Security Issues and Solutions in Wireless Sensor Networks

Rutuja Jadhav
School of computer
Science & Engineering
Vellore Institute of technology
Tamil Nadu, India

Vatsala
School of Computer
science & Engineering
Vellore Institute of Technology
Tamil Nadu, India

ABSTRACT
This paper focuses and talks about the wide and varied areas of applications wireless sensor networks have taken over today, right from military surveillance and smart home automation to medical and environmental monitoring. It also gives a gist why security is a primary issue of concern even today for the same, discussing the existing solutions along with outlining the security issues and suggesting possible directions of research over the same.

This paper is about the security of wireless sensor networks. These networks create new security threats in comparison to the traditional methods due to some unique characteristics of these networks. A detailed study of the threats, risks and attacks need to be done in order to come up with proper security solutions. Here the paper presents the unique characteristics of these networks and how they pose new security threats. There are several security goals of these networks. These goals and requirements must be kept in mind while designing of security solutions for these networks. It also describes the various attacks that are possible at important layers such as data-link, network, physical and transport layer.

Keywords
Wireless Sensor Network, sensor nodes, threats, attacks, solutions, security scheme, limitations

1. INTRODUCTION
A wireless sensor network is a domain-specific wireless network [2].Wireless Sensor Networking is a communication technology which applies embedded system technology to the wireless technology. In a wireless sensor, each device is called a sensor node and every node is connected to one or many other sensor nodes. A wireless sensor network is a heterogeneous system of these sensors. These sensors are cost-effective and consume very low power. They are very small in size and have low communication bandwidth. They are ad-hoc networks. The main aim of a wireless sensor network is to gather information from the physical world. They monitor the physical or environmental state such as sound, temperature, pressure, vibrations or pollutants and communicate data through the network accordingly. The sensors used in these networks collect data, process the data and pass the data through the central node [3]. The WSNs are bi-directional and help in controlling sensor activities. They do not need much infrastructure to operate in. Currently, the sensors used in this technology do not exist at micro or nano level. Scientists are working towards this goal as the size of the sensors will determine how and where the network could be used. They are beneficial in the environments and infrastructures where wires are not suitable. They can be terrestrial, underground as well as underwater [4]. They can be used in any environment, helping its popularity among the networks. It provides cheaper solutions to real-world problems. Due to the various advantages of WSNs, they find use in various fields such as military , environmental applications such as detection of forest fires, floods etc. health applications , various home and commercial applications [11][15]. But, it generates new security threats. It modifies the security risk profile [1]. It has various security issues due to its design, storage and energy limitations. The attackers would use those security flaws making the network vulnerable to various types of attack. So, security is one of the fundamental requirements for any network. The overall security goals remain the same as with traditional networks such as availability, data integrity and authentication.

Since a WSN has wide range of applications in military, homeland security and other areas involving mission-critical tasks, security becomes an essential aspect for such deployments in hostile environments.

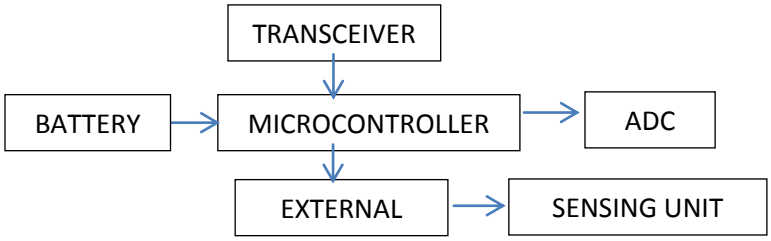
Sensor data consists of actively monitoring the surroundings and easily deducing the info and data monitored. The unrequired and unnecessary data leakage results in privacy breaches of people. One of the distinct aspects of sensor networks involves eavesdropping and packet injection. On account of all these factors considered together, the WSN structure demands safety, security of sensitive data and offers privacy to people. The reason it happens to be a crux issue of concern is difficulty caused due to resource limitation. The sensor nodes are susceptible to physical captures. On account of the structural complexity, anti-jamming is tedious and very difficult. Other underlying factors also include overall cost optimization, maintaining it as low as possible since node constraints asymmetric cryptography for frequent topological changes adds to the expense. Resource consumption and maximization of security level create a conflict between themselves. It is difficult to have centralized keying techniques. All these challenges and hurdles emphasize on the need of eliminating the complexity and complications making a more robust security model in a WSN.

Section 1 discusses the architecture of a wireless sensor network followed by the characteristics of the network in section 2. In section 3, security issues with these networks are discussed. There are some unique characteristics which create some new security issues which cannot be overcome by traditional means. In the next section 4, primary and the secondary goals that are needed to be achieved by these networks and the security protocols are presented. In section 5, the various types of attacks in different layers are discussed. Then we talk about the security and design issues of a wireless sensor network today.

2. ARCHITECTURE OF WSN

A wireless sensor network commonly abbreviated as WSN is a network consisting of distributed sensor nodes capable of processing and gathering sensory information and establishing communication with other connected nodes. The nodes are also termed as specialized transducers possessing vital information to monitor and record conditions commonly being temperature, humidity, sound, power-voltage, chemical concentrations, etc. The design and structure of a node primarily consists of the following:

- **Sensing Unit**: Consists of sensors and ADC
- **Processing unit** : Has the memory and microcontrollers to process and store output
- **Communication Unit** : Most of the applications have it as radio, transducer to generate signals and transceiver to receive them
- **Power unit** :Includes batteries majorly



A BASIC SENSOR NODE LAYOUT

A wireless sensor network consists of the following important components. Sensor nodes are field devices. They are responsible for the routing of packets. Each sensor node has three subsystems; Sensor subsystem is responsible for sensing the environment. Processing subsystem performs local computations on the sensed data and communication system. Communication subsystem is for message exchanging with neighboring sensor nodes [3]. The major components of a sensor node are - Controller processes data and performs various tasks. It controls the functions of other parts. A transceiver performs the functions and has applications those of a transmitter and a receiver together.

There are various types of transmission such as radio frequency, infrared rays, and optical communication. The communications are mostly based on RF. The sensor nodes have some storage constraints so; an external memory is used for storage. A power source supplies power to the nodes. Sensors are the hardware devices that sense in any change in the physical conditions. The data from sensors is first converted to digital data with the help of ADC that passes it to microcontrollers for the processing. A wireless sensor network has gateway points that handle communication between the field devices and the host. A network is responsible for network configuration and monitoring of the health of the network. It also manages routing tables. A security manager handles the key generation and its management.

3. CHARACTERISTICS OF WSN

Wireless sensor networks have some unique properties and features. Generally, the sensor nodes configure themselves into a network on their own. The sensor nodes are deployed densely. Due to the clusters formed by the sensor nodes, multiple nodes collaborate to sense data that may lead to redundancy of data. The sensor nodes used in these networks are very small in size and hence, make them suitable for different environments. They have a lack of data storage and power. Sensor nodes can easily be damaged as they are used under some uncontrollable environment conditions. These networks are application specific as different designs are required by different designs. A wireless sensor network follows many to one traffic pattern .Data from different sensor nodes are communicated to a central node. It consists of sensor nodes that vary in their sizes, computing power etc. This is one of the unique characteristics of this network and is known as heterogeneity of nodes.

4. SECURITY ISSUES OF WSN

The network can easily be attacked and the nodes can be physically tampered with. This is because the nodes are deployed densely and hence they can interact very closely with the environment. This network can also be operated unattended. Attackers may access the nodes and extract all the confidential information. They can also discard the data or modify it. Attackers can also target the routing information which may misguide the traffic of the network. A sensor network is monitored remotely so, any physical tampering may go undetected. The attackers can target the transmission without disturbing the network. This can happen due to unreliable wireless medium. We may have unreliable communication in spite of having the reliable channel. This happens on conflicts of two packets if they meet in their path. It is a major problem in the highly crowded network [12]. A sensor is very small in size and his limited memory and storage space. So, for the security purpose, the code for security algorithms must be very small. A sensor cannot be easily replaced once it is deployed due to high cost. Therefore, the battery charge must be conserved to increase the life of the network. Sensor nodes generate significant redundant data. This may lead to a large number of transmissions. This may lead to the loss in energy efficiency. The nodes in the network may vary in size, power consumption and energy efficiency. This property is called heterogeneity. So, the links between sensors may not be symmetric [4][12][13][14].

5. DESIGN CHALLENGES FOR A WSN

The challenges can be broadly classified as hardware, software or environmental. The hardware structure of a sensor network consists of a node having sensors and mote. [22]

5.1 Hardware Issues:

5.1.1 Consumption of power and energy:

The limitation over power resources help determining the lifetime of a network. It is significant to have an appropriate battery type ensuring optimal consumption of power and avoid overcharge or discharge and resultant heating [22].

5.1.2 Memory chips architecture:

Expense and volatility issue of memory chips should be considered. Ideally, memory chips should be non-expensive, non-volatile [21] and should be able to be reprogrammed.

5.1.3 Maintenance of apt radio range:

It is necessary to have a wide radio range of about 2-5 km [22] on an average since the inability of proper infrastructure of communication in the environment is an issue of concern. Appropriate network connectivity and data gathering needs to be addressed with robust solutions.

5.1.4 Software Issues:

Dealing with the operating system is the main concern under software design issues.

Resource and memory management of OS

5.1.5 Concurrency mechanism:

All actions require real time response as routing and processing of data [22] hence it's important to have a concurrency mechanism for the same.

5.2 Issues with respect to the Environment

5.2.1 Issue of reliability:

Reliability is primarily maintenance of functionalities of the network. An ideal design should ensure that the failure of node shouldn't affect the performance of the wireless sensor network.

The reliability of WSN can be modelled with the help of Poisson distribution [24]

Rk (t) = e –xkt where xk =failure rate of sensor node k

Scalability and reliability are inversely coupled in a wireless sensor network structure.

Localization deals with determining the positions of nodes.

Other topological issues of concern include affecting latency, capacity, robustness, data gathering, production cost [24] and query processing, scheduling and security.

6. SECURITY ATTACKS

Any attempt to expose, steal, alter, modify or gain unauthorized access is defined as an attack. The sensor nodes are physically unprotected and hence, a wireless sensor network is very vulnerable to attacks. An attack can broadly be classified into two types. In a passive attack, the attackers only monitor the communication channel but, in an active attack ,the attacker modifies the data stream as well[1]. There are different attacks at different layers of the network. At the physical layer, the attackers try to exploit the nodes physically. Jamming is a kind of DoS attack in which the operations of a network get disrupted . In this attack, the attacker interfaces with the communication frequencies. There are various types of jamming attacks. In reactive jamming, a jam signal is transmitted when traffic is sensed. A constant jamming attack corrupts the packets. A deceptive jamming attack sends a stream of bytes in the network. Another type of attack common in this layer is tampering. In this attack, the attacker may access the sensor node physically. He might add some additional sensor nodes to the network. The network gets disturbed and hence, the services get stopped. This attack poses a threat to the availability, integrity and confidentiality of the data. In path-based denial of service (DoS) attack, a large number of packets is sent by the attacker to the base station. This results in exploitation of the energy of the network. It is a threat to the data availability and authenticity. A node outage attack stops the service of the node such as collection of data, reading etc. It can be applied both physically and logically. The data link layer looks after the framing, addressing, error control and flow control of the data. Several attacks can happen at this layer. The data of the packet changes by a small amount when two different nodes transmit the data together on the same frequency. Due to this, the packet becomes unacceptable and the data is discarded. These collisions may be created by an attacker on purpose. There is another type of attack known as exhaustion. In this attack, the source node is forced to retransmit the data again and again which decreases the energy level of the sensor node. With continuous collision and exhaustion attacks, the attacker can cause the other nodes to miss their transmission on time. This can cause degradation in the performance of the network. This is known as unfairness. Many networks use a two-way handshake mechanism for communication. An attacker can continuously request to send the packet. This can flood the network link. This attack is known as interrogation. The network layer is responsible for the routing of packets from one node to another. There are some attacks at this layer which exploit the routing process in wireless sensor networks. An attacker can spoof or alter the routing information thus, creating routing loops, generating false messages etc. This is known as spoofing of routing information. In internet smurf attack, the attacker tries to steal the victim node address. In Sybil attack, a node gives an illusion of its presence at more than one different location. In sinkhole attack, the attacker does not let the base station obtain useful information by stimulating all the traffic from neighboring nodes to it, creating a sinkhole. In selective forwarding, the attacker adds some malicious nodes in the data which do not accept some data some data and discard it. Thus, the network does not forward all the messages .If the malicious node is located near the base station, the effect gets worse as more number of nodes route data through this node. In wormhole attack, two different distant nodes are given an illusion that they are close to each other. So, the data received at one point in the network is directly directed to some other point. There is another type of attack at the data link layer. This is known as hello flood attack, where every node considers the adversary as its neighbor and thinks that the routing information sent by the sender is within its radio range. Hence, the energy of the network gets wasted as the nodes try to send messages to a receiver that is beyond their frequency range [4]. The transport layer is responsible for the delivery of the whole message in correct order. There are some attacks that can be made at this level. In floating, new connection requests are repeatedly created until a maximum limit is reached by the resources. Hence, any further genuine request is avoided. In de-synchronization, the sequence number of the packets gets modified. Thus, there is a disruption of the communication protocol. This results in degradation of energy. The DoS attack can be applied in all the layers such as data link, network layer, and transport layer. In this attack, fake packets are injected by the attackers thus, affecting the availability, integrity and authenticity of the data [3][4][6][7].

7. SECURITY GOALS

There are some goals that the wireless sensor network needs to achieve the security of the information and the network itself. The goals can be classified as primary and secondary goals. The primary goals are-Data confidentiality can be ensured through encryption or the use of the shared key. The message communicated through the network must remain confidential. A sensor node must not disclose its data to the neighboring nodes. It is very important to achieve the sensor nodes may carry same sensitive data. The origin of data is identified to ensure its reliability. This is known as data authentication. The network should ensure the reliability of data and should confirm that the data has not been tampered with. This is known as data integrity. There can be a loss of data integrity if there is a loss or damage of data in the network. The network must be available to communicate the messages and should be able to use the resources. This is known as data availability. There are some secondary goals as well. The data to be communicated must be recent and old messages should not be replayed. To ensure data freshness, a

time-related can be added into the packet. The sensor nodes should be independent, self-organized and self-healing. This property is known as self-organization of the network. The network should be able to automatically and accurately locate other sensors in the network. Any non-secured location information can easily be manipulated by an attacker. This property of the network is known as secure-localization. The sensor nodes need time-synchronization in order to work in collaboration. The security protocol should be able to minimize the impact of an attack if it occurs. It should detect failed sensor nodes and update the topology to work with the remaining functioning nodes. This is known as robustness against attacks. The protocols should ensure the broadcast authentication .An attacker can modify the commands broadcasted by the base station to the sensor nodes. The sensor nodes can accept those modified commands and perform incorrect operations. A large number of sensor nodes can be deployed in a WSN. Even the network size can be extended by adding extra nodes. This property is known as scalability. The security protocols should be able to deal with the increasing network size [4][5][8][9][10].

8. PROPOSED SOLUTIONS

For a secure group management of a wireless sensor network, a necessary data analysis can be performed where authentication of the output of sensor is ensured to be from a valid group. The nodes comprising the actual groups of the network may face frequent and drastic transitions which are also responsible for performing many key services [17] .Hence we need a system with strong secure protocols for the group management and security admitting entry of any new member. Also, it is important for the solution to be time and energy efficient.

The nature of WSN also in-built susceptibility to several intrusion forms .In quite a lot wired networks a segment is dedicated for analysis and monitoring of data at various sinks which adds to the expenses, consumes memory and energy [16].To overcome these circumstances we need to pinpoint towards a robust structured solution understanding the applications and threat models prevalent [17][19].

Fine sensing and dense nodes adds to the characteristics of an ideal WSN. Hence, there is a strong need for secure data aggregation structure [17]. The sensed values must be aggregated avoiding huge amount of traffic at the base station [20].

The issues demand a need for hybrid key-based protocols since single key-based aren't optimal in nature. Public key group and pairwise keying consume excessive amounts of energy. Thus, for significant sensor networks, mixing pairwise and group-keying are possible solutions [24].On basis of architecture, the wireless sensor network should have all secure locations dedicated for aggregation [17].

To the issue of jamming, spread spectrum communication can be offered as a way out till the jammers figure out and come up with the actual technique to block a wider part of radio frequency band [27].

Code spreading is another way out for the mentioned issues of concern but requires a lot of power consumption [27].For tampering; it is important to provide resistant packaging but is costly. Programming of nodes and erasing sensitive data on capture are alternative solutions possible for the same. To defend against data being spoofed, authentication and encryption are necessary and recommended. Resending failed messages coupled with selective forwarding, redundancy through multipath routing are adequate and sufficient.

8.1 Solutions over attacks:

The issue of link layer encryption can be addressed with the assistance of selective forwarding and sinkhole [22]. The Sybil attacks can be stopped.

The wormhole concept can make use of private channelized approach.

HELLO flood is another major challenge which can be addressed by verifying the bi-directionality of a link[21]

The issue of an outsider authentication can be resolved using a globally shared key. This also ensures selective forwarding and stops sinkhole and Sybil attacks.

For efficient selective forwarding multi-path routing and routing based on probabilistic approach can be used[17].

Sinkhole can be made more efficient, robust and better by verification of routing metric data for instance the latent energy, available energy.

For the symmetric keys of Sybil problem, verification of identities of the corresponding neighbors can be useful[19].

9. SECURITY SCHEMES

Zigbee security scheme is keying over hardware-based symmetry featured.

Multipath and multiphase routing based stations and verification in bi-directional aspects is another security scheme which adopts secret sharing in probabilistic approach to overcome the Hello Flood Attacks [25][26][27]

The security of communication can be addressed with efficient and coherent data spoofing resource management which ensures protection of the network as a whole.

TIK security scheme faces wormhole attacks, spoofing of the available information and data. This is done with the assistance of symmetric cryptography requiring accurate time synchronization amongst all parties comprised in the communication aspect.

The en-route filtering based on statistics faces[27] information spoofing to be one of the major threats .The detection and dropping false reports during forwarding process is ensured as an implicit feature

TinyPK, TinySec security scheme faces Data and information spoofing,message replay as the major attacks. The underlying features comprising message authenticity, confidentiality while working in link layer of the architecture.

SNEP and µTESLA face similar issues and problems as of TinyPK and TinySec providing replay protection , weak freshness and low communication overhead as the highlighting features.

SMECN which represents Small Minimum Energy Communication Network along with LEACH abbreviated as Low Energy Adaptive Clustering Hierarchy pose protocols for network layer of WSNs to be one of the significant threats. The different type addressing routing information through WSN along with results of finding and directing the packet along the most efficient and optimized path to traverse to its destination comprises some of the features.

Jamming; in form of JAM DoS attacks can also be addressed through avoidance of jammed region by using neighbouring nodes which are coalesced.

Randomized key pre-distribution and resource testing of radio have issues of Sybil attacks using radio resource and verification along with authentication of position, registration procedure and code for detection[26]

Predistribution of data and spoofing of data with randomized key is a proposed security system model which protects the network even if part of it is compromised providing the necessary authentication and verification measures for the corresponding nodes of wireless sensor network.

SMACS which is abbreviated as Self Organized Medium Access Control for the sensor networks and EARS which stands for Eavesdrop and Register face the primary threat attack of Data link layer protocol for WSNs. Both are responsible for various features as medium access, multiplexing and demultiplexing of data streams along with data frame detection. The error control is ensured through correction of transmission errors [26].

DoS attacks which are wormhole based use wormholes to avoid jamming.

REWARD faces black hole attacks which make use of geographic routing. The featured benefits comprise broadcasting the inter-radio behaviour to detect and analyse attacks such as black hole attacks.

10. LIMITATIONS OF WSNs

Each and every type of security mechanism needs specific amount of resources for its own mechanism to function. The sensor nodes usually hold data, program and energy which face their own limitations

Energy limitation issue: The factors leading to energy depletion need careful intervention which comprises of varied aspects such as total energy consumed in consumption of security in encryption, decryption along the total amount of energy spent in storage and security parameters for instance the ones involving cryptography.

Memory limitation issue: It is another issue around which the crux of solutions revolves to maintain an efficient security mechanism with optimized memory.

11. CONCLUSION

The emerging technology and idea of wireless sensor network are finding a wide market and applications in various fields. The applications are ranging from healthcare, smart home, improving the standard of living with better food and water [22], enhanced safety and security, to energy efficient smart grids, intelligent buildings to high-confidence transport and asset tracking [16][20].One of the primary reasons for this wide spectrum to develop is because of the translating power of sensing and identification activities into services that can be provided and deployed.

The paper discusses and gives a gist about structural architecture, challenges in design and security areas and also talks about the existing security mechanisms and security schemes, their features and limitations.

This application sustains a potential future with “Internet of Things” which shows feasible possibilities in net few years. The data can be in heterogeneous format as images, sound, distance, etc.

12. REFERENCES

[1] Wireless Network Security: Vulnerabilities, Threats and Countermeasures, Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim ,International Journal of Multimedia and Ubiquitous Engineering

[2] Wireless Network Security, Yang Xiao, Hui Chen, Shuhui Yang, Yi-Bing Lin, and Ding-Zhu Du, EURASIP Journal on Wireless Communications and Networking

[3] A Survey of Wireless Sensor Network Security, Mr. Prasad Mahajan, Miss Priyanka Bhute, International Journal of Advanced Research in Computer and Communication Engineering

[4] Security in Wireless Sensor Network , Pritesh Patel, Nikhil Lende, International Journal of Advanced Research in Computer Engineering & Technology

[5] Review of Security Attacks and Issues in Wireless Sensor Network, Mohammad Ziaullah, Roshan Ara, Prakash Shetty, IJREAT International Journal of Research in Engineering & Advanced Technology

[6]Wireless Network Security 802.11, Bluetooth and Handheld Devices, Tom Karygiannis Les Owens, NIST, National Institute Of Standards and Technology

[7] WIRELESS SENSOR NETWORK SECURITY ANALYSIS, Hemanta Kumar Kalita, Avijit Kar, International Journal of Next-Generation Networks (IJNGN)

[8] A SURVEY ON AUTHENTICATION AND SECURITY MAINTENANCE IN WIRELESS SENSOR NETWORK, Ms.L.Devi., Dr.S.P.Shantharajah, International Journal of Computer Science and Mobile Computing

[9] Wireless Sensor Networks: Security Issues, Challenges and Solutions, Vikash Kumar, Anshu Jain, P N Barwal, International Journal of Information & Computation Technology.

[10] Security Threats in Wireless Sensor Networks, Sushma, Deepak Nandal, Vikas Nandal, IJCSMS Interna tional Journal of Computer Science & Management Studies.

[11] Security Solutions for Wireless Sensor Networks, Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA, General Papers

[12] Wireless Sensor Network Security: A Survey, John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.) pp. – - – c °2006 Auerbach Publications, CRC Press

[13]Security Issues In Wireless Sensor Networks, Yenumula B Reddy, SENSORCOMM 2011

[14] Routing Protocols in Wireless Sensor Networks – A Survey, Shio Kumar Singh, M P Singh , and D K Singh, International Journal of Computer Science & Engineering Survey (IJCSES)

[15] Protocol Design and Implementation for Wireless Sensor Networks, PIERGIUSEPPE DI MARCO, KTH Electrical Engineering

[16] Wireless Sensor Network Security: A SurveyJohn Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin

Chaudhary Department of Computer Science Wayne State University

[17] SECURITY IN WIRELESS SENSOR NETWORKSBy ADRIAN PERRIG, JOHN STANKOVIC, and DAVID WAGNER COMMUNICATIONS OF THE ACM June 2004/Vol. 47, No. 6

[18] Issues in Wireless Sensor Networks Gowrishankar.S 1, T.G.Basavaraju 2, Manjaiah D.H 3, Subir Kumar Sarkar 4 Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

[19] Some issues and challenges of Wireless Sensor Networks Himani Chawla CSE Dept. Maharishi markandeshwar university Ambala, Haryana, India Volume 4, Issue 7, July 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[21] Security Issues in Wireless Sensor Networks: Attacks and Countermeasures Kahina CHELLI Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 1 - 3, 2015, London, U.K.

[22] Design Issues and Challenges in Wireless Sensor Networks Khushboo Gupta PhD Research scholar Department of Computer Science Engineering Uttar Pradesh technical university, Lucknow, India Vaishali Sikka M.Tech (Information Technology) Department of Computer Science Engineering Banasthali Vidhyapith, Jaipur, IndiaInternational Journal of Computer Applications (0975 – 8887) Volume 112 – No 4, February 2015

[23] SECURITY IN WIRELESS SENSOR NETWORKS: KEY MANAGEMENT MODULE IN SOOAWSN Mohammed A. Abuhelaleh and Khaled M. Elleithy School of Engineering University Of Bridgeport, Bridgeport,CT

[24] Security in Wireless Sensor Networks: Attacks and SolutionsSwati Bartariya, Ashutosh RastogiInternational Journal of Advanced Research in Computer and Communication Engineering

[25] Wireless Sensor Networks Attacks and Solutions Naser Alajmi Computer Science and Engineering Department, University of BridgeportInternational Journal of Computer Science and Information Security

[26] Secure Wireless Sensor Networks: Problems and Solutions Fei Hu * Jim Ziobro ** Jason Tillett *** Neeraj K. SharmaIEEE Vol 1- Number 4

[27] Security in Wireless Sensor Networks By Koffka Khan, Wayne Goodridge & Diana RagbirGlobal Journal of Computer Science and Technology Network, Web & Security Volume 12 Issue 16 Version 1.0

[28] A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks Dr. G. Padmavathi, Prof and Head, Dept. of Computer Science Mrs. D. Shanmugapriya, Lecturer, Dept. of Information Technology, Avinashilingam University for Women, Coimbatore, India

[29] SECURING WIRELESS SENSOR NETWORKS: A SURVEY YUN ZHOU AND YUGUANG FANG, UNIVERSITY OF FLORIDA YANCHAO ZHANG, NEW JERSEY INSTITUTE OF TECHNOLOGYIEEE communication surveys

[30] Routing Protocols in Wireless Sensor Networks Luis Javier Garcaí Villalba *, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera and Cláudia Jacy Barenco Abbas