Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.326 – 337

A SURVEY ON ANALOGY ON WIRELESS SENSOR NETWORKS

Abhishek Deb
B.E Student, Department of Information Science and Engineering, New Horizon College of Engineering, Bangalore, India
Email: debabhishek85@gmail.com

Akhil N Gaikwad
B.E Student, Department of Information Science and Engineering, New Horizon College of Engineering, Bangalore, India
Email: akhilgaikwad567@gmail.com

Mrs. Vandana C P
Assistant Professor, Department of Information Science and Engineering, New Horizon College of Engineering, Bangalore, India

Abstract: A Wireless Sensor networks (WSN) is an emerging technology and has a great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. Wireless sensor networks are characterized by severely constrained computational and energy resources, and an ad hoc operational environment. Wireless sensor networks (WSN) are currently receiving significant attention due to their unlimited potential. However, it is still very early in the lifetime of such systems and many research challenges exist. This technique has become an essential tool in many applications that requires communication between one or more sender's and multiple receivers. Since multiple users can use this technique simultaneously over a single channel, security has become a huge concern. Even though there are numerous ways to secure a wireless network and protect the network from numerous attacks, providing 100% security and maintaining confidentiality is a huge challenge in recent trends.

Keywords: wireless sensor networks, security for wireless networks, analogy for wireless networks.

1. INTRODUCTION

A Wireless sensor network (WSN) is a group of distributed sensors to monitor and record the physical and environment conditions such as temperature, sound, pressure, etc. and organize the collected data to a central location. It consists of a number of sensor nodes(few tens to thousands) working together to monitor a region to obtain data about the environment such sensor network nodes has typically several parts: a radio transceiver with an

internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

WSN are usually highly susceptible to collusion attacks thus ascertaining trustworthiness of data and reputation of sensor nodes is crucial for WSN. As the performance of very low power processors dramatically improves, future aggregator nodes will be capable of performing more sophisticated data aggregation algorithms, thus making WSN less vulnerable to attacks. Iterative filtering algorithms simultaneously aggregate data from multiple sources and provide trust assessment of these sources, usually in a form of corresponding weight factors assigned to data provided by each source. To address security issues, an improvement for iterative filtering techniques is proposed by providing an initial approximation for such algorithms which makes them not only collusion robust, but also more accurate and faster converging.

Due to a need for robustness of monitoring and low cost of the nodes, wireless sensor networks are usually redundant. Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the computing power and energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks. This cannot be remedied by cryptographic methods, because the attackers generally gain complete access to information stored in the compromised nodes. For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes. Thus, better, more sophisticated algorithms are needed for data aggregation in the future WSN.

In the presence of stochastic errors such algorithm should produce estimates which are close to the optimal ones in information theoretic sense. Thus, for example, if the noise present in each sensor is a Gaussian independently distributed noise with zero mean, then the estimate produced by such an algorithm should have a variance close to the Cramer- Rao lower bound (CRLB) [2], i.e, it should be close to the variance of the Maximum Likelihood Estimator (MLE). However, such estimation should be achieved without supplying to the algorithm the variances of the sensors, unavailable in practice.

The algorithm should also be robust in the presence of non-stochastic errors, such as faults and malicious attacks, and, besides aggregating data, such algorithm should also provide an assessment of the reliability and trustworthiness of the data received from each sensor node.

Trust and reputation systems have a significant role in supporting operation of a wide range of distributed systems, from wireless sensor networks and e-commerce infrastructure to social networks, by providing an assessment of trustworthiness of participants in such distributed systems. A trustworthiness assessment at any given moment represents an aggregate of the behaviour of the participants up to that moment and has to be robust in the presence of various types of faults and malicious behaviour. There are a number of incentives for attackers to manipulate the trust and reputation scores of participants in a distributed system, and such manipulation can severely impair the performance of such a system [3]. The main target of malicious attackers are aggregation algorithms of trust and reputation systems [4].

1.1 Types of WSNs (Wireless Sensor Networks)

The types of Wireless Sensor Network(WSN) are depended on the environment so that they can be deployed underwater, underground, on land, and so on. They are:-

1. Terrestrial WSNs
2. Underground WSNs
3. Underwater WSNs

4. Multimedia WSNs
5. Mobile WSNs

1. Terrestrial WSNs

Terrestrial WSNs are capable of communicating base stations efficiently, and consist of hundreds to thousands of wireless sensor nodes deployed either in unstructured (ad hoc) or structured (Preplanned) manner. In an unstructured mode, the sensor nodes are randomly distributed within the target area that is dropped from a fixed plane. The preplanned or structured mode considers optimal placement, grid placement, and 2D, 3D placement models.

In this WSN, the battery power is limited; however, the battery is equipped with solar cells as a secondary power source. The Energy conservation of these WSNs is achieved by using low duty cycle operations, minimizing delays, and optimal routing, and so on.

2. Underground WSNs:-

The underground wireless sensor networks are more expensive than the terrestrial WSNs in terms of deployment, maintenance, and equipment cost considerations and careful planning. The WSNs networks consist of a number of sensor nodes that are hidden in the ground to monitor underground conditions. To relay information from the sensor nodes to the base station, additional sink nodes are located above the ground.

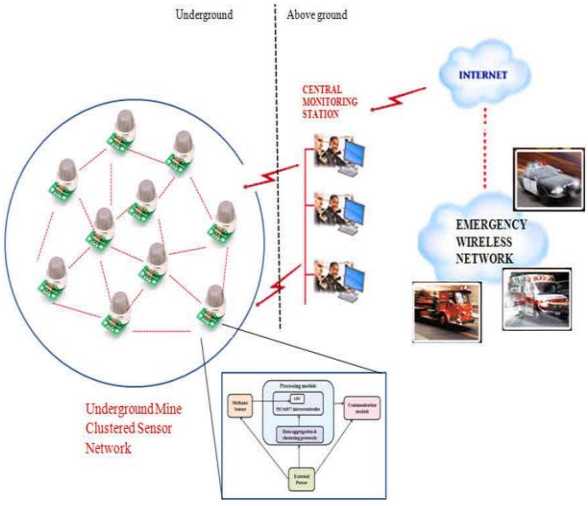

fig :-Underground WSNs

The underground wireless sensor networks deployed into the ground are difficult to recharge. The sensor battery nodes equipped with a limited battery power are difficult to recharge. In addition to this, the underground environment makes wireless communication a challenge due to high level of attenuation and signal loss.

3. Under Water WSNs:-

More than 70% of the earth is occupied with water. These networks consist of a number of sensor nodes and vehicles deployed under water. Autonomous underwater vehicles are used for gathering data from these sensor nodes. A challenge of underwater communication is a long propagation delay, and bandwidth and sensor failures.

Under water WSNs are equipped with a limited battery that cannot be recharged or replaced. The issue of energy conservation for under water WSNs involves the development of underwater communication and networking techniques.

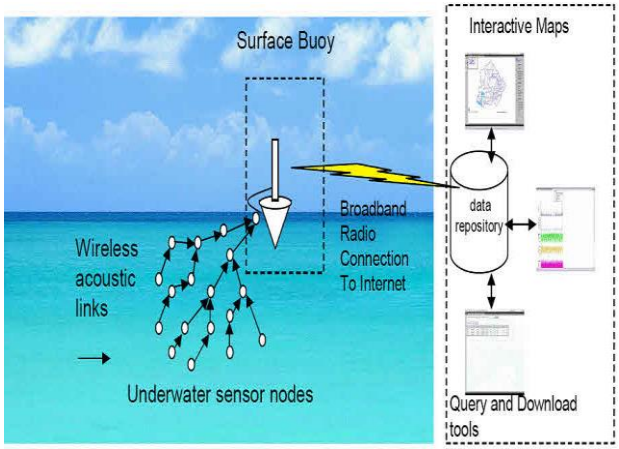

fig:- Underwater WSNs

4. Multimedia WSNs:- Multimedia wireless sensor networks have been proposed to enable tracking and monitoring of events in the form of multimedia, such as imaging, video, and audio. These networks consist of low-cost sensor nodes equipped with microphones and cameras. These nodes are interconnected with each other over a wireless connection for data compression, data retrieval and correlation.

The challenges with the multimedia WSN include high energy consumption, high bandwidth requirements, data processing and compressing techniques. In addition to this, multimedia contents require high bandwidth for the contents to be delivered properly and easily.

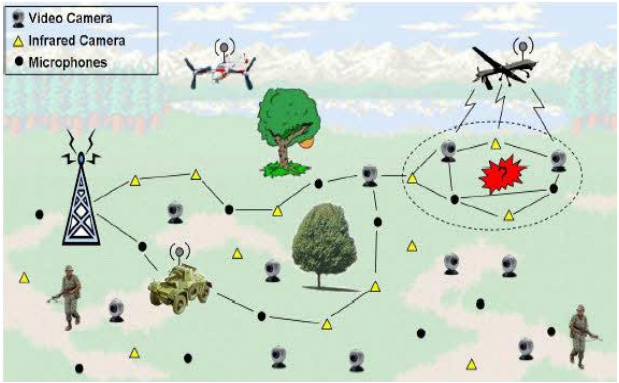

fig :-Multimedia WSNs

5. Mobile WSNs

These networks consist of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes have the ability to compute sense and communicate.

The mobile wireless sensor networks are much more versatile than the static sensor networks. The advantages of MWSN over the static wireless sensor networks include better and improved coverage, better energy efficiency, superior channel capacity, and so on.

2. Types of Attacks in WSN

2.1. Passive and active attacks criteria

Attacks can be classified into two major categories, according the interruption of communication act, namely passive attacks and active attacks.

Passive attack obtain data exchanged in the network without interrupting the communication. When it is referred to an active attack it can be affirmed that the attack implies the disruption of the normal functionality of the network, meaning information interruption, modification, or fabrication. Examples of passive attacks are traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay. Traffic analysis: Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication.

Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack): A Denial-of service attack (DoS attack) or distributed denial-of service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS

attacks typically target sites or services hosted on high profile web servers such as banks, credit card payment gateways, and even root name servers [5] [6].

Replay attack: A replay attack is a breach of security in which information is stored without authorization and then retransmitted to trick the receiver into unauthorized operations such as false identification or authentication or a duplicate transaction. For example, messages from an authorized user who is logging into a network may be captured by an attacker and resent (replayed) the next day. Even though the messages may be encrypted, and the attacker may not know what the actual keys and passwords are, the retransmission of valid logon messages is sufficient to gain access to the network.

The attacks can also be classified into external attacks and internal attacks, according the domain of the attacks. Some papers refer to outsider and insider attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights. Attacks on different layers of the Internet model: The attacks can be further classified according to the five layers of the Internet model. Table1 presents a classification of various.

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, Eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

Table 1 Security Attacks on Each Layer of the Internet Model

2.2. Cryptography and non-cryptography related attacks

Some attacks are non-cryptography related, and others are cryptographic primitive attacks. Table 2 shows cryptographic primitive attacks and the examples.

Cryptographic Primitive Attacks	Examples
Pseudorandom number attack	Nonce, timestamp, initialization vector (IV
Digital signature attack	RSA signature, ElGamal signature, digital signature standard (DSS)
Hash collision attack	SHA-0, MD4, MD5, HAVAL-128, RIPEMD

Table 2 Cryptographic Primitive Attacks

2.3. Physical layer attacks

Wireless communication is broadcast by nature. A common radio signal is easy to jam or intercept. An attacker could overhear or disrupt the service of a wireless network physically. Eavesdropping: Eavesdropping is the intercepting and security attacks on each layer of the Internet model. Some attacks can be launched at multiple layers

2.4. Link layer attacks

The Mobile Ad Hoc Network (MANET) is an open multipoint peer-to-peer network architecture. Specifically, one-hop connectivity among neighbors is maintained by the link layer protocols, and the network layer protocols extend the connectivity to other nodes in the network. Attacks may target the link layer by disrupting the cooperation of the layer's protocols. Wireless medium access control (MAC) protocols have to coordinate the transmissions of the nodes on the common transmission medium. Because a token-passing bus MAC protocol is not suitable for controlling a radio channel, IEEE 802.11 protocol is specifically devoted to wireless LANs. The IEEE 802.11 MAC protocol uses distributed contention resolution mechanisms for sharing the wireless channel. The IEEE 802.11 working group proposed two algorithms for contention resolution. One is a fully distributed access protocol called the distributed coordination function (DCF). The other is a centralized access protocol called the point coordination function (PCF). PCF requires a central decision maker such as a base station. DCF uses a carrier sense multiple access/collision avoidance protocol (CSMA/CA) for resolving channel contention among multiple wireless hosts.

2.5. Network layer attacks

A variety of attacks targeting the network layer have been identified and heavily studied in research papers. By attacking the routing protocols, attackers can absorb network traffic, inject themselves into the path between the source and destination, and thus control the network traffic flow. The traffic packets could be forwarded to a non-optimal path, which could introduce significant delay. In addition, the packets could be forwarded to nonexistent path and get lost. The attackers can create routing loops, introduce severe network congestion, and channel contention into certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, causing the network to partition, which triggers excessive network control traffic, and further intensifies network congestion and performance degradation Attacks at the routing discovery phase: There are malicious routing attacks that target the routing discovery or maintenance phase by not following the specifications of the routing protocols. Routing message flooding attacks, such as hello flooding, RREQ flooding, acknowledgement flooding, routing table overflow, routing cache poisoning, and routing loop are simple examples of routing attacks targeting the route discovery phase. Proactive routing algorithms, such as DSDV and OLSR, attempt to discover routing information before it is needed, while reactive algorithms, such as DSR and AODV, create routes only when they are needed. Thus, proactive algorithms performs worse than on demand schemes because they do not accommodate the dynamic of WSN and MANETs, clearly proactive algorithms require many costly broadcasts. Proactive algorithms are more vulnerable to routing table overflow attacks.

2.6. Transport layer attacks

The objectives of TCP-like Transport layer protocols in WSN include setting up of end-to-end connection, end to-end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection. Similar to TCP protocols in the Internet, the mobile node is vulnerable to the classic SYN flooding attack or session hijacking attacks [1] [3] [4]. However, a WSN has a higher channel error rate when compared with wired networks. Because TCP does not have any mechanism to distinguish whether a loss was caused by congestion, random error, or malicious attacks, TCP multiplicatively decreases its congestion window upon experiencing losses, which degrades network performance significantly.

SYN flooding attack: The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection.

For two nodes to communicate using TCP, they must first establish a TCP connection using a three-way handshake. The three messages exchanged during the handshake allow both nodes to learn that the other is ready to communicate and to agree on initial sequence numbers for the conversation. During the attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The SYN-ACK packets are sent out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the response of ACK packet. Without receiving the ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed size table while it awaits the acknowledgement of the three-way handshake, all of these pending connections could overflow the buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection.

Session hijacking: Session hijacking takes advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter. In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target and then performs a DoS attack on the victim. Thus the attacker impersonates the victim node and continues the session with the target.

2.7. Multi-layer attacks

Some security attacks can be launched from multiple layers instead of a particular layer. Examples of multilayer attacks are denial of service (DoS), man-in-the middle, and impersonation attacks.

Denial of service: Denial of service (DoS) attacks could be launched from several layers. An attacker can employ signal jamming at the physical layer, which disrupts normal communications. At the link layer, malicious nodes can occupy channels through the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks.

Impersonation attacks: Impersonation attacks are launched by using other node's identity, such as MAC or IP address. Impersonation attacks sometimes are the first step for most attacks, and are used to launch further, more sophisticated attacks.

Man-in-the-middle attacks: An attacker sits between the sender and the receiver and sniffs any information being sent between two ends. In some cases the attacker may impersonate the sender to communicate with the receiver, or impersonate the receiver to reply to the sender.

2.8. Cryptographic primitive attacks

Most security holes are due to poor implementation, i.e. weakness in security protocols. For example, authentication protocols and key exchange protocols are often the target of malicious attacks. Cryptographic primitives are considered to be secure; however, recently some problems were discovered, such as collision attacks on hash function, e.g. SHA-1. Pseudorandom number attacks, digital signature attacks, and hash collision attacks are discussed as following.

Pseudorandom number attacks: To make packets fresh, a timestamp or random number (nonce) is used to prevent a replay attack. The session key is often generated from a random number. In the public key infrastructure the shared secret key can be generated from a random number too. The conventional random number generators in most programming languages are designed for statistical randomness, not to resist prediction by cryptanalysts. In the optimal case, random numbers are generated based on physical sources of randomness that cannot be predicted. The noise from an electronic device or the position of a pointer device is a source of such randomness. However, true random numbers are difficult to generate. When true physical randomness is not available, pseudorandom numbers must be used. Cryptographic pseudorandom generators typically have a large pool (seed value) containing randomness.

Digital signature attacks: The RSA public key algorithm can be used to generate a digital signature. The signature scheme has one problem: it could suffer the blind signature attack. The user can get the signature of a message and use the signature and the message to fake another message's signature. The attack models for digital signature can

be classified into known-message, chosen-message, and key- only attacks. In the known message attack, the attacker knows a list of messages previously signed by the victim. In the chosen-message attack, the attacker can choose a specific message that it wants the victim to sign. But in the key-only attack, the adversary only knows the verification algorithm, which is public. Hash collision attacks: The goal of a collision attack is to find two messages with the same hash, but the attacker cannot pick what the hash will be. Collision attacks were announced in SHA-0, MD4, MD5, HAVAL-128, and RIPEMD. Normally all major digital signature techniques (including DSA and RSA) involve first hashing the data and then signing the hash value.

3. COLLUSION ATTACK

Sensors are usually deployed in unattended or even hostile environments, and an adversary may capture or compromise sensor nodes. Node compromise [5] occurs when an attacker gains control of a node in the network after deployment. Once in control of that node, the attacker can alter the node to listen to information in the network, input malicious data, cause DOS, black hole, or any one of a number of attacks on the network. Once this happens, the compromised nodes can easily inject false data reports of nonexistent events. Even worse, when an adversary compromises more nodes and combines all the obtained secret keys, the adversary can freely forge the event reports which not only "happen" at the locations where the nodes are compromised, but also at arbitrary locations in the field. These fabricated reports not only produce false alarms, but also waste valuable network resources, such as energy and bandwidth, when delivering the falsified reports to the base station. Therefore, it is important to design an effective filtering scheme to defend and minimize the impacts of false data injection attack.

The four main attacks caused by the compromised node are:

- A compromised node purposely drops aggregation message.
- A compromised node alters a message being relayed to the sink
- A compromised node purposely falsifies its own sensed reading
- A compromised node purposely falsifies the aggregate value it is relaying to its parent in a hierarchical network structure

Layer-wise node	**Compromisation attack**
Physical layer	Jamming attack
Data Link layer	Jamming attack, collision attack
Network Layer	False routing information, selective forwarding, disrupt routing protocol
Transport layer	False data injection, Packet dropping, Interrogation attack

Table 1: Layer-wise node and its compromisation attack.

4. APPLICATIONS OF WSN

Wireless sensor network has a lots of applications like security, monitoring, biomedical research, tracking etc. basically these application are used on emergency services. The applications of the sensor network are categorized into various classes such as Environmental data collection, Military applications, Security monitoring, sensor node tracking, health application, home application, and hybrid networks.

i. Environmental Data Collection

Environmental data collection application are used to collect various sensor data in a period of time. In the environmental data collection application, a large number of nodes continuously sensing and transmitting data back to a set of base stations that store the data using traditional methods. In typical usage scenario, the nodes will be evenly distributed over an outdoor environment. In environmental monitoring applications, it is not essential that the nodes develop the optimal routing strategies on their own. Instead, it may be possible to calculate the optimal routing topology outside of the network and then communicate the necessary sensor data to the nodes as required. This is possible because the physical topology of the network is relatively constant. While the time variant nature of RF communication may cause connectivity between two nodes to be intermittent, the overall topology of the network will be relatively stable.

ii. Military Applications

Most of the elemental knowledge of sensor networks is basic on the defence application at the beginning, especially two important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology form the Defence Advanced Research Project Agency (DARPA), sensor networks are applied very successfully in the military sensing. Now wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems. In the battlefield context, rapid deployment, self-organization, fault tolerance security of the network should be required. The sensor devices or nodes should provide following services: like Monitoring friendly forces, equipment and ammunition, Battlefield surveillance, Reconnaissance of opposing forces, Targeting, Battle damage assessment Nuclear, biological and chemical attack detection reconnaissance.

iii. Security Monitoring

Security monitoring networks are collected of nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors to detect an anomaly. A key difference between security monitoring and environmental monitoring is that security networks are not actually collecting any data. This has a significant impact on the optimal network architecture. Each node has to frequently check the status of its sensors but it only has to transmit a data report when there is a security violation. The immediate and reliable communication of alarm messages is the primary system requirement. These are "report by exception" networks. It is confirmed that each node is still present and functioning. If a node were to be disabled or fail, it would represent a security violation that should be reported. For security monitoring applications, the network must be configured so that nodes are responsible for confirming the status of each other. The optimal topology of a security monitoring network will look quite different from that of a data collection network. In a collection tree, each node must transmit the data of all of its decedents. The accepted norm for security systems today is that each sensor should be checked approximately once per hour. In security networks, a vast majority of the energy will be spend on confirming the functionality of neighboring nodes and in being prepared to instantly forward alarm announcements. Actual data transmission will consume a small fraction of the network energy.

iv. Node tracking scenarios

There are many condition where one would like to track the location of important assets or personnel. Current inventory control systems attempt to track objects by recording the last checkpoint that an object passed through. However, with these systems it is not possible to determine the current location of an object. For example, UPS

tracks every shipment by scanning it with a barcode whenever it passes through routing centers. The system breaks down when objects do not flow from checkpoint to checkpoint. In typical work environments it is impractical to expect objects to be continuously passed through checkpoints. With wireless sensor networks, objects can be tracked by simply tagging them with a small sensor node. The sensor node will be tracked as it moves through a field of sensor nodes that are deployed in the environment at known locations. Instead of sensing environmental data, these nodes will be deployed to sense the RF messages of the nodes attached to various objects. The nodes can be used as active tags that announce the presence of a device. A database can be used to record the location of tracked objects relative to the set of nodes at known locations. With this system, it becomes possible to ask where an object is currently, not simply where it was last scanned . Unlike sensing or security networks, node tracking applications will continually have topology changes as nodes move through the network. While the connectivity between the nodes at fixed locations will remain relatively stable, the connectivity to mobile nodes will be continually changing.

v. Health Applications

Sensor networks are also widely used in health care area. In some modern hospital sensor networks are constructed to monitor patient physiological data, to control the drug administration track and monitor patients and doctors and inside a hospital. In spring 2004 some hospital in Taiwan even use RFID basic of above named applications to get the situation at first hand. Long-term nursing home [9]: this application is focus on nursing of old people. In the town farm cameras, pressure sensors, orientation sensors and sensors for detection of muscle activity construct a complex network. They support fall detection, unconsciousness detection, vital sign monitoring and dietary/exercise monitoring.

vi. Home Application

Along with developing commercial application of sensor network it is not so hard to image that Home application will step into our normal life in the future. Many concepts are already designed by researcher and architects, like "Smart Environment: Some are even realized. Let's see the concept "the intelligent home": After one day hard work you come back home. At the front door the sensor detects you are opening the door, then it will tell the electric kettle to boil some water and the air condition to be turned on. You sit in the sofa lazily. The light on the table and is automatically on because the pressure sensor under the cushion has detected your weight. The TV is also on. One sensor has monitored that you are sitting in front of it. "I'm simply roasting. The summer time in Asia is really painful."You think and turn down the temperature of the air condition. At the sometime five sensors in every corner in the room are measuring the temperature. Originally there is also sensor in the air condition. But it can only get the temperature at the edge of the machine not the real temperature in the room. So the sensors in the room will be detecting the environment. The air condition will turn to sleep mode until all the sensors get the right temperature. The light on the corridor, in the washing groom and balcony are all installed with sensor and they can be turned on or turn out automatically. Even the windows are also attached with vibratory sensors connected to police to against thief.

REFERENCES

Journal Papers:

[1] F.L. Lewis , Wireless Sensor Networks paper.

[2] S. Bandyopadhyay, E. J. Coyle, An energy efficient hierarchical clustering algorithm for wireless sensor networks, IEEE Conference on Computer

[3] Mike Horton, John Suh, Vision for Wireless Sensor Networks IEEE 2005. Communication (INFOCOM)

[4] F. Akyildiz and I.H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges,"; Ad Hoc Networks, vol. 2, no. 4, pp. 351-367, Oct. 2004.

[5] J. Yick, B. Mukherjee, D. Ghosal, Analysis of a Prediction-based Mobility Adaptive Tracking Algorithm, in: Proceedings of the IEEE Second International Conference on Broadband Networks (BROADNETS), Boston, 2005.

[6] A. Mpitziopoulos, D. Gavalas, A survey on jamming attacks and countermeasures in WSNs, Surv. Tutor. 11(4) (2009) http://dx.doi.org/10.1109/SURV.2009.090404

Books:
[7]Behrouz A. Forouzan , Data Communication and Networking.

