ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (67-76), Month: April-June 2014, Available at: www.researchpublish.com

A Survey on Wireless Sensor Network Security

Payal Arora, Asha Gupta

CSE Department
Dronacharya College of Engineering, Greater Noida, U.P.

Abstract: **As Wireless Sensor Networks has ability to cope with node failures and it helps in mobility of nodes. So WSN needs effective security mechanisms because sensor networks may interact with sensitive data. This paper includes an overview on security and describes some unique security challenges a WSNs faces with. We will discuss about some security threats and review some proposed security challenges for WSNs.**

Keywords: **WSN, Security, Threats, Challenges, Attacks.**

1. INTRODUCTION

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one or more sensors. WSNs also measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. Due to potentially low cost solution [1] the WSNs are becoming very popular. Some securities techniques are implemented on WSNs due to their lack of data storage and power [2].In addition, there are many attacks designed to exploit the unreliable communication channels and unattended operation of wireless sensor networks.

2. Background of sensor

2.1 Technology:

WSNs form a particular class of ad hoc networks that operate with little or no infrastructure. WSNs are gaining momentum as they have great potential for both research and commercial applications. The sensor network nodes themselves are ideally low-priced, very small devices. They typically consist of a collection of application specific sensors, a wireless transceiver, a simple general purpose processor, possibly assisted by limited, amount of special-purpose hardware, and an energy unit that may be a battery or a mechanism to obtain energy from the environment. We cannot assume that sensor nodes will be tamper- resistant, although we will consider the availability of such tamper-resistant nodes for future applications. Sensor nodes are distributed over a potentially vast geographical area to form a static, multi-hop, self-organizing network. However, also mobile WSNs and mobility within WSN are conceivable.[3]

3. Applications of sensor networks

Traditionally, WSNs have been used in the context of high-end applications such as radiation and nuclear-threat detection systems; weapon sensors for ships; battle-field reconnaissance and surveillance; military command, control, communications, intelligence, and targeting systems; biomedical applications; habitat sensing; and seismic monitoring. Recently, interest has been extended to networked biological and chemical sensors for national security applications. Applications with potential growth in the near future include military sensing, physical security, process control, air traffic control, traffic surveillance, video surveillance, industrial and manufacturing automation, distributed robotics, weather sensing, environment monitoring, and building and structure monitoring. List of some potentially applications are:

- Industrial automation
- Automated and smart homes
- Video surveillance
- Traffic monitoring
- Medical device monitoring
- Monitoring of weather conditions
- Air traffic control
- Robot control.

4. Networking Topologies and Protocols

Wireless sensor networking topologies generally fall into four categories: one-way, bi-directional, star and mesh topology. The first networking protocols were simple one-way communication links, still common in applications such as tire pressure monitoring systems, garage door openers and television remote controls. As the need for more advanced topologies became apparent, networking engineers developed low-memory protocols for bi-directional, star and finally mesh technologies. In addition, the industry is making the transition from proprietary to standardized protocols, similar to the transition in MCUs from proprietary instruction sets and toward 8051-based cores for 8-bit processing and ARM-based solutions for 32-bit applications. Having a set of standardized networking protocols such as ZigBee and its variants removes the burden of continuous development costs and frees vendors to focus on their specific applications.

The emergence of cost-effective mesh topologies enables new applications where traditional star topologies come up short. For example, a home lighting application can quickly exceed 30 lights and sensors. A Wi-Fi router is frequently unable to provide whole-house coverage due to multipath propagation or shadowing, but a mesh topology ensures a robust connection to all locations in the house with lowest cost-per-node. Furthermore, mesh topologies enabled by ZigBee software such as Silicon Labs' Ember Net PRO allow hundreds and potentially thousands of nodes on a single network, much more than the number of devices permitted by Bluetooth (seven) or Wi-Fi.

5. SECURITY

While the future of WSNs is very prospective, WSNs will not be successfully deployed if security, dependability and privacy issues are not addressed adequately. These issues become more important because WSNs are usually used for very critical applications. Furthermore, WSNs are very vulnerable and thus attractive to attacks because of their limited prices and human-unattended deployment.

Security deals with:

- Confidentiality (encryption)
- Integrity (e.g., identity Management, digital signatures)
- Availability (protection from denial of Service).

Explanation of security Requirements:

1. DATA CONFIDENTIALITY

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following

• A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.

• In many applications nodes communicate highly sensitive data, e.g. key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.

• Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

2. DATA INTEGRITY

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

3. AVAILABILITY

Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the availability of a sensor and sensor network for the following reasons:

• Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
• Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.
• A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.

The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network.

6. CHALLENGES

For WSNs to become truly ubiquitous, a number of challenges must be overcome. Challenges and limitations of wireless sensor networks include the following:

- Limited functional capabilities, including problems of size
- Power factors
- Node costs
- Environmental factors
- Transmission channel factors
- Topology management complexity and node distribution
- Standards versus proprietary solutions
- Scalability

7. Feasibility of Basic Security Schemes in Wireless Sensor Networks

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, nonrepudiation, and anti-playback [5].The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased.Forthe secure transmission of various types of information over networks, several cryptographic, steganography and other techniques are used which are well known. In this section, we discuss the network security fundamentals and how the techniques are meant for wireless sensor networks.

7.1 Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power [6] [7] [8] [9]. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the

sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks. Moreover, some critical questions arise when applying encryption schemes to WSNs like, how the keys are generated or disseminated. How the keys are managed, revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for the network. As minimal (or no) human interaction for the sensors, is a fundamental feature of wireless sensor networks, it becomes an important issue how the keys could be modified time to time for encryption. Adoption of pre-loaded keys or embedded keys could not be an efficient solution.

7.2 Steganography

While cryptography aims at hiding the content of a message, steganography aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.) .The main objective of steganography is to modify the carrier in a way that is not perceptible and hence, it looks just like ordinary. It hides the existence of the covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to steganography and processing multimedia data (like audio, video) with the inadequate resources of the sensors is difficult and an open research issue.

7.3 Physical Layer Secure Access

Physical layer secure access in wireless sensor networks could be provided by using frequency hopping. A dynamic combination of the parameters like hopping set (available frequencies for hopping), dwell time (time interval per hop) and hopping pattern (the sequence in which the frequencies from the available hopping set is used) could be used with a little expense of memory, processing and energy resources. Important points in physical layer secure access are the efficient design so that the hopping sequence is modified in less time than is required to discover it and for employing this both the sender and receiver should maintain a synchronized clock.

8. SECURITY THREATS IN WSNs

The sensor nodes are distributed deployed in uncontrollable environment for the collection of security-sensitive information .Individual sensor nodes rely on multi-hop wireless communication to deliver the sensed data to a remote base station. In a basic WSN scenario, resource constraint, wireless communication, security-sensitive data, uncontrollable environment, and even distributed deployment are all vulnerabilities. These vulnerabilities make WSNs suffer from an amazing number of security threats. WSNs can only be used in the critical applications after the potential security threats are eliminated.

Traditional WSNs are affected by various types of attacks. These attacks can be categorized as:

1. Attacks on secrecy and authentication
2. Silent attacks on service integrity
3. Attacks on network availability

Cryptographic techniques can be used to prevent against the secrecy and authentication attacks. In silent attacks, the attacker compromises a sensor node and feeds wrong data. Attacks on network availability are also known as denial of service (DoS) attacks. If DoS attacks are promoted successfully, it can badly degrade the functioning of WSNs.
Below we discuss the DoS attacks on different layers of networks.

A. DoS attacks on the physical layer Physical layer are engaged with frequency selection, carrier frequency generation, signal detection, modulation and data encryption. Jamming is the most common way of injecting DoS attack on this layer.

B. DoS attacks on the link layer Link layer is exposed to multiplexing of data streams, data frame detection, medium access control and error control. The attacks when elevated on this layer results in collision, resource exhaustion and unfairness in allocation of frames.

C. DoS attacks on the network layer Network layer is exposed to different types of attacks such as spoofed routing information, selective forwarding, sinkhole, Sybil, wormhole, hello flood and acknowledgment flooding.

D. DoS attacks on the transport layer Transport layer is exposed to flooding attack and de-synchronization attack.
E. DoS attacks on the application layer Application layer are exposed to logic errors and buffer overflow.

9. Attacks in Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here we point out the major attacks in wireless sensor networks.

9.1 Denial of Service:

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.
Various DoS attacks on different layers are discussed below.

A. Jamming: Jamming is one of the basic yet destructive attacks that attempt to interrupt in physical layer of the WSN structure. Jamming can be of two types- constant jamming and intermittent jamming. Constant jamming affects the complete obstruct of the whole network whereas in intermittent jamming nodes are capable of communicating data periodically but not continuously.

B. Physical Attack: Physical attacks give the adversary the endowment to reconstruct the nodes and thus the network functioning at physical layer. The attacker can abstract source code which ultimately provides attacker the information about the network that can alter the code to get admittance into the network. Attacker can substitute the nodes with the illegal and detrimental ones, thus negotiating the functioning of the whole sensor network. Various types of physical attacks are listed below in the table with their definitions, threats and effects.

Attacks Definition Threat Effects Signal/ radio jamming. The attacker tries to transfer radio signals issued by the sensors to the receiving antenna. Availability, integrity Radio interference, resource exhaustion Device tampering attack, node capturing attack Direct physical approach, conquered and redeem nodes Availability, integrity, authenticity, confidentiality Corrupt/ transform physically, halt/modify node's functions, software susceptibilities, fully manages the hooked nodes Path-Based DOS Amalgamation of attacks Availability, authenticity Nodes battery discharge, network interruption, minimizing network's availability Node outage Halting the working of nodes Availability, integrity Halts nodes operations, bombarding a diversity of other attacks Eavesdropping Observing the essence of conversation by tapping venture to information Confidentiality Bombarding other attacks, citing delicate data, remove the privacy protection and minimizing data confidentiality

C. Collision: Collision is a type of link layer jamming that occurs when two nodes try to transfer data at the same time and at the same frequency. An attacker may cause collisions in particular packets such as ACK control messages. The effected packets are transmitted again, increasing the energy and time cost for transmission. Such an attack reduces the network perfection.

D. Exhaustion: Exhaustion occurs at the link layer. This attack dominates the power resources of the nodes by causing them to retransmit the message even when there is no collision or late collision.

E. Unfairness MAC protocols at link layer administer the communications in networks by constraining priority schemes for seamless correlation. It is possible to use these protocols thus affecting the precedence schemes, which ultimately results in decrease in service.

F. Neglect and Greed Attack: This attack occurs at the network layer. When a packet is transmitted from a sender to a receiver, then in between both these nodes, there occur a number of other nodes through which the packet is routed before reaching to the final destination. Transmission is said to be successful when the packet is completely reached to its destination. In the meanwhile, malicious node can force multi-hopping in the network, either by splashing some packets or by routing the packets towards a wrong node. This attack disturbs the behavior of the adjoining nodes, which may not be able to receive or send messages.

G. Homing: In homing attack, the attacker investigates the network traffic at the network layer to interpret the geological area of cluster heads or base station adjoining nodes. It then implements some other attacks on these crucial nodes, so as to physically destroy them that further cause major destruction to the network.

H. Routing Information Alteration (spoofing): It occurs at the network layer. In this, an adversary spots the routing information in the network by modifying or replaying the routing information to disturb the traffic in the network. This attack can create new routing paths, attracts or repels the network traffic from selected nodes, lengthen or shorten the source routes, generates false error messages, causes network division and maximizes the end-to-end latency.

I. Black holes: It is also known as sinking holes occurring at the network layer. It builds a covenant node that seems to be very attractive in the sense that it promotes zero-cost routes to neighboring nodes with respect to the routing algorithm. Nodes adjoining to these harmful nodes collide for immense bandwidth, thus resulting into resource contention and message destruction.

J. Flooding: Flooding also occurs at the network layer. An adversary constantly sends requests for connection establishment to the selected node. To hit each request, some resources are allocated to the adversary by the targeted node. This may result into effusion of the memory and energy resources of the node being bombarded.

K. Sybil Attack: This again is a network layer attack. In this, an awful node presents more than one character in a network. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. The Sybil attack is efficient enough to stroke other fault tolerant schemes such as disparity, multi path routing, routing algorithms, data aggregation, voting, fair resource allocation, and topology maintenance and misbehavior detection. The fake node implies various identities to other nodes in the network and thus occurs to be in more than one place at a time. In this way, it disturbs the geographical routing protocols. It can collide the routing algorithms by constructing many routes from only one node.

L. Selective Forwarding: Selective forwarding is a network layer attack. In this, an adversary covenants a node, that it scrupulously forwards some messages and plunge the others. This hampers the quality of service in WSN. If the attacker will drop all the packets then the adjoining nodes will become conscious and may evaluate it to be a flaw. To avoid this, the attacker smartly forwards the selective data. To figure out this type of attack is a very tedious job.

M. Worm holes: In the wormhole attack, pair of awful nodes firstly discovers a wormhole at the network layer. A wormhole is a low-latency junction between two sections of a network. The malicious node receives packets in one section of the network and sends them to another section of the network. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location. This may cause congestion and retransmission of packets squandering the energy of innocent nodes.

N. Hello Flood Attacks: Hello flood attack uses HELLO message to advertise itself to its adjoining nodes and a node receiving this message may consider that it is within radio vicinity of the sensor. In this type of attack, an adversary with a high radio transmission range and processing power sends HELLO message to a number of sensor nodes which are scattered in a large area within a WSN. It gives an illusion that the malicious node is their neighbor. When the assured

nodes will send message to the base station, then it passes through the malicious node as this node provides the shortest route to the base station as an illusion. When the information reaches the attacker, the victim is betrayed by it. This leads to data congestion and thus complicates the data flow in the network.

O. Acknowledgement Spoofing: Acknowledgements play a significant role in certifying the quality of service and creating another links. Acknowledgement spoofing attack is introduced on routing algorithms at the network layer that needs transmission of acknowledgement messages. An attacker may eavesdrop packet transference from its adjoining nodes and swindle the acknowledgements, thereby sending wrong information to the nodes.

P. De-synchronization: De-synchronization occurs at the transport layer. This attack tries to disturb an existing connection. An adversary continuously swindles packets to an end host. This host then demands retransmission of dropped frames and hence the energy of nodes is wasted, therefore degrading the performance of the whole network.

Q. Interrogation: An interrogation attack imposes on the two way handshake (request-to-send/clear-to-send) that several MAC protocols use to reduce the hidden-node problem. An adversary can misuse a node's resources by frequently sending RTS messages to obtain CTS responses from a directed adjoining node.

9.2 Attacks on Information in transit:

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks. As sensor nodes typically have short range of transmission and scarce resource, an attacker with high processing power and larger communication range could attack several sensors at the same time to modify the actual information during transmission.

10. Obstacles of Sensor Security

- Very Limited Resources
- Unreliable Communication
- Unattended Operation[4]

11. Proposed Security Schemes and Related Work

In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchers around the world. In this section we review and map various security schemes proposed or implemented so far for wireless sensor networks.

11.1 Security Schemes for Wireless Sensor Networks

There are various methods for secure routing in wireless sensor networks. It tell us how to design secure distributed sensor networks with multiple supply voltages to reduce the energy consumption on computation and therefore to extend the network's life time. It aims at increasing energy efficiency for key management in wireless sensor networks and uses Youngish network model for its application. Wood et al. studies DoS attacks against different layers of sensor protocol stack. JAM presents a mapping protocol which detects a jammed region in the sensor network and helps to avoid the faulty region to continue routing within the network, thus handles DoS attacks caused by jamming.

In the authors show that wormholes those are so far considered harmful for WSN could effectively be used as a reactive defense mechanism for preventing jamming DoS attacks. Ye et. al. presents a statistical en-route filtering (SEF) mechanism to detect injected false data in sensor network and focus mainly on how to filter false data using collective secret and thus preventing any single compromised node from breaking the entire system. SNEP & µTESLA are two secure building blocks for providing data confidentiality, data freshness and broadcast authentication. Tiny Sec proposes a link layer security mechanism for sensor networks which uses an efficient symmetric key encryption protocol.

Newsome et. al. proposes some defense mechanisms against Sybil attack in sensor networks. Kulkarni et al. analyzes the problem of assigning initial secrets to users in ad-hoc sensor networks to ensure authentication and privacy during their communication and points out possible ways of sharing the secrets. It presents a probabilistic secret sharing protocol to defend Hello flood attacks. The scheme uses a bidirectional verification technique and also introduces multi-path multi-base station routing if bidirectional verification is not sufficient to defend the attack.

Security Schemes	Attacks Deterred	Network Architecture	Major Features
JAM	DoS Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbor nodes
Wormhole based	DoS Attack (Jamming)	Hybrid (mainly wireless partly wired) sensor network	Uses wormholes to avoid jamming
Statistical En-Route Filtering	Information Spoofing	Large number of sensors, highly dense wireless sensor network	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution etc.	Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting Sybil entity
Bidirectional Verification, Multi-path multi-base station routing [	Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On Communication Security	Information or Data Spoofing	Traditional wireless sensor network	Efficient resource management, Protects the network even if part of the network is compromised
TIK	Wormhole Attack, Information or Data Spoofing	Traditional wireless sensor network	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Key Predistribution	Data and information spoofing, Attacks in information in Transit	Traditional wireless sensor network	Provide resilience of the network, Protect the network even if part of the network is compromised Provide authentication measures for sensor nodes
REWARD	Black hole attacks	Traditional wireless sensor network	Uses geographic routing, Takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect

			black hole attack
Tiny Sec	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Focuses on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP & µTESLA	Data and Information Spoofing, Message Replay Attacks	Traditional wireless sensor network	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead

REWARD is a routing algorithm which fights against black holes in the network. It proposes separate security schemes for data with various sensitivity levels and a location-based scheme for wireless sensor networks that protects the rest of the network, even when parts of the network are compromised. It implements symmetric key cryptographic algorithms with delayed key disclosure on motes to establish secure communication channels between a base station and sensors within its range and propose key pre-distribution schemes, which target to improve the resilience of the network. In Table we summarize various security schemes along with their main properties proposed so far for wireless sensor networks.

12. Holistic Security in Wireless Sensor Networks

A holistic approach aims at improving the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach could be the best option.

12.1 Holistic view of Security in wireless sensor networks

The holistic approach has some basic principles like, in a given network; security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not surpass the assessed security risk at a specific time, if there is no physical security ensured for the sensors, the security measures must be able to exhibit a graceful degradation if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measures should be developed to work in a decentralized fashion. If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building security layers as in the holistic approach, protection could be established for the overall network.

13. Conclusion

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. Even if holistic security could be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming day.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–114, August 2002.

[2] Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.) 2006 Auerbach Publications, CRC Press.

[3] Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA,Security Solutions for Wireless Sensor Networks.

[4] D. W. Carman, P. S. Krus, and B. J. Matt. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[5] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security forSensor Networks", CADIP Research Symposium, 2002, available at,http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf

[6] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no.5, 2002, pp. 521-534.

[7] Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003).vol.1, pp. 335 - 340.

[8] Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets, M., and Tuan, T., "PicoRadios for wireless sensor networks: the next challenge in ultra-low power design" 2002 IEEE International Solid-State Circuits Conference (ISSCC 2002), Volume 1, 3-7 Feb. 2002, pp. 200 –201.

[9] Hollar, S, "COTS Dust", Master's Thesis, Electrical Engineering and Computer Science Department, UC Berkeley, 2000.

[10] http://image.sciencenet.cn/olddata/kexue.com.cn/bbs/upload/12615WSN-2007.pdf