

Πανεπιστήμιο Μακεδονίας
ΠΜΣ Πληροφοριακά Συστήματα
Τεχνολογίες Τηλεπικοινωνιών & Δικτύων
Καθηγητής: Α.Α. Οικονομίδης

University of Macedonia
Master Information Systems
Networking Technologies
Professor: A.A. Economides

SENSOR NETWORKS

από
ΠΑΝΑΓΙΩΤΗΣ ΜΥΛΩΝΑΣ

Θεσσαλονίκη
Φεβρουάριος 2009

ΠΕΡΙΛΗΨΗ

Το σύγγραμμα αυτό παρουσιάζει σημαντικά θέματα των δικτύων αισθητήρων. Στο πρώτο κεφάλαιο αρχικά περιγράφει την έννοια των δικτύων αισθητήρων και στην συνέχεια περιγράφει την έρευνα δικτύων αισθητήρων στον 21ο αιώνα. Επιπρόσθετα αναφέρεται η χρήση αυτών των δικτύων στην παρακολούθηση περιβάλλοντος και βιότοπου και στην ασφάλεια των υποδομών. Στην συνέχεια το δεύτερο κεφάλαιο περιγράφει την έννοια των ασύρματων δικτύων αισθητήρων, τις εφαρμογές τους και τα χαρακτηριστικά τους. Επίσης αναφέρει τις πλατφόρμες, το υλικό και τους αλγορίθμους που χρησιμοποιούν. Στο τρίτο κεφάλαιο δίνεται μεγαλύτερη έμφαση στην χρήση αυτών των δικτύων αναλύοντας τις έννοιες παρακολούθησης και ελέγχου του περιβάλλοντος αναφέροντας παραδείγματα χρήσης. Στο τέταρτο κεφάλαιο αναφέρεται η έννοια της δικτύωσης σύννεφου η οποία μπορεί να έχει εφαρμογή και στα δίκτυα αισθητήρων. Τέλος, στο πέμπτο κεφάλαιο αναλύεται η ασφάλεια των ασύρματων δικτύων αισθητήρων με ένα χαρακτηριστικό παράδειγμα.

The present text presents major issues of sensor networks. The first chapter describes the concept of sensor networks and then describes the research of sensor networks in the 21st century. . In addition, make mention of usage of these networks to environmental and habitat monitoring and security infrastructure. Then, in second chapter the concept of wireless sensor networks, their applications and their features are described. It also reports the platforms, hardware and the algorithms they use. In third chapter a greater emphasis on the use of networks by analyzing the concepts of monitoring and control of the environment giving examples of use is explained. In the fourth chapter the concept of cloud networking which can be applied in sensor networks is presented. Finally, in the fifth chapter the security of wireless sensor networks is analyzed with a characteristic example.

ΠΕΡΙΕΧΟΜΕΝΑ

Περίληψη.....	2
Περιεχόμενα.....	3
Εισαγωγή - Παρουσίαση Θέματος.....	4
1 Δίκτυα Αισθητήρων.....	5
1.1 Η έρευνα δικτύων αισθητήρων του 21ου αιώνα.....	6
1.2 Παρακολούθηση περιβάλλοντος και βιότοπου.....	7
1.3 Ασφάλεια Υποδομών.....	7
2. Ασύρματο Δίκτυο Αισθητήρων (WSN)	8
2.1 Εφαρμογές	8
2.2 Χαρακτηριστικά.....	9
2.3 Πλατφόρμες.....	9
2.4 Υλικό.....	9
2.5 Αλγόριθμοι.....	10
3. Περιβαλλοντικός Έλεγχος.....	10
3.1 Ορισμός Περιβαλλοντικής παρακολούθησης.....	11
3.2 Έλεγχος συμμόρφωσης.....	11
3.3 Έλεγχος περιβαλλοντικών επιπτώσεων.....	12
4. Cloud networking.....	12
4.1 Cloud computing.....	13
4.2 Κύρια Χαρακτηριστικά του Cloud computing.....	14
5. Ασφάλεια Ασύρματων Δικτύων.....	14
5.1 Αρχιτεκτονική Συστήματος.....	15
5.2 Πρωτόκολλο Ασφαλείας.....	16
6. Συμπεράσματα.....	19
Βιβλιογραφία.....	20

ΕΙΣΑΓΩΓΗ - ΠΑΡΟΥΣΙΑΣΗ ΘΕΜΑΤΟΣ

Η πρόσφατη και ραγδαία ανάπτυξη στις ασύρματες επικοινωνίες και στην ηλεκτρονική τεχνολογία έδωσαν ώθηση στην ανάπτυξη και υλοποίηση χαμηλού κόστους και κατανάλωσης αισθητήρια τα οποία είναι μικρά σε μέγεθος και επικοινωνούν με αξιοπιστία σε μικρές αποστάσεις. Αυτοί οι μικροί κόμβοι αισθητήρων οι οποίοι έχουν δυνατότητα επεξεργασίας δεδομένων και εξαρτήματα επικοινωνίας (ασύρματη ή ενσύρματη) συνιστούν ένα δίκτυο αισθητήρων. Τα δίκτυα αισθητήρων αποτελούν σημαντική βελτίωση των παραδοσιακών αισθητήρων.

Ένα δίκτυο αισθητήρων αποτελείται από μεγάλο αριθμό κόμβων αισθητήρων τα οποία είναι τοποθετημένα σε κοντινές αποστάσεις και επικοινωνούν μεταξύ τους απευθείας είτε μέσω ενός κεντρικού κόμβου, είτε είναι τοποθετημένα σε μακρινές αποστάσεις και χρησιμοποιούν άλλα δίκτυα, όπως το διαδίκτυο, για την περισυλλογή των δεδομένων τους ή την επικοινωνία τους. Έχουν προταθεί πολλές τοπολογίες δικτύωσης τους. Μια πιθανή δικτύωση τους είναι και η χρήση της δικτύωσης σύννεφου όπως περιγράφεται στη πορεία του συγγράμματος.

Τα τελευταία χρόνια οι έρευνες εστιάζονται στα ασύρματα δίκτυα αισθητήρων. Οι μελέτες των ασύρματων δικτύων αισθητήρων (WSN) περιλαμβάνουν το σχεδιασμό υλικού και συστημάτων, δικτύωση, διανεμημένους αλγόριθμους, μοντέλα προγραμματισμού, διαχείριση δεδομένων, την ασφάλεια και τους κοινωνικούς παράγοντες. Τα WSNs χρησιμοποιούνται σε διάφορα πεδία όπως στρατιωτικό, ανίχνευση και αποφυγή καταστροφής, βιομηχανία, περιβαλλοντικός έλεγχος και θέματα γεωργίας κ.λπ. Στο σημείο αυτό πρέπει να αναφερθεί ότι παρακάτω εξετάζεται ο περιβαλλοντικός έλεγχος και τα προγράμματα που τον εφαρμόζουν.

Λόγω της ποικιλομορφίας εφαρμογής τους σε τόσο πολλά θέματα η ασφάλεια για τα WSNs γίνεται ένα σύνθετο και κρίσιμο ζήτημα. Επειδή για κάθε εφαρμογή, υπάρχει διαφορετικός τύπος των πιθανών επιθέσεων απαιτείται κάθε φορά ένα διαφορετικό επίπεδο ασφάλειας. Η ανάπτυξη ενός αποδοτικού συστήματος ασφάλειας καθορίζεται από τους περιορισμούς που έχουν τα WSNs όπως το μέγεθος των αισθητήρων, της μνήμης, της ταχύτητας επεξεργασίας, της ενέργειας μπαταριών κ.λπ.

Το ζήτημα της ασφάλειας των δικτύων αυτών είναι πολύ σημαντικό και αξίζει να αναφερθούμε παραπάνω εξετάζοντας ένα προτεινόμενο πρωτόκολλο ασφαλείας.

1. Δίκτυα Αισθητήρων

Τα δίκτυα αισθητήρων αναμφισβήτητα είναι βασική τεχνολογία για το μέλλον. Σήμερα είναι χαμηλού κόστους, έξυπνες συσκευές με πολλούς κόμβους αισθητήρων, δικτυωμένους μέσω των ασύρματων συνδέσεων ή και του Διαδικτύου που μπορούν να επεκταθούν εύκολα, παρέχουν πρωτοφανείς δυνατότητες οργάνωσης και ελέγχου σπιτιών, των πόλεων, και του περιβάλλοντος [1]. Επιπλέον, τα δικτυωμένα αισθητήρια παρέχουν την τεχνολογία για μια ευρύ γκάμα συστημάτων στον αμυντικό χώρο, η οποία προωθεί νέες ικανότητες για αναγνώριση και επιτήρηση καθώς επίσης και άλλες στρατηγικές εφαρμογές. Ειδικά έξυπνα αισθητήρια μίας χρήσης τα *microsensors* [2] μπορούν να εφαρμοστούν σε έδαφος, στον αέρα, κάτω από το νερό, στους οργανισμούς, στα οχήματα, και στο εσωτερικό κτηρίων. Ένα σύστημα των δικτυωμένων αισθητήρων μπορεί να ανιχνεύσει και να παρακολουθήσει απειλές (π.χ. τροχοφόρα οχήματα, προσωπικό, χημικούς και βιολογικούς συντελεστές) και να χρησιμοποιηθεί για τη παρακολούθηση περιοχής. Αξίζει να σημειωθεί ότι τα τελευταία χρόνια παρατηρείται έντονα η χρήση αισθητήρων σε αγροτικούς τομείς [3]. Στο μέλλον κάθε κόμβος αισθητήρων θα έχει ενσωματώσει την ικανότητα επεξεργασίας των δεδομένων με μεγαλύτερη ταχύτητα, και θα έχει ενδεχομένως πολλαπλάσιους αισθητήρες, που θα λειτουργούν στο ακουστικό, σεισμικό, υπέρυθρο (IR) πεδίο, καθώς επίσης και εικονολήπτες και *microradars*. Επίσης θα έχει μεγαλύτερη μνήμη για αποθήκευση, ασύρματες συνδέσεις με τους γειτονικούς κόμβους, και γνώση θέσης και προσδιορισμού θέσης μέσω του GPS ή τοπικών αλγορίθμων προσδιορισμού θέσης.

Ο πίνακας 1 [2] συνοψίζει με τη σειρά τις ιδιότητες στα γενικά δίκτυα αισθητήρων. Οι παρούσες και πιθανές εφαρμογές των δικτύων αισθητήρων περιλαμβάνουν: στρατιωτικοί αισθητήρες, φυσική ασφάλεια, έλεγχος εναέριας κυκλοφορίας, επιτήρηση κυκλοφορίας, τηλεοπτική επιτήρηση, βιομηχανική και κατασκευαστική αυτοματοποίηση, διανεμημένη ρομποτική, παρακολούθηση περιβάλλοντος, και οικοδόμηση και παρακολούθηση υποδομών. Οι αισθητήρες σε αυτές τις εφαρμογές μπορούν να είναι μικροί ή μεγάλοι, και τα δίκτυα μπορούν να συνδεθούν με καλώδιο ή ασύρματα. Να αναφερθεί ότι τα ασύρματα δίκτυα των *micro sensors* προσφέρουν πιθανώς τον καλύτερο τρόπο αντίληψης-αίσθησης [4], δηλαδή θεωρούνται αποδοτικότεροι αισθητήρες.

ΠΙΝΑΚΑΣ 1

Sensors	<i>Size:</i> small (e.g., micro-electro mechanical systems (MEMS)), large (e.g., radars, satellites) <i>Number:</i> small, large <i>Type:</i> passive (e.g., acoustic, seismic, video, IR, magnetic), active (e.g., radar, lidar) <i>Composition or mix:</i> homogeneous (same types of sensors), heterogeneous (different types of sensors) <i>Spatial coverage:</i> dense, sparse <i>Deployment:</i> fixed and planned (e.g., factory networks), ad hoc (e.g., air-dropped) <i>Dynamics:</i> stationary (e.g., seismic sensors), mobile (e.g., on robot vehicles)
Sensing entities of interest	<i>Extent:</i> distributed (e.g., environmental monitoring), localized (e.g., target tracking) <i>Mobility:</i> static, dynamic <i>Nature:</i> cooperative (e.g., air traffic control), non-cooperative (e.g., military targets)
Operating environment	Benign (factory floor), adverse (battlefield)
Communication	<i>Networking:</i> wired, wireless <i>Bandwidth:</i> high, low
Processing architecture	Centralized (all data sent to central site), distributed (located at sensor or other sites), hybrid
Energy availability	Constrained (e.g., in small sensors), unconstrained (e.g., in large sensors)

Η ανάπτυξη των δικτύων αισθητήρων απαιτεί τεχνολογίες από τρεις διαφορετικούς ερευνητικούς τομείς: ανίχνευση, επικοινωνία, και υπολογισμός (συμπεριλαμβανομένου του υλικού, του λογισμικού, και των αλγορίθμων). Κατά συνέπεια, οι συνδυασμένες και χωριστές πρόοδοι σε κάθε μια από αυτές τις περιοχές έχουν οδηγήσει την έρευνα στα δίκτυα αισθητήρων. Τα παραδείγματα παλαιότερων δικτύων αισθητήρων περιλαμβάνουν τα δίκτυα ραντάρ χρησιμοποιούμενα στον έλεγχο εναέριας κυκλοφορίας. Επίσης, το δίκτυο ενέργειας, με τους πολλούς αισθητήρες του, μπορεί να θεωρηθεί ως ένα μεγάλο δίκτυο αισθητήρων. Αυτά τα δύο συστήματα αναπτύχθηκαν με εξειδικευμένους υπολογιστές και χρήση γνώσεων και υποδομών επικοινωνίας, πριν ο όρος *sensor networks* εισαχθεί στη μόδα.

1.1 Η έρευνα δικτύων αισθητήρων του 21ου αιώνα

Πρόσφατες προόδους στην επεξεργασία και στην επικοινωνία έχουν προκαλέσει μια σημαντική άνοδο στην έρευνα των δικτύων αισθητήρων και την έχουν φέρει πιο κοντά στην επίτευξη του αρχικού οράματος. Οι μικροί και ανέξοδοι αισθητήρες που βασίζονται σε microelectromechanical [5] τεχνολογία συστημάτων (MEMS), την ασύρματη δικτύωση, και τους ανέξodus χαμηλής ισχύος επεξεργαστές επιτρέπουν την επέκταση των ασύρματων ειδικών δικτύων για τις διάφορες εφαρμογές. Εξετάζοντας το μέλλον, προβλέπεται ότι οι πρόοδοι στην τεχνολογία MEMS θα παραγάγουν τους αισθητήρες που είναι ικανότεροι και ευπροσάρμοστοι. Παραδείγματος χάριν, η Dust Inc. κατασκευάζει τους αισθητήρες MEMS που μπορούν να αισθανθούν και να επικοινωνήσουν και είναι αρκετά μικροσκοπικοί που χωρούν μέσα σε ένα κυβικό χιλιοστόμετρο.

Στο παρακάτω πίνακα φαίνεται η εξέλιξη των αισθητήρων ανά ιδιότητα.

ΠΙΝΑΚΑΣ 2

	Yesterday (1980's – 1990's)	Today (2000 – 2003)	Tomorrow (2010)
Manufacturer	Custom contractors, e.g., for TRSS	Commercial: Crossbow Technology, Inc. Sensoria Corp., Ember Corp.	Dust, Inc. and others to be formed
Size	Large shoe box and up	Pack of cards to small shoe box	Dust particle
Weight	Kilograms	Grams	Negligible
Node architecture	Separate sensing, processing and communication	Integrated sensing, processing and communication	Integrated sensing, processing and communication
Topology	Point-to-point, star	Client server, peer to peer	Peer to peer
Power supply lifetime	Large batteries; hours, days and longer	AA batteries; days to weeks	Solar; months to years
Deployment	Vehicle-placed or air-drop single sensors	Hand-emplaced	Embedded, "sprinkled" left-behind

Στην παρακάτω εικόνα φαίνεται η εξέλιξη στο μέγεθος των αισθητήρων.



Σχήμα 1

1.2 Παρακολούθηση περιβάλλοντος και βιότοπου

Η παρακολούθηση περιβάλλοντος και βιότοπου [6] γίνεται με την βοήθεια των δικτύων αισθητήρων, αφού οι μεταβλητές που ελέγχονται, π.χ., θερμοκρασία, κατανέμονται συνήθως μια μεγάλη περιοχή. Το πρόσφατα Κέντρο Ενσωματωμένων Αισθητήριων Δικτύων (CENS), με έδρα το Λος Άντζελες, εστιάζει στον περιβαλλοντικό έλεγχο βιότοπων [7]. Οι περιβαλλοντικοί αισθητήρες χρησιμοποιούνται στην μελέτη της απόκρισης της βλάστησης στις κλιματολογικές αλλαγές και τις ασθένειες, και οι ακουστικοί και αισθητήρες απεικόνισης μπορούν να προσδιορίσουν, να ακολουθήσουν, και να μετρήσουν τον πληθυσμό των πουλιών και άλλων ειδών.

Ένα αξιόλογο παράδειγμα είναι το Σύστημα Επιτήρησης του Αμαζονίου (SIVAM) [8]. Σε πολύ μεγάλη κλίμακα, το σύστημα παρέχει περιβαλλοντική παρακολούθηση, την εμπορία ναρκωτικών, και τον έλεγχο εναέριας κυκλοφορίας για τη λεκάνη του Αμαζονίου. Υποστηριγμένο από την κυβέρνηση της Βραζιλίας, αυτό το μεγάλο δίκτυο αισθητήρων αποτελείται από διαφορετικούς τύπους διασυνδεδεμένων αισθητήρων συμπεριλαμβανομένου του ραντάρ, καμερών και των περιβαλλοντικών αισθητήρων. Οι αισθητήρες εικονολήψεων είναι στο διάστημα, τα ραντάρ βρίσκονται στα αεροσκάφη, και οι περιβαλλοντικοί αισθητήρες είναι συνήθως στο έδαφος. Το δίκτυο επικοινωνίας που συνδέει τους αισθητήρες λειτουργεί με τις διαφορετικές ταχύτητες. Παραδείγματος χάριν, τα μεγάλης ταχύτητας δίκτυα συνδέουν τους αισθητήρες στους δορυφόρους και τα αεροσκάφη, ενώ τα μικρότερης ταχύτητας δίκτυα συνδέουν τους επίγειους αισθητήρες.

1.3 Ασφάλεια Υποδομών

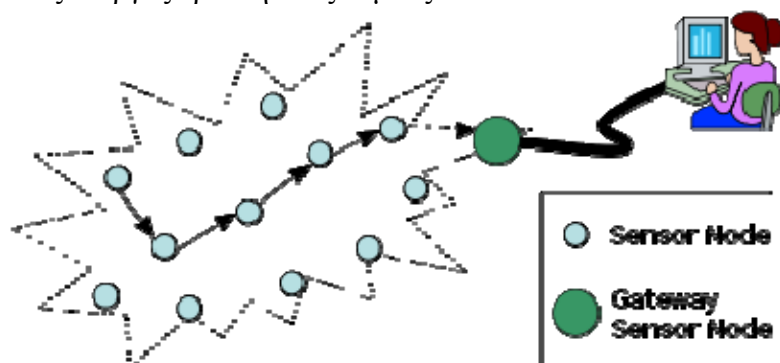
Τα δίκτυα αισθητήρων ασφάλειας υποδομών μπορούν να χρησιμοποιηθούν για εφαρμογές ασφάλειας και φύλαξης υποδομής. Κρίσιμα κτήρια και εγκαταστάσεις όπως οι εγκαταστάσεις παραγωγής ενέργειας και τα κέντρα επικοινωνίας πρέπει να προστατευθούν από πιθανούς τρομοκράτες. Συνήθως, δίκτυα με αισθητήρες όρασης, ακουστικοί αισθητήρες, και άλλοι αισθητήρες μπορούν να επεκταθούν γύρω από αυτές τις εγκαταστάσεις. Αυτοί οι αισθητήρες παρέχουν την έγκαιρη ανίχνευση των πιθανών απειλών.

Ακόμα κι αν οι σταθεροί αισθητήρες που συνδέονται με ένα σταθερό δίκτυο επικοινωνίας προστατεύουν τις περισσότερες εγκαταστάσεις, τα ασύρματα ad hoc δίκτυα μπορούν να παρέχουν περισσότερη ευελιξία και πρόσθετη κάλυψη όταν απαιτείται. Τα δίκτυα αισθητήρων μπορούν επίσης να χρησιμοποιηθούν για να ανιχνεύσουν τις βιολογικές, χημικές, και πυρηνικές επιθέσεις. Τα παραδείγματα τέτοιων δικτύων μπορούν να βρεθούν στην αναφορά [9], η οποία περιγράφει επίσης άλλες χρήσεις των δικτύων αισθητήρων.

2. Ασύρματο Δίκτυο Αισθητήρων (WSN)

Ένα ασύρματο δίκτυο αισθητήρων (WSN) είναι ένα ασύρματο δίκτυο που αποτελείται από διανεμημένες αυτόνομες συσκευές στο χώρο που χρησιμοποιούν τους αισθητήρες για να ελέγξουν τις φυσικές ή περιβαλλοντικές συνθήκες, όπως η θερμοκρασία, ήχος, δόνηση, πίεση, κίνηση ή οι ρύποι, σε διαφορετικό χώρο [10]. Η ανάπτυξη των ασύρματων δικτύων αισθητήρων παρακινήθηκαν αρχικά από τις στρατιωτικές εφαρμογές όπως η επιτήρηση πεδίων μαχών. Εντούτοις, τα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται τώρα σε πολλούς τομείς, συμπεριλαμβανομένου του περιβάλλοντος και της παρακολούθησης βιότοπων, των εφαρμογών υγειονομικής περίθαλψης, της βασικής αυτοματοποίησης, και του ελέγχου της κυκλοφορίας. Εκτός από έναν ή περισσότερους αισθητήρες, κάθε κόμβος σε ένα δίκτυο αισθητήρων είναι εξοπλισμένος με έναν ραδιοπομποδέκτη ή άλλη ασύρματη συσκευή επικοινωνιών, έναν μικροελεγκτή, και μια πηγή ενέργειας, συνήθως μια μπαταρία. Το κόστος των κόμβων αισθητήρων είναι μεταβλητό, κυμαινόμενο από τις εκατοντάδες ευρώ ως μερικά σέντς, ανάλογα με το μέγεθος του δικτύου αισθητήρων και η πολυπλοκότητα που απαιτείται. Το μέγεθος και το κόστος των κόμβων αισθητήρων οδηγεί στους αντίστοιχους περιορισμούς στα χαρακτηριστικά του κάθε κόμβου όπως η ενέργεια, η μνήμη, η υπολογιστική ταχύτητα και το εύρος φάσματος.

Ένα δίκτυο αισθητήρων αποτελεί συνήθως ένα ασύρματο ad-hoc δίκτυο, που σημαίνει ότι κάθε αισθητήρας υποστηρίζει έναν αλγόριθμο δρομολόγησης multi-hop (διάφοροι κόμβοι μπορούν να διαβιβάσουν τα πακέτα δεδομένων στη βάση)[11][12]. Στην πληροφορική και στις τηλεπικοινωνίες, τα ασύρματα δίκτυα αισθητήρων είναι ένας ενεργός ερευνητικός τομέας.



Σχήμα 2. Τυπικό Multihop ασύρματο δίκτυο αισθητήρων

2.1 Εφαρμογές

Οι εφαρμογές για WSNs είναι πολλές και ποικίλες, αλλά χαρακτηριστικά περιλαμβάνουν την επιτήρηση, τη παρακολούθηση και τον έλεγχο. Οι συγκεκριμένες εφαρμογές για WSNs περιλαμβάνουν τον έλεγχο βιότοπων, παρακολούθηση αντικειμένου, έλεγχος πυρηνικών αντιδραστήρων, πυρανίχνευση, και παρακολούθηση κυκλοφορίας. Σε μια χαρακτηριστική εφαρμογή, ένα WSN είναι διασπαρμένο σε μια περιοχή όπου προορίζεται να συλλέξει τα δεδομένα μέσω των κόμβων αισθητήρων του.

2.2 Χαρακτηριστικά

Τα μοναδικά χαρακτηριστικά ενός WSN περιλαμβάνουν:

- Περιορισμένη ενέργεια κατανάλωσης
- Ικανότητα αντοχής σε σκληρές περιβαλλοντικές συνθήκες
- Ικανότητα να ανταπεξέρχεται σε αποτυχίες των κόμβων
- Ευκινησία των κόμβων
- Δυναμική τοπολογία
- Αποτυχίες επικοινωνίας
- Ετερογένεια των κόμβων
- Δυνατότητα επέκτασης

Οι κόμβοι αισθητήρων είναι σαν μικροί υπολογιστές. Αποτελούνται συνήθως από μια μονάδα επεξεργασίας με περιορισμένη υπολογιστική δύναμη και περιορισμένη μνήμη, τους αισθητήρες (συμπεριλαμβανομένων βοηθητικών στοιχείων κυκλώματος), μια συσκευή επικοινωνίας (συνήθως ραδιοπομποδέκτες ή εναλλακτικά οπτική επαφή), και μια πηγή ενέργειας συνήθως υπό μορφή μπαταρίας. Άλλα πιθανά μέρη που το αποτελούν είναι μονάδες ενεργειακής συγκομιδής (π.χ. ηλιακή), δευτεροβάθμια ASICs, και ενδεχομένως δευτεροβάθμιες συσκευές επικοινωνίας (π.χ. rs-232 ή USB).

Οι σταθμοί βάσεων είναι ένα ή περισσότερα διακεκριμένα συστατικά του WSN με πολύ περισσότερη υπολογιστική ισχύς, μνήμη και ενέργεια. Ενεργούν ως πύλη μεταξύ των κόμβων αισθητήρων και του τελικού χρήστη.

2.3 Πλατφόρμες

Αυτήν την περίοδο διάφορα πρότυπα επικυρώνονται είτε είναι υπό ανάπτυξη για τα ασύρματα δίκτυα αισθητήρων. Το ZigBee είναι πρότυπο δικτύωσης προοριζόμενο για χρήσεις όπως η ενσωματωμένη αντίληψη, η ιατρική συλλογή δεδομένων, οι καταναλωτικές συσκευές όπως τηλεχειριστήρια τηλεόρασης και η βασική αυτοματοποίηση. Το Zigbee προέρχεται από μια μεγάλη κοινοπραξία των φορέων βιομηχανίας. Το WirelessHART είναι μια επέκταση του πρωτοκόλλου Hart και σχεδιάζεται συγκεκριμένα για τις βιομηχανικές εφαρμογές όπως την παρακολούθηση και τον έλεγχο διαδικασίας. Το WirelessHART προστέθηκε στη γενική ακολουθία πρωτοκόλλου Hart ως τμήμα του Hart 7 (προδιαγραφή), η οποία εγκρίθηκε από το ίδρυμα επικοινωνίας Hart.

2.4 Υλικό

Η βασική πρόκληση είναι να παραχθεί χαμηλότερου κόστους και μικροσκοπικοί κόμβοι αισθητήρων. Όσον αφορά αυτούς τους στόχους, οι σημερινοί κόμβοι αισθητήρων είναι κυρίως πρωτότυπα. Η μικρογράφηση και το χαμηλότερο κόστος μπορεί να επιτευχθούν από την πρόσφατη και μελλοντική πρόοδο στα πεδία MEMS και NEMS.

Η ενέργεια είναι το πιο ανεπαρκές στοιχείο των κόμβων WSN, και καθορίζει την διάρκεια ζωής των WSNs. Τα WSNs προορίζονται να επεκταθούν σε πλήθος στα διάφορα περιβάλλοντα, συμπεριλαμβανομένων των απομακρυσμένων περιοχών, με τις ad-hoc επικοινωνίες. Για αυτόν τον λόγο, οι αλγόριθμοι και τα πρωτόκολλα πρέπει να αντιμετωπίσουν τα ακόλουθα ζητήματα:

- Μεγιστοποίηση διάρκειας ζωής
- Σταθερότητα και ανοχή σφαλμάτων
- Ιδιο-ρύθμιση

Είναι αξιοσημείωτο να αναφερθούν ότι μερικά από τα θέματα που ερευνούνται για το λογισμικό WSN είναι η Ασφάλεια και Κινητικότητα (όταν κινούνται οι κόμβοι αισθητήρων ή οι σταθμοί βάσεων).

2.5 Αλγόριθμοι

Τα WSNs αποτελούνται από έναν μεγάλο αριθμό κόμβων αισθητήρων, επομένως, ένας αλγόριθμος για ένα WSN είναι ένας διανεμημένος αλγόριθμος. Στα WSNs ο κρίσιμότερος πόρος είναι ενέργεια. Για αυτόν τον λόγο, η αλγοριθμική έρευνα σε WSN εστιάζει συνήθως στη μελέτη και το σχέδιο των ενεργειακών αλγορίθμων για τη μετάδοση δεδομένων από τους κόμβους αισθητήρων στους σταθμούς βάσεων. Η μετάδοση δεδομένων είναι συνήθως multi-hop (από τον κόμβο σε κόμβο, προς τους σταθμούς βάσεων), λόγω στην πολυωνυμική αύξηση του ενέργεια-κόστους της ραδιο μετάδοσης όσον αφορά την απόσταση μετάδοσης. Στο τελευταίο κεφάλαιο θα περιγράψουμε έναν από αυτούς τους αλγόριθμους ο οποίος εστιάζει στη ασφαλή επικοινωνία.

3 Περιβαλλοντικός Έλεγχος

Ο περιβαλλοντικός έλεγχος παρέχει την ανατροφοδότηση για τις πραγματικές περιβαλλοντικές μεταβλητές. Τα αποτελέσματα από τον έλεγχο καθορίζουν την επιτυχία των μέτρων που λαμβάνονται για την προστασία και τον έλεγχο του περιβάλλοντος. Χρησιμοποιούνται επίσης για να εξασφαλίσουν την συμμόρφωση σύμφωνα με τα περιβαλλοντικά πρότυπα, και για να διευκολύνουν οποιοδήποτε αναγκαίο σχεδιασμό προγράμματος ή λειτουργικές αλλαγές. Η σημασία του μπορεί να διευκρινιστεί με τη χρησιμοποίηση ενός υποθετικού παραδείγματος εγκαταστάσεων επεξεργασίας υγρών απόβλητων. Οι εγκαταστάσεις έχουν γίνει σύμφωνα με το περιβαλλοντικό διοικητικό σχέδιο που ορίζεται από την Environmental Impact Assessment (EIA)[13][14]. Εντούτοις, λόγω έλλειψης των κεφαλαίων και κακής διαχείρισης, ή ανεπαρκείς δεξιότητες, οι εγκαταστάσεις δυσλειτουργούν. Χωρίς έλεγχο, οι κακές συνέπειες που προκλήθηκαν θα μπορούσαν να συνεχιστούν κατά τρόπο αόριστο. Με τον έλεγχο τα προβλήματα μπορούν να αναγνωριστούν και να επιλυθούν. Παραδείγματος χάριν, υποθέστε ότι οι εγκαταστάσεις επεξεργασίας απόβλητων που περιγράφονται ανωτέρω λειτουργούν όπως αρχικά προγραμματίζονται. Το λαμβάνον σώμα του υγρού λύματος, παραδείγματος χάριν ένας ποταμός, υποτίθεται ότι είχε την ικανότητα να αφομοιώσει τα απόβλητα που είχε λάβει από την αρχική επεξεργασία. Εάν ένα μεγάλο ποσό ύδατος αφαιρείται καθώς αφαιρείται ποσότητα λύματος, η αφομοιωτική ικανότητα του ποταμού θα μειωθεί. Το πρόγραμμα ελέγχου θα εμφάνιζε ότι η ποιότητα νερού έχει επιδεινωθεί και μια δευτεροβάθμια επεξεργασία απαιτείται. Αυτή η κατάσταση μπορεί να αποφευχθεί με τον κατάλληλο περιβαλλοντικό προγραμματισμό.

Ένα πρόγραμμα ελέγχου, χρειάζεται για να εξασφαλιστούν διορθωτικές ενέργειες όταν το απαιτούν τα αποτελέσματα ελέγχου. Είναι ένας αποδεδειγμένος τρόπος να εξασφαλιστεί αποτελεσματική εφαρμογή των μέτρων για τον περιορισμό

των δυσλειτουργιών. Με την εφαρμογή προγραμμάτων περιβαλλοντολογικού ελέγχου μειώνουν τους περιβαλλοντικούς κινδύνους που συνδέονται με το πρόγραμμα, και επιτρέπουν τις τροποποιήσεις προγράμματος όπου απαιτείται. Ένα άριστο παράδειγμα ενός αποτελεσματικού προγράμματος ελέγχου είναι το τμήμα άρδευσης του Tarim Basin Project στις ΗΠΑ. Οι προηγούμενες εγκαταστάσεις άρδευσης στην περιοχή δεν περιέλαβαν την κατάλληλη αποξήρανση, και εμφανίστηκε εδαφολογική αλάτωση, με συνέπεια τις μεγάλες μειώσεις των συγκομιδών. Το πρόγραμμα Tarim, που άρχισε το 1992, παρέχει την επαρκή αποξήρανση για να αποτρέψει την πρόσθετη αλάτωση, και για να αντιστρέψει μερικές από τη ζημίες που έγιναν ήδη. Ήταν μεγάλη ανάγκη να ληφθούν τα στοιχεία όσον αφορά την έκταση του προβλήματος κατά τη διάρκεια της λειτουργίας προγράμματος. Το ΕΙΑ όρισε ένα λεπτομερές, συνεχές πρόγραμμα ελέγχου για να αξιολογηθούν τα πραγματικά αποτελέσματα και να βελτιστοποιηθούν οι τεχνικές άρδευσης.

3.1 Ορισμός Περιβαλλοντικής παρακολούθησης

Γενικά, τα προγράμματα περιβαλλοντικού ελέγχου συλλέγουν τα δεδομένα για έναν ή περισσότερους από τους ακόλουθους σκοπούς (Everitt, 1992):

1. για να καθιερώσουν μια βασική γραμμή, δηλαδή συγκεντρώνοντας τις πληροφορίες για τα βασικά χαρακτηριστικά περιοχών πριν από την ανάπτυξη κάθε συστήματος ή για να προσδιορίσουν τις υπάρχουσες περιβαλλοντικές συνθήκες.
2. για να υπολογίσουν τυχόν αλλαγές στο περιβάλλον, το οποίο μπορεί να συγκριθεί με αλλαγές που παρατηρούνται σε μια άλλη συγκεκριμένη περιοχή
3. για να κάνουν συγκρίσεις μεταξύ διαφορετικών καταστάσεων (παραδείγματος χάριν, προ-ανάπτυξη και μετα-ανάπτυξη σε διαφορετικές αποστάσεις από μια πηγή) για να ανιχνεύσει τις αλλαγές και
4. για να κάνουν συγκρίσεις σε ένα επίπεδο προτύπων ή στόχων.

3.2 Έλεγχος συμμόρφωσης

Ο έλεγχος συμμόρφωσης είναι συνήθως εφαρμογή του περιβαλλοντικού ελέγχου. Ο σκοπός του ελέγχου συμμόρφωσης είναι να εξασφαλιστεί ότι η ποιότητα ή η ποσότητα ενός περιβαλλοντικού στοιχείου δεν αλλάζει από μια ανθρώπινη δραστηριότητα πέρα από προσδιορισμένα πρότυπα του επιπέδου κανονισμού. Ένα παράδειγμα του ελέγχου συμμόρφωσης είναι ένα πρόγραμμα δειγματοληψίας που διευθύνεται είτε από τη βιομηχανία είτε από την κυβέρνηση για να εξασφαλίσει ότι οι συγκεντρώσεις ενός μολυσματικού παράγοντα δεν υπερβαίνουν ένα προσδιορισμένο επίπεδο είτε στα απόβλητα αποχέτευσης είτε στα λαμβάνοντα ύδατα. Είναι αυτονόητο στον έλεγχο συμμόρφωσης η υπόθεση ότι εάν το χαρακτηριστικό που ελέγχεται είναι μέσα στα αποδεκτά όρια, τότε τα αποτελέσματα θα είναι μέσα στα αποδεκτά όρια. Ο έλεγχος συμμόρφωσης δεν ενδιαφέρεται για τον καθορισμό αποτελεσμάτων.

3.3 Έλεγχος περιβαλλοντικών επιπτώσεων

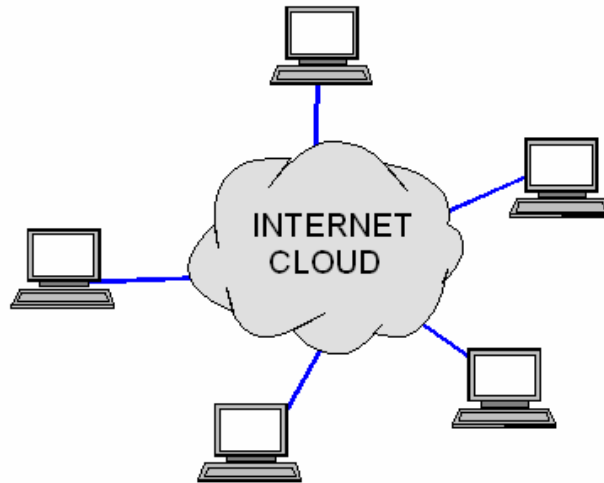
Όταν οι στόχοι του προγράμματος ελέγχου απαιτούν τα πραγματικά αποτελέσματα να καθορίζονται, απαιτείται έλεγχος περιβαλλοντικών επιπτώσεων. Ο έλεγχος περιβαλλοντικών επιπτώσεων έχει οριστεί ως η επαναλαμβανόμενη μέτρηση των περιβαλλοντικών παραμέτρων για να εξετάσει τις συγκεκριμένες υποθέσεις των αποτελεσμάτων της ανθρώπινης δραστηριότητας στο περιβάλλον (LGL Ltd. και λοιποί το 1984). Το Conover (1985) πρόσθεσε σε αυτόν τον καθορισμό την έννοια ότι τα μέτρα περιβαλλοντικού ελέγχου αλλάζουν με σκοπό τη σύσταση των σχέσεων αιτίας-επίδρασης. Αυτό το εγχειρίδιο υιοθετεί τον ακόλουθο ορισμό του περιβαλλοντικού ελέγχου: *Ο έλεγχος περιβαλλοντικών επιπτώσεων είναι η επαναλαμβανόμενη και συστηματική μέτρηση των χαρακτηριστικών των περιβαλλοντικών παραμέτρων για να εξετάσει τις συγκεκριμένες υποθέσεις των αποτελεσμάτων της ανθρώπινης δραστηριότητας στο περιβάλλον. Ο περιβαλλοντικός έλεγχος κυρίως καθορίζει τις περιβαλλοντικές επιπτώσεις των ανθρώπινων δραστηριοτήτων, και δευτερευόντως χρησιμοποιείται για να αυξήσει την κατανόηση των σχέσεων αιτίας-επίδρασης μεταξύ της ανθρώπινης δραστηριότητας και της περιβαλλοντικής αλλαγής.*

Οι επιπτώσεις αυτού του ορισμού είναι ότι:

1. τα προγράμματα περιβαλλοντικού ελέγχου πρέπει να περιλάβουν την επαναλαμβανόμενη δειγματοληψία κατά τη διάρκεια διάφορων ετών
2. τα προγράμματα περιβαλλοντικού ελέγχου πρέπει να είναι επιστημονικά και να βασίζονται σε βάσιμες υποθέσεις
3. τα προγράμματα δειγματοληψίας σχεδιάζονται με σκοπό να εξετάσουν τις υποθέσεις και πρέπει να είναι τέτοια ώστε τα αποτελέσματα να μπορούν να χρησιμοποιηθούν για να ανιχνεύσουν διαφορές στο χώρο και χρόνο.
4. τα προγράμματα περιβαλλοντικού ελέγχου πρέπει να στοχεύουν να προσδιορίσουν τις εμπειρικές συνδέσεις μεταξύ των ανθρώπινων δραστηριοτήτων και των αποτελεσμάτων τους στο περιβάλλον.

4 Cloud networking

Οι τοπολογίες οι οποίες μπορούν να δικτυωθούν τα αισθητήρια είναι πολλές. Μια τοπολογία από αυτές που μπορεί να εφαρμοστεί και είναι αποδεκτό ότι ίσως να αποτελέσει τη βασική δικτύωση στο μέλλον είναι το Cloud networking. Το Cloud networking είναι η διασύνδεση των στοιχείων που την απαρτίζουν ώστε να ανταποκριθεί στις απαιτήσεις που είναι συνυφασμένες με τον υπολογισμό cloud. Η Cloud δικτύωση επιτρέπει στους χρήστες να επιλέξουν ένα τεράστιο δίκτυο υπολογιστών που μπορεί να έχει πρόσβαση από μεγάλες αποστάσεις από ένα κινητό τηλέφωνο, φορητό υπολογιστή ή φορητή συσκευή για πληροφορίες ή δεδομένα.

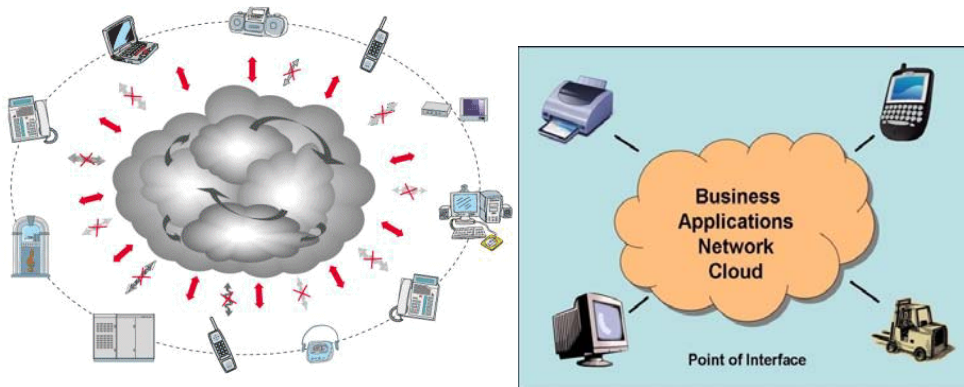


Σχήμα 3

Επιπρόσθετα, η δικτύωση σύννεφου είναι η δικτύωση των υποδομών που απαιτούνται για την υποστήριξη του cloud computing, το οποίο απαιτεί βελτίωση του δικτύου σε επεκτασιμότητα, αξιοπιστία, και στην καθυστέρηση πέρα από ότι τα παραδοσιακά δίκτυα έχουν προσφέρει. Η διάσταση των υπολογιστικών αναγκών του σύννεφου υπολογιστών δικτύου είναι τουλάχιστον μία τάξη μεγέθους μεγαλύτερη από ότι για τα παραδοσιακά δίκτυα.

4.1 Cloud computing

Cloud computing είναι διαδικτυακή εφαρμογή και χρησιμοποιεί την τεχνολογία των υπολογιστών ("υπολογισμούς"), σύμφωνα με την οποία δυναμικά κλιμακωτοί, συχνά εικονικοί πόροι και υπηρεσίες παρέχονται μέσω του Διαδικτύου. Οι χρήστες δεν χρειάζεται να έχουν γνώση, εμπειρία και ελέγχου επί της τεχνολογικής υποδομής "στο σύννεφο" που υποστηρίζει την διαδικασία.



Σχήμα 4

Η έννοια ενσωματώνει το λογισμικό ως υπηρεσία, Web 2.0 και άλλες πρόσφατες, με την οποία το κοινό 'θέμα' (εφαρμογή) είναι προσβάσιμο από το Διαδίκτυο για την ικανοποίηση των αναγκών των υπολογιστών των χρηστών. Ένα συχνά αναφερόμενο παράδειγμα είναι το Google Apps, το οποίο παρέχει κοινές επιχειρηματικές εφαρμογές online που είναι προσβάσιμο από τον web browser, ενώ το λογισμικό και τα δεδομένα είναι αποθηκευμένα σε διακομιστές της Google.

Το σύννεφο είναι σχήμα λόγου για το Internet, με βάση τον τρόπο με τον οποίο που απεικονίζεται το δίκτυο υπολογιστών με διαγράμματα, και είναι μια αφηρημένη έννοια για την περίπλοκη υποδομή που κρύβει.

Η δικτύωση 'σύννεφου' μπορεί να χρησιμοποιηθεί και στην δικτύωση αισθητήρων. Προφανές λόγω του μεγάλου αριθμού αισθητήρων και της μεγάλης απόστασης μεταξύ τους, η ευκολία πρόσβασης πρέπει να γίνει πιο προσιτή στους απλούς χρήστες και αυτό γίνεται με την δυνατότητα μεγάλων δικτύων. Ιδιαίτερα το cloud computing χρησιμοποιείται για να κάνει την πρόσβαση στα τερματικά των αισθητήριων πιο εύκολη και να παρέχει πολλά οφέλη. Κάποια από αυτά τα χαρακτηριστικά περιγράφονται παρακάτω.

4.2 Κύρια Χαρακτηριστικά του Cloud computing

Για τους τελικούς χρήστες, υπάρχουν πέντε βασικά πλεονεκτήματα

- 1) Πολύ μικρή επένδυση κεφαλαίων που απαιτούνται για την ανάπτυξη εφαρμογών σε κλιμακωτό επίπεδο.
- 2) Τα προγράμματα και τα δεδομένα διανέμονται για να μπορούν να γίνουν κλιμακώτα-επεκτάσιμα και ανεκτά σε βλάβες.
- 3) Τα προγράμματα μπορούν να προσπελαστούν από οποιαδήποτε συσκευή, συμπεριλαμβανομένων των ασύρματων και κινητών επικοινωνιών.
- 4) Καταργεί παραδοσιακούς server και θέματα διαχείρισης αποθήκευσης και Συντήρησης.
- 5) Επιτρέπει την πρόσβαση σε εφαρμογές και να διαμοιράσουν πληροφορίες.

Για τους προμηθευτές, υπάρχουν επίσης τέσσερα βασικά πλεονεκτήματα

- 1) Η ανθεκτικότητα και η σταθερότητα των πλατφόρμων σύννεφων επιτρέπει το χαμηλότερο κόστος υλικού
- 2) Με τον διαμοιρασμό των χρήσεων του υλικού αυξάνεται το κέρδος και η απόδοση χρήσης.
- 3) Επιτρέπει νέα και πολύ οικονομικά αποδοτικά επιχειρηματικά μοντέλα
- 4) Τα κέντρα δεδομένων μπορούν να βρίσκονται οπουδήποτε στη χώρα

5 Ασφάλεια Ασύρματων Δικτύων

Τα ασύρματα δίκτυα αισθητήρων αποτελούνται από πολλούς φθηνούς ασύρματους κόμβους, όπου ο κάθε ένας έχει την ικανότητα να λειτουργεί ως αισθητήριο χρησιμοποιώντας ισχύ υπολογιστική και ισχύ λόγω επικοινωνίας. Λόγω στον περιορισμένο της υπολογιστικής ισχύς, της ενέργειας, και αποθηκευτικών διαθέσιμων πόρων οι ασυμμετρικοί κρυπτογραφικοί αλγόριθμοι των κόμβων αισθητήρων δεν μπορούν να παρέχουν ασφάλεια στα ασύρματα δίκτυα αισθητήρων. Για αυτό τον λόγο έχουν ερευνηθεί διάφοροι αλγόριθμοι ώστε να παρέχουν ασφάλεια με ελάχιστη υπολογιστική ισχύς και χρήση μικρής δέσμης μνήμης. Παρακάτω εξετάζεται ένα πρωτόκολλο ασφάλειας για τα ασύρματα δίκτυα αισθητήρων, το οποίο δεν καταναλώνει πολλή ενέργεια έναντι των συμβατικών πρωτόκολλων ασφάλειας. Αυτό το πρωτόκολλο ασφάλειας είναι ένα πιστοποιημένο σύστημα που είναι ενεργειακά αποδοτικό στα ασύρματα δίκτυα αισθητήρων. Στο εγγύς μέλλον, τα ασύρματα δίκτυα αισθητήρων αναμένονται να αποτελούνται από χιλιάδες κόμβους, ώστε να λειτουργούν με περιορισμένη κατανάλωση ενέργειας [15].

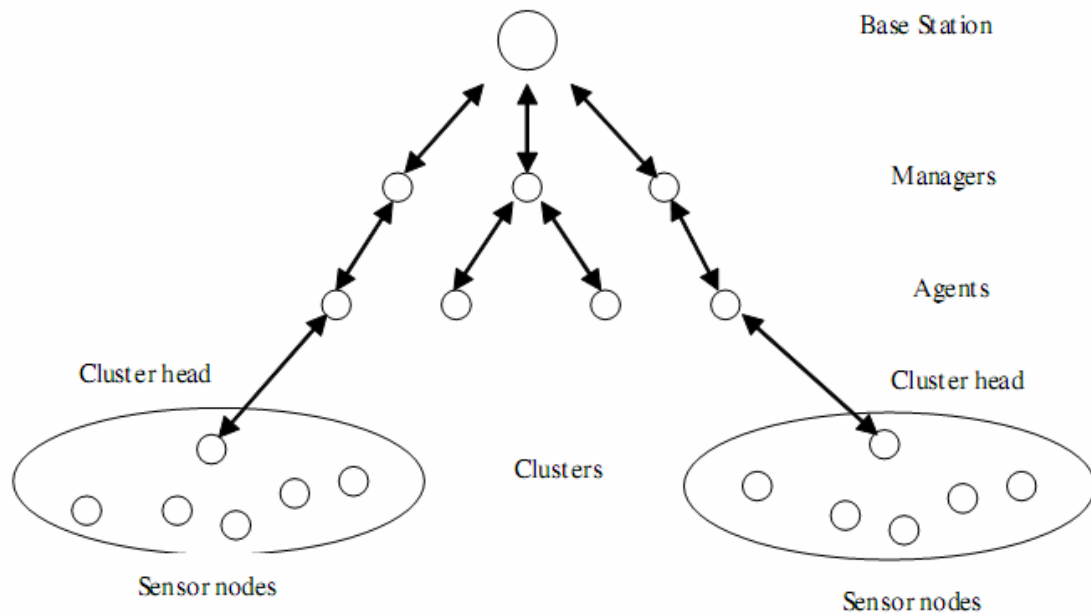
Τα δίκτυα αισθητήρων αναμένονται να επεκταθούν ευρέως σε πολλούς τομείς σε εμπορικές, αστικές, και στρατιωτικές εφαρμογές συμπεριλαμβανομένης της

επιτήρησης, της καταδίωξης οχημάτων, παρακολούθηση κλίματος και ελέγχου βιότοπων, νοσημότητας, ιατρικής, και συλλογή ακουστικών δεδομένων . Αν και πολλοί από αυτούς τους τομείς εφαρμογής απαιτούν ένα ορισμένο επίπεδο ασφάλειας πληροφοριών, δυστυχώς λίγη έρευνα για την ασφάλεια στα δίκτυα αισθητήρων έχει αναφερθεί μέχρι τώρα.

Αφού οι κόμβοι των ασύρματων αισθητήρων έχουν περιορισμένη ενέργεια, η ασφάλεια στα ασύρματα δίκτυα αισθητήρων είναι δύσκολο να υλοποιηθεί με αξιοπιστία σε σχέση με τις συμβατικές εφαρμογές ασφάλειας δικτύων. Παραδείγματος χάριν, οι ασυμμετρικοί κρυπτογραφικοί αλγόριθμοι δεν ισχύουν στα ασύρματα δίκτυα αισθητήρων λόγω περιορισμών στη ενέργεια κατανάλωσης και αποθηκευτικών πόρων διαθέσιμα στους κόμβους αισθητήρων [16][17]. Παρακάτω παρουσιάζετε ένα πρωτόκολλο ασφάλειας για την επικοινωνία στα ασύρματα δίκτυα αισθητήρων χρησιμοποιώντας το συνδυασμό συμμετρικής βασικής κρυπτογράφησης και της τεχνολογίας CDMA για την πιστοποίηση και συλλογή των δεδομένων λαμβάνοντας υπόψη τους ενεργειακούς περιορισμούς[18].

5.1 Αρχιτεκτονική Συστήματος

Αυτό το πρωτόκολλο ασφάλειας που παρουσιάζεται εδώ είναι βασισμένο στην ιεραρχική δομή των ασύρματων αισθητήρων. Η αρχιτεκτονική είναι self-organizing και έχει τέσσερα μέρη: ένα σταθμό, τους διαχειριστές, τους πράκτορες, και τους κόμβους βάσεων όπως φαίνεται στο σχήμα 5. Ο σταθμός βάσης είναι η μονάδα χωρίς περιορισμούς στη διαθεσιμότητα μνήμης. Οι πράκτορες και οι διαχειριστές θεωρούνται ανώτεροι από τους κόμβους αισθητήρων με περισσότερες υπολογιστικές ικανότητες. Κάθε τομέας αποτελείται από 8-10 κόμβους αισθητήρων. Τουλάχιστον ένας πράκτορας επικοινωνεί με έναν τομέα. Η κεφαλή κάθε τομέα επιλέγεται δυναμικά σε κάθε τομέα για να παρέχει την επικοινωνία μεταξύ των κόμβων και του αντίστοιχου πράκτορά τους. Κάθε διαχειριστής παρέχει την επικοινωνία μεταξύ του σταθμού βάσεων και των πρακτόρων. Κάθε κόμβος αισθητήρων διαθέτει το δικό του τμήμα στο κλειδί (Ks) για να χρησιμοποιηθεί στις ασφαλείς επικοινωνίες με τους πράκτορες. Με τον ίδιο τρόπο οι πράκτορες και οι διαχειριστές έχουν τα κλειδιά τους (Ka) και (Km) αντίστοιχα. Στο σταθμό βάσης παρατίθεται ο κατάλογος όλων των κλειδιών των αισθητήρων, των πρακτόρων και των διαχειριστών. Επίσης σε κάθε κόμβο αισθητήρων ανατίθεται ένας κωδικός CDMA. Μετά την επέκταση και εγκατάσταση του δικτύου, οι πράκτορες λαμβάνουν τον κατάλογο με τα κλειδιά των αισθητήρων από τη βάση και των αντίστοιχων κωδικών CDMA των κόμβων αισθητήρων ανά τομέα τους από το σταθμό βάσης. Ο σταθμός βάσης παρέχει επίσης το κλειδί συνόδου-περιόδου (Kses) στο διαχειριστή και στους πράκτορες, κάθε περίοδο, για να αποτρέψει επαναληπτικές συγκρούσεις και για να ανανεώνει τα δεδομένα πιο συχνά.



Σχήμα 5. Αρχιτεκτονική συστήματος

5.2 Πρωτόκολλο Ασφαλείας

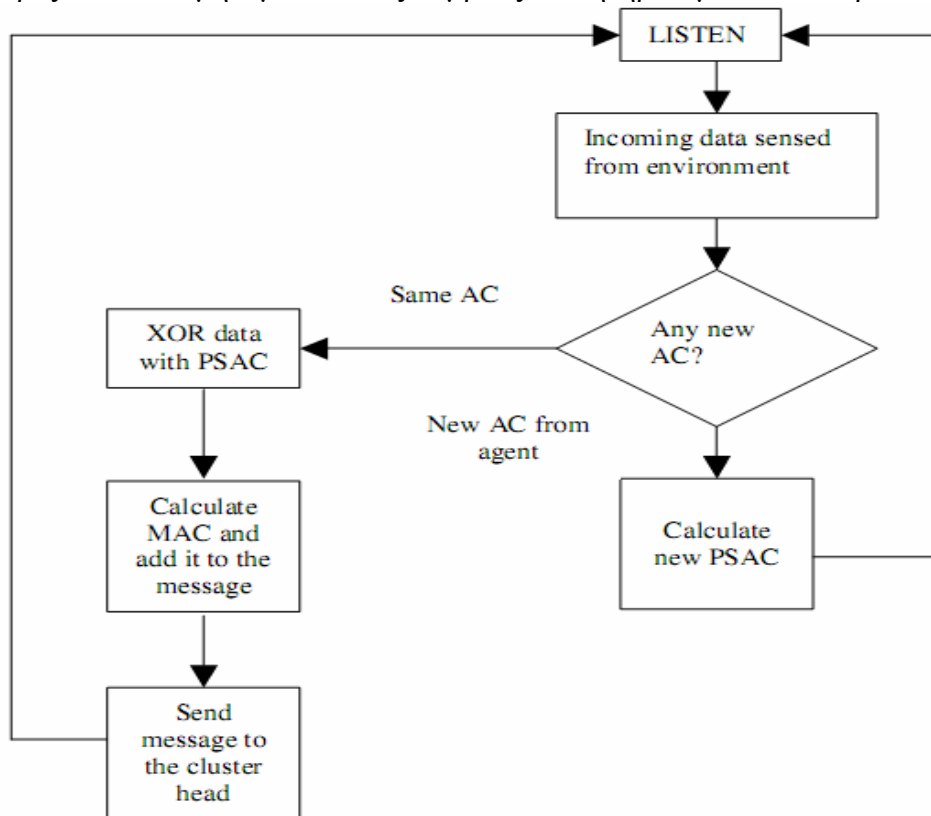
Η επικοινωνία σε αυτό το δίκτυο αισθητήρων είναι αμφίδρομη, από το σταθμό βάσης στους κόμβους αισθητήρων και αντίστροφα. Παρακάτω θα περιγραφεί το πρωτόκολλο ασφάλειας μεταξύ των πρακτόρων και των κόμβων αισθητήρων και στις δύο κατευθύνσεις. Το πρωτόκολλο ασφάλειας μπορεί να εφαρμοστεί με τον ίδιο τρόπο μεταξύ των πρακτόρων και του σταθμού βάσης. Ο πράκτορας παράγει τον κώδικα (AC) πιστοποίησης με την κρυπτογράφηση του κλειδιού συνόδου επικοινωνίας (Kses) με το κλειδί των πρακτόρων (Ka) και έπειτα εκτελεί hash διαδικασία στην έξοδο. Η hash διαδικασία είναι το 'κομμάτισμα' ενός πακέτου δεδομένων σε μικρότερα, συνήθως μονοί αριθμοί που θα εξυπηρετήσουν ως δείκτες σε κάποιο πίνακα δεδομένων. Το κλειδί συνόδου επικοινωνίας παρέχεται από το σταθμό βάσεων περιοδικά .

$$AC = \text{Authentication Code} = \text{Hash}((\text{Encrypt})K_a (K_{ses}))$$

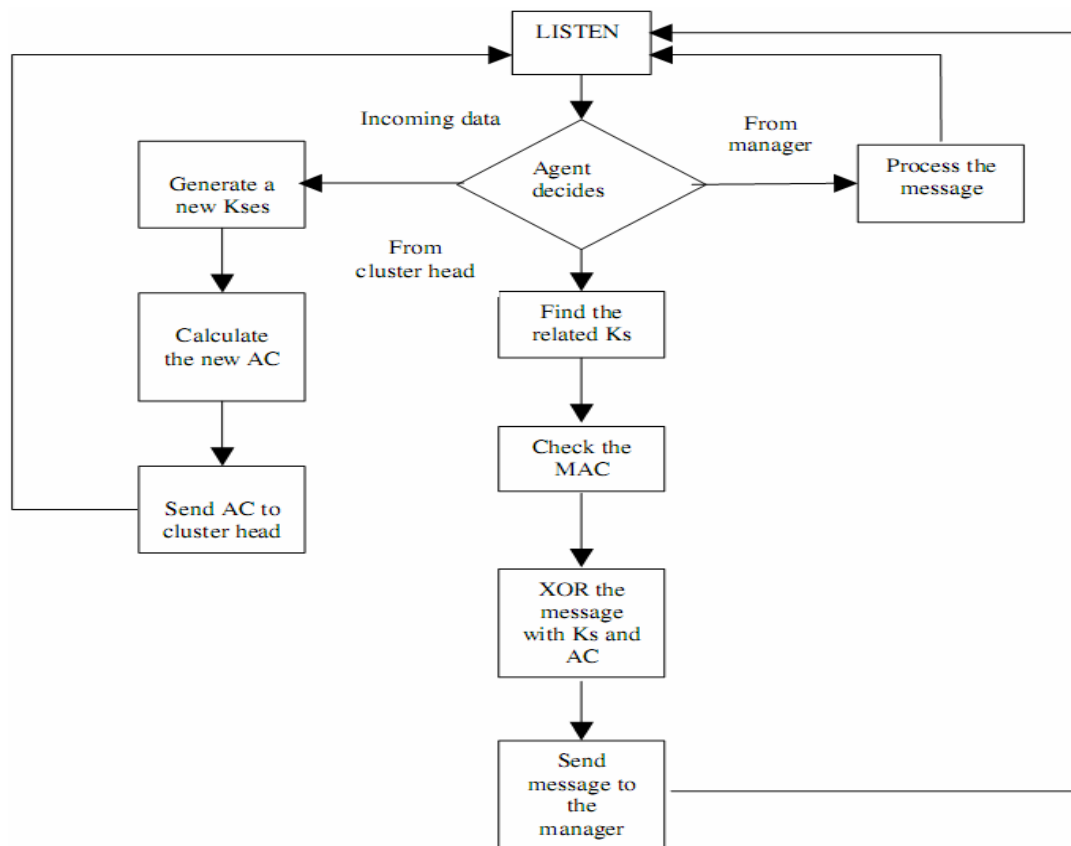
Κατόπιν ο πράκτορας στέλνει το AC σε όλους τους κόμβους αισθητήρων όλων των τομέων μέσω της κεφαλής των τομέων. Κατά τη λήψη του AC, κόμβος αισθητήρα πραγματοποιεί XOR τον AC με το κλειδί του (Ks) για να παράγει τον προσωπικό κώδικα πιστοποίησης αισθητήρων (PSAC - Personal Sensor Authentication Code). Αυτή η διαδικασία ξαναγίνεται όποτε ο πράκτορας παράγει ένα νέο Kses και μεταδίδει ευρέως ένα νέο AC.

$$\text{Personal Sensor Authentication Code (PSAC)} = AC \oplus K_s$$

Όταν ένας κόμβος αισθητήρων θέλει να στείλει δεδομένα στον πράκτορα μέσω του κεφαλιού του τομέα, πρώτα πραγματοποιεί XOR τα δεδομένα με το PSAC, κατόπιν προσθέτει τον κώδικα πιστοποίησης μηνυμάτων (MAC) στο τέλος του πακέτου, και στέλνει έπειτα το πακέτο μέσω του κώδικα CDMA του όπως φαίνεται στο σχήμα 6. Προτού να στείλει ο κόμβος αισθητήρων τα κρυπτογραφημένα δεδομένα συγκεντρώνονται στην κεφαλή σε ένα νέο πακέτο. Μόλις συλλεχτούν μαζί τα δεδομένα η κεφαλή του τομέα αποφασίζει ποιοι κόμβοι αισθητήρων πρέπει να επικοινωνήσουν. Μόνο εκείνοι οι κόμβοι αισθητήρων θα χρησιμοποιήσουν τους αντίστοιχους κώδικες τους PSAC και CDMA για να στείλουν τα δεδομένα τους. Αυτή η τεχνική είναι ένα ενεργειακά αποδοτικό πρωτόκολλο που αυξάνει τη διάρκεια ζωής των κόμβων αισθητήρων. Κατά τη λήψη των δεδομένων στο κώδικα CDMA, ο πράκτορας βγάζει αρχικά το αντίστοιχο Ks εκείνου του κώδικα. Χρησιμοποιώντας το Ks, ο πράκτορας ελέγχει τη MAC που βλέπει εάν τα δεδομένα τροποποιήθηκαν. Εάν δεν υπάρχει καμία τροποποίηση, ο πράκτορας πραγματοποιεί XOR τα δεδομένα με το Ks και το τρέχον AC. Το αποτέλεσμα είναι να πάρουμε τα πραγματικά δεδομένα που στάλθηκαν από τον κόμβο αισθητήρων όπως φαίνεται στο σχήμα 7. Οι πράκτορες έστειλαν μηνύματα στους κόμβους αισθητήρων με τον ίδιο τρόπο.



Σχήμα 6. Ενέργειες του κόμβου αισθητήρα



Σχήμα 7. Ενέργειες του πράκτορα

6 Συμπεράσματα

Παραπάνω περιγράφηκε ένα πρωτόκολλο ασφάλειας για τα ασύρματα δίκτυα αισθητήρων με τη χρησιμοποίηση συμμετρικού κλειδιού κρυπτογραφίας και των κωδικών CDMA. Αυτό το πρωτόκολλο ασφαλείας μπορεί να εφαρμοστεί στα ασύρματα δίκτυα αισθητήρων, δεδομένου ότι δεν περιλαμβάνει κρυπτογραφικές λειτουργίες που απαιτούν μεγάλη μνήμη και μεγάλη ισχύ επεξεργασίας.

Ο κακόβουλος χρήστης δεν μπορεί ποτέ να 'κλέψει' το AC διότι παράγεται με μια hash λειτουργία. Επιπλέον χρησιμοποιεί τη λειτουργία XOR, η οποία μπορεί να ολοκληρωθεί από πολυπλέκτη υλικού χωρίς οποιαδήποτε πρόσθετη κατανάλωσης ενέργεια. Είναι ένα πρωτόκολλο ασφαλείας το οποίο αναμφισβήτητα αυξάνει την ασφάλεια μεταδόσεων δεδομένων στα ασύρματα δίκτυα αισθητήρων.

Επιπρόσθετα παρουσιάστηκε η έννοια της παρακολούθησης και ελέγχου του περιβάλλοντος. Αναφέρθηκε η χρήση του προγράμματος την παρακολούθηση του περιβάλλοντος και περιγράφηκε με παραδείγματα. Τέλος έγινε μια μικρή αναφορά στην γνωστή δικτύωση σύννεφου η οποία μπορεί να εφαρμοστεί και στα δίκτυα αισθητήρων.

Η έννοια των δικτύων από αισθητήρες εισήχθη αρχικά πριν από δύο ή περισσότερο δεκαετίες και ήταν περισσότερο ένα όραμα. Οι πρώτοι ερευνητές βρήκαν πολλές δυσκολίες από την ικανότητα των αισθητήρων, των υπολογιστών, και των δικτύων επικοινωνίας. Ακόμα κι αν τα οφέλη των δικτύων αισθητήρων αναγνωρίστηκαν γρήγορα, η χρήση τους περιορίστηκε συνήθως στα μεγάλα στρατιωτικά συστήματα. Οι τεχνολογικές πρόοδοι στην προηγούμενη δεκαετία έχουν αλλάξει εντελώς την κατάσταση. Η τεχνολογία MEMS, η πιο αξιόπιστη ασύρματη επικοινωνία, και η χαμηλού κόστους κατασκευή έχουν οδηγήσει στους μικρούς, μικρού κόστους και ισχυρούς αισθητήρες με την ενσωματωμένη επεξεργασία και την ασύρματη ικανότητα δικτύωσης. Τέτοια ασύρματα δίκτυα αισθητήρων μπορούν να χρησιμοποιηθούν σε πολλές νέες εφαρμογές, που κυμαίνονται από τον περιβαλλοντικό έλεγχο ως τη βιομηχανική χρήση, καθώς επίσης και τις παραδοσιακές στρατιωτικές εφαρμογές. Στην πραγματικότητα, οι εφαρμογές περιορίζονται μόνο από τη φαντασία μας. Δίκτυα των μικρών, ενδεχομένως μικροσκοπικών αισθητήρων που ενσωματώνονται σε πολλούς τομείς της κοινωνίας: στα κτήρια και τα μηχανήματα, και ακόμη και στους ανθρώπους, που εκτελούν τον αυτοματοποιημένο συνεχή και διακριτό έλεγχο, θα μπορούσε δραστικά να ενισχύσει την κατανόηση του φυσικού περιβάλλοντός μας.

Βιβλιογραφία

- [1] Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, 2005 CRC Press.
- [2] Chee-Yee Chong; Kumar, S.P., Sensor networks: evolution, opportunities, and challenges, Proceedings of the IEEE, Volume 91, Issue 8, Aug. 2003 Page(s): 1247 - 1256
- [3] Ning Wang, Naiqian Zhang, Maohua Wang, Wireless sensors in agriculture and food industry—Recent development and future perspective, Computers and Electronics in Agriculture 50 (2006) 1–14
- [4] 10 emerging technologies that will change the world, Technol. Rev., vol. 106, no. 1, pp. 33–49, Feb. 2003.
- [5] J.W. Gardner, V. K Varadan, and O. O. Awadelkarim, Microsensors, MEMS and Smart Devices. New York: Wiley, 2001.
- [6] D. Steere, A. Baptista, D. McNamee, C. Pu, and J. Walpole, “Research challenges in environmental observation and forecasting systems,” in Proc. 6th Int. Conf. Mobile Computing and Networking (MOBICOMM), 2000, pp. 292–299.
- [7] B. Charny. (2002, Dec.) Wireless research senses the future. ZDNet News [Online] Available: <http://zdnet.com.com/2100-1105-976377.html>
- [8] D. Jensen. (2002, June) SIVAM: Communication, navigation and surveillance for the Amazon. Avionics Mag. [Online] Available: <http://www.aviationtoday.com/reports/avionics/previous/0602/0602sivam.htm>
- [9] R. Hills. (2001, July/Aug.) Sensing for danger. Sci. Technol. Rep. [Online] Available: <http://www.llnl.gov/str/JulAug01/Hills.htm>
- [10] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” Computer Networks, vol. 38, pp. 393–422, 2002.
- [11] Römer, Kay; Friedemann Mattern (December 2004). "The Design Space of Wireless Sensor Networks". *IEEE Wireless Communications* **11** (6): 54–61. doi:10.1109/MWC.2004.1368897
- [12] Topology Control in Wireless Ad Hoc and Sensor Networks, Paolo Santi, 2005 Wiley
- [13] A. Mainwaring, D Culler, J Polastre, R Szewczyk, J. Anderson, Wireless sensor networks for habitat monitoring, Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, 2002, pp. 88-97.
- [14] Guillermo Barrenetxea, Francois Ingelrest, Gunnar Schaefer, and Martin Vetterli, Wireless Sensor Networks for Environmental Monitoring: The SensorScope Experience, Communications, 2008 IEEE International Zurich Seminar on Volume, Issue, 12-14 March 2008 Page(s): 98 – 101
- [15] A. Sinha and A. Chandrakasan, “Dynamic power management in wireless sensor networks” IEEE Design and Test of Computers, pp. 62-74, March-April 2001.
- [16] K. Sohrabi, J Gao, V. Ailawadhi, G.J. Pottie, Protocols for self-organization of a wireless sensor network, IEEE Personal Communications, 2000
- [17] H. Çam, S. Ozdemir, D. Muthuavinashiappan, and P. Nair, "Energy-efficient security protocol for wireless sensor networks", IEEE VTC Fall 2003 Conference, October 4-9, Orlando, 2003
- [18] Suat Ozdemir and Prashant Nair, Wireless Sensor Network Security, REAS Symposium 2003 at Arizona State University
- [19] http://en.wikipedia.org/wiki/Cloud_computing
- [20] http://en.wikipedia.org/wiki/Wireless_Sensor_Networks
- [21] <http://www.wsn-security.info/>