International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 5, August 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Review on Wireless Sensor Network Security

Vijay Kumar Kalakar[1], Hirdesh Chack[2], Syed Tariq Ali[1]

[1,2]Lecturer, Department of Electronics and Telecommunication,
[1]Government Women's Polytechnic College, Bhopal, Madhya Pradesh, India
[2]Government Polytechnic College, Jatara, Madhya Pradesh, India

ABSTRACT

Wireless sensor networks are attracting more and more coverage. A number of surveillance, regulation, and tracking systems have been developed for different scenarios in recent years. Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks. We also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks.

KEYWORDS: *Wireless sensor networks, Security, Attack, Holistic, Challenge*

How to cite this paper: Vijay Kumar Kalakar | Hirdesh Chack | Syed Tariq Ali "A Review on Wireless Sensor Network Security" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-5, August 2020, pp.329-334, URL: www.ijtsrd.com/papers/ijtsrd31837.pdf

I. INTRODUCTION

The Wireless Sensor Networks (WSNs) can be defined as a wireless, self-configured network without infrastructure, which monitors physical, environmental and sound conditions, temperature , vibration, pressures, movement and pollutants and collectively transfers their information via the network to a principal place or sink, where data can be monitored and analyzed. A sink or base station acts as a networking interface. By injecting queries and collecting results from the sink, you can get the required information from the network [1, 2].

Wireless sensor networks (WSN) are an ad hoc network system where resource-contracted sensor nodes are used to track and manage functions of a specific type. One or more detection units, a single processor, a memory, a communication element and a power source comprise a typical configuration of the sensor nodes. These sensors are then used to calculate a certain physical magnitude from the surrounding environment [3, 4].

In general, hundreds of thousands of sensor nodules in a wireless sensor network. Radio signals may be used to contact the sensor nodes. A wireless node has sensor and computing equipment, radio transceivers and control supplies [5]. The resource limitations of individual nodes in a wireless sensor network (WSN) are limited: there is little speed of transmission, storage space and bandwidth of communication. After the sensor nodes are installed, they often coordinate themselves through multi-shop connectivity to an effective network infrastructure. And onboard sensors begin to capture useful details. Wireless sensor devices also respond to "control site" queries to provide sensing samples or to perform specific directives. Whether constant or event controlled operation mode of the sensor nodes is feasible. For geographic details and positioning purposes, global positioning system (GPS) and local positioning algorithms may be used [1, 4].

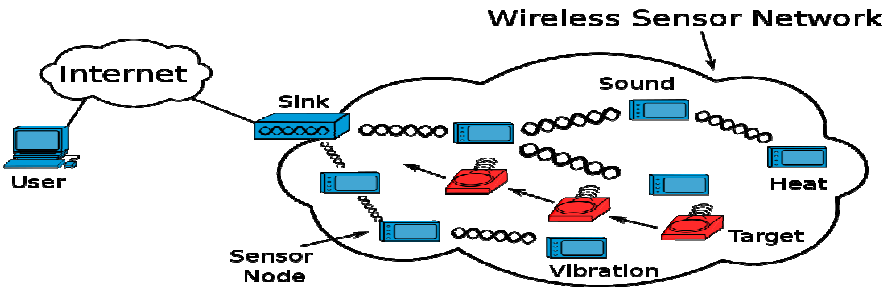

Figure1. Wireless sensor network.

The interaction between sensors takes place with wireless transceivers in the case of a wireless sensor network. Numerous scholars focused on different problems relevant to these forms of networks owing to the enticing characteristics of wireless

sensor networks. Although routing approaches and the simulation of wireless sensors for networks are becoming a major concern, the safety issues are not yet completely addressed. Throughout this article, we address protection concerns and threats for wireless sensor networks of the next decade and explore the main criteria for comprehensive analysis [7].

II. STRUCTURE OF A WIRELESS SENSOR NETWORK

The Wireless Sensor Network structure consists of different radio communications network topologies. The following is a short discussion of the network topologies applicable to wireless sensor networks [5, 6]:

Star network (Single point-to – multipoint)

A star network is a topology for communication that can be sent and/or received from a single station to certain remote nodes. You cannot send messages to each other via remote nodes. This form of network has the benefit of being quick, enabling the remote node to retain a minimal energy consumption. Low latency communication between the remote node and the base station is also possible. The downside of such a network is that it needs to be inside the radio propagation spectrum of all specific nodes and not as reliable as other networks because of the need to control the network on a single node.

Mesh Network

A mesh network can transmit data to a node within the radio transmission range of a network. This enables what is regarded as multi-hop contact, i.e., to be done by an intermediary node where a node wants to transmit a message to another node which is not inside the radio transmission range. Redundancy and scalability benefit from this network topology. If a node fails, any other node within its range can still be communicated by a distance node, which can transmission the message to the required place.

Hybrid Star-Mesh Network

A hybrid between the star and the mesh network offers the communication network to be robust and versatile whilst maintaining the ability to minimize the power consumption of wireless sensors. The lowest power sensor nodes are not capable of forwarding messages in this network topology. This ensures a minimum energy consumption. However, there are other nodes in the network that can be transferred from low power nodes to other nodes on the network with multihop capabilities [8].

III. STRUCTURE OF A WIRELESS SENSOR NODE

Four fundamental components such as the sensor unit, processor unit, transceiver unit and power unit shown in the figure are presented at a sensor Node. There are additional components dependent on applications such as a location search system, a power generator and a mobilizer. Two sub-units: sensors, and digital converter analog (ADCs) are usually made up of sensing units [9].

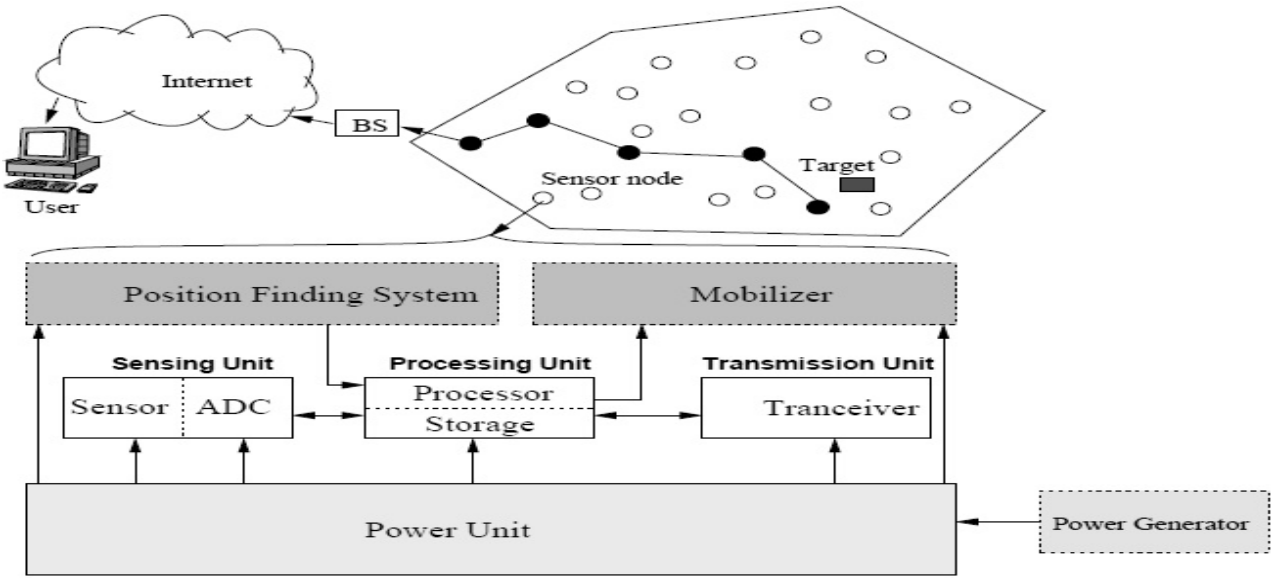

Figure 2 Components of a sensor node

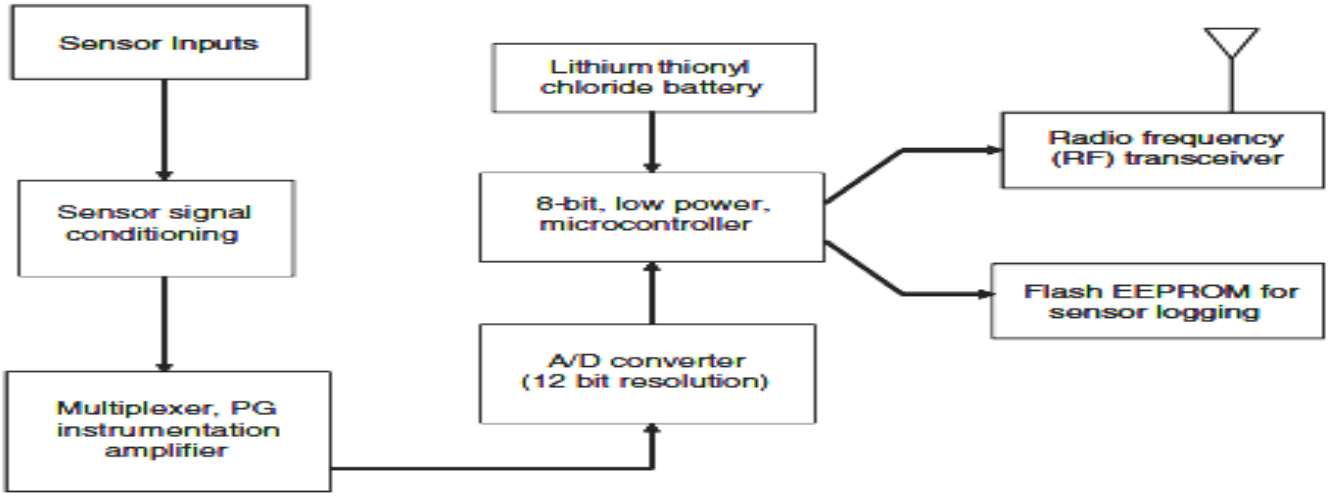

Figure 3 Functional block diagram of a sensor node

The sensors convert analog signals into digital signals through ADC and then relay them into the treatment unit. The processing unit is usually linked to a small storage unit and can manage the processes by which the sensor node works with other nodes to perform tasks. The network node is attached to a transceiver array. The control generator is one of the key components of a sensor node. A power-scavenging unit, such as solar cells, can support power units. The remaining sub-units of the node depend on the application [10].

IV. SECURITY ISSUES IN WIRELESS SENSOR NETWORK

Many security risks and assaults in wireless networks are much like their wired equivalent, though others have wireless networking included. Wireless networks are generally more vulnerable to different security threats since the unguided medium is more vulnerable to safety attacks than the guided medium. A simple eavesdropper candidate is the radio nature of wireless communication. In most cases, different security issues and threats associated with the wireless ad-hoc networks that we consider also apply to wireless sensor networks.

While the ad-hoc networks are self-organized, decentralized topology, the peer-to - peer networks that comprise a group of mobile nodes and the centralized entity is not available; the networks with a wireless sensor may include a command node or base station (central entity often referred to as a sink). The big challenge, however, is caused by the resource limitation of small sensors [7, 8].

WSNs are vulnerable against so many attacks. Attackers can attack the radio transmission; add their own data bits to the channel, replay old packets and any other type of attack. A secure network ought to support all security properties. Attackers may deploy some malicious nodes in the network with similar capabilities as of normal node or may overwrite the memory of normal deployed node by capturing them.

Attacks in wireless sensor network are shown in Figure 4. They are roughly categorized as follows: A) Based on Routing B) Based on Capability C) Based on Protocol Layer.

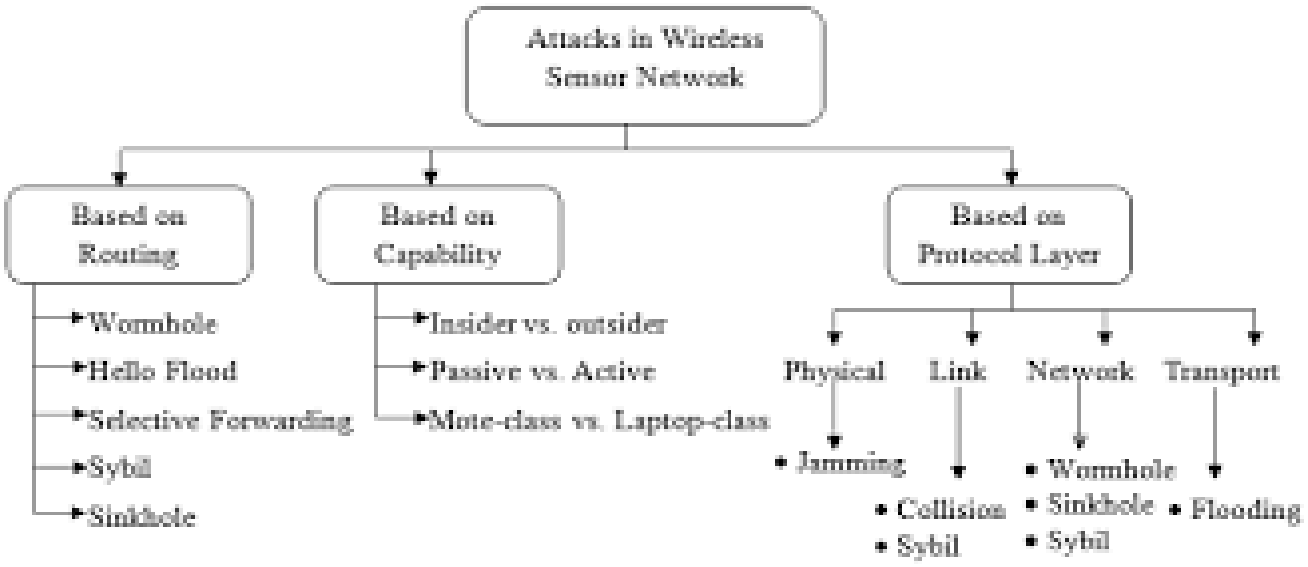

Figure 4 Attack classification in WSN

4.1. Based on Capability

The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or/ as well as active or passive attack against the network.

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network. These attacks can be prevented by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated.

While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks.

When the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network. Active attacks can an internal or an external attack. The active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network.

Being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. This attack brings the attacker in strong position where attacker can modify, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network. In Passive attack, the attacker listen to network in order to get information, what is going on in the network? It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

4.2. Based on Protocol Layer

WSN is divided into different layers. The working of each layer is different. The attacks on the basis of protocol layers are explained below:

A. Physical Layer

Physical layer is used for transmitting information in raw bits over the wireless or wired medium. It is easy to jam a common radio signal. In general, physical layer attacks are categorized as: Eavesdropping, Tampering and Jamming. In eavesdropping attack, an unauthorized receiver reads the messages. Jamming attack implements under DoS attack. It is the interference with the radio frequency used by the network nodes. This completely changes the working of network.

B. Link Layer

Data link layer is utilized to ensure the proper communication on physical layer between nodes. This layer is in charge of multiplexing, error detection, packets collision prevention, repeated transmission of data and so on. Link-layer threats include collisions, interrogation, and packet replay. Error detection and correcting codes can be used to decrease the number of collisions but due to this the routing overhead in the network is increased. Another connection layer danger to WSNs is the denial-of-sleep attack, in which node is unable to go to into the sleep mode. This decreases the whole network lifetime.

C. Network Layer

For the data routing between nodes, nodes to sink, node to BS, node to CH, and vice versa, this layer is responsible. A direct attack on Routing protocols by the attackers can have impact on network data traffic, indulge themselves into the data path between the source and destination, and by this control the data flow. This infers that effective and powerful routing protocols are required to manage node failure and security attacks. Some routing protocol attacks are: wormhole attacks, acknowledgement spoofing, selective forwarding, black holes and so forth.

D. Transport Layer

Transport Layer is utilized to build up a communication link for outer sensor network joined with the internet. This can be considered as the most complex issue in WSNs. Attacks of the transport layer protocol are flooding and desynchronization. Flooding attack is used to deplete the node's memory by sending numerous requests for connection establishment. In the de-synchronization attack, the attacker node forges packets to at least one or both ends of a connection using different sequence numbers on the packets. In this way, host requests for retransmission of the missed packet frames.

V. SECURITY PROTOCOLS IN SENSOR NETWORKS

Cryptography is a basic technique to achieve the security in a network. This establishes a secure relationship between two end points. In this, sender encrypts the original data and receiver decrypts the received data to obtain an original data. Different types of keys are used in the process of cryptography. The various protocols that are proposed by different authors for solving the security issue in WSN are:

A. SPINs

SPIN (Sensor Protocols for Information via Negotiation) protocol works in three steps. First, a node advertises the ADV packet containing the metadata. If the received node is interested in the data then it sends the request for data using REQ packet. Finally, the advertiser node after receiving request sends the DATA packet to the requestor node. It performs best in small size networks because of its efficiency and high latency properties. Typical SPIN consists of two secure building blocks named as μTESLA (Timed Efficient Stream Loss-tolerant Authentication) and SNEP (Sensor Network Encryption Protocol).

SNEP provides confidentiality, authentication and integrity. It uses the concept of encryption. To authenticate the data, MAC (Message authentication Code) is used. It adds 8 bytes to the message. To reduce the communication overhead, SNEP uses a shared counter between sender node and

receiver node. After each block counter gets incremented. Counter helps in identifying the freshness of data. In TESLA, digital signatures are used to authenticate the data packet. Sink node computes a MAC on the packet after receiving the packet with the secret key to send an authenticated packet back to source. After receiving a packet, node confirms that the sink does not disclose the computed MAC key to other nodes. With this, receiving node assures that data packet is original and no alterations are done in the packet.

B. LEAP

LEAP (Localized Encryption and Authentication Protocol) is a protocol with key management scheme that is very efficient with its security mechanisms used for large scale distributed sensor networks. It generally supports for inside network processing such as data aggregation. In-network processing results in reduction of the energy consumption in network. To provide the confidentiality and authentication to the data packet, LEAP uses multiple keys mechanism. For each node four keys are used known as individual, pair wise, cluster and group key. All are symmetric keys and use as follows:

- Individual Key: It is the unique key used for the communication between source node and the sink node.
- Pair wise Key: It is shared with another sensor nodes.
- Cluster Key: It is used for locally broadcast messages and shares it between the node and all its surrounding neighboring nodes.
- Group Key: globally shared key used by all the network nodes

These keys can also be used by other non-secured protocols to increase the network security. LEAP is satisfies several security and performance requirements of WSN. LEAP is used to defend against HELLO Floods Attack, Sybil Attack and Wormhole Attack.

C. TINYSEC

TINYSEC is link layer security architecture for WSNs. It is a lightweight protocol. It supports integrity, confidentiality and authentication. To achieve confidentiality, encryption is done by using CBC (Cipher-block chaining) mode with cipher text stealing, and authentication is done using CBC-MAC. No counters are used in TINYSEC. Hence, it doesn't check the data freshness. Authorized senders and receivers share a secret key to compute a MAC. TINYSEC has two different security options. One is for authenticated and encrypted messages (TinySec-AE) and another is for authenticated messages (TinySec-Auth). In TinySec-AE, the data payload is encrypted and the received data packet is authenticated with a MAC. In TinySec-Auth mode, the entire packet is authenticated with a MAC, but on the other hand the data payload is not encrypted.

In CBC, Initialization Vector (IV) is used to achieve semantic security. Some of the messages are same with only little variation. In that case IV adds the variation to the encrypted process. To decrypt the message receiver must use the IV. IVs are not secret and are included in the same packet with the encrypted data.

D. ZIGBEE

ZIGBEE is a typical wireless communication technology. It is used in various applications such as military security, home automation and environment monitoring. IEEE 802.15.4 is a standard used for ZIGBEE. It supports data confidentiality and integrity. To implement the security mechanism ZIGBEE uses 128 bit keys. A trust center is used in ZIGBEE which authenticates and allows other devices/nodes to join the network and also distribute the keys. Generally, ZIGBEE coordinator performs this function. Three different roles in ZIGBEE are:

- Trust Manager: It authenticates the devices which are requesting to join the network.
- Network Manager: It manages the network keys and helps to maintain and distribute the network keys.
- Configuration Manager: It configures the security mechanism and enables end-to-end security between devices.

VI. 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.

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.

VII. CONCLUSIONS

This paper emphasizes the WSN's safety issue. Safety in the network sensor is the major challenge. Safe contact is needed for some applications such as the military. Certain security requirements must be met for a secure communication network. Centered on different criteria, this paper discusses security risks. Specific procedures have been developed to satisfy the safety requirements.

In many mission-critical applications, the wireless sensor networks continue to grow and become widely utilized. Therefore, the need for protection is paramount. The wireless sensor network, however, suffers from several limitations including low energy levels, processing and storage, unreliable communication and unattended operation, etc. However, it is a major research challenge to develop and make this detection mechanism efficient. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of todays proposed security schemes are based on specific network models. As a collective attempt to follow a specific model to guarantee each layer's protection is not feasible, in the future, the

development of security protocols for each layer would lead to a challenging investigation integrating all procedures for each layer in partnership.

REFERENCES

[1] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.

[3] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.

[4] Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.

[5] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor 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] Saleh, M. and Khatib, I. A., "Throughput Analysis of WEP Security in Ad Hoc Sensor Networks", Proc. The Second International Conference on Innovations in Information Technology (IIT'05), September 26-28, Dubai, 2005.