Ερωτήσεις - Απαντήσεις
Διαδίκτυο των Πραγμάτων - ΔΙΠΑΕ

Σημείωση: Το παρόν έγγραφο ναι μεν απαντάει ολοκληρωμένα στις ερωτήσεις, ωστόσο οι απαντήσεις σκοπεύουν στο να μπορέσει ο αναγνώστης να μάθει και να κατανοήσει το αντικείμενο της εκάστοτε ερώτησης-απάντησης. Στην πραγματικότητα, δεν θα χρειαστεί να γράψετε όλα αυτά τα κατεβατά, αλλά τα πιο σημαντικά κομμάτια από εκεί μέσα, εκτός αν η ερώτηση ζητάει συγκεκριμένο αριθμό λέξεων.

ΘΕΜΑ 1

1. Γνωρίζουμε ότι το πρωτόκολλο IEEE 802.11ah (του οποίου η προτυποποίηση ολοκληρώνεται πολύ σύντομα) προβλέπει ρυθμούς μετάδοσης λίγων δεκάδων Mbit/s. Αυτό δεν αποτελεί ένα παράδοξο την στιγμή που τα πρότυπα IEEE 802.11ac/ad (του 2012/2013) προβλέπουν ρυθμούς μετάδοσης περίπου 6 Gbit/s;

   Απάντηση:

   Το πρωτόκολλο IEEE 802.11ah, επίσης γνωστό ως Wi-Fi HaLow, και τα πρότυπα IEEE 802.11ac/ad εξυπηρετούν διαφορετικούς σκοπούς και στοχεύουν σε διαφορετικές περιπτώσεις χρήσης, γεγονός που εξηγεί το προφανές παράδοξο στους ρυθμούς μετάδοσης. Το IEEE 802.11ah έχει σχεδιαστεί για συνδεσιμότητα χαμηλής ισχύος και μεγάλης εμβέλειας, κατάλληλη για εφαρμογές του Διαδικτύου των Πραγμάτων (IoT). Λειτουργεί σε ζώνες κάτω του 1 GHz (π.χ. 900 MHz), επιτρέποντας καλύτερη διείσδυση μέσα από τοίχους και μεγαλύτερη εμβέλεια σε σύγκριση με ζώνες υψηλότερων συχνοτήτων. Το πρωτόκολλο προσφέρει ρυθμούς μετάδοσης έως και μερικές δεκάδες Mbit/s, οι οποίοι είναι επαρκείς για συσκευές IoT που συνήθως δεν απαιτούν υψηλό ρυθμό μετάδοσης δεδομένων. Επιπλέον, το IEEE 802.11ah μπορεί να καλύψει αποστάσεις έως και 1 km ή και περισσότερο, που είναι πολύ μεγαλύτερη από την τυπική εμβέλεια του τυπικού Wi-Fi.

   Αντίθετα, τα IEEE 802.11ac και IEEE 802.11ad στοχεύουν στην παροχή ασύρματης συνδεσιμότητας υψηλής ταχύτητας για γενική καταναλωτική χρήση, συμπεριλαμβανομένης της ροής βίντεο υψηλής ευκρίνειας, του gaming κ.α.. Το IEEE 802.11ac λειτουργεί στη ζώνη των 5 GHz, ενώ το IEEE 802.11ad λειτουργεί στη ζώνη των 60 GHz. Αυτά τα πρότυπα υποστηρίζουν σημαντικά υψηλότερους ρυθμούς δεδομένων, με το IEEE 802.11ac να φτάνει έως και 6,9 Gbit/s και το IEEE 802.11ad έως και 7 Gbit/s. Ωστόσο, η εμβέλειά τους είναι πιο περιορισμένη σε σύγκριση με το IEEE 802.11ah, ιδίως για το IEEE 802.11ad, το οποίο είναι αποτελεσματικό σε μικρότερες αποστάσεις λόγω της υψηλότερης συχνότητας και της σχετικής εξασθένησης.

   Πηγές: Διαφάνειες "W3.2 Slides - Introduction to Wireless and Mobile Networks" και "W6.1 Slides - IEEE 802.11 (Part 1)", όπως και γενικές γνώσεις σχετικά με τα πρότυπα IEEE και τις εφαρμογές τους.

2. Να αναπτύξετε σύντομα τα βασικά χαρακτηριστικά των εφαρμογών «Smart Grid» (Έξυπνη Διαχείριση Ενέργειας) και Intelligent Transportation (Έξυπνων Μεταφορών).

Απάντηση:

Smart Grid

Ένα από τα βασικά χαρακτηριστικά των εφαρμογών του έξυπνου δικτύου είναι η ενισχυμένη παρακολούθηση και ο έλεγχος, που επιτρέπει την παρακολούθηση της ροής της ηλεκτρικής ενέργειας σε πραγματικό χρόνο, επιτρέποντας τον ακριβή έλεγχο της διανομής και της κατανάλωσης ενέργειας. Αυτό συμβάλλει στην αποτελεσματική εξισορρόπηση της προσφοράς και της ζήτησης. Επιπλέον, τα smart grid ενσωματώνουν κατανεμημένους ενεργειακούς πόρους, όπως η ηλιακή και η αιολική ενέργεια, διευκολύνοντας την αποκεντρωμένη παραγωγή ενέργειας και μειώνοντας την εξάρτηση από τις κεντρικές μονάδες παραγωγής ενέργειας. Ένα άλλο σημαντικό χαρακτηριστικό είναι η αυτοματοποιημένη ανίχνευση και επιδιόρθωση βλαβών, όπου προηγμένοι αισθητήρες και συστήματα επικοινωνίας επιτρέπουν τον γρήγορο εντοπισμό και την απομόνωση των βλαβών. Τα συστήματα απόκρισης ζήτησης διαδραματίζουν επίσης κρίσιμο ρόλο, προσαρμόζοντας τα πρότυπα κατανάλωσης ενέργειας με βάση δεδομένα σε πραγματικό χρόνο, δίνοντας κίνητρα στους καταναλωτές να μειώσουν τη χρήση σε περιόδους αιχμής για την αποφυγή υπερφορτώσεων και τη μείωση του κόστους. Επιπλέον, τα έξυπνα δίκτυα εφαρμόζουν λύσεις αποθήκευσης ενέργειας, όπως η αποθήκευση ενέργειας σε μπαταρίες, για την αποθήκευση της πλεονάζουσας ενέργειας που παράγεται σε περιόδους χαμηλής ζήτησης, ώστε να γίνει χρήση της σε περιόδους υψηλής ζήτησης.

Intelligent Transportation

Βασικό χαρακτηριστικό των ITS είναι η διαχείριση της κυκλοφορίας. Αυτό περιλαμβάνει την παρακολούθηση και τον έλεγχο της ροής της κυκλοφορίας σε πραγματικό χρόνο με τη χρήση αισθητήρων, καμερών και δικτύων επικοινωνίας για τη μείωση της συμφόρησης και τη βελτίωση της αποδοτικότητας της κυκλοφορίας. Η επικοινωνία οχήματος προς υποδομή (Vehicle-to-Infrastructure - V2I) είναι μια άλλη σημαντική πτυχή, η οποία επιτρέπει στα οχήματα να επικοινωνούν με την οδική υποδομή, όπως τα φανάρια και τις πινακίδες. Ομοίως, η επικοινωνία οχήματος με όχημα (Vehicle-to-Vehicle - V2V) επιτρέπει στα οχήματα να μοιράζονται μεταξύ τους πληροφορίες σχετικά με την ταχύτητα, τη θέση και τις οδικές συνθήκες, μειώνοντας τον κίνδυνο ατυχημάτων και βελτιώνοντας τη συνολική οδική ασφάλεια. Τα ITS ενισχύουν επίσης την αποτελεσματικότητα και την αξιοπιστία των συστημάτων δημόσιων μεταφορών μέσω της παρακολούθησης σε πραγματικό χρόνο, της βελτιστοποίησης διαδρομών και των συστημάτων πληροφόρησης επιβατών. Επιπλέον, χρησιμοποιούν αισθητήρες και τεχνολογίες επικοινωνίας για την παροχή πληροφοριών σε πραγματικό χρόνο σχετικά με τις διαθέσιμες θέσεις στάθμευσης, μειώνοντας τον χρόνο αναζήτησης στάθμευσης και μειώνοντας τη συμφόρηση.

Πηγές: Διαφάνειες "W1.1 Slides - Introduction" και "W3.2 Slides - Introduction to Wireless and Mobile Networks".

3. Ποια είναι τα τρία (3) πιο σημαντικά κριτήρια σύγκρισης που θα μπορούσαμε να χρησιμοποιήσουμε για την σύγκριση των πρωτοκόλλων πρόσβασης για το IoT; Να συγκρίνετε σύντομα μεταξύ τους τα πρωτόκολλα IEEE 802.11ax, IEEE 802.15.4 και IEEE 802.11ah (χρησιμοποιώντας τα κριτήρια που αναφέρατε προηγουμένως)

Απάντηση:

Τρία πιο σημαντικά κριτήρια σύγκρισης για τα πρωτόκολλα πρόσβασης στο IoT:

Κατά την αξιολόγηση πρωτοκόλλων πρόσβασης για το Διαδίκτυο των Πραγμάτων (IoT), τρία κρίσιμα κριτήρια σύγκρισης είναι η εμβέλεια/κάλυψη, η κατανάλωση ενέργειας και ο ρυθμός δεδομένων.

- **Εμβέλεια και κάλυψη:** Αυτό το κριτήριο αξιολογεί την απόσταση στην οποία ένα πρωτόκολλο μπορεί να επικοινωνήσει αποτελεσματικά. Είναι απαραίτητο επειδή οι συσκευές IoT πρέπει συχνά να λειτουργούν σε διαφορετικά περιβάλλοντα, από συμπαγείς εσωτερικούς χώρους έως εκτεταμένες εξωτερικές περιοχές. Η αποτελεσματική εμβέλεια επηρεάζει την υποδομή που απαιτείται για την υποστήριξη του δικτύου, όπως ο αριθμός των σημείων πρόσβασης ή των πυλών που απαιτούνται.
- **Κατανάλωση ενέργειας:** Η κατανάλωση ενέργειας είναι ζωτικής σημασίας, ιδίως για τις συσκευές IoT που λειτουργούν με μπαταρία. Η χαμηλή κατανάλωση ισχύος παρατείνει τη διάρκεια ζωής της μπαταρίας των συσκευών, μειώνοντας τη συχνότητα συντήρησης ή αντικατάστασης της μπαταρίας. Η αποδοτική χρήση ενέργειας είναι ζωτικής σημασίας για τη βιωσιμότητα και την πρακτικότητα των αναπτύξεων IoT, ιδίως σε απομακρυσμένες ή δυσπρόσιτες τοποθεσίες.
- **Ρυθμός δεδομένων:** Ο ρυθμός δεδομένων υποδεικνύει την ταχύτητα με την οποία μπορούν να μεταδοθούν δεδομένα μέσω του δικτύου. Οι διάφορες εφαρμογές IoT έχουν διαφορετικές απαιτήσεις ρυθμού δεδομένων. Για παράδειγμα, οι εφαρμογές που περιλαμβάνουν ροή βίντεο σε πραγματικό χρόνο απαιτούν υψηλότερους ρυθμούς δεδομένων σε σύγκριση με την απλή μετάδοση δεδομένων αισθητήρων.

Σύγκριση των IEEE 802.11ax, IEEE 802.15.4 και IEEE 802.11ah

Εμβέλεια και κάλυψη:

- Το IEEE 802.11ax (Wi-Fi 6) έχει σχεδιαστεί για να παρέχει υψηλή απόδοση σε σχετικά περιορισμένες περιοχές, όπως σπίτια, γραφεία και δημόσια hotspots. Λειτουργεί τόσο στις ζώνες 2,4 GHz όσο και στις ζώνες 5 GHz, προσφέροντας καλή κάλυψη που συνήθως περιορίζεται σε μερικές εκατοντάδες μέτρα.
- Το IEEE 802.15.4 είναι βελτιστοποιημένο για εφαρμογές χαμηλής ισχύος και χαμηλού ρυθμού μετάδοσης δεδομένων και γενικά καλύπτει μικρότερες αποστάσεις από το Wi-Fi. Λειτουργώντας στη ζώνη των 2,4 GHz και σε άλλες ζώνες κάτω των GHz (π.χ. 868/915 MHz), μπορεί να επιτύχει εμβέλειες έως και 100 μέτρα περίπου, που είναι επαρκείς για πολλές εφαρμογές δικτύων αισθητήρων.
- Το IEEE 802.11ah (Wi-Fi HaLow) στοχεύει σε εφαρμογές IoT μεγάλης εμβέλειας. Λειτουργεί στη ζώνη κάτω του 1 GHz, παρέχοντας σημαντικά μεγαλύτερη κάλυψη, έως

και 1 km ή και περισσότερο. Αυτό το καθιστά κατάλληλο για μεγάλης κλίμακας υπαίθριες και αγροτικές εφαρμογές IoT.

Κατανάλωση ενέργειας:

- Το IEEE 802.11ax δεν είναι πρωτίστως βελτιστοποιημένο για χαμηλή κατανάλωση ενέργειας, καθώς στοχεύει στην παροχή υψηλής απόδοσης και απόδοσης δεδομένων για καταναλωτικές συσκευές. Παρόλο που περιλαμβάνει χαρακτηριστικά για τη βελτίωση της απόδοσης, οι απαιτήσεις ισχύος του είναι υψηλότερες, καθιστώντας το λιγότερο ιδανικό για συσκευές IoT που λειτουργούν με μπαταρία.
- Το IEEE 802.15.4 υπερέχει στην αποδοτικότητα ισχύος, καθιστώντας το ιδανικό για συσκευές IoT που βασίζονται στην ισχύ της μπαταρίας. Η χαμηλή του κατανάλωση ισχύος παρατείνει τη διάρκεια ζωής της μπαταρίας της συσκευής, η οποία είναι κρίσιμη για εφαρμογές όπου οι συσκευές αναμένεται να λειτουργούν για μεγάλα χρονικά διαστήματα χωρίς συντήρηση.
- Το IEEE 802.11ah προσφέρει ισορροπία μεταξύ εμβέλειας και κατανάλωσης ενέργειας. Αν και δεν είναι τόσο αποδοτικό σε ισχύ όσο το IEEE 802.15.4, έχει σχεδιαστεί για να είναι πιο αποδοτικό σε ισχύ από τα παραδοσιακά πρότυπα Wi-Fi, καθιστώντας το κατάλληλο για συσκευές που λειτουργούν με μπαταρία και απαιτούν συνδεσιμότητα μεγαλύτερης εμβέλειας.

Ρυθμός δεδομένων:

- Το IEEE 802.11ax προσφέρει πολύ υψηλούς ρυθμούς δεδομένων, που φθάνουν έως και αρκετά Gbit/s. Αυτό το καθιστά κατάλληλο για εφαρμογές έντασης δεδομένων, όπως η ροή βίντεο, αλλά υπερβολικό για τις περισσότερες εφαρμογές IoT που απαιτούν χαμηλότερους ρυθμούς δεδομένων.
- Το IEEE 802.15.4 υποστηρίζει χαμηλότερους ρυθμούς δεδομένων, συνήθως μεταξύ 20-250 Kbit/s, οι οποίοι είναι επαρκείς για πολλές εφαρμογές IoT που μεταδίδουν μικρές ποσότητες δεδομένων, όπως οι μετρήσεις αισθητήρων.
- Το IEEE 802.11ah παρέχει μέτριους ρυθμούς δεδομένων, έως και μερικές δεκάδες Mbit/s. Αυτό είναι υψηλότερο από το IEEE 802.15.4, καθιστώντας το κατάλληλο για εφαρμογές IoT που απαιτούν μέτριους ρυθμούς δεδομένων σε μεγαλύτερες αποστάσεις, όπως κάμερες παρακολούθησης ή συστήματα παρακολούθησης περιβάλλοντος.

Πηγές: Διαφάνειες "W6.1 Slides - IEEE 802.11 (Part 1)" και "W9.1 Slides - Open Challenges", όπως και γενικές γνώσεις σχετικά με τα πρότυπα IEEE και τις εφαρμογές τους.

4. Γιατί η διευθυνσιοδότηση (addressing) και η ασφάλεια/ιδιωτικότητα (security/privacy) αποτελούν σημαντικά ζητήματα του IoT; Να αναφέρετε κάποιες λύσεις οι οποίες έχουν προταθεί για την αποτελεσματική αντιμετώπιση τους.

Απάντηση:

Σημασία της διευθυνσιοδότηση και της ασφάλειας/ιδιωτικότητας στο IoT:

- **Διευθυνσιοδότηση:** Στο πλαίσιο του Διαδικτύου των Πραγμάτων (IoT), η διευθυνσιοδότηση είναι ζωτικής σημασίας επειδή επιτρέπει τη μοναδική ταυτοποίηση και επικοινωνία με δισεκατομμύρια συνδεδεμένες συσκευές. Χωρίς κατάλληλα συστήματα διευθυνσιοδότησης, θα ήταν αδύνατο να δρομολογηθούν σωστά τα δεδομένα, να διαχειριστούν οι συσκευές ή να διασφαλιστεί η αποτελεσματική επικοινωνία εντός του δικτύου.
- **Ασφάλεια/Ιδιωτικότητα:** Η ασφάλεια και η προστασία της ιδιωτικής ζωής αποτελούν κρίσιμα ζητήματα στο IoT λόγω της ευαίσθητης φύσης των δεδομένων που μεταδίδονται και των πιθανών επιπτώσεων των παραβιάσεων της ασφάλειας. Οι συσκευές IoT συχνά συλλέγουν και μεταδίδουν προσωπικές, βιομηχανικές και ευαίσθητες πληροφορίες, γεγονός που τις καθιστά πρωταρχικούς στόχους για επιθέσεις στον κυβερνοχώρο. Οι παραβιάσεις της ασφάλειας μπορούν να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση, κλοπή δεδομένων και χειραγώγηση των συσκευών, γεγονός που μπορεί να έχει σοβαρές συνέπειες, ιδίως σε κρίσιμες εφαρμογές όπως η υγειονομική περίθαλψη, τα έξυπνα σπίτια και τα βιομηχανικά συστήματα ελέγχου.

Προτεινόμενες λύσεις:

Διευθυνσιοδότηση:

- **Υιοθέτηση του IPv6:** Καθώς ο αριθμός των συσκευών IoT συνεχίζει να αυξάνεται εκθετικά, τα παραδοσιακά σχήματα διευθυνσιοδότησης, όπως το IPv4, είναι ανεπαρκή λόγω του περιορισμένου χώρου διευθύνσεών τους. Αυτό καθιστά αναγκαία τη χρήση πιο κλιμακούμενων λύσεων όπως το IPv6, το οποίο προσφέρει έναν πολύ μεγαλύτερο χώρο διευθύνσεων για να εξυπηρετήσει τον πολλαπλασιασμό των συσκευών IoT.
- **Ιεραρχική διευθυνσιοδότηση:** Η εφαρμογή ιεραρχικών συστημάτων διευθυνσιοδότησης μπορεί να βοηθήσει στην αποτελεσματικότερη διαχείριση μεγάλου αριθμού συσκευών IoT με την οργάνωσή τους σε μια δομημένη ιεραρχία. Η προσέγγιση αυτή απλοποιεί τη δρομολόγηση και τη διαχείριση των συσκευών εντός του δικτύου.

Ασφάλεια/Ιδιωτικότητα:

- **Κρυπτογράφηση:** Οι τεχνικές κρυπτογράφησης, όπως το TLS (Transport Layer Security) και το DTLS (Datagram Transport Layer Security), χρησιμοποιούνται ευρέως για την προστασία των δεδομένων κατά τη μεταφορά. Αυτά τα πρωτόκολλα διασφαλίζουν ότι τα δεδομένα που ανταλλάσσονται μεταξύ των συσκευών IoT και των διακομιστών είναι κρυπτογραφημένα, καθιστώντας δύσκολη την υποκλοπή και αποκρυπτογράφηση των πληροφοριών από μη εξουσιοδοτημένα μέρη.
- **Αυθεντικοποίηση και εξουσιοδότηση:** Ισχυροί μηχανισμοί ελέγχου ταυτότητας, όπως ο έλεγχος ταυτότητας δύο παραγόντων (2FA) και τα ψηφιακά πιστοποιητικά, διασφαλίζουν ότι μόνο εξουσιοδοτημένες συσκευές και χρήστες μπορούν να έχουν πρόσβαση στο δίκτυο IoT και στους πόρους του. Ο έλεγχος πρόσβασης βάσει ρόλων (RBAC) μπορεί να

περιορίσει περαιτέρω την πρόσβαση σε ευαίσθητα δεδομένα και λειτουργίες με βάση το ρόλο του χρήστη.

- **Ανωνυμοποίηση και συγκέντρωση δεδομένων:** Για την προστασία της ιδιωτικής ζωής των χρηστών, μπορούν να χρησιμοποιηθούν τεχνικές ανωνυμοποίησης δεδομένων για την αφαίρεση των προσωπικών πληροφοριών (personally identifiable information - PII) από σύνολα δεδομένων. Επιπλέον, η συγκέντρωση δεδομένων μπορεί να χρησιμοποιηθεί για τον συνδυασμό δεδομένων από πολλαπλές πηγές με τρόπο ώστε τα μεμονωμένα σημεία δεδομένων να μην μπορούν να εντοπιστούν σε συγκεκριμένους χρήστες ή συσκευές.
- **Τεχνολογία blockchain:** Το Blockchain μπορεί να παρέχει μια αποκεντρωμένη και απαραβίαστη μέθοδο για την εξασφάλιση των συναλλαγών δεδομένων και την ακεραιότητα των δεδομένων, και μπορεί να ενισχύσει την ασφάλεια στα δίκτυα IoT αποτρέποντας τις μη εξουσιοδοτημένες μεταβολές των δεδομένων.

Πηγές: Διαφάνειες "W4.1 Slides - Introduction to IoT (Part 2)" και "W5.1 Slides - Ad hoc Sensor Networks", όπως και γενικές γνώσεις σχετικά με το IoT και τις προκλήσεις του.

5. Να αναφέρετε τις πιο σημαντικές διαφορές και ομοιότητες μεταξύ των Wireless Sensor Networks (WSNs) και των Mobile Ad-Hoc Networks. Ποιες είναι οι πιο σημαντικές προκλήσεις/ζητήματα που πρέπει να αντιμετωπίσουμε σε κάθε ένα από αυτά; Ποιες είναι οι κυριότερες αιτίες ενεργειακής σπατάλης σε ένα WSN;

Απάντηση:

Ομοιότητες:

- **Αυτο-οργάνωση:** Τόσο τα WSN όσο και τα Mobile Ad-Hoc Networks (MANET) είναι ικανά να αυτο-οργανώνονται. Δεν βασίζονται σε μια σταθερή υποδομή και μπορούν να σχηματίζουν δυναμικά δίκτυα με βάση τους διαθέσιμους κόμβους.
- **Επικοινωνία πολλαπλών βημάτων (Multi-hop Communication):** Και οι δύο τύποι δικτύων χρησιμοποιούν επικοινωνία πολλαπλών βημάτων για τη μεταβίβαση δεδομένων από τον ένα κόμβο στον άλλο, επεκτείνοντας την εμβέλεια του δικτύου.
- **Ασύρματη επικοινωνία:** Τόσο τα WSN όσο και τα MANET λειτουργούν ασύρματα, χρησιμοποιώντας επικοινωνία ραδιοσυχνοτήτων για την ανταλλαγή δεδομένων μεταξύ των κόμβων.

Διαφορές:

1. **Σκοπός και εφαρμογή:**
    a. Τα WSN έχουν σχεδιαστεί κυρίως για την παρακολούθηση και τη συλλογή δεδομένων από το περιβάλλον. Χρησιμοποιούνται συχνά σε εφαρμογές όπως η περιβαλλοντική παρακολούθηση, η υγειονομική περίθαλψη και ο βιομηχανικός αυτοματισμός.
    b. Τα MANET έχουν σχεδιαστεί για την παροχή στιβαρής και ευέλικτης επικοινωνίας μεταξύ κινητών συσκευών. Χρησιμοποιούνται συνήθως σε

στρατιωτικές επιχειρήσεις, αποκατάσταση καταστροφών και σενάρια κινητής δικτύωσης.

2. **Χαρακτηριστικά κόμβων:**
    a. Τα WSN αποτελούνται συνήθως από κόμβους αισθητήρων που διαθέτουν περιορισμένη επεξεργαστική ισχύ, μνήμη και ενεργειακούς πόρους. Έχουν σχεδιαστεί ώστε να είναι χαμηλού κόστους και ενεργειακά αποδοτικοί.
    b. Τα MANET αποτελούνται από ισχυρότερους κόμβους (π.χ. φορητούς υπολογιστές, smartphones) που έχουν καλύτερες δυνατότητες επεξεργασίας, περισσότερη μνήμη και μεγαλύτερη ενεργειακή χωρητικότητα.
3. **Κινητικότητα:**
    a. Τα WSN έχουν γενικά στατικούς κόμβους, αν και υπάρχουν ορισμένες εφαρμογές κινητών δικτύων αισθητήρων. Η πρωταρχική εστίαση είναι στη συλλογή δεδομένων και όχι στην κινητικότητα των κόμβων.
    b. Τα MANET έχουν κόμβους που συχνά είναι ιδιαίτερα κινητικοί και το δίκτυο πρέπει συχνά να προσαρμόζεται στις αλλαγές της τοπολογίας λόγω της μετακίνησης των κόμβων.
4. **Κατανάλωση ενέργειας:**
    a. Τα WSN δίνουν προτεραιότητα στην ενεργειακή απόδοση για την παράταση της λειτουργικής ζωής των κόμβων αισθητήρων, οι οποίοι συνήθως λειτουργούν με μπαταρίες.
    b. Τα MANET λαμβάνουν επίσης υπόψη την ενεργειακή απόδοση, αλλά οι κόμβοι διαθέτουν συνήθως περισσότερους ενεργειακούς πόρους σε σύγκριση με τους κόμβους WSN.

Προκλήσεις/προβλήματα στα WSNs και MANETs

WSNs:

- **Ενεργειακή απόδοση:** Η παράταση της διάρκειας ζωής της μπαταρίας των κόμβων αισθητήρων είναι κρίσιμη. Τεχνικές όπως ο κύκλος λειτουργίας (duty cycle), η ενεργειακά αποδοτική δρομολόγηση και η συγκέντρωση δεδομένων είναι απαραίτητες για την ελαχιστοποίηση της κατανάλωσης ενέργειας.
- **Επεκτασιμότητα (Scalability):** Διαχείριση μεγάλου αριθμού κόμβων αισθητήρων και εξασφάλιση αποτελεσματικής συλλογής και επικοινωνίας δεδομένων χωρίς υπερφόρτωση του δικτύου.
- **Ανοχή σφαλμάτων:** Εξασφάλιση της συνέχισης της λειτουργίας του δικτύου παρά τις βλάβες των κόμβων, γεγονός που απαιτεί ισχυρά πρωτόκολλα για τη δρομολόγηση δεδομένων και τη διαχείριση των κόμβων.

MANETs:

- **Δρομολόγηση:** Ανάπτυξη αποτελεσματικών πρωτοκόλλων δρομολόγησης που μπορούν να χειριστούν τη δυναμική τοπολογία λόγω της κινητικότητας των κόμβων. Τα πρωτόκολλα πρέπει να προσαρμόζονται γρήγορα στις αλλαγές και να διατηρούν αξιόπιστη επικοινωνία.
- **Ποιότητα υπηρεσιών (Quality of Service - QoS):** Διασφάλιση ότι το δίκτυο μπορεί να ικανοποιήσει τις απαιτήσεις QoS για διαφορετικούς τύπους εφαρμογών, όπως η επικοινωνία σε πραγματικό χρόνο και η ροή δεδομένων.

- **Ασφάλεια:** Προστασία του δικτύου από διάφορες απειλές ασφαλείας, όπως υποκλοπές, αλλοίωση δεδομένων και μη εξουσιοδοτημένη πρόσβαση, ιδίως σε ένα αποκεντρωμένο και κινητό περιβάλλον.

Κύριες αιτίες σπατάλης ενέργειας σε ένα WSN

- **Αδρανής ακρόαση:** Οι κόμβοι καταναλώνουν ενέργεια ακούγοντας το κανάλι για πιθανή επικοινωνία, ακόμη και όταν δεν μεταδίδουν ή λαμβάνουν ενεργά δεδομένα. Αυτή είναι μια σημαντική πηγή σπατάλης ενέργειας.
- **Overhearing:** Οι κόμβοι μπορεί να καταναλώνουν ενέργεια λαμβάνοντας πακέτα που προορίζονται για άλλους κόμβους.
- **Συγκρούσεις πακέτων:** Όταν δύο κόμβοι μεταδίδουν ταυτόχρονα, τα πακέτα τους μπορεί να συγκρουστούν, με αποτέλεσμα να απαιτούνται επαναμεταδόσεις και να σπαταλάται ενέργεια.
- **Υπερφόρτωση πακέτων ελέγχου:** Η αποστολή πακέτων ελέγχου για τη διαχείριση του δικτύου (π.χ. ενημερώσεις δρομολόγησης, μηνύματα συγχρονισμού) καταναλώνει ενέργεια που διαφορετικά θα μπορούσε να χρησιμοποιηθεί για τη μετάδοση δεδομένων.
- **Υψηλή ισχύς μετάδοσης:** Η μετάδοση σε υψηλότερα επίπεδα ισχύος από τα απαραίτητα αυξάνει την κατανάλωση ενέργειας.

Πηγές: Διαφάνειες "W5.1 Slides - Ad hoc Sensor Networks", "W3.2 Slides - Introduction to Wireless and Mobile Networks" και "W2.2 Slides - Revision (Link layer)", όπως και γενικές γνώσεις σχετικά με το IoT και τις αρχές δικτύωσης.

6. Να αναφέρετε σύντομα τα βασικά χαρακτηριστικά των Έξυπνων Πόλεων (Smart Cities) και τις υπηρεσίες που μπορούν να προσφέρουν/υποστηρίξουν με την έλευση προηγμένων τεχνολογιών δικτύωσης (π.χ. 5G).

Απάντηση:

Κύρια χαρακτηριστικά των έξυπνων πόλεων

- **Συνδεσιμότητα:** Εκτεταμένη χρήση συσκευών και αισθητήρων IoT που συνδέονται μέσω δικτύων υψηλής ταχύτητας, όπως το 5G, παρέχοντας δεδομένα και επικοινωνία σε πραγματικό χρόνο.
- **Λήψη αποφάσεων με βάση τα δεδομένα:** Επεξεργασία και ανάλυση των τεράστιων όγκων δεδομένων που παράγονται, επιτρέποντας τη λήψη τεκμηριωμένων αποφάσεων και την προγνωστική ανάλυση.
- **Αυτοματοποίηση:** Εφαρμογή αυτοματοποιημένων συστημάτων για διάφορες αστικές λειτουργίες, μειώνοντας την ανθρώπινη παρέμβαση και αυξάνοντας την αποδοτικότητα.
- **Βιωσιμότητα:** Εστίαση στη μείωση των περιβαλλοντικών επιπτώσεων μέσω έξυπνης διαχείρισης της ενέργειας, μείωσης των αποβλήτων και αποδοτικής χρήσης των πόρων.
- **Ανθεκτικότητα:** Δημιουργία ισχυρών συστημάτων που μπορούν να προσαρμόζονται και να ανακάμπτουν από διαταραχές, είτε πρόκειται για φυσικές καταστροφές, είτε για βλάβες υποδομών, είτε για επιθέσεις στον κυβερνοχώρο.

- **Διαλειτουργικότητα:** Διασφάλιση της απρόσκοπτης συνεργασίας διαφορετικών συστημάτων και συσκευών, η οποία διευκολύνεται από τυποποιημένα πρωτόκολλα και διεπαφές.

Υπηρεσίες που προσφέρουν οι έξυπνες πόλεις

Με την έλευση προηγμένων τεχνολογιών δικτύωσης όπως το 5G, οι έξυπνες πόλεις μπορούν να προσφέρουν ένα ευρύ φάσμα υπηρεσιών, όπως:

- **Έξυπνη διαχείριση της κυκλοφορίας:** Παρακολούθηση και έλεγχος των κυκλοφοριακών ροών σε πραγματικό χρόνο με τη χρήση αισθητήρων και καμερών, μειώνοντας τη συμφόρηση και βελτιστοποιώντας τις διαδρομές των μέσων μαζικής μεταφοράς. Η χαμηλή καθυστέρηση του 5G επιτρέπει γρήγορες προσαρμογές και καλύτερο συντονισμό.
- **Έξυπνη στάθμευση:** Πληροφορίες σε πραγματικό χρόνο σχετικά με τη διαθεσιμότητα χώρων στάθμευσης, μειώνοντας τον χρόνο αναζήτησης θέσεων στάθμευσης, γεγονός που ανακουφίζει την κυκλοφοριακή συμφόρηση και μειώνει τις εκπομπές ρύπων.
- **Δημόσια ασφάλεια και προστασία:** Ενισχυμένη επιτήρηση με κάμερες υψηλής ανάλυσης και ανάλυση βίντεο σε πραγματικό χρόνο, σε συνδυασμό με συστήματα ταχείας απόκρισης για καταστάσεις έκτακτης ανάγκης. Το υψηλό εύρος ζώνης του 5G υποστηρίζει τη μετάδοση μεγάλων ροών βίντεο.
- **Περιβαλλοντική παρακολούθηση:** Συνεχής παρακολούθηση της ποιότητας του αέρα και του νερού, των επιπέδων θορύβου και άλλων περιβαλλοντικών παραμέτρων.
- **Διαχείριση ενέργειας:** Έξυπνα δίκτυα και έξυπνοι μετρητές για αποτελεσματική διανομή και κατανάλωση ενέργειας, ενσωμάτωση ανανεώσιμων πηγών ενέργειας και βελτίωση της ενεργειακής απόδοσης.
- **Διαχείριση αποβλήτων:** Βελτιστοποίηση των διαδρομών και των χρονοδιαγραμμάτων συλλογής απορριμμάτων με βάση δεδομένα σε πραγματικό χρόνο από έξυπνους κάδους, που οδηγούν σε εξοικονόμηση κόστους και βελτίωση της αστικής καθαριότητας.
- **Υγειονομική περίθαλψη:** Οι υπηρεσίες τηλεϊατρικής, η απομακρυσμένη παρακολούθηση ασθενών και η ανάλυση δεδομένων υγείας βελτιώνουν την παροχή υγειονομικής περίθαλψης και την πρόσβαση, ιδίως σε υποβαθμισμένες περιοχές. Ο χαμηλός λανθάνων χρόνος (latency) του 5G είναι ζωτικής σημασίας για αυτές τις εφαρμογές.
- **Έξυπνα κτίρια:** Αυτοματοποίηση των συστημάτων διαχείρισης κτιρίων για φωτισμό, θέρμανση, εξαερισμό και κλιματισμό (HVAC), βελτιώνοντας την ενεργειακή απόδοση και την άνεση.

Πηγές: Διαφάνειες "W3.1 Slides - Introduction to IoT (Part 1)" και "W4.1 Slides - Introduction to IoT (Part 2)", όπως και γενικές γνώσεις σχετικά με τις έννοιες της έξυπνης πόλης και τις εφαρμογές προηγμένων τεχνολογιών δικτύωσης.

7. Να σχολιάσετε την φράση «Δεν υπάρχει μια και μοναδική ασύρματη τεχνολογία που μπορεί να υποστηρίξει όλες τις εφαρμογές IoT».

Απάντηση:

Η φράση "Δεν υπάρχει μία και μοναδική ασύρματη τεχνολογία που να μπορεί να υποστηρίξει όλες τις εφαρμογές IoT" αντικατοπτρίζει τις διαφορετικές απαιτήσεις και προκλήσεις των περιπτώσεων χρήσης IoT. Οι εφαρμογές IoT ποικίλλουν σε μεγάλο βαθμό ως προς τις ανάγκες τους για ρυθμό δεδομένων, εμβέλεια, κατανάλωση ενέργειας, καθυστέρηση και αξιοπιστία. Για παράδειγμα, η βιντεοεπιτήρηση (video surveillance) απαιτεί υψηλούς ρυθμούς δεδομένων, ενώ οι αισθητήρες θερμοκρασίας χρειάζονται μόνο χαμηλούς ρυθμούς δεδομένων. Ομοίως, οι εφαρμογές μικρής εμβέλειας σε ένα έξυπνο σπίτι μπορεί να χρησιμοποιούν Bluetooth, ενώ οι εφαρμογές μεγάλης εμβέλειας, όπως η παρακολούθηση της γεωργίας, απαιτούν τεχνολογίες όπως το LoRaWAN ή το NB-IoT. Η κατανάλωση ενέργειας είναι ένας άλλος κρίσιμος παράγοντας- συσκευές που λειτουργούν με μπαταρίες σε απομακρυσμένες τοποθεσίες χρειάζονται εξαιρετικά αποδοτικές τεχνολογίες ενέργειας όπως το Zigbee, ενώ η υψηλότερη κατανάλωση ενέργειας του Wi-Fi το καθιστά λιγότερο κατάλληλο για τέτοιες εφαρμογές. Οι εφαρμογές πραγματικού χρόνου απαιτούν επικοινωνία χαμηλής καθυστέρησης, σε αντίθεση με την περιβαλλοντική παρακολούθηση, η οποία μπορεί να ανεχθεί υψηλότερες καθυστερήσεις.

Κάθε ασύρματη τεχνολογία έχει τα δικά της αντισταθμιστικά οφέλη. Το Wi-Fi προσφέρει υψηλούς ρυθμούς δεδομένων, αλλά καταναλώνει περισσότερη ενέργεια και έχει μικρότερη εμβέλεια. Τα Bluetooth και Zigbee είναι εξαιρετικά για επικοινωνία χαμηλής ισχύος και μικρής εμβέλειας, ενώ τα LoRaWAN και Sigfox είναι ιδανικά για εφαρμογές μεγάλης εμβέλειας και χαμηλού ρυθμού δεδομένων. Για την αντιμετώπιση αυτών των διαφορετικών αναγκών, οι υβριδικές λύσεις συχνά ενσωματώνουν πολλαπλές τεχνολογίες, αξιοποιώντας τα δυνατά τους σημεία για την κάλυψη διαφορετικών απαιτήσεων εφαρμογών. Έτσι, καμία μεμονωμένη τεχνολογία δεν μπορεί να υποστηρίξει αποτελεσματικά το τεράστιο φάσμα εφαρμογών IoT.

Πηγές: Διαφάνειες "W3.1 Slides - Introduction to IoT (Part 1)" και "W5.1 Slides - Ad hoc Sensor Networks", όπως και γενικές γνώσεις σχετικά με το IoT και τις τεχνολογίες ασύρματης επικοινωνίας.

8. Τι είναι η προτυποποίηση, γιατί μας χρειάζεται και ποια διαδικασία ακολουθούμε σε γενικές γραμμές για να την επιτύχουμε; Να αναφέρετε σύντομα κάποια πρότυπα που μπορούν να χαρακτηριστούν «IoT πρότυπα».

Απάντηση:

Η προτυποποίηση αναφέρεται στη διαδικασία ανάπτυξης και εφαρμογής τεχνικών προτύπων για τη διασφάλιση της συνέπειας, της συμβατότητας και της διαλειτουργικότητας προϊόντων και υπηρεσιών μεταξύ διαφορετικών κατασκευαστών και βιομηχανιών. Περιλαμβάνει τη θέσπιση κανόνων και κατευθυντήριων γραμμών που βοηθούν στη δημιουργία μιας ενιαίας προσέγγισης της τεχνολογίας και των διαδικασιών.

Η προτυποποίηση είναι απαραίτητη για διάφορους λόγους:

- **Διαλειτουργικότητα:** Εξασφαλίζει ότι οι συσκευές και τα συστήματα από διαφορετικούς κατασκευαστές μπορούν να συνεργάζονται απρόσκοπτα.

- **Ποιότητα και ασφάλεια:** Καθορίζει πρότυπα ελάχιστης ποιότητας και ασφάλειας, εξασφαλίζοντας αξιόπιστα και ασφαλή προϊόντα.
- **Αποδοτικότητα και μείωση του κόστους:** Εξορθολογίζει την παραγωγή και μειώνει το κόστος, ελαχιστοποιώντας τις παραλλαγές στο σχεδιασμό και τις διαδικασίες παραγωγής.
- **Πρόσβαση στην αγορά και θεμιτός ανταγωνισμός:** Διευκολύνει την πρόσβαση στην αγορά εξασφαλίζοντας τη συμμόρφωση με τα διεθνή πρότυπα, επιτρέποντας τον θεμιτό ανταγωνισμό και την καινοτομία.

Η διαδικασία προτυποποίηση περιλαμβάνει συνήθως διάφορα βασικά βήματα:

- **Προσδιορισμός της ανάγκης:** Αναγνώριση της ανάγκης για ένα πρότυπο, συχνά λόγω τεχνολογικών εξελίξεων ή απαιτήσεων της αγοράς.
- **Συγκρότηση επιτροπών:** Σύσταση επιτροπών και ομάδων εργασίας που αποτελούνται από εμπειρογνώμονες του κλάδου, ενδιαφερόμενους φορείς και ρυθμιστικούς φορείς.
- **Σύνταξη:** Ανάπτυξη σχεδίων προτύπων μέσω συνεργατικών προσπαθειών, συζητήσεων και συναίνεσης μεταξύ των μελών των επιτροπών.
- **Δημόσια αναθεώρηση:** Κοινοποίηση των σχεδίων προτύπων στο κοινό και στους ενδιαφερόμενους φορείς του κλάδου για σχόλια και παρατηρήσεις.
- **Αναθεώρηση:** Αναθεώρηση του σχεδίου με βάση τα σχόλια και διεξαγωγή περαιτέρω αναθεωρήσεων και εγκρίσεων.
- **Οριστικοποίηση και δημοσίευση:** Οριστικοποίηση και δημοσίευση του προτύπου, ακολουθούμενη από την εφαρμογή και την υιοθέτησή του.

(ίσως να λείπει κάτι από εδώ)

Αρκετά πρότυπα έχουν αναπτυχθεί ειδικά για το IoT για την αντιμετώπιση της διαλειτουργικότητας, της ασφάλειας και της αποτελεσματικότητας:

- **IEEE 802.15.4:** Ένα πρότυπο για ασύρματα προσωπικά δίκτυα χαμηλού ρυθμού (LR-WPANs), που χρησιμοποιείται συνήθως στα πρωτόκολλα Zigbee και Thread, κατάλληλο για εφαρμογές χαμηλής ισχύος και χαμηλού ρυθμού δεδομένων.
- **IPv6:** Η έκδοση 6 του πρωτοκόλλου Διαδικτύου παρέχει μεγαλύτερο χώρο διευθύνσεων, απαραίτητο για τον τεράστιο αριθμό συσκευών IoT.
- **MQTT:** Ένα ελαφρύ πρωτόκολλο ανταλλαγής μηνυμάτων για μικρούς αισθητήρες και κινητές συσκευές, που βελτιστοποιεί το εύρος ζώνης του δικτύου και την κατανάλωση ενέργειας.
- **CoAP:** Το πρωτόκολλο περιορισμένων εφαρμογών έχει σχεδιαστεί για απλά ηλεκτρονικά συστήματα με περιορισμένη επεξεργαστική ισχύ και μνήμη, διευκολύνοντας την επικοινωνία σε περιορισμένα περιβάλλοντα.
- **LoRaWAN:** Ένα πρωτόκολλο δικτύου χαμηλής ισχύος, ευρείας περιοχής, σχεδιασμένο για επικοινωνία μεγάλης εμβέλειας και αποδοτική χρήση της μπαταρίας, ιδανικό για αγροτικές και βιομηχανικές εφαρμογές IoT.

Πηγές: Διαφάνειες "W3.1 Slides - Introduction to IoT (Part 1)", "W5.1 Slides - Ad hoc Sensor Networks" και "W2.2 Slides - Revision (Link layer)", όπως και γενικές γνώσεις του IoT και των διαδικασιών προτυποποίησης.

9. Να δώσετε ένα σύντομο ορισμό, τα βασικά χαρακτηριστικά και παραδείγματα εφαρμογών για την Επικοινωνία Μηχανής-με-Μηχανή (Machine-to-Machine - M2M)

Απάντηση:

Η επικοινωνία μεταξύ μηχανών (M2M) αναφέρεται στην άμεση ανταλλαγή δεδομένων μεταξύ συσκευών χωρίς ανθρώπινη παρέμβαση. Περιλαμβάνει τη χρήση αισθητήρων, ενεργοποιητών και άλλων συσκευών για τη συλλογή, τη μετάδοση και την αυτόνομη επεξεργασία πληροφοριών, επιτρέποντας στα αυτοματοποιημένα συστήματα να λειτουργούν πιο αποδοτικά και αποτελεσματικά.

Βασικά χαρακτηριστικά της επικοινωνίας M2M

- **Αυτόνομη λειτουργία:** Οι συσκευές επικοινωνούν και εκτελούν εργασίες χωρίς ανθρώπινη παρέμβαση, μειώνοντας την ανάγκη για χειροκίνητη παρακολούθηση και έλεγχο.
- **Συνδεσιμότητα:** Χρησιμοποιεί διάφορες τεχνολογίες επικοινωνίας, όπως δίκτυα κινητής τηλεφωνίας, Wi-Fi, Bluetooth και ενσύρματες συνδέσεις, ώστε να διασφαλίζεται ότι οι συσκευές μπορούν να επικοινωνούν σε διαφορετικές εμβέλειες και περιβάλλοντα.
- **Ανταλλαγή δεδομένων σε πραγματικό χρόνο:** Διευκολύνει την άμεση μετάδοση και επεξεργασία δεδομένων, επιτρέποντας την έγκαιρη λήψη αποφάσεων και ενεργειών.
- **Επεκτασιμότητα:** Υποστηρίζει μεγάλο αριθμό συνδεδεμένων συσκευών, καθιστώντας το κατάλληλο για εκτεταμένες αναπτύξεις σε βιομηχανικές και εμπορικές εφαρμογές.
- **Διαλειτουργικότητα:** Εξασφαλίζει ότι συσκευές διαφορετικών κατασκευαστών μπορούν να συνεργάζονται απρόσκοπτα μέσω τυποποιημένων πρωτοκόλλων και διεπαφών.
- **Απομακρυσμένη παρακολούθηση και έλεγχος:** Επιτρέπει την κεντρική διαχείριση συσκευών και συστημάτων, συχνά μέσω πλατφορμών που βασίζονται σε cloud, παρέχοντας ορατότητα και έλεγχο.

Παραδείγματα εφαρμογών για την επικοινωνία M2M

- **Έξυπνη μέτρηση:** Η επικοινωνία M2M χρησιμοποιείται σε μετρητές κοινής ωφέλειας (ηλεκτρισμού, νερού, φυσικού αερίου) για την αυτόματη συλλογή δεδομένων κατανάλωσης και τη διαβίβασή τους στους παρόχους κοινής ωφέλειας. Αυτό βελτιώνει την ακρίβεια της τιμολόγησης, επιτρέπει την παρακολούθηση σε πραγματικό χρόνο και υποστηρίζει πρωτοβουλίες διαχείρισης ενέργειας.
- **Βιομηχανικός αυτοματισμός:** Σε βιομηχανικές και βιοτεχνικές εγκαταστάσεις, η επικοινωνία M2M συνδέει μηχανήματα και εξοπλισμό για την παρακολούθηση της απόδοσης, την πρόβλεψη των αναγκών συντήρησης και τη βελτιστοποίηση των διαδικασιών παραγωγής, βελτιώνοντας την αποδοτικότητα και μειώνοντας τον χρόνο διακοπής λειτουργίας.
- **Υγειονομική περίθαλψη:** Η M2M επιτρέπει την απομακρυσμένη παρακολούθηση ασθενών μέσω συνδεδεμένων ιατρικών συσκευών που συλλέγουν και μεταδίδουν

δεδομένα υγείας (π.χ. καρδιακός ρυθμός, αρτηριακή πίεση) στους παρόχους υγειονομικής περίθαλψης, επιτρέποντας τη συνεχή παρακολούθηση και την έγκαιρη παρέμβαση.

- **Διαχείριση εφοδιαστικής αλυσίδας (supply chain management):** Η διαχείριση της εφοδιαστικής αλυσίδας είναι ένας άλλος τομέας που έχει μεταμορφωθεί μαζικά από την παρουσία της M2M. Οι διαχειριστές μπορούν να παρακολουθούν το απόθεμα, να προγραμματίζουν τους χρόνους παράδοσης, να εκτιμούν ποια είδη πρέπει να ανεφοδιαστούν και να αποκτήσουν πληροφορίες σχετικά με το ποιες εγκαταστάσεις παραγωγής λειτουργούν σε δυναμικότητα.
- **Έξυπνη γεωργία:** Η επικοινωνία M2M χρησιμοποιείται στη γεωργία ακριβείας για την παρακολούθηση των συνθηκών του εδάφους, τον έλεγχο των συστημάτων άρδευσης και τη διαχείριση της υγείας των ζώων.
- **Οικιακός αυτοματισμός:** Οι έξυπνες οικιακές συσκευές, όπως θερμοστάτες, συστήματα ασφαλείας και έλεγχοι φωτισμού, χρησιμοποιούν την επικοινωνία M2M για να παρέχουν αυτοματοποιημένη και απομακρυσμένη διαχείριση του οικιακού περιβάλλοντος, ενισχύοντας την άνεση και την ενεργειακή απόδοση.

Πηγές: Διαφάνειες "W1.1 Slides - Introduction to IoT" και "W5.1 Slides - Ad hoc Sensor Networks", όπως και γενικές γνώσεις της επικοινωνίας M2M.

10. Να δώσετε ένα ορισμό για το IoT και να αναλύσετε τα κύρια επικοινωνιακά ζητήματα που σχετίζονται με αυτό.

Απάντηση:

Ορισμός του IoT

Το Διαδίκτυο των πραγμάτων (IoT) αναφέρεται στο δίκτυο διασυνδεδεμένων φυσικών συσκευών που επικοινωνούν και ανταλλάσσουν δεδομένα μεταξύ τους μέσω του διαδικτύου. Αυτές οι συσκευές, συχνά ενσωματωμένες με αισθητήρες, λογισμικό και άλλες τεχνολογίες, συλλέγουν και μεταδίδουν δεδομένα για να βελτιώσουν την αποτελεσματικότητα, την ακρίβεια και την ευκολία διαφόρων συστημάτων και εφαρμογών. Το IoT επιτρέπει έναν πιο έξυπνο, πιο διασυνδεδεμένο κόσμο, όπου τα αντικείμενα μπορούν να αλληλεπιδρούν και να ανταποκρίνονται στο περιβάλλον τους αυτόνομα.

Κύρια ζητήματα επικοινωνίας στο IoT

- **Επεκτασιμότητα**: Καθώς ο αριθμός των συνδεδεμένων συσκευών αυξάνεται εκθετικά, το δίκτυο IoT πρέπει να είναι ικανό να κλιμακώνεται για να φιλοξενήσει δισεκατομμύρια συσκευές. Η επεκτασιμότητα περιλαμβάνει τη διαχείριση της αυξημένης κίνησης, τη διατήρηση της απόδοσης και τη διασφάλιση ότι το δίκτυο μπορεί να διαχειριστεί τα δεδομένα που παράγονται από έναν τεράστιο αριθμό συσκευών. Οι αποτελεσματικές αρχιτεκτονικές και πρωτόκολλα δικτύου είναι απαραίτητες για την υποστήριξη τέτοιων αναπτύξεων μεγάλης κλίμακας χωρίς υποβάθμιση της ποιότητας των υπηρεσιών.

- **Διαλειτουργικότητα**: Οι συσκευές IoT προέρχονται από διάφορους κατασκευαστές και λειτουργούν με διαφορετικές πλατφόρμες και πρωτόκολλα. Η διασφάλιση ότι αυτές οι ετερογενείς συσκευές μπορούν να επικοινωνούν και να συνεργάζονται απρόσκοπτα αποτελεί σημαντική πρόκληση. Οι προσπάθειες τυποποίησης, όπως η υιοθέτηση κοινών πρωτοκόλλων επικοινωνίας (π.χ. MQTT, CoAP) και διεπαφών, είναι ζωτικής σημασίας για την επίτευξη διαλειτουργικότητας. Οι λύσεις ενδιάμεσου λογισμικού που μεταφράζουν μεταξύ διαφορετικών πρωτοκόλλων και πλατφορμών μπορούν επίσης να βοηθήσουν στη γεφύρωση των κενών συμβατότητας.
- **Καθυστέρηση (latency) και επικοινωνία σε πραγματικό χρόνο**: Πολλές εφαρμογές IoT, όπως τα αυτόνομα οχήματα, ο βιομηχανικός αυτοματισμός και η παρακολούθηση της υγειονομικής περίθαλψης, απαιτούν μετάδοση δεδομένων σε πραγματικό χρόνο και επικοινωνία χαμηλής καθυστέρησης. Τεχνικές όπως η υπολογιστική ακμής (edge computing), όπου η επεξεργασία δεδομένων πραγματοποιείται πιο κοντά στην πηγή των δεδομένων (στα "άκρα" του δικτύου), μπορούν να μειώσουν σημαντικά την καθυστέρηση και να βελτιώσουν τους χρόνους απόκρισης.
- **Εύρος ζώνης και απόδοση δεδομένων**: Η αποτελεσματική διαχείριση του εύρους ζώνης για την αποφυγή της συμφόρησης και τη διασφάλιση της ομαλής ροής δεδομένων είναι ένα κρίσιμο ζήτημα επικοινωνίας. Οι τεχνολογίες δικτύων όπως το 5G προσφέρουν υψηλότερους ρυθμούς δεδομένων και χωρητικότητα, οι οποίοι είναι απαραίτητοι για την υποστήριξη των υψηλών απαιτήσεων ρυθμού μετάδοσης των εφαρμογών IoT.
- **Ενεργειακή απόδοση**: Πολλές συσκευές IoT λειτουργούν με μπαταρίες και αναπτύσσονται σε απομακρυσμένες ή δυσπρόσιτες τοποθεσίες. Τα αποδοτικά πρωτόκολλα επικοινωνίας που ελαχιστοποιούν την κατανάλωση ενέργειας είναι απαραίτητα για την παράταση της διάρκειας ζωής της μπαταρίας και τη μείωση του κόστους συντήρησης. Τεχνικές όπως το duty cycling, όπου οι συσκευές εναλλάσσονται μεταξύ ενεργών και αναπαυτικών καταστάσεων, και τα πρότυπα επικοινωνίας χαμηλής κατανάλωσης ενέργειας (π.χ. Zigbee, LoRa) είναι ζωτικής σημασίας για ενεργειακά αποδοτικά δίκτυα IoT.
- **Ασφάλεια και προστασία της ιδιωτικής ζωής**: Η διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της αυθεντικότητας των δεδομένων είναι ζωτικής σημασίας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης και παραβίασης δεδομένων. Η κρυπτογράφηση, τα ασφαλή πρωτόκολλα επικοινωνίας (π.χ. TLS, DTLS) και οι ισχυροί μηχανισμοί ελέγχου ταυτότητας είναι απαραίτητα για τη διασφάλιση των δικτύων IoT. Επιπλέον, η διασφάλιση του απορρήτου των δεδομένων των χρηστών είναι κρίσιμη, ιδίως σε εφαρμογές που αφορούν ευαίσθητες πληροφορίες, όπως δεδομένα υγείας ή προσωπικής θέσης.
- **Διαχείριση δικτύου**: Η διαχείριση ενός τεράστιου και ποικίλου δικτύου συσκευών IoT περιλαμβάνει την αποτελεσματική παρακολούθηση, διαμόρφωση και ενημέρωση των συσκευών. Τα αυτοματοποιημένα εργαλεία διαχείρισης δικτύου που μπορούν να χειριστούν εργασίες όπως η παροχή συσκευών, οι ενημερώσεις υλικολογισμικού και η ανίχνευση σφαλμάτων είναι απαραίτητα για τη διατήρηση της υγείας και της απόδοσης των δικτύων IoT.

Πηγές: Διαφάνειες "W1.1 Slides - Introduction", "W2.1 Slides - Revision (Introduction to Networking)", "W2.2 Slides - Revision (Link layer)", "W3.1 Slides - Introduction to IoT (Part 1)", "W5.1 Slides - Ad hoc Sensor Networks" και "W9.1 Slides - Open Challenges", όπως και γενικές γνώσεις σχετικά με το IoT και τις επικοινωνιακές προκλήσεις του.

11. Να σχολιάσετε την πρόταση: «Μεταξύ των περιορισμών που έχουν τα δίκτυα IEEE 802.11 είναι η χρήση του φάσματος των συχνοτήτων Industrial Scientific Medical (ISM), η κατανάλωση ενέργειας, η απουσία σχεδιασμού (planning) του δικτύου και η χρήση μηχανισμών Carrier Sense Multiple Access (CSMA)».

Απάντηση:

Η πρόταση υπογραμμίζει διάφορους περιορισμούς των δικτύων IEEE 802.11, ιδίως στο πλαίσιο της χρήσης τους για εφαρμογές IoT. Ας εξετάσουμε λεπτομερώς καθέναν από αυτούς τους περιορισμούς:

1. Χρήση του φάσματος συχνοτήτων ISM (Industrial Scientific Medical)

Τα δίκτυα IEEE 802.11, συμπεριλαμβανομένου του Wi-Fi, λειτουργούν κυρίως στις ζώνες ISM (2,4 GHz και 5 GHz). Ενώ αυτές οι ζώνες είναι μη αδειοδοτημένες και ευρέως διαθέσιμες, είναι επίσης πολύ συμφορημένες. Αυτή η συμφόρηση μπορεί να οδηγήσει σε παρεμβολές από άλλες συσκευές όπως το Bluetooth, μικροκύματα και άλλα δίκτυα Wi-Fi, υποβαθμίζοντας δυνητικά την απόδοση. Σε περιβάλλοντα με πολύ κόσμο, οι παρεμβολές αυτές μπορεί να προκαλέσουν μειωμένους ρυθμούς δεδομένων, αυξημένη καθυστέρηση και συχνότερες αποσυνδέσεις, γεγονός που μπορεί να είναι προβληματικό για εφαρμογές που απαιτούν αξιόπιστη και συνεπή συνδεσιμότητα.

2. Κατανάλωση ενέργειας

Τα δίκτυα Wi-Fi έχουν συνήθως υψηλότερη κατανάλωση ενέργειας σε σύγκριση με άλλες ειδικές για το IoT ασύρματες τεχνολογίες, όπως το Zigbee (IEEE 802.15.4) ή το LoRaWAN. Αυτή η υψηλότερη κατανάλωση ενέργειας οφείλεται κυρίως στην ανάγκη διατήρησης υψηλών ρυθμών δεδομένων και υποστήριξης πολύπλοκων σχημάτων διαμόρφωσης (modulation schemes). Για τις συσκευές IoT που λειτουργούν με μπαταρία, η συχνή επαναφόρτιση ή αντικατάσταση της μπαταρίας μπορεί να είναι ανέφικτη, καθιστώντας την κατανάλωση ενέργειας σημαντικό περιορισμό. Το ζήτημα αυτό περιορίζει την καταλληλότητα των δικτύων IEEE 802.11 για πολλές εφαρμογές IoT που απαιτούν μεγάλη διάρκεια ζωής της μπαταρίας και ενεργειακή απόδοση.

3. Έλλειψη σχεδιασμού δικτύου

Τα δίκτυα Wi-Fi συχνά αναπτύσσονται χωρίς εκτεταμένο σχεδιασμό δικτύου, ιδίως σε οικιακά περιβάλλοντα και περιβάλλοντα μικρών γραφείων. Αυτή η έλλειψη σχεδιασμού μπορεί να οδηγήσει σε μη βέλτιστη κάλυψη, παρεμβολές και μη αποδοτική χρήση του διαθέσιμου φάσματος. Αντίθετα, τα δίκτυα κινητής τηλεφωνίας (cellular networks) και ορισμένα, ειδικά για το IoT, δίκτυα επωφελούνται από λεπτομερή σχεδιασμό και διαχείριση, εξασφαλίζοντας καλύτερες επιδόσεις και αξιοπιστία. Για εγκαταστάσεις IoT μεγάλης κλίμακας, ο ad-hoc

χαρακτήρας του σχεδιασμού του δικτύου Wi-Fi μπορεί να οδηγήσει σε προβλήματα με την επεκτασιμότητα και την κάλυψη, επηρεάζοντας τη συνολική αποτελεσματικότητα του δικτύου.

4. Χρήση μηχανισμών Carrier Sense Multiple Access (CSMA)

Τα δίκτυα Wi-Fi βασίζονται σε μηχανισμούς Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) για τη διαχείριση της πρόσβασης στο κοινόχρηστο μέσο επικοινωνίας. Αν και το CSMA/CA βοηθά στη μείωση των συγκρούσεων με την ακρόαση του καναλιού πριν από τη μετάδοση, δεν είναι εντελώς απαλλαγμένο από συγκρούσεις και μπορεί να οδηγήσει σε αναποτελεσματικότητα, ιδίως σε υψηλά φορτία κυκλοφορίας. Το πρόβλημα του κρυφού σταθμού (hidden terminal problem), όπου δύο συσκευές εκτός εμβέλειας συγκρούονται σε έναν κοινό δέκτη, και το πρόβλημα του εκτεθειμένου σταθμού (exposed terminal problem), όπου μια συσκευή αναβάλλει άσκοπα τη μετάδοση, είναι εγγενή προβλήματα του CSMA/CA. Τα προβλήματα αυτά μπορεί να οδηγήσουν σε μειωμένη απόδοση και αυξημένη καθυστέρηση, γεγονός που μπορεί να αποβεί επιζήμιο για τις ευαίσθητες στον χρόνο εφαρμογές IoT.

Πηγές: Διαφάνειες "W3.2 Slides - Introduction to Wireless and Mobile Networks" και"W6.1 Slides - IEEE 802.11 (Part 1)", όπως και γενικές γνώσεις για τις τεχνολογίες ασύρματης επικοινωνίας.

12. Να αναπτύξετε σύντομα τα βασικά χαρακτηριστικά που αφορούν τις επικοινωνίες των εφαρμογών στη «γεωργία ακριβείας» (precision agriculture) και στην «προληπτική συντήρηση» (predictive maintenance).

Απάντηση:

Γεωργία ακριβείας:

- **Δίκτυα αισθητήρων:** Η γεωργία ακριβείας βασίζεται σε ένα δίκτυο αισθητήρων που είναι κατανεμημένοι σε όλους τους αγρούς για την παρακολούθηση διαφόρων περιβαλλοντικών παραμέτρων, όπως η υγρασία του εδάφους, η θερμοκρασία, η υγρασία, τα επίπεδα θρεπτικών ουσιών και η υγεία των καλλιεργειών. Αυτοί οι αισθητήρες συλλέγουν συνεχώς δεδομένα και τα διαβιβάζουν σε ένα κεντρικό σύστημα για ανάλυση.
- **Ασύρματη συνδεσιμότητα:** Δεδομένης της μεγάλης έκτασης που καλύπτουν συχνά τα γεωργικά χωράφια, χρησιμοποιούνται συνήθως τεχνολογίες ασύρματης επικοινωνίας όπως το LoRaWAN, το NB-IoT και το Zigbee. Αυτές οι τεχνολογίες παρέχουν επικοινωνία μεγάλης εμβέλειας με χαμηλή κατανάλωση ενέργειας, γεγονός που τις καθιστά κατάλληλες για αισθητήρες που λειτουργούν με μπαταρίες.
- **Συλλογή και ανάλυση δεδομένων:** Τα δεδομένα που συλλέγονται από τους αισθητήρες μεταδίδονται σε μια cloud-based πλατφόρμα ή σε τοπικό server, όπου αναλύονται με τη χρήση αλγορίθμων ανάλυσης δεδομένων και μηχανικής μάθησης. Η ανάλυση αυτή βοηθά στη λήψη τεκμηριωμένων αποφάσεων σχετικά με την άρδευση, τη λίπανση, την καταπολέμηση των παρασίτων και τη συγκομιδή.

- **Παρακολούθηση σε πραγματικό χρόνο:** Η παρακολούθηση σε πραγματικό χρόνο επιτρέπει στους αγρότες να ανταποκρίνονται άμεσα στις αλλαγές των περιβαλλοντικών συνθηκών, αποτρέποντας ζημιές στις καλλιέργειες και βελτιστοποιώντας τη χρήση των πόρων. Οι ειδοποιήσεις μπορούν να αποστέλλονται στις κινητές συσκευές των αγροτών για άμεση δράση.
- **Αυτοματοποίηση και έλεγχος:** Η ενσωμάτωση με αυτοματοποιημένα συστήματα, όπως συστήματα άρδευσης, επιτρέπει τον ακριβή έλεγχο με βάση τα δεδομένα των αισθητήρων. Για παράδειγμα, ένα αυτοματοποιημένο σύστημα άρδευσης μπορεί να προσαρμόζει τα επίπεδα νερού σε πραγματικό χρόνο με βάση τις ενδείξεις υγρασίας του εδάφους, εξασφαλίζοντας τη βέλτιστη χρήση του νερού.

Προληπτική συντήρηση:

- **Αισθητήρες μηχανημάτων:** Η προληπτική συντήρηση βασίζεται σε αισθητήρες που είναι εγκατεστημένοι στα μηχανήματα για την παρακολούθηση κρίσιμων παραμέτρων, όπως οι δονήσεις, η θερμοκρασία, η πίεση και οι ακουστικές εκπομπές. Αυτοί οι αισθητήρες συλλέγουν συνεχώς δεδομένα για τον εντοπισμό ενδείξεων φθοράς ή πιθανών βλαβών.
- **Ασύρματη επικοινωνία:** Παρόμοια με τη γεωργία ακριβείας, η προγνωστική συντήρηση χρησιμοποιεί συχνά τεχνολογίες ασύρματης επικοινωνίας, όπως Wi-Fi, Bluetooth και δίκτυα κινητής τηλεφωνίας, για τη μετάδοση δεδομένων από αισθητήρες σε κεντρικά συστήματα παρακολούθησης. Η επιλογή της τεχνολογίας εξαρτάται από το περιβάλλον και τις ειδικές απαιτήσεις, όπως ο ρυθμός δεδομένων και η εμβέλεια.
- **Επεξεργασία και ανάλυση δεδομένων:** Τα δεδομένα που συλλέγονται από τους αισθητήρες μεταδίδονται σε ένα κεντρικό σύστημα ή σε μια πλατφόρμα νέφους, όπου επεξεργάζονται και αναλύονται με τη χρήση προηγμένων αλγορίθμων ανάλυσης και μηχανικής μάθησης. Αυτοί οι αλγόριθμοι μπορούν να εντοπίσουν μοτίβα και ανωμαλίες που υποδεικνύουν πιθανές βλάβες του εξοπλισμού.
- **Ειδοποιήσεις σε πραγματικό χρόνο:** Όταν το σύστημα εντοπίζει μια ανωμαλία ή μια κατάσταση που μπορεί να οδηγήσει σε βλάβη, στέλνει ειδοποιήσεις σε πραγματικό χρόνο στο προσωπικό συντήρησης. Αυτό επιτρέπει την έγκαιρη παρέμβαση, αποτρέποντας απρογραμμάτιστες διακοπές λειτουργίας και μειώνοντας το κόστος συντήρησης.
- **Ιστορικά δεδομένα και ανάλυση τάσεων:** Τα συστήματα προληπτικής συντήρησης χρησιμοποιούν επίσης ιστορικά δεδομένα για την πρόβλεψη μελλοντικών βλαβών και τη βελτιστοποίηση των προγραμμάτων συντήρησης.
- **Ενσωμάτωση με συστήματα διαχείρισης συντήρησης:** Τα συστήματα προγνωστικής συντήρησης συχνά ενσωματώνονται με μηχανογραφημένα συστήματα διαχείρισης συντήρησης (Computerized Maintenance Management Systems - CMMS) για τον εξορθολογισμό των ροών εργασίας συντήρησης.

Πηγές: Διαφάνειες "W1.1 Slides - Introduction to IoT" και "W3.1 Slides - Introduction to IoT (Part 1)", όπως και γενικές γνώσεις για τις εφαρμογές του IoT σε διάφορες βιομηχανίες.

13. Τι γνωρίζετε για το μηχανισμό Enhanced RTS/CTS στο πρωτόκολλο IEEE 802.11ac;

Απάντηση:

Το πρωτόκολλο IEEE 802.11ac, γνωστό και ως Wi-Fi 5, περιλαμβάνει αρκετές αναβαθμίσεις για τη βελτίωση των επιδόσεων σε σχέση με τα προηγούμενα πρότυπα Wi-Fi. Μια τέτοια αναβάθμιση είναι ο βελτιωμένος μηχανισμός Request to Send/Clear to Send (RTS/CTS). Ο μηχανισμός αυτός έχει σχεδιαστεί για να μετριάσει τα προβλήματα που σχετίζονται με την ασύρματη επικοινωνία, ιδίως αυτά που προκαλούνται από κρυφούς σταθμούς και συμφόρηση του δικτύου.

Βασικά χαρακτηριστικά του βελτιωμένου RTS/CTS στο IEEE 802.11ac:

- **Σκοπός:** Ο πρωταρχικός σκοπός του μηχανισμού RTS/CTS είναι η αποφυγή συγκρούσεων σε ένα ασύρματο δίκτυο. Αυτό είναι ιδιαίτερα σημαντικό σε περιβάλλοντα με υψηλή κυκλοφορία δικτύου και πολυάριθμες συσκευές, κάτι που είναι σύνηθες σε περιοχές όπου αναπτύσσεται το IEEE 802.11ac.
- **Βασική λειτουργία:** Σε μια τυπική ανταλλαγή RTS/CTS, ένας σταθμός (station - STA) που θέλει να μεταδώσει δεδομένα στέλνει ένα πλαίσιο RTS στο σημείο πρόσβασης (access point - AP). Εάν το AP είναι έτοιμο να λάβει, απαντά με ένα πλαίσιο CTS. Αυτή η ανταλλαγή δεσμεύει το μέσο, ενημερώνοντας τους άλλους σταθμούς να περιμένουν, μειώνοντας έτσι την πιθανότητα σύγκρουσης.
- **Ενισχυμένα χαρακτηριστικά στο 802.11ac:**
    - **Κράτηση καναλιού:** Ο βελτιωμένος μηχανισμός RTS/CTS στο IEEE 802.11ac μπορεί να κάνει κράτηση όχι μόνο ενός καναλιού, αλλά πολλαπλών καναλιών. Αυτό είναι ζωτικής σημασίας για τη λειτουργία του 802.11ac, η οποία συχνά περιλαμβάνει ευρύτερα κανάλια (π.χ. 80 MHz ή 160 MHz) σε σύγκριση με τα προηγούμενα πρότυπα.
    - **Επιλογή ρυθμού PHY:** Τα πλαίσια RTS/CTS στο 802.11ac μπορούν να μεταδοθούν σε διαφορετικούς φυσικούς ρυθμούς (physical rates - PHY). Αυτή η ευελιξία επιτρέπει στο δίκτυο να προσαρμόζεται καλύτερα στις ποικίλες συνθήκες και να βελτιστοποιεί την απόδοση.
    - **Μειωμένη επιβάρυνση:** Με τη χρήση μικρότερης διάρκειας για την ανταλλαγή RTS/CTS και την ενσωμάτωση άλλων βελτιώσεων αποδοτικότητας, ο βελτιωμένος μηχανισμός μειώνει την επιβάρυνση (overhead), γεγονός που συμβάλλει στη διατήρηση υψηλής απόδοσης.
- **Πρόβλημα κρυφού σταθμού:** Ο βελτιωμένος μηχανισμός RTS/CTS αντιμετωπίζει αποτελεσματικά το πρόβλημα του κρυφού σταθμού, όπου δύο συσκευές δεν μπορούν να ανιχνεύσουν η μία τις μεταδόσεις της άλλης λόγω απόστασης ή εμποδίων, αλλά μπορούν να προκαλέσουν συγκρούσεις σε έναν κοινό δέκτη. Με τη δέσμευση του μέσου μέσω των ανταλλαγών RTS/CTS, οι συγκρούσεις ελαχιστοποιούνται.

Πηγές: Διαφάνειες "W6.1 Slides - IEEE 802.11 (Part 1)" και "W3.2 Slides - Introduction to Wireless and Mobile Networks".

14. Να αναφέρετε σύντομα τρεις (3) ερευνητικές προκλήσεις για τα Ασύρματα Δίκτυα Αισθητήρων (WSNs); Ποιες είναι οι κυριότερες αιτίες ενεργειακής σπατάλης σε ένα WSN; *(παρόμοια με την ερώτηση 5)*

Απάντηση:

Τρεις ερευνητικές προκλήσεις για τα ασύρματα δίκτυα αισθητήρων (WSN)

- **Ενεργειακή απόδοση:** Μία από τις πρωταρχικές ερευνητικές προκλήσεις στα WSNs είναι η βελτιστοποίηση της κατανάλωσης ενέργειας. Οι κόμβοι αισθητήρων λειτουργούν συχνά με μπαταρίες και η αντικατάσταση ή η επαναφόρτιση των μπαταριών σε απομακρυσμένες ή δυσπρόσιτες τοποθεσίες μπορεί να είναι ανέφικτη. Η έρευνα επικεντρώνεται στην ανάπτυξη ενεργειακά αποδοτικών πρωτοκόλλων, υλικού χαμηλής κατανάλωσης ενέργειας και τεχνικών συλλογής ενέργειας για την παράταση της λειτουργικής ζωής του δικτύου.
- **Επεκτασιμότητα και διαχείριση δικτύου:** Καθώς τα WSN μπορεί να αποτελούνται από μεγάλο αριθμό κόμβων, η αποτελεσματική διαχείριση ενός τέτοιου δικτύου αποτελεί σημαντική πρόκληση. Η έρευνα στρέφεται προς κλιμακούμενες αρχιτεκτονικές δικτύων, αποτελεσματικές μεθόδους συγκέντρωσης δεδομένων και πρωτόκολλα αυτοοργάνωσης που μπορούν να χειριστούν μεγάλης κλίμακας αναπτύξεις χωρίς συμβιβασμούς στην απόδοση ή την αξιοπιστία.
- **Ασφάλεια και προστασία της ιδιωτικής ζωής:** Η εξασφάλιση ασφαλούς επικοινωνίας στα WSNs είναι κρίσιμη, ιδίως όταν αυτά αναπτύσσονται σε ευαίσθητες εφαρμογές όπως η στρατιωτική επιτήρηση (military surveillance) ή η υγειονομική περίθαλψη. Η έρευνα σε αυτόν τον τομέα περιλαμβάνει την ανάπτυξη ελαφριών μεθόδων κρυπτογράφησης, ασφαλών πρωτοκόλλων δρομολόγησης και συστημάτων ανίχνευσης εισβολών που μπορούν να προστατεύσουν το δίκτυο από διάφορες απειλές ασφαλείας, διατηρώντας παράλληλα χαμηλή κατανάλωση ενέργειας.

Κύριες αιτίες σπατάλης ενέργειας σε ένα WSN

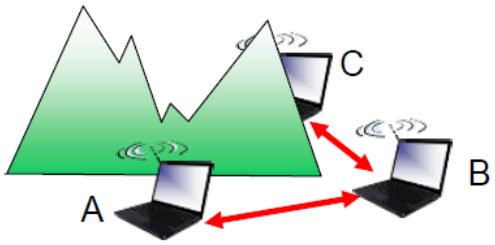
- **Αδρανής ακρόαση:** Οι κόμβοι καταναλώνουν ενέργεια ακούγοντας το κανάλι για πιθανή επικοινωνία, ακόμη και όταν δεν μεταδίδουν ή λαμβάνουν ενεργά δεδομένα. Αυτή είναι μια σημαντική πηγή σπατάλης ενέργειας.
- **Overhearing:** Οι κόμβοι μπορεί να καταναλώνουν ενέργεια λαμβάνοντας πακέτα που προορίζονται για άλλους κόμβους.
- **Συγκρούσεις πακέτων:** Όταν δύο κόμβοι μεταδίδουν ταυτόχρονα, τα πακέτα τους μπορεί να συγκρουστούν, με αποτέλεσμα να απαιτούνται επαναμεταδόσεις και να σπαταλάται ενέργεια.
- **Υπερφόρτωση πακέτων ελέγχου:** Η αποστολή πακέτων ελέγχου για τη διαχείριση του δικτύου (π.χ. ενημερώσεις δρομολόγησης, μηνύματα συγχρονισμού) καταναλώνει ενέργεια που διαφορετικά θα μπορούσε να χρησιμοποιηθεί για τη μετάδοση δεδομένων.
- **Υψηλή ισχύς μετάδοσης:** Η μετάδοση σε υψηλότερα επίπεδα ισχύος από τα απαραίτητα αυξάνει την κατανάλωση ενέργειας.

Πηγές: Διαφάνειες "W5.1 Slides - Ad hoc Sensor Networks" και "W3.1 Slides - Introduction to IoT (Part 1)".

15. Να περιγράψετε σύντομα το πρόβλημα του κρυφού σταθμού (hidden station problem) στα ασύρματα τοπικά δίκτυα. Με ποιον μηχανισμό επιλύεται το εν λόγω πρόβλημα; Ποια είναι η επίδραση και πότε ενεργοποιείται αυτός ο μηχανισμός;

Απάντηση:

Το πρόβλημα του κρυφού σταθμού εμφανίζεται στα ασύρματα τοπικά δίκτυα (WLAN) όταν δύο ή περισσότερες συσκευές (σταθμοί) που δεν βρίσκονται η μία εντός της εμβέλειας μετάδοσης της άλλης επικοινωνούν με ένα κοινό σημείο πρόσβασης (access point - AP) ή έναν άλλο σταθμό. Αυτοί οι σταθμοί είναι "κρυμμένοι" ο ένας από τον άλλο, δηλαδή δεν μπορούν να ανιχνεύσουν ο ένας τις μεταδόσεις του άλλου. Αυτό μπορεί να οδηγήσει σε συγκρούσεις πακέτων στο AP ή στο σταθμό λήψης, καθώς κάθε κρυμμένος σταθμός μπορεί να προσπαθήσει να μεταδώσει ταυτόχρονα χωρίς να γνωρίζει τη δραστηριότητα του άλλου.



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B

Μηχανισμός επίλυσης του προβλήματος του κρυφού σταθμού: RTS/CTS

Ο μηχανισμός Request to Send/Clear to Send (RTS/CTS) χρησιμοποιείται για την αντιμετώπιση του προβλήματος του κρυφού σταθμού. Ακολουθεί ο τρόπος λειτουργίας του:

- **Πλαίσιο RTS:** Όταν ένας σταθμός (σταθμός A) θέλει να μεταδώσει δεδομένα, στέλνει πρώτα ένα πλαίσιο RTS στο AP ή στο σταθμό λήψης (σταθμός B).

- **Πλαίσιο CTS:** Εάν το μέσο είναι ελεύθερο και ο σταθμός Β είναι έτοιμος να λάβει, απαντά με ένα πλαίσιο CTS. Αυτό το πλαίσιο λαμβάνεται τόσο από τον σταθμό Α όσο και από οποιονδήποτε άλλο σταθμό (σταθμό C) εντός της εμβέλειας του σταθμού Β.
- **Μετάδοση δεδομένων:** Μετά τη λήψη του πλαισίου CTS, ο σταθμός Α συνεχίζει τη μετάδοση δεδομένων. Ο σταθμός C, έχοντας ακούσει το πλαίσιο CTS, γνωρίζει να αναβάλει τη μετάδοσή του μέχρι το κανάλι να είναι και πάλι ελεύθερο.

Επίδραση: Ο μηχανισμός RTS/CTS ουσιαστικά δεσμεύει το κανάλι για μια συγκεκριμένη μετάδοση δεδομένων, αποτρέποντας άλλους σταθμούς από το να μεταδίδουν ταυτόχρονα και να προκαλούν συγκρούσεις. Εξασφαλίζει ότι όλοι οι σταθμοί εντός της εμβέλειας μετάδοσης του AP ή του σταθμού λήψης γνωρίζουν την επικείμενη ανταλλαγή δεδομένων, μειώνοντας έτσι την πιθανότητα συγκρούσεων που προκαλούνται από κρυφούς σταθμούς.

Ενεργοποίηση: Ο μηχανισμός RTS/CTS συνήθως ενεργοποιείται υπό συγκεκριμένες συνθήκες, όπως:

- **Μεγάλα πακέτα δεδομένων:** Κατά τη μετάδοση μεγάλων πακέτων δεδομένων, καθώς οι συγκρούσεις θα ήταν πιο δαπανηρές από άποψη χρόνου και ενέργειας επαναμετάδοσης.
- **Περιβάλλοντα υψηλής κίνησης:** Σε δίκτυα με υψηλή κυκλοφορία ή πολυάριθμους κρυφούς σταθμούς, για την αποτελεσματικότερη διαχείριση της πρόσβασης στο μέσο.
- **Κατώφλι διαμόρφωσης:** Οι διαχειριστές δικτύου μπορούν να διαμορφώσουν ένα κατώτατο όριο μεγέθους πακέτου πάνω από το οποίο χρησιμοποιείται το RTS/CTS. Αυτό εξασφαλίζει ότι ο μηχανισμός χρησιμοποιείται μόνο όταν είναι επωφελής, εξισορροπώντας την επιβάρυνση των ανταλλαγών RTS/CTS με την ανάγκη αποφυγής συγκρούσεων.

Πηγές: Διαφάνειες "W3.2 Slides - Introduction to Wireless and Mobile Networks" και "W6.1 Slides - IEEE 802.11 (Part 1)".

16. Είναι απαραίτητοι και οι δυο μηχανισμοί ανίχνευσης (virtual και physical carrier sensing) στα πρωτόκολλα IEEE 802.11; Δικαιολογείστε την απάντηση σας. Επιπλέον, για ποιους λόγους δεν επιτυγχάνεται ο ονομαστικός ρυθμός μετάδοσης; (π.χ. 6,9 Gbps για το IEEE 802.11ac).

Απάντηση:

Αναγκαιότητα και των δύο μηχανισμών ανίχνευσης στα πρωτόκολλα IEEE 802.11

Τόσο η ανίχνευση εικονικών φορέων όσο και η ανίχνευση φυσικών φορέων αποτελούν βασικά συστατικά των πρωτοκόλλων IEEE 802.11, διαδραματίζοντας κρίσιμο ρόλο στη διασφάλιση αποτελεσματικής και αξιόπιστης επικοινωνίας στα ασύρματα δίκτυα. Η ανίχνευση φυσικού φορέα περιλαμβάνει την ακρόαση του ασύρματου καναλιού για να ανιχνεύσει αν είναι ελεύθερο ή κατειλημμένο, με βάση τα επίπεδα ενέργειας του σήματος. Εάν το κανάλι είναι κατειλημμένο, ο

σταθμός αναβάλλει τη μετάδοσή του. Η εικονική ανίχνευση φορέα, από την άλλη πλευρά, χρησιμοποιεί το διάνυσμα κατανομής δικτύου (Network Allocation Vector - NAV), το οποίο είναι ένας χρονοδιακόπτης που υποδεικνύει την περίοδο κατά την οποία το κανάλι θα είναι κατειλημμένο, με βάση πληροφορίες από τα πλαίσια RTS ή CTS. Αυτό βοηθά στη διαχείριση της πρόσβασης στο μέσο, ιδιαίτερα σε σενάρια όπου η φυσική ανίχνευση φορέα από μόνη της δεν επαρκεί.

Η αναγκαιότητα και των δύο μηχανισμών έγκειται στις συμπληρωματικές λειτουργίες τους. Η φυσική ανίχνευση από μόνη της δεν μπορεί να αντιμετωπίσει όλα τα σενάρια, ιδίως εκείνα που περιλαμβάνουν κρυφούς κόμβους. Η εικονική ανίχνευση φέροντος μετριάζει το πρόβλημα των κρυφών κόμβων εξασφαλίζοντας ότι οι σταθμοί που είναι κρυμμένοι μεταξύ τους γνωρίζουν τις τρέχουσες μεταδόσεις και αναβάλλουν τις δικές τους αναλόγως. Αυτός ο συνδυασμός μειώνει σημαντικά την πιθανότητα συγκρούσεων, βελτιώνοντας τη συνολική απόδοση και αποδοτικότητα του δικτύου. Ενώ η φυσική ανίχνευση φέροντος παρέχει άμεση ανίχνευση της κατάστασης του καναλιού, η εικονική ανίχνευση φέροντος διαχειρίζεται τον προγραμματισμό της μετάδοσης, καθιστώντας και τους δύο μηχανισμούς απαραίτητους.

Λόγοι μη επίτευξης του ονομαστικού ρυθμού μετάδοσης

Ο ονομαστικός ρυθμός μετάδοσης πρωτοκόλλων όπως το IEEE 802.11ac, ο οποίος μπορεί να φτάσει έως και τα 6,9 Gbps, συχνά δεν επιτυγχάνεται σε πρακτικά σενάρια λόγω διαφόρων παραγόντων. Οι παρεμβολές σήματος και ο θόρυβος από άλλες συσκευές και φυσικά εμπόδια μπορούν να υποβαθμίσουν την ποιότητα του σήματος, οδηγώντας σε χαμηλότερους πραγματικούς ρυθμούς μετάδοσης. Τα γενικά έξοδα του δικτύου, συμπεριλαμβανομένων των πλαισίων ελέγχου (RTS/CTS, ACK), των επικεφαλίδων του επιπέδου MAC και των πλαισίων διαχείρισης, καταναλώνουν ένα μέρος του διαθέσιμου εύρους ζώνης, μειώνοντας τον πραγματικό ρυθμό δεδομένων. Η απόσταση και η εξασθένηση του σήματος (signal attenuation) παίζουν επίσης ρόλο, καθώς οι συσκευές που βρίσκονται σε μεγαλύτερη απόσταση από το σημείο πρόσβασης έχουν ασθενέστερα σήματα και χαμηλότερους ρυθμούς δεδομένων.

Επιπλέον, η συμφόρηση του καναλιού σε περιβάλλοντα με πολλές συσκευές μπορεί να οδηγήσει σε αυξημένες συγκρούσεις και επαναμεταδόσεις, μειώνοντας τον πραγματικό ρυθμό δεδομένων. Περιβαλλοντικοί παράγοντες όπως τοίχοι, δάπεδα, υγρασία και θερμοκρασία μπορούν να επηρεάσουν τη διάδοση και την εξασθένηση του σήματος. Οι ανεπάρκειες του πρωτοκόλλου, όπως τα μη βέλτιστα σχήματα διαμόρφωσης και κωδικοποίησης, επηρεάζουν περαιτέρω την απόδοση. Οι δυνατότητες των συσκευών ποικίλλουν επίσης, με ορισμένες συσκευές να μην μπορούν να υποστηρίξουν τα υψηλότερα σχήματα διαμόρφωσης και κωδικοποίησης που απαιτούνται για μέγιστους ρυθμούς. Τέλος, οι κανονιστικοί περιορισμοί (regulatory constraints) και η διαθεσιμότητα συνεχούς φάσματος μπορούν να περιορίσουν τη χρήση ευρύτερων καναλιών (π.χ. 80 MHz ή 160 MHz) που απαιτούνται για την επίτευξη υψηλότερων ρυθμών, ιδίως σε πολυσύχναστες ζώνες συχνοτήτων.

Πηγές: Διαφάνειες "W3.2 Slides - Introduction to Wireless and Mobile Networks" και "W6.1 Slides - IEEE 802.11 (Part 1)".

17. Να αιτολογήσετε σύντομα ποιοι δείκτες απόδοσης (KPIs) είναι σημαντικοί σε 5G εφαρμογές του Απτού Διαδικτύου (Tactile Internet) και της αυτόνομης οδήγησης (autonomous driving).

Απάντηση:

Απτικό Διαδίκτυο:

- **Καθυστέρηση:** Η εξαιρετικά χαμηλή καθυστέρηση είναι ζωτικής σημασίας για το απτικό διαδίκτυο, όπου απαιτείται επικοινωνία σε πραγματικό χρόνο και απτική ανατροφοδότηση. Εφαρμογές όπως η απομακρυσμένη χειρουργική, η εικονική πραγματικότητα και ο βιομηχανικός αυτοματισμός χρειάζονται λανθάνουσες περιόδους από άκρο σε άκρο μικρότερες από 1 χιλιοστό του δευτερολέπτου για να λειτουργήσουν αποτελεσματικά.
- **Αξιοπιστία:** Η υψηλή αξιοπιστία εξασφαλίζει ότι τα δεδομένα μεταδίδονται με ακρίβεια και συνέπεια χωρίς σφάλματα. Αυτό είναι ζωτικής σημασίας για εφαρμογές όπου ακόμη και μικρές διακοπές ή σφάλματα μπορούν να έχουν σημαντικές συνέπειες, όπως στις ιατρικές διαδικασίες ή στην κατασκευή ακριβείας.
- **Ρυθμός δεδομένων:** Οι επαρκείς ρυθμοί δεδομένων είναι απαραίτητοι για την υποστήριξη του μεγάλου όγκου ανταλλαγής δεδομένων που απαιτείται για τον έλεγχο και την ανατροφοδότηση σε πραγματικό χρόνο. Αν και δεν είναι τόσο απαιτητικές όσο ορισμένες άλλες εφαρμογές, απαιτείται επαρκές εύρος ζώνης για να διασφαλιστεί η ομαλή λειτουργία και η απόκριση.
- **Διαθεσιμότητα:** Η συνεχής διαθεσιμότητα του δικτύου είναι απαραίτητη για την αποφυγή διακοπών των υπηρεσιών. Για το Tactile Internet, το οποίο βασίζεται στην αλληλεπίδραση σε πραγματικό χρόνο, οποιαδήποτε διακοπή λειτουργίας μπορεί να οδηγήσει σε λειτουργικές αποτυχίες.

Αυτόνομη οδήγηση:

- **Καθυστέρηση:** Η εξαιρετικά χαμηλή καθυστέρηση είναι ζωτικής σημασίας για την αυτόνομη οδήγηση, ώστε να διασφαλίζεται η επικοινωνία σε πραγματικό χρόνο μεταξύ των οχημάτων (V2V) και με την υποδομή (V2I). Η χαμηλή καθυστέρηση επιτρέπει την άμεση ανταπόκριση στις δυναμικές συνθήκες οδήγησης και στους πιθανούς κινδύνους, πράγμα που είναι ζωτικής σημασίας για την ασφάλεια.
- **Αξιοπιστία:** Η υψηλή αξιοπιστία είναι απαραίτητη για να διασφαλιστεί ότι τα κρίσιμα δεδομένα, όπως οι πληροφορίες αισθητήρων και οι εντολές ελέγχου, μεταδίδονται χωρίς σφάλματα. Τα αυτόνομα οχήματα εξαρτώνται από ακριβή και έγκαιρα δεδομένα για τη λήψη ασφαλών αποφάσεων οδήγησης.
- **Ρυθμός δεδομένων:** Οι υψηλοί ρυθμοί δεδομένων είναι σημαντικοί για τη διαχείριση των μεγάλων όγκων δεδομένων που παράγονται από πολλαπλούς αισθητήρες, κάμερες και συστήματα LIDAR στα αυτόνομα οχήματα. Τα δεδομένα αυτά πρέπει να επεξεργάζονται και να ανταλλάσσονται γρήγορα, ώστε να είναι δυνατή η λήψη αποφάσεων σε πραγματικό χρόνο.
- **Κάλυψη:** Η εκτεταμένη κάλυψη δικτύου είναι απαραίτητη για την υποστήριξη της αυτόνομης οδήγησης σε διάφορα περιβάλλοντα, συμπεριλαμβανομένων των αστικών, προαστιακών και αγροτικών περιοχών. Η συνεπής συνδεσιμότητα διασφαλίζει ότι τα

οχήματα μπορούν να διατηρούν επικοινωνία με άλλα οχήματα και υποδομές ανά πάσα στιγμή.
- **Ασφάλεια:** Τα ισχυρά μέτρα ασφαλείας είναι κρίσιμα για την προστασία της ακεραιότητας των δεδομένων και του απορρήτου των επικοινωνιών στην αυτόνομη οδήγηση. Αυτό περιλαμβάνει την προστασία από επιθέσεις στον κυβερνοχώρο που θα μπορούσαν δυνητικά να θέσουν σε κίνδυνο τον έλεγχο και την ασφάλεια των οχημάτων, αλλά και των επιβατών τους.

Πηγές: Διαφάνειες "W3.1 Slides - Introduction to IoT (Part 1)" και "W9.1 Slides - Open Challenges", καθώς και γενικές γνώσεις και πληροφορίες προερχόμενες από τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunication Union - ITU).

ΘΕΜΑ 2

Στο σχεδιασμό μιας εφαρμογής IoT για έξυπνο σπίτι, απαντήστε επαρκώς στις παρακάτω ερωτήσεις:

1. Περιγράψτε ενδεικτικά IoT στοιχεία (συσκευές) που θα περιλαμβάνει η εφαρμογή που θα σχεδιάσετε.

Απάντηση:

- **Έξυπνοι θερμοστάτες:** Αυτές οι συσκευές ελέγχουν τα συστήματα θέρμανσης και ψύξης του σπιτιού, ρυθμίζοντας τις θερμοκρασίες με βάση τις προτιμήσεις του χρήστη και τις εισόδους των αισθητήρων.
- **Έξυπνα φώτα:** Τα συνδεδεμένα συστήματα φωτισμού μπορούν να ελέγχονται εξ αποστάσεως και να προγραμματίζονται να λειτουργούν με βάση την ώρα της ημέρας ή την πληρότητα, ενισχύοντας την άνεση και την ενεργειακή απόδοση.
- **Έξυπνες κλειδαριές:** Παρέχουν αυξημένη ασφάλεια, επιτρέποντας το απομακρυσμένο κλείδωμα/ξεκλείδωμα και την παρακολούθηση της κατάστασης της πόρτας. Συχνά περιλαμβάνουν χαρακτηριστικά όπως είσοδος χωρίς κλειδί και ενσωμάτωση με άλλα συστήματα ασφαλείας.
- **Έξυπνες κάμερες:** Οι κάμερες ασφαλείας με χαρακτηριστικά όπως η ανίχνευση κίνησης, η νυχτερινή όραση και η απομακρυσμένη προβολή συμβάλλουν στη διασφάλιση της ασφάλειας και της προστασίας του σπιτιού.
- **Έξυπνες συσκευές:** Συσκευές όπως έξυπνα ψυγεία, πλυντήρια ρούχων και φούρνοι μπορούν να παρακολουθούνται και να ελέγχονται εξ αποστάσεως, προσφέροντας ευκολία και πιθανή εξοικονόμηση ενέργειας.
- **Φωνητικοί βοηθοί:** Συσκευές όπως το Amazon Echo ή το Google Home λειτουργούν ως κεντρικοί κόμβοι για τον έλεγχο διαφόρων έξυπνων οικιακών συσκευών μέσω φωνητικών εντολών.
- **Έξυπνες πρίζες:** Αυτά επιτρέπουν τον απομακρυσμένο έλεγχο των συνδεδεμένων συσκευών, συμβάλλοντας στη διαχείριση της κατανάλωσης ενέργειας και στην ευκολία.
- **Έξυπνοι συναγερμοί:** Ενσωματωμένοι ανιχνευτές καπνού, CO2 και αισθητήρες διαρροής νερού που μπορούν να στέλνουν ειδοποιήσεις στα smartphones των χρηστών για άμεση δράση.

2. Στο 2ο βήμα σχεδιασμού (στρατηγική ανάπτυξης) θα επιλέξετε μια έτοιμη πλατφόρμα (ποια) ή προσαρμοσμένη λύση και γιατί;

Απάντηση:

Για τη στρατηγική ανάπτυξης, η επιλογή μιας έτοιμης πλατφόρμας, όπως η Google Nest ή η Amazon Alexa, είναι συχνά πιο συμφέρουσα για μια έξυπνη οικιακή εφαρμογή IoT. Αυτές οι πλατφόρμες προσφέρουν πολλά πλεονεκτήματα:

- **Συμβατότητα:** Οι καθιερωμένες πλατφόρμες όπως η Google Nest και η Amazon Alexa υποστηρίζουν ένα ευρύ φάσμα συσκευών και υπηρεσιών τρίτων, εξασφαλίζοντας απρόσκοπτη ενσωμάτωση και συμβατότητα.
- **Επεκτασιμότητα:** Οι έτοιμες πλατφόρμες είναι σχεδιασμένες ώστε να κλιμακώνονται εύκολα, φιλοξενώντας την προσθήκη νέων συσκευών και υπηρεσιών ανάλογα με τις ανάγκες, χωρίς να απαιτείται εκτεταμένη προσαρμοσμένη ανάπτυξη.
- **Ασφάλεια και ενημερώσεις:** Αυτές οι πλατφόρμες επωφελούνται από τακτικές ενημερώσεις ασφαλείας και βελτιώσεις που παρέχονται από μεγάλες, εξειδικευμένες ομάδες, διασφαλίζοντας ότι το σύστημα παραμένει ασφαλές και ενημερωμένο με τα τελευταία χαρακτηριστικά.
- **Αποδοτικότητα χρόνου και κόστους:** Η χρήση μιας υπάρχουσας πλατφόρμας μειώνει το χρόνο και το κόστος που σχετίζονται με την ανάπτυξη μιας προσαρμοσμένης λύσης από το μηδέν. Επιτρέπει στους προγραμματιστές να επικεντρωθούν στην προσαρμογή και τη βελτίωση της εφαρμογής και όχι στην κατασκευή της υποκείμενης υποδομής.
- **Εμπειρία χρήστη:** Οι έτοιμες πλατφόρμες διαθέτουν καθιερωμένες διεπαφές χρήστη με τις οποίες οι χρήστες είναι ήδη εξοικειωμένοι, μειώνοντας την καμπύλη εκμάθησης και αυξάνοντας την υιοθέτηση από τους χρήστες.

3. Στο 6ο Βήμα σχεδιασμού (Αποθήκευση δεδομένων) θα επιλέξετε αποθήκευση στο cloud ή τοπικά (edge computing) και γιατί;

Απάντηση:

Στο 6ο βήμα σχεδιασμού (Αποθήκευση δεδομένων), η αποθήκευση στο cloud είναι γενικά η προτιμώμενη επιλογή για μια έξυπνη οικιακή εφαρμογή IoT. Οι λόγοι περιλαμβάνουν:

- **Επεκτασιμότητα:** Η αποθήκευση στο cloud παρέχει πρακτικά απεριόριστη χωρητικότητα αποθήκευσης, επιτρέποντας την εύκολη κλιμάκωση καθώς αυξάνεται ο αριθμός των συσκευών και ο όγκος των δεδομένων.
- **Προσβασιμότητα:** Τα δεδομένα που είναι αποθηκευμένα στο cloud είναι προσβάσιμα από οπουδήποτε και ανά πάσα στιγμή, παρέχοντας στους χρήστες παρακολούθηση σε πραγματικό χρόνο και έλεγχο των συσκευών έξυπνου σπιτιού τους μέσω εφαρμογών για κινητά τηλέφωνα ή διεπαφών ιστού.
- **Συντήρηση και αξιοπιστία:** Οι πάροχοι υπηρεσιών cloud αναλαμβάνουν τη συντήρηση, τα αντίγραφα ασφαλείας και την αποκατάσταση καταστροφών, εξασφαλίζοντας υψηλή διαθεσιμότητα και αξιοπιστία χωρίς να απαιτείται σημαντική επένδυση υποδομής από τον χρήστη.

- **Ενσωμάτωση με υπηρεσίες cloud:** Η αποθήκευση στο cloud επιτρέπει την απρόσκοπτη ενσωμάτωση με διάφορες υπηρεσίες που βασίζονται στο cloud, όπως η ανάλυση δεδομένων, η μηχανική μάθηση και οι προηγμένες πλατφόρμες διαχείρισης IoT, ενισχύοντας τη λειτουργικότητα και την ευφυΐα του συστήματος έξυπνου σπιτιού.
- **Αποδοτικότητα κόστους:** Οι λύσεις αποθήκευσης στο σύννεφο λειτουργούν συχνά σε μοντέλο pay-as-you-go, επιτρέποντας στους χρήστες να πληρώνουν μόνο για τον αποθηκευτικό χώρο και τις υπηρεσίες που χρησιμοποιούν, γεγονός που μπορεί να είναι πιο αποδοτικό από τη διατήρηση τοπικών server.

4. Ποια θεωρείτε ως σημαντικά προβλήματα ασφάλειας για την παραπάνω IoT εφαρμογή και γιατί;

Απάντηση:

Για να διασφαλιστεί η ασφάλεια και η ακεραιότητα μιας εφαρμογής IoT για έξυπνα σπίτια, πρέπει να αντιμετωπιστούν διάφορα σημαντικά ζητήματα ασφάλειας:

- **Κρυπτογράφηση δεδομένων:** Όλα τα δεδομένα που μεταδίδονται μεταξύ των συσκευών και του cloud πρέπει να κρυπτογραφούνται για να προστατεύονται από υποκλοπή και αλλοίωση από μη εξουσιοδοτημένα μέρη/πρόσωπα. Αυτό περιλαμβάνει τόσο τα δεδομένα σε κατάσταση ηρεμίας όσο και τα δεδομένα κατά τη μεταφορά.
- **Αυθεντικοποίηση και εξουσιοδότηση:** Θα πρέπει να εφαρμόζονται ισχυροί μηχανισμοί ελέγχου ταυτότητας, όπως ο έλεγχος ταυτότητας δύο παραγόντων (2FA), ώστε να διασφαλίζεται ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση και να ελέγχουν τις έξυπνες οικιακές συσκευές. Επιπλέον, ο έλεγχος πρόσβασης βάσει ρόλων (RBAC) μπορεί να περιορίσει την πρόσβαση σε ευαίσθητες λειτουργίες με βάση τους ρόλους των χρηστών.
- **Ασφάλεια συσκευών:** Η διασφάλιση ότι όλες οι συσκευές διαθέτουν ενημερωμένο υλικολογισμικό και security patches είναι ζωτικής σημασίας για την προστασία από ευπάθειες που θα μπορούσαν να αξιοποιηθούν από επιτιθέμενους. Οι αυτόματες ενημερώσεις και οι μηχανισμοί ασφαλούς εκκίνησης μπορούν να βοηθήσουν στη διατήρηση της ασφάλειας των συσκευών.
- **Ασφάλεια δικτύου:** Η διασφάλιση του οικιακού δικτύου με ισχυρά τείχη προστασίας, συστήματα ανίχνευσης εισβολών και ισχυρή κρυπτογράφηση Wi-Fi (π.χ. WPA3) μπορεί να αποτρέψει τη μη εξουσιοδοτημένη πρόσβαση στο δίκτυο και τις συνδεδεμένες συσκευές.
- **Απόρρητο:** Η προστασία του απορρήτου των δεδομένων των χρηστών είναι απαραίτητη, ιδίως δεδομένης της ευαίσθητης φύσης των δεδομένων που συλλέγονται από τις έξυπνες οικιακές συσκευές. Η εφαρμογή αυστηρών πολιτικών χειρισμού δεδομένων και η διασφάλιση της συμμόρφωσης με τους κανονισμούς περί προστασίας της ιδιωτικής ζωής (π.χ. GDPR) μπορούν να συμβάλουν στην προστασία της ιδιωτικής ζωής των χρηστών.
- **Φυσική ασφάλεια:** Η φυσική πρόσβαση στις συσκευές θα πρέπει να περιορίζεται για την αποφυγή αλλοίωσης. Αυτό περιλαμβάνει την εξασφάλιση των έξυπνων κλειδαριών και των καμερών από μη εξουσιοδοτημένη πρόσβαση ή φυσική χειραγώγηση.

ΘΕΜΑ 3

Ένα όχημα χωρίς οδηγό θα πρέπει να μπορεί να λειτουργεί, συλλέγοντας και επεξεργάζοντας δεδομένα (από αισθητήρες και Internet services), σε πραγματικό χρόνο και μάλιστα με ελάχιστο χρόνο απόκρισης. Για αυτό το IoT περιβάλλον, απαντήστε επαρκώς στις παρακάτω ερωτήσεις:

1. Περιγράψτε για κάθε ένα από τα πέντε επίπεδα του IoT OSI (END POINTS, CONNECTIVITY, MIDDLEWARE, IOT SERVICES, APPS) ενδεικτικά τι μπορεί να περιέχει ώστε να λειτουργεί με επάρκεια και ασφάλεια το όχημα χωρίς οδηγό; (~250 λέξεις)

   Απάντηση:

   End Points: Αυτό το επίπεδο περιλαμβάνει όλους τους αισθητήρες και τους ενεργοποιητές που είναι ενσωματωμένοι στο όχημα χωρίς οδηγό. Βασικά στοιχεία είναι το LIDAR, το RADAR, οι κάμερες, οι αισθητήρες υπερήχων και οι μονάδες GPS. Αυτοί οι αισθητήρες συλλέγουν δεδομένα σε πραγματικό χρόνο για το περιβάλλον του οχήματος, συμπεριλαμβανομένων των εμποδίων, των οδικών συνθηκών και του εντοπισμού θέσης. Οι ενεργοποιητές περιλαμβάνουν συστήματα πέδησης, συστήματα οδήγησης και έλεγχο του γκαζιού.

   Connectivity: Αυτό το επίπεδο παρέχει την υποδομή επικοινωνίας που είναι απαραίτητη για τη μετάδοση δεδομένων. Περιλαμβάνει ασύρματες τεχνολογίες όπως το 5G, το Wi-Fi και την επικοινωνία V2X (Vehicle-to-Everything), επιτρέποντας τη γρήγορη και αξιόπιστη ανταλλαγή δεδομένων μεταξύ του οχήματος, άλλων οχημάτων και της υποδομής.

   Middleware: Το επίπεδο ενδιάμεσου λογισμικού διαχειρίζεται την ενσωμάτωση και την επεξεργασία δεδομένων. Περιλαμβάνει συστήματα συγκέντρωσης, φιλτραρίσματος και προεπεξεργασίας δεδομένων που διαχειρίζονται τον τεράστιο όγκο δεδομένων από διάφορους αισθητήρες. Το ενδιάμεσο λογισμικό υποστηρίζει επίσης πρωτόκολλα επικοινωνίας, αποθήκευση δεδομένων και υπηρεσίες ασφαλείας, διασφαλίζοντας ότι τα δεδομένα είναι συνεπή, αξιόπιστα και έτοιμα για ανάλυση.

   IoT Services: Αυτό το στρώμα παρέχει προηγμένες υπηρεσίες, όπως ανάλυση δεδομένων σε πραγματικό χρόνο, αλγόριθμους μηχανικής μάθησης και διαδικασίες λήψης αποφάσεων. Αυτές οι υπηρεσίες ερμηνεύουν τα δεδομένα αισθητήρων, προβλέπουν πιθανούς κινδύνους και δημιουργούν εντολές οδήγησης. Παραδείγματα περιλαμβάνουν τον προγραμματισμό διαδρομής, την ανίχνευση εμποδίων, τη διαχείριση της κυκλοφορίας και τη διάγνωση οχημάτων.

   Apps: Το επίπεδο εφαρμογών αποτελείται από διεπαφές χρήστη και εφαρμογές που αλληλεπιδρούν με τα συστήματα του οχήματος. Αυτό περιλαμβάνει τον πίνακα οργάνων του χρήστη, τα συστήματα πλοήγησης και τις εφαρμογές για κινητά τηλέφωνα για απομακρυσμένη παρακολούθηση και έλεγχο. Οι εφαρμογές παρέχουν επίσης ενημερώσεις σχετικά με την κατάσταση και την απόδοση του οχήματος, βελτιώνοντας την εμπειρία του χρήστη και την ασφάλεια.

2. Ποια θεωρείτε ως σημαντικά προβλήματα ασφάλειας στο παραπάνω περιβάλλον. Στο 2ο επίπεδο του IoT OSI (CONNECTIVITY) από πλευράς πρωτοκόλλων ασφάλειας τι θα μπορούσε να περιέχεται (~150 λέξεις)

Απάντηση:

Προβλήματα ασφαλείας: Τα βασικά ζητήματα ασφάλειας σε ένα περιβάλλον οχημάτων χωρίς οδηγό περιλαμβάνουν την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των δεδομένων. Οι επιθέσεις στον κυβερνοχώρο, όπως η παραβίαση των συστημάτων ελέγχου των οχημάτων, μπορεί να έχουν σοβαρές συνέπειες. Η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα, όπως η τοποθεσία και οι προσωπικές πληροφορίες, εγκυμονεί κινδύνους για την προστασία της ιδιωτικής ζωής. Η εξασφάλιση ασφαλών διαύλων επικοινωνίας για την αποτροπή υποκλοπών και αλλοιώσεων είναι ζωτικής σημασίας.

Πρωτόκολλα ασφαλείας επιπέδου Connectivity: Στο επίπεδο συνδεσιμότητας (Connectivity), η εφαρμογή ισχυρών πρωτοκόλλων ασφαλείας είναι απαραίτητη. Αυτά τα πρωτόκολλα περιλαμβάνουν:

- **TLS (Transport Layer Security):** Εξασφαλίζει την ασφαλή μετάδοση δεδομένων μεταξύ του οχήματος και των εξωτερικών υπηρεσιών.
- **IPsec (ασφάλεια πρωτοκόλλου διαδικτύου):** Παρέχει ασφάλεια για τις επικοινωνίες πρωτοκόλλου διαδικτύου με την αυθεντικοποίηση και την κρυπτογράφηση κάθε πακέτου IP.
- **DTLS (Datagram Transport Layer Security):** Ασφαλίζει εφαρμογές που βασίζονται σε datagram, όπως αυτές που χρησιμοποιούν UDP, ζωτικής σημασίας για τη μετάδοση δεδομένων σε πραγματικό χρόνο στην επικοινωνία V2X.
- **Πρωτόκολλα ασφαλείας V2X:** Εξειδικευμένα πρωτόκολλα για την επικοινωνία οχήματος με οτιδήποτε που διασφαλίζουν την ακεραιότητα και την αυθεντικότητα των δεδομένων μεταξύ οχημάτων και υποδομών.

3. Στο 3ο (MIDDLEWARE) και 4ο επίπεδο (IoT SERVICES) θα προτείνατε να λειτουργούν στο cloud ή edge computing και γιατί; (~150 λέξεις)

Απάντηση:

Για τα επίπεδα middleware και IoT services, μια υβριδική προσέγγιση που χρησιμοποιεί τόσο το edge όσο και το cloud computing είναι συχνά ιδανική. Το Edge Computing θα πρέπει να χρησιμοποιείται για εργασίες επεξεργασίας ευαίσθητης χρονικής διάρκειας. Με την επεξεργασία δεδομένων πιο κοντά στην πηγή, το edge computing μειώνει την καθυστέρηση και εξασφαλίζει ανταπόκριση σε πραγματικό χρόνο, η οποία είναι κρίσιμη για την ασφάλεια στην αυτόνομη οδήγηση. Αυτό περιλαμβάνει εργασίες όπως η ανίχνευση εμποδίων, η πέδηση έκτακτης ανάγκης και η συγχώνευση δεδομένων τοπικών αισθητήρων.

Το cloud computing είναι κατάλληλο για εργασίες που απαιτούν σημαντική υπολογιστική ισχύ και αποθήκευση, αλλά είναι λιγότερο ευαίσθητες στον χρόνο. Αυτό περιλαμβάνει την εκπαίδευση μοντέλων μηχανικής μάθησης, την ανάλυση μεγάλων δεδομένων και την

αποθήκευση ιστορικών δεδομένων. Το cloud computing μπορεί επίσης να παρέχει ενημερώσεις και υπηρεσίες συνολικής βελτιστοποίησης, όπως ανάλυση μοτίβων κυκλοφορίας και βελτιστοποίηση διαδρομών, αξιοποιώντας τους εκτεταμένους υπολογιστικούς πόρους και τη συνδεσιμότητά του.

Συνδυάζοντας το edge computing και το cloud computing, τα οχήματα χωρίς οδηγό μπορούν να επιτύχουν βέλτιστες επιδόσεις, εξισορροπώντας τις ανάγκες επεξεργασίας σε πραγματικό χρόνο με ισχυρές δυνατότητες ανάλυσης και αποθήκευσης δεδομένων.
