρώνονται στο impact των διαφόρων μεθοδολογιών sampling πάνω στις μετρήσεις του traffic (Cassel and Amer, 1988), (Ribeiro B, Towsley D, Ye T, Bolot ,2006), (Kumar A, Xu J. Sketch,06)
στην επίδοση διαφόρων λειτουργιών του δικτύου σε σχέση με τις μετρήσεις που λαμβάνονται, όπως το monitoring, το SLA compliance, το anomaly detection και το traffic classification
Ανάμεσα στις πλείστες εφαρμογές των μετρήσεων που αφορούν το traffic, το traffic classification έχει λάβει πρόσφατα σημαντική προσοχή από την επιστημονική κοινότητα. Το να μπορείς να αναγνωρίζεις ορθώς την εφαρμογή που σχετίζεται με συγκεκριμένα traffic flows είναι αντικειμενικά ζωτικής σημασίας, με την έννοια πως αυτή η γνώση είναι απαραίτητη για ένα μεγάλο αριθμό από tasks διαχείρισης, όπως για παράδειγμα η διαφοροποιημένη μεταχείριση για quality of service είτε service level agreements που επιτάσσουν τη συλλογή μόνο των πιο σημαντικών. (Carela-Espaol V, Barlet-Ros P, Cabellos-Aparicio A, Sol-Pareta,2005) (Zander S, Nguyen T, Armitage G, 2005) (Finamore A, Mellia M, Meo M, Rossi D. Kiss,2010)

Αναπόφευκτα, από τη στιγμή που τα δεδομένα ως προιόν δειγματοληψίας είναι τα μόνα δεδομένα διαθέσιμα στην πλειονότητα των real life εφαρμογών, η ερώτηση που τίθεται είναι αν και κατά πόσον το classification είναι ακόμα εφικτό με τόσο μειωμένη σε μέγεθος πληροφορία
Γενικώς το packet sampling δεν είναι ένα concept τόσο καινούριο σε σύλληψη. Η κατηγοριοποίηση των μεθόδων packet sampling αποτελεί standardized framework ως IETF RFC (Zseby T, Molina M, Duffield N, Niccolini S, Raspall,2009). Μία πρώτη διαφοροποίηση μπορεί να γίνει με βάση του scheme το οποίο μπορεί να είναι deterministic, random ή content-based. Στη συνέχεια μπορούμε να διαφοροποιήσουμε τις μεθόδους sampling το τι επιλέγεται ως selection trigger, που αφορά τον αριθμό των πακέτων και το ποσό του χρόνου ανάμεσα σε 2 ξεχωριστά γεγονότα δειγματοληψίας. Όσον αφορά το selection scheme εκτεταμένη έρευνα έχει δείξει πως οι στατιστικές ιδιότητες της μεθόδου του random sampling, ιδιαίτερα σε context stratified declination καθιστούν αυτή τη μέθοδο πιο ισχυρή και σταθερή όσον αφορά τον κίνδυνο επιθέσεων και εισχώρησης(Paxson V.2006). Από την άλλη, πρόσφατες έρευνες καταδεικνύουν πως το statistical multiplexing του traffic μπορεί να έχει παρόμοιο αποτέλεσμα με την εφαρμογή της μεθοδολογίας του random selection, ειδικά αν ληφθεί υπόψη ο υπολογισμός του traffic volume. Όσον αφορά το πιο αποτελεσματικό selection trigger υπάρχει σχετική ομοφωνία της επιστημονικής κοινότητας Οι time-based triggers είναι λιγότερο σταθεροί από αυτούς που είναι packet-based, γιατί υποφέρουν από την, εν γένει, απρόβλεπτη φύση του traffic του εκάστοτε δικτύου. Κάποιες ερευνητικές δουλειές έχουν προτείνει πιο εκλεπτυσμένες μεθόδους που βοηθούν στον υπολογισμό συγκεκριμένων features του traffic, όπως για παράδειγμα trajectory sampling for spatial properties (Duffield NG, Grossglauser, 2000) ή scetches for flow-size(Kumar A, Xu J. Sketch,06) . Άλλες δουλειές έχουν προτείνει adaptive sampling rate όσον αφορά το traffic load για να μειώσουν το estimation error από συγκεκριμένα metrics του traffic.
Εκτός από τη διερεύνηση των ιδιοτήτων του sampling και της επιρροής που έχει σε traffic measurements, ερευνητές έχουν μελετήσει τις πιθανές εφαρμογές των δειγματοληπτειμμένων πληροφοριών για διάφορα administration tasks του δικτύου, όπως network management, SLA verification, anomaly detection και traffic classification. Αξίζει να λεχθεί πως αυτού του είδους η εκτίμηση δεν μπορεί εύκολα να διαχωρίσει τα αποτελέσματα του packet sampling από τα εγγενή ζητήματα απόδοσης της ίδιας της εφαρμογής. (Jiang H, Moore AW, Ge Z, Jin S, Wang J. 2007)

3.2 Πολιτικές sampling

1. Systematic sampling: Τα πακέτα δειγματοληπτούνται με ντετερμινιστικό τρόπο επιλέγοντας 1 από κ πακέτα.
2. Random sampling: Τα πακέτα δειγματοληπτούνται τυχαία, συγκεκριμένα κάθε πακέτο δειγματοληπτείται ξεχωριστά με ρυθμό ρ=1/κ. Εφόσον η όλη διαδικασία είναι εντελώς τυχαία, τα πακέτα μπορεί να δειγματοληπτειθούν σε σειρά ή μπορεί να υπάρχουν συνεχόμενα μη δειγματοληπτημένα πακέτα
3. Stratified sampling: κ συνεχόμενα πακέτα μαζεύονται σε ένα group, στο οποίο ένα πακέτο δειγματοληπτείται τυχαία.

4. Systematic SYN sampling: είναι η υπέρθεση 2 ξεχωριστών μεθόδων. (i) μία systematic sampling που επιλέγει κάθε κ-ιοστό πακέτο.(ii)μία διαδικασία που επιλέγει όλα τα TCP πακέτα που κατέχουν SYN flag ενεργή.

Οι πρώτες 3 μέθοδοι sampling ανήκουν στην οικογένεια των αλγορίθμων που είναι unbiased, που αποτελούν την πιο απλή κατηγορία αλγορίθμων, εν γένει, και δεν έχουν καμία γνώση σχετική με κάποια ιδιότητα του traffic. Αυτοί οι αλγόριθμοι είναι lightweight, εφαρμόζονται κυρίως σε εξοπλισμό δικτύου και για αυτό υπάρχει ιδιαίτερο ενδιαφερον για την απόδοσή τους. Αντίθετα ο τελευταίος αλγόριθμος ανήκει στην κατηγορία smart sampling, καθώς εισάγεται κάποιο intelligence στην επιλογή κατάλληλου πακέτου, δηλαδή του πακέτου που περιέχει την καταλληλότερη πληροφορία. Δεν υπάρχει εγγενές όριο στο ποσό του intelligence που μπορεί να εφαρμοστεί σε μία τέτοια μέθοδο sampling και, κατά συνέπεια έχουν προταθεί πολλές διαφορετικές μέθοδοι sampling που να είναι smart. Ωστόσο, πρέπει συνεχώς να έχει κανείς στο μυαλό του πως ο σκοπός του sampling είναι να μειώσει το computational load, κατά συνέπεια υπάρχει η βούληση να κρατιέται το sampling policy όσο το δυνατόν απλούστερο. Σε μεγάλο βαθμό το systematic NYC sampling αποτελεί ένα καλό tradeoff, ειδικά όσον αφορά το traffic classification. Από τη μία βελτιώνεται ο υπολογισμός κάποιων συνολικών traffic counters, όπως για παράδειγμα το συνολικό flow length που γενικά διαδραματίζουν βασικό ρόλο στο traffic classification. Επίσης διασφαλίζει πως τουλάχιστον ένα πακέτο από κάθε flow θα δειγματοληπτηθεί ή αλλιώς πως κάθε πακέτο θα ληφθεί, σε κάποιο βαθμό υπόψη. Από την άλλη πλευρά η υπολογιστική πολυπλοκότητα είναι πολύ χαμηλά, καθώς αυτός ο αλγόριθμος επιτάσσει απλά έναν μετρητή και κάποιο βασικό έλεγχο του header κάθε πακέτου, όπως επίσης και κάποιο fixed offset για το αν θα δειγματοληπτηθεί ή όχι κάποιο πακέτο.

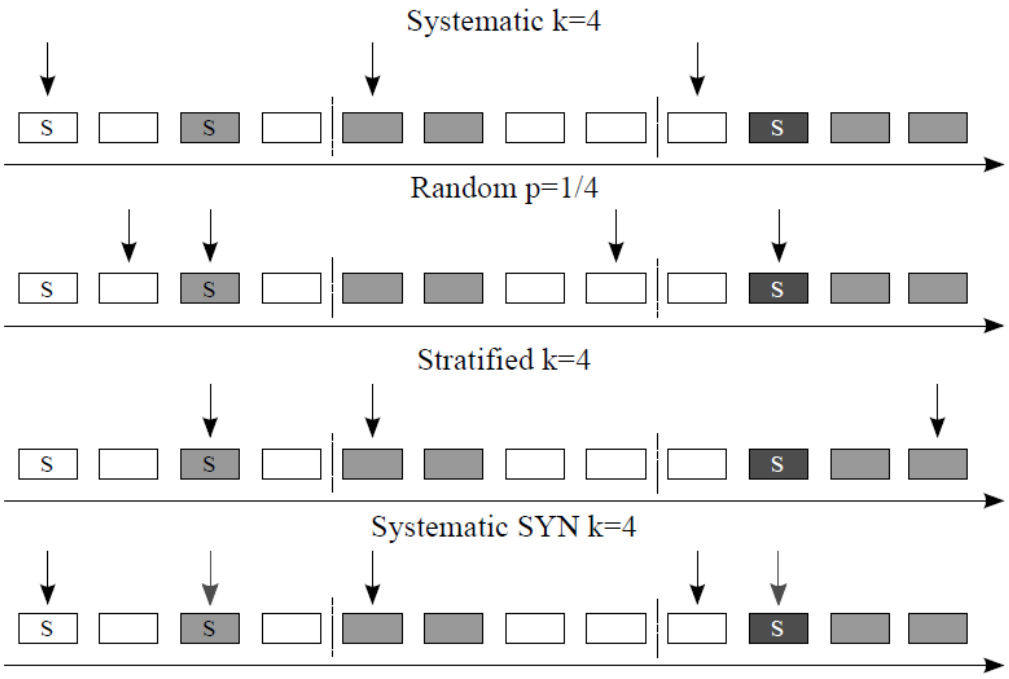


Figure 1. Illustration of sampling policies.

3.3 Χρήση μετρήσεων από adaptive packet sampling με σκοπό την επίτευξη traffic classification σε multimedia

Με τον τεράστιο όγκο multimedia δεδομένων που αποστέλλονται σήμερα μέσω Internet η χρήση του packet sampling για traffic measurements χρησιμοποιείται ευρέως από χειριστές δικτύων. Η τεχνική adaptive packet sampling από την οπτική του classification έχει ως κυριότερη αρχή του sampling method να επιλεγούν όσο το δυνατόν περισσότερα πακέτα με όσο το δυνατόν χαμηλότερο occurrence rate βασιζόμενη σε 2 χρήσιμα features του multimedia traffic. Το packet size και το Packet Inter Arrival Time.
Το Internet έχει αποδείξει μία εξαιρετική ικανότητα να προσαρμόζεται σε νέα services. Η εξέλιξη του Internet έχει προκαλέσει τη δημιουργία διαφόρων εφαρμογών multimedia και η κινητικότητα των χρηστών, πιθανότατα, θα μεταφράζεται σε κινητικότητα των services. Η έκρηξη των υπηρεσιών που σχετίζονται με multimedia αναγκάζει τον επαναπροσδιορισμό του connotation όλων των δεδομένων που προέρχονται από traffic.Παράλληλα η ευρεία χρησιμοποίηση των application layer protocols μεταφράζεται άμεσα σε μεγαλύτερη ποικιλότητα των δεδομένων που προέρχονται από traffic που μετακινείται μέσω Internet.
Σαν αποτέλεσμα της τεράστιας εξέλιξης των multimedia services, καθώς και της αυξημένης ταχύτητας μετάδοσης οι διάφορες εταιρείες και οι Internet Service Providers (ISPs) πρέπει να αντιμετωπίσουν το συνεχώς αυξανόμενο traffic και τον τεράστιο αριθμό μετρήσεων, καθώς επίσης και το πως θα συγκεντρώσουν και θα επεξεργαστούν τον τεράστιο αριθμό από δεδομένα προερχόμενα από traffic.
Ανάμεσα στις διάφορες εφαρμογές μετρήσεων προερχόμενων από traffic, το traffic classification προσελκύει ιδιαίτερο ενδιαφέρον. Η πιο παραδοσιακή προσέγγιση για traffic classification βασίζεται σε well-known transport layer port αριθμούς, όμως

πλέον αποτελεί μία λιγότερο έμπιστη μέθοδο, καθώς οι πιο σύγχρονες εφαρμογές του Internet να αποκρύπτουν τα identifications με τη χρήση random ports
(J. Fan, D. Wu, A. Nucci, R. Keralapura, and L. Gao, 2009)

.
Γενικώς υπάρχουν 3 βασικότερες μεθοδολογίες για classification. Η πρώτη είναι η DPI (Deep Packet Inspection) η οποία αναζητά γνωστές signatures στα payloads των πακέτων. Η δεύτερη κατηγορία μεθόδων είναι host behaviour based που ψάχνει τα κρυμμένα connection patterns μεταξύ των hosts. Η τελευταία γενική κατηγορία μεθόδων για traffic classification είναι βασισμένη σε τεχνικές machine learning με χρήση στατιστικών χαρακτηριστικών του traffic όπως το packet size, h διάρκεια του flow.
Οι DPI (Deep Packet inspection) μέθοδοι παρέχουν συνήθως καλό performance αλλά δυσκολεύονται ιδιαίτερα όταν πρόκειται για εφαρμογές που είναι κρυπτογραφημένες και υπόκεινται σε κυβερνητικούς κανονισμούς.
Η απόδοση των μεθόδων που είναι host behaviour based εξαρτάται σε μεγάλο βαθμό από τοπολογικές τοποθεσίες και traffic mixes, αλλά οι συγκεκριμένες μέθοδοι δεν έχουν ιδιαίτερη αξιοπιστία όσον αφορά την ταυτοποίηση του τύπου της εφαρμογής για μονά πακέτα (H. Kim, K. Claffy, M. Fomenkov, D. Barman, M. Faloutsos, and K. Lee,
2008)

.
Η έρευνα σε traffic classification προσανατολίζεται σε αναγνώριση εφαρμογών του δικτύου αποκτώντας γνώση εσωτερικών μοτίβων σε εξωτερικά παρατηρούμενα χαρακτηριστικά των πακέτων και των flows.
(M. Canini, W. Li, M. Zadnik, and A. W. Moore,2009)

Επομένως στατιστικές μέθοδοι που είναι βασισμένες σε machine learning θεωρούνται αρκετά ελπιδοφόρες και σταθερές όσον αφορά την απόδοση τους σε σχέση με το encryption, το privacy και το protocol obfuscation.
Παρόλα αυτά τα sampled data τείνουν να γίνουν το μόνο είδος data διαθέσιμα από multimedia traffic. Η ερώτηση που εγείρεται είναι αν το να επιτευχθεί classification είναι ακόμα εφικτό μετά την απώλεια πληροφορίας λόγω του sampling. Η έρευνα με στόχο την εξέταση του κατά πόσο το traffic sampling επηρεάζει το traffic classification υποδεικνύει πως η απόδοση του classification μειώνεται σημαντικά. Κατά συνέπεια υπάρχει άμεση ανάγκη να επιλεγούν σε κάθε περίπτωση τα πακέτα που περιέχουν την πιο χρήσιμη πληροφορία.

3.4 Packet-sampling ή Flow-sampling

Οι ερευνητές έχουν κατηγοριοποιήσει τις μεθόδους sampling σε 2 βασικές κατηγορίες : το packet-sampling και το flow-sampling. Οι μέθοδοι packet-sampling δουλεύουν στο επίπεδο των πακέτων του δικτύου (K. Bartos and M. Rehak,2002) και κάθε πακέτο επιλέγεται με μία μεθοδολογία που μπορεί να είναι είτε ντετερμινιστική είτε τυχαία. Σε σχέση με το flow-sampling, το packet-sampling παρέχει το βασικό πλεονέκτημα ότι έχει μειωμένες απαιτήσεις σε κατανάλωση

μνήμης και CPU power στους routers, καθώς επίσης έχει δυνατότητα να κάνει monitor μεγαλύτερες ταχύτητες σε επίπεδο δικτύου. Όσον αφορά το flow sampling, το traffic συγκεντρώνεται σε flows και η δειγματοληψία διεξάγεται πάνω σε όλο το flow και όχι σε συγκεκριμένα πακέτα. Η συνολική απόδοση του flow sampling είναι καλύτερη από αυτή του packet sampling αλλά οι απαιτήσεις σε μνήμη και υπολογιστική δύναμη της CPU καθιστούν αυτές τις μεθόδους απαγορευτικές για τα περισσότερα είδη εφαρμογών.(N. Hohn and D. Veitch, 2006)

3.5 Προβλήματα που προκαλούνται από μεθόδους packet-sampling

Παρότι το packet-sampling είναι, εν γένει, ευκολότερο στην εφαρμογή του εισήγαγε κάποια θεμελιώδη θέματα. Πρώτα από όλα ο ρυθμός των πακέτων σε κάθε flow αλλάζει σημαντικά κατά τη διάρκεια μεταφοράς του ίδιου του flow, κάτι το οποίο καθιστά αρκετά δύσκολη την ταυτοποίηση των mice flows από τα elephant flows. Επίσης ο χρόνος άφιξης ενός flow είναι δυναμικός. Ένας από τους λόγους που συμβαίνει κάτι τέτοιο είναι πως υπάρχει transmission delay λόγω του congestion στην ουρά του router και τα χρονομεταβλητά κανάλια των transmission paths. Τελικώς η ίδια η διάρκεια του flow μεταβάλλεται συνεχώς και ένα συγκεκριμένο flow παραμένει active για τυχαία διάρκεια. Όλα τα παραπάνω συνηγορούν πως πρέπει το sampling probability να μεταβάλλεται ανάλογα με τις αλλαγές που επισυμβαίνουν στο traffic.

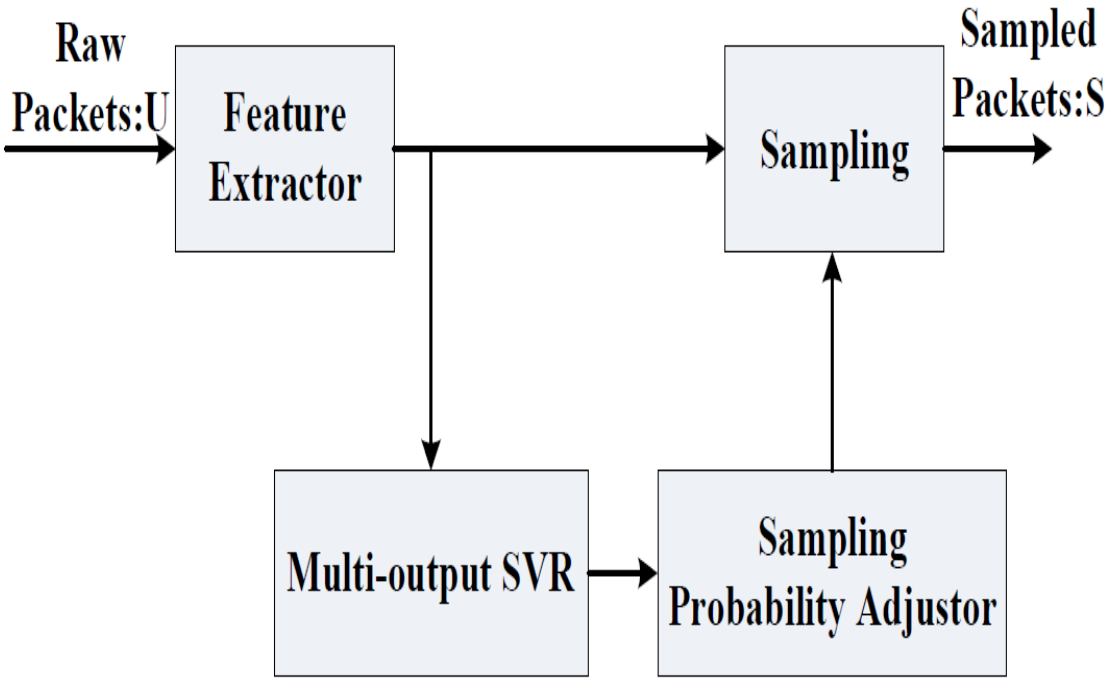
3.6 Ιδανικό μοντέλο packet Sampler για traffic classification

Σε γενικότερο framework ο σκοπός του ιδανικού packet sampler είναι να επιλέξει πακέτα κατά τέτοιο τρόπο ώστε να επιτύχει τη λιγότερη απώλεια πληροφορίας όπως αυτή ορίζεται από συγκεκριμένους δείκτες. Παρόλα αυτά, διαφορετικά χαρακτηριστικά του traffic, είναι πολύ πιθανόν να έχουν διαφορετικό impact στην απόδοση του classification. Αυτό οφείλεται στο γεγονός πως οι διάφορες μέθοδοι classification χρησιμοποιούν ως input διαφορετικά χαρακτηριστικά των πακέτων. Επομένως ορισμένα χαρακτηριστικά είναι πιο αντιπροσωπευτικά για το σκοπό του classification.(J. Fan, D. Wu, A. Nucci, R. Keralapura, and L. Gao,2009)
Η έρευνα σε μεγάλο βαθμό καταδεικνύει πως το traffic σχετιζόμενο με multimedia έχει ισχυρή συσχέτιση με 2 χαρακτηριστικά, συγκεκριμένα με το packet size και με το inter arrival time. Η χρήση αυτών των 2 χαρακτηριστικών από κάποιον classifier μπορεί να επιτύχει μεγάλο accuracy ως προς το traffic classification σε multimedia. Το γεγονός αυτό υποδεικνύει πως αυτά τα 2 χαρακτηριστικά εμπεριέχουν σημαντική πληροφορία όσον αφορά το κάθε flow, καθώς επίσης υπάρχει και συσχέτιση μεταξύ τους. Κατά συνέπεια αν επιλεγούν πακέτα ανάλογα με το packet size και το inter arrival time υπάρχει καλή πιθανότητα να αποκτηθεί ένα αντιπροσωπευτικό dataset από το ολικό traffic, ενώ παράλληλα θα μειωθεί ο συνολικός αριθμός των δεδομένων σε ένα μέγεθος αρκετά πιο διαχειρίσιμο.

Αν κάθε πακέτο που προέρχεται από multimedia traffic ονομαστεί P, μπορεί να ταυτοποιηθεί από 2 χαρακτηριστικά, το Packet Size (PS) και το Inter Arrival Time (IAT),<PS,IAT>. Από την οπτική του traffic classification είναι σημαντικό να επιλεγούν όλα τα αντιπροσωπευτικά πακέτα με κάποια μέθοδο sampling. Από την άλλη χάνεται το νόημα του efficiency όσο αυξάνεται ο αριθμός επιλεγμένων πακέτων με ίδια δυάδα χαρακτηριστικών <PS,IAT>, καθώς αυτά τα πακέτα μπορεί να προέρχονται από τον ίδιο τύπο application με καλή πιθανότητα. Κατά συνέπεια, η κυριότερη αρχή της μεθόδου δειγματοληψίας είναι να δειγματοληπτηθούν όσο το δυνατόν περισσότερα πακέτα με διαφορετικό ζεύγος τιμών <PS,IAT>.

3.8 Αρχιτεκτονική του συστήματος του adaptive packet sampling

Αφού περιγράφηκε η ιδέα του ιδανικού sampling ακολουθεί η περιγραφή όλης της αρχιτεκτονικής του ιδανικού συστήματος packet sampling. Όλα τα πακέτα που έχουν συγκεντρωθεί επεξεργάζονται από τον component του συστήματος που λέγεται Feature Extractor module, ο οποίος ζητά, σε κάθε περίπτωση, πακέτα σε σχέση με το Packet Size και το Inter Arrival Time μεταξύ των αφίξεων των πακέτων μέσα σε κάθε γενικό packet flow. Η έξοδος του Feature Extractor προωθείται σε ένα multi-output SVR (Support Vector Regression) predictor module το οποίο κάνει μία πρόβλεψη για το επόμενο Packet Size και το Inter Arrival Time ταυτόχρονα για το επόμενο εισερχόμενο πακέτο. Ανάλογα με τις προβλέψεις τιμών των Packet Size και Inter Arrival Time ο component που ονομάζεται sampling probability adjustor μεταβάλλει το sampling probability αναλόγως. Τελικά το sampling module λαμβάνει το sampled set το οποίο, εν συνεχεία, τροφοδοτείται στον classifier.



3.9 Multi-output Support Vector Regression για traffic prediction

Το Support Vector Regression (SVR) είχε ως σκοπό το χτίσιμο ενός μοντέλου της εξόδου κάποιας διαδικασίας ή ενός συστήματος που εξαρτάται από ένα set από παράγοντες, δοσμένης εισόδου x d διαστάσεων και εξόδου y μονοδιάστατης. Το SVR είναι παραδοσιακά χρησιμοποιούμενο με μόνο μία έξοδο και η περίπτωση με τις πολλαπλές εξόδους έρχεται όταν η έξοδος είναι διάνυσμα d διαστάσεων αντί για βαθμωτή ποσότητα.
Το πρόβλημα του multi-output regression θα μπορούσε να διαχωριστεί σε έναν αριθμό από μονοδιάστατα προβλήματα και σε κάποιες περιπτώσεις το να γίνει minimum variance estimation είναι αντίστοιχο με το να γίνει multi-output vector regression. Όμως αυτή η περίπτωση δεν αντιστοιχεί στο πρόβλημα της πρόβλεψης του packet size και του Inter Arrival Time, δηλαδή δεν μπορεί να γίνει χρήση δύο μονοδιάστατων Support Vector Regression (SVR) για τρεις βασικούς λόγους. (1) Υπάρχει μία σχέση ανάμεσα σε δύο μεταβλητές εισόδου οπότε θα μειωθεί το prediction error χρησιμοποιώντας την πρόβλεψη των packet size και inter arrival time ταυτοχρόνως από το να διαιρεθεί σε 2 χωριστά μονοδιάστατα προβλήματα.(2) Η μη ευαίσθητη ζώνη που ορίζεται από τον εκάστοτε υπολογισμό δεν αντιμετωπίζει ισότιμα κάθε training sample. (3)Η πρόβλεψη των packet size και inter arrival time αντίστοιχα χρησιμοποιώντας Support Vector Regression (SVR) θα μπορούσε να δημιουργήσει το πρόβλημα ότι ένα δείγμα θα αποτελούσε Support vector για την πρόβλεψη του Packet Size, ενώ το ίδιο δείγμα δε θα αποτελούσε support vector για την πρόβλεψη του Inter Arrival Time, γεγονός το οποίο δεν κάνει επαρκή χρήση της συσχέτισης των δύο μεγεθών.(F. Perez-Cruz, G. Camps-Vails, and E. Soria-Olivas)

3.10 Αλγόριθμος για classification

Συνολικά 2 αλγόριθμοι για classification λαμβάνονται υπόψη : ο VOVclassifier και ο SVM.
Ο VOVclassifier στηρίζεται σε 2 κύρια χαρακτηριστικά των πακέτων σε flows που προέρχονται από video ή ήχο: Packet Size και Inter Arrival Time. Η προσέγγιση πρώτα μοντελοποιεί κάθε flow σαν δυσδιάστατη στοχαστική διαδικασία και στη συνέχεια Power Spectral Density Analysis ώστε να βρει τα κρυμμένα μοτίβα που αποτελούν, εν γένει, το δακτυλικό αποτύπωμα του εκάστοτε flow. Τα αποτυπώματα είναι μοναδικά για κάθε flow φωνής ή video όπως επίσης και για κάθε multimedia εφαρμογή που παράγει αυτά τα flows, η οποία μπορεί εύκολα να κατηγοριοποιηθεί ως ένας υπόχωρος φωνής και video. Αυτοί οι υπόχωροι μπορούν να διαχωριστούν στη συνέχεια από ένα γραμμικό classifier.
Ο Support Vector Machine (SVM) classifier, στην αρχική του μορφή είναι binary classifier όπου η έξοδος του classifier είναι είτε θετική είτε αρνητική. Μία multi-class classification μπορεί να εφαρμοστεί συνδυάζοντας πολλαπλούς binary classifiers κάνοντας χρήση της pairwise coupling method (T. Hastie and R. Tibshirani,)
. Ο binary SVM είναι ένας classifier που διακρίνει τα δεδομένα σε δύο κατηγορίες. Κάθε σημείο αντιπροσωπεύεται από ένα πολυδιάστατο διάνυσμα. Κάθε ένα σημείο των δεδομένων ανήκει σε μία από τις δύο κλάσεις. Ο συνολικός στόχος είναι να επιτευχθεί μέγιστος διαχωρισμός ανάμεσα σε αυτές τις 2 κλάσεις που επιτυγχάνεται

εισάγοντας ένα υπερεπίπεδο διαχωρισμού. Αυτό το υπερεπίπεδο οφείλει να μεγιστοποιεί το μέγεθος ανάμεσα σε αυτές τις δύο κλάσεις το οποίο ονομάζεται και ως optimum separating hyperplane.

3.11 Υπολογιστική Πολυπλοκότητα

Η απόδοση των τεχνικών sampling περιγράφονται σε όρους απαιτήσεων της CPU. Πρώτα από όλα είναι σημαντικό να κατανοήσει κανείς ότι η συγκεκριμένη τεχνική για sampling συμπεριλαμβάνει 3 διαφορετικές διαδικασίες. MSVR model training, διαδικασία πρόβλεψης για Packet Size και Inter Arrival Time και επιλογή των πακέτων αντιστοίχως. Το πρώτο σχετίζεται με τη λύση ενός προβλήματος βελτιστοποίησης που λύνεται από μία επαναληπτική διαδικασία. Το δεύτερο συμπεριλαμβάνει μόνο έναν περιορισμένο αριθμό από απλές πράξεις που μπορούν να συλλεγούν με χρήση κάποιου regression function. Το τελευταίο περιλαμβάνει μία σύγκριση ανάμεσα σε προβλεπόμενες τιμές και προηγούμενη πληροφορία.Αυτές οι διαδικασίες πραγματοποιούνται σε εγγενώς διαφορετικές χρονικές κλίμακες και η πρώτη από αυτές θα διαρκέσει το περισσότερο λόγω της επαναληπτικότητας. Πείραμα [adaptive sampling] πραγματοποιήθηκε με δύο μεγέθη από multimedia traffic σε τρεις μεθόδους sampling και συγκεκριμένα adaptive sampling με πρόβλεψη packet size και inter arrival time ταυτοχρόνως, adaptive sampling με πρόβλεψη packet size και inter arrival time ξεχωριστά και random sampling. Συγκεκριμένα το adaptive sampling με ταυτόχρονη πρόβλεψη των δύο παραγόντων απαιτεί περισσότερο χρόνο υπολογισμού από τις υπόλοιπες μεθόδους. Η μέθοδος του random sampling απαιτεί το λιγότερο χρόνο υπολογισμού αλλά έχει τη χειρότερη απόδοση όσον αφορά το sampling.

TABLE II: CPU TIME NEEDED TO SAMPLE INPUT PACKETS BY USING THREE TYPES OF SAMPLING METHODS (MS)

Raw Packets	Random sampling	Adaptive R	Adaptive S
300 000	771	1026	1978
8 400 000	13321	20801	28986

References

1. Ευφροσύνη Θ. Ζώτου, 2012, "Σύγχρονες Τεχνολογίες Πρόσβασης και Διαδικτύου σε Έξυπνα Δίκτυα (SmartGrids)"

2. I-scoop.eu. (2018). *The Internet of Things (IoT) - essential IoT business guide*. [online] Available at: https://www.i-scoop.eu/internet-of-things-guide/#Understanding_IoT [Accessed 29 Oct. 2018].

3. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), pp.2347-2376

4.IERC Cluster Book, 2014,' Internet of Things: From Research and Innovation to Market Deployment'

5. Καλύβας Βασίλειος,2015,"Αρχιτεκτονική και Λειτουργία οικιακού δικτύου smart home"

6. Today's Motor Vehicles. (2018). Caterpillar advancing Internet of Things strategy - Today's Motor Vehicles. [online] Available at: http://www.todaysmotorvehicles.com/article/truck-design-caterpillar-uptake-internet-of-things-030615

7.Geng Wu, Talwar, S., Johnsson, K., Himayat, N. and Johnson, K. (2011). M2M: From mobile to embedded internet. IEEE Communications Magazine, 49(4), pp.36-43.

8. Παντισκα Λεονάρδος,2016, "Έξυπνα Ενεργειακά Δίκτυα: Διαχείριση και Εφαρμογές"

9. Drinkwater, D. (2018). How IoT is helping Airbus to make better planes - and bigger revenues.

10. Services, P., Software, C., Technologies, C. and Instrumentation, M. (2018). *Cisco IOS NetFlow*. [online] Cisco. Available at: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html

11. Manageengine.com. (2018). *Real-Time NetFlow Analyzer | NetFlow Traffic Analysis & Monitor Tool*. [online] Available at: https://www.manageengine.com/products/netflow/

12. Duffield, N., Lund, C. and Thorup, M. (2004). Flow sampling under hard resource constraints. *ACM SIGMETRICS Performance Evaluation Review*, 32(1), p.85.

13. Managing traffic flow to stop DOS attack. (2000). Network Security, 2000(4), p.4.

14. Chaudhuri, S., Motwani, R. and Narasayya, V. (1998). Random sampling for histogram construction. ACM SIGMOD Record, 27(2), pp.436-447.

15. Cassel, L. and Amer, P. (1988). Management of distributed measurement over interconnected networks. IEEE Network, 2(2), pp.50-56.

16. Claffy KC, Polyzos GC, Braun H. Application of sampling methodologies to network traffic characterization. *Proc. of ACM SIGCOMM '93*, San Francisco, CA, USA, 1993.

17. Kumar A, Xu J. Sketch guided sampling - using on-line estimates of flow size for adaptive data collection. *IEEE INFOCOM '06,* Barcelona, Spain, 2006.

18.Ribeiro B, Towsley D, Ye T, Bolot JC. Fisher information of sampled packets: an application to flow size estimation. *Proc. of ACM SIGCOMM '06,* Rio de Janeriro, Brazil, 2006.

19. Carela-Espaol V, Barlet-Ros P, Cabellos-Aparicio A, Sol-Pareta J. Analysis of the impact of sampling on netflow
traffic classification. *Elsevier Computer Networks* 2011; **55**(5):1083 – 1099.

20. Zander S, Nguyen T, Armitage G. Automated traffic classification and application identification using machine
learning. 2005; 250 –257, doi:10.1109/LCN.2005.35

21. Finamore A, Mellia M, Meo M, Rossi D. Kiss: Stochastic packet inspection classifier for udp traffic. *IEEE/ACM
Trans. Netw.* 2010; **18**(5):1505–1515.

22. Paxson V. End-to-end routing behavior in the internet. *SIGCOMM Comput. Commun. Rev.* 1996; **26**(4):25–38, doi:http://doi.acm.org/10.1145/248157.248160.

23. Duffield NG, Grossglauser M. Trajectory sampling for direct traffic observation. *SIGCOMM Comput. Commun.Rev.* 2000; **30**(4):271–282, doi:http://doi.acm.org/10.1145/347057.347555.

24. Jiang H, Moore AW, Ge Z, Jin S, Wang J. Lightweight application classification for network management. *Proc. Of ACM SIGCOMM INM '07*, Kyoto, Japan, 2007.

25. J. Fan, D. Wu, A. Nucci, R. Keralapura, and L. Gao, "Protocol oblivious classification of multimedia traffic," Security and Communication Networks, vol. 4, pp. 357–371, 2009.

26. H. Kim, K. Claffy, M. Fomenkov, D. Barman, M. Faloutsos, and K. Lee, "Internet traffic classification demystified: myths, caveats, and the best practices," in *Proc. ACM CoNEXT Conference*, 2008, pp. 1–12

27. T. Hastie and R. Tibshirani, "Classification by pairwise coupling," *Advances in Neural Information Processing Systems*, vol. 26, pp. 451-800, 1998.

28. J. Erman, A. Mahanti, M. Arlitt, I. Cohen, and C. Williamson, "Offline/realtime traffic classification using semi-supervised learning," *Performance Evaluation*, vol. 64, pp. 1194–1213, 2007.

29. J. Fan, D. Wu, A. Nucci, R. Keralapura, and L. Gao, "Protocol oblivious classification of multimedia traffic," Security and Communication Networks, vol. 4, pp. 357–371, 2009.