# Security Challenges in Wireless Sensor Networks

Madhumita Panda

*Assistant Professor, Computer Science, SUIIT, Sambalpur University, Odisha, India*

***Abstract-*** Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications. As Wireless sensor networks continues to grow, they become vulnerable to attacks and hence the need arises for effective security mechanisms. The intent of this paper is to investigate the major design challenges in wireless sensor networks and how cryptographic algorithms can be used as a tool to save WSN from various threats.

***Keywords-*** Wireless Sensor Network, Security design challenges, Security requirements, Symmetric and Asymmetric cryptography

## I. INTRODUCTION

Wireless sensor networks (WSN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. These networks will consist of hundreds or thousands of self-organizing, low-power, low-cost wireless nodes deployed to monitor and affect the environment [1]. Figure 1 shows structure of a typical WSN.

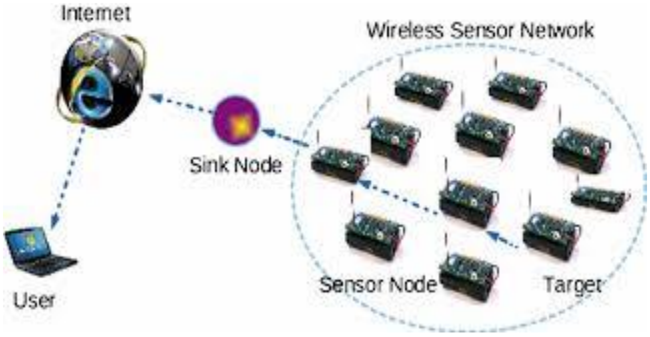

Fig.1: Wireless Sensor Network

Due to continue growth of wireless sensor networks, the need for more effective security mechanisms is also increasing. As sensor networks interact with sensitive data and usually operate in hostile unattended environments and are characterized by limited power supplies, low bandwidth, small memory sizes and limited energy, this leads to a very demanding environment to provide security.

The rest of the paper is organized as follows. In section II we summarize the major design obstacles for the sensor networks security. In section III the requirements of WSNs security are listed. Section IV gives a brief introduction to cryptography and how cryptography can be used as a tool for security in WSN. Section V of the paper gives out the research issues carried out on WSN . Finally, section VI concludes the paper giving future work.

.

## II. MAJOR DESIGN CHALLENGES

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. The extreme resource limitations of sensor nodes and unreliable communication medium in unattended environments make it very difficult to directly employ the existing security approaches on a sensor platform due to the complexity of the algorithms [2] [3] [4] [5]. To develop useful security mechanism, an understanding of these challenges within WSNs provides a basis for further works on sensor networks security

### a. Very Limited Resources

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor. As physical size decreases, so does energy capacity. The underlying energy constraints end up creating computational and storage limitations that lead to a new set of design issues[6].

- ***Limited Memory and Storage Space***: A sensor is a tiny device with only a small amount of memory usually ranges from 2 KB to 256 KB while the storage for the code ranges from 32 KB to 2 GB. Inorder to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.
- ***Power Limitation*****:** A Sensor node has to economize with the shipped battery, i.e. the supplied energy must outlet the sensor's life. Sensor nodes need to operate autonomously for prolonged periods of time after deployment and it is not possible to easily replace or recharge the battery. So the energy consumption must be minimized for long life and this necessitates both the power efficiency of the hardware along with the efficiency of security and other routing protocols The energy of a sensor node is consumed by mainly three essential components: the sensor unit, the communication unit and the computation unit. Because of the limited energy reserves, energy is often one of the primary metrics in WSNs routing algorithms[7].
- ***Transmission range*****:** To minimize the energy needed for communication it is very common that sensor nodes use a rather small transmission range.This results in the necessity of using multiple-hops to transfer data from a source to a destination node through a large network.

### b. Unreliable Communication

One of the major threats to sensor security is the very nature of the wireless communication medium, which is inherently insecure[8].

• ***Unreliable Transfer*****:** Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. Higher channel error rate also forces the software developer to devote resources to error handling. More importantly, if the protocol lacks the appropriate error handling it is possible to lose critical security packets. This may include, for example, a cryptographic key.

• ***Conflicts***: Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. Conflicts may occur due to packets colliding meet in the middle of transfer resulting in failure of transfer . More details about the effect of wireless communication can be found at [9].

• ***Latency*****:** The packet-based multihop routing in WSNs increases the latency due to congestion in the network and additionally require processing time. Besides, the routing process in WSNs is often causing delays: For example, if a routing algorithm uses different paths between a source and a destination to distribute energy load, not always the shortest path is used so that additional delays are predictable.

### c. Unattended Operation

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main issues to unattended sensor nodes:

• ***Exposure to Physical Attacks:*** The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in asecure place and mainly faces attacks from a network.

• ***Managed Remotely*****:** Remote management of a sensor network makesit virtually impossible to detect physical tampering (i.e., through tamper proof seals) and physical maintenance issues (e.g., battery replacement).

• ***Lack of Central Management Point*****:** A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, andfragile. Perhaps most importantly, the longer that a sensor is left unattended the more likely that an adversary has compromised the node.

## III. WSNs SECURITY REQUIREMENTS

Sensor networks are a type of distributed networks and share some commonalities with a typical computer network, at the same time pose unique requirements and constraints. Therefore, security goals for WSN encompass both the typical network requirements and the special unique requirements suited for WSNs. In this section, the main security goals for WSNs are summarized [3] [4] [9] [10] [11].

***Confidentiality*****:** It is the ability to hide message from a passive attacker and is the most important issue in network security. A sensor network should not leak sensor reading to neighbouring networks. Simple method to keep sensitive data secret is to encrypt the data with a secret key that only the intended receivers' possess, hence achieving confidentiality. As public key cryptography is too expensive to be used in the resource constrained sensor networks, most of the proposed protocols use symmetric key encryption methods.

***Authentication*****:** Authentication ensures the reliability of the message by identifying its origin. In a WSN the issue of authentication should address the following requirements:[1] communicating node is the one that it claims to be(ii)the receiver should verify that the received packets have undeniably come from the actual sensor node**.** For Authentication to be achieved the two parties should share a secret key to compute message authentication code(MAC) of all communicated data. The receiver will verify the authentication of the received message by using the MAC key.

***Integrity*****:** is preventing the information from unauthorized modification. Data authentication can provide data integrity also.

***Availability*****:** Availability is of importance for maintaining an operational network.. Availability ensures that services and information can be accessed at the time they are required. In sensor networks there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks**.**

## IV. CRYPTOGRAPHY

Cryptography schemes are often utilized to meet the basic security requirements of confidentiality and integrity in networks. Basically, the major challenge for employing any efficient security scheme in WSNs is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensor nodes, as well as the limited communication capacity [12] [13]. For secure transmission of various types of information over sensor networks, two cryptographic techniques are used: symmetric key ciphers and asymmetric key ciphers.

### a. Symmetric Key Cryptography

Symmetric encryption(also called as secret-key cryptography) uses a single secret key for both encryption and decryption as shown in Figure 2.

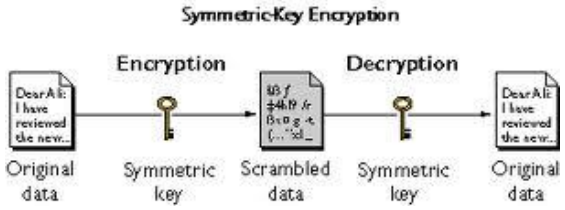

Fig.2: Symmetric -Key Cryptography

This key has to be kept secret in the network, which can be quite hard in the exposed environment where WSNs are used .To achieve the security requirements, several researchers have focused on evaluating crypto graphical algorithms in WSNs and proposing energy efficient ciphers. Symmetric key algorithms are much faster computationally than asymmetric algorithms as the encryption process is less complicated. Examples are AES,3DES etc.

**b. Asymmetric Key Cryptography**

Asymmetric encryption (also called public-key cryptography) uses two related keys (public and private) for data encryption and decryption, and takes away the security risk of key sharing. The private key is never exposed.

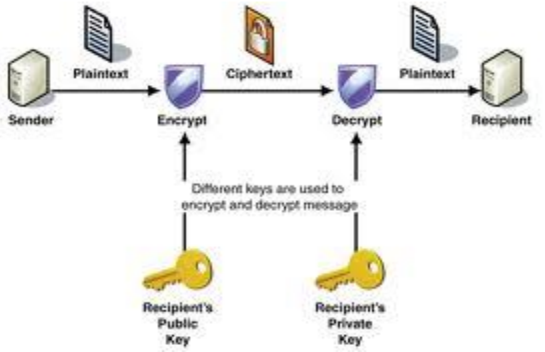

Fig.3: Asymmetric Key Cryptography.

A message that is encrypted by using the public key can only be decrypted by applying the same algorithm and using the matching private key. Likewise, a message that is encrypted by using the private key can only be decrypted by using the matching public key. Examples are RSA,ECC etc.

## V. RESEARCH ISSUES OF WIRELESS SENSOR NETWORK SECURITY

We first focus on some use and advantage gained on use of Symmetric Key Cryptography due to the assumption that symmetric cryptography has a higher effectiveness and require less energy consumption, in contrast to public key cryptography. Also the memory requirement of Symmetric algorithm is lesser as compared to Asymmetric. [14].

In [15], the authors propose LEAP (Localized Encryption and Authentication Protocol); a key management protocol intended to support a several communication patterns. In this protocol, each node stores four types of keys: individual, pairwise, cluster, and group. An individual key is a key shared between a node and the base station.

In [16], the authors focus on developing cost-saving mechanisms while weakening the threat model. They propose Key Infection, a lightweight security protocol suitable for use in noncritical commodity sensor networks where an attacker can monitor only a fixed percentage of communication channels.

According to [17]public key is used in some applications for secure communications eg.SSL(Secure Socket Layer) and IPSec standards both use it for their key agreement protocols.But it consumes more energy and it is more expensive as compared to symmetric key.

According to [18],the more consumption of computational resources of public key techniques is due to the fact that it uses two keys. One of which is public and is used for encryption ,and everyone can encrypt a message with it and other is private on which only decryption takes place and both the keys has a mathematical link, the private key can be derived from a public key. In order to protect it from attacker the derivation of private key from public is made difficult as possible like taking factor of a large number which makes it impossible computationally. Hence,it shows that more computation is involved in asymmetric key techniques thus we can say that symmetric key is better to choose for WSN.

Public key Cryptography was omitted from the use in WSN because of its great consumption of energy and bandwidth which was very crucial in sensor network. Now a days a sensor become powerful in terms of CPU and memory power so, recently there has been a change in the research community from symmetric key cryptography to public key cryptography. Also symmetric key does not scale well as the number of nodes grows[19].

Arazi et al. [20] describe the efficiency of public-key cryptography for WSNs and the corresponding issues that need to be considered. Particularly, ECC is highlighted as suitable technique forWSN which provides a good trade-off between key size and security.

Liu and Ning [21] also emphasize that ECC is oneof the most efficient types of public key cryptographyin WSNs. The steps of design, implementation andevaluation of TinyECC, a configurable and flexible libraryfor ECC operations in WSNs, are presented. The libraryprovides a number of optimization switches that can becombined according to the developer's needs for a certainapplication, resulting in different execution times andresource consumptions. The TinyECC library was alsoevaluated on several sensor platforms; including MICAz,Tmote Sky, and Imotel; to find the most computationally efficient and the most storage efficient configurations.

[22]described the efficiency of public-key cryptography for WSNs and the corresponding issues that need to be considered. Particularly, ECC is highlighted as suitable technique for WSN which provides a good trade-off between key size and security. Lopez, 2006 focused on the security issues by analysing the use of symmetric cryptography in contrast with public-key cryptography. The author also discussed the important role of elliptic curve cryptography in this field.

In [23], Malan et al. demonstrate a working implementation of Diffie-Hellman based on the Elliptic Curve Discrete Logarithm Problem. In addition, they show that public keys can be generated within 34 seconds, and that shared secrets can be distributed among nodes in a sensor network within the same, using just over 1 kilobyte of SRAM and 34 kilobytes of ROM. So, public-key infrastructure is viable on the MICA2 for infrequent distribution of shared secrets.

## VI. CONCLUSION AND FUTURE WORK

Due to continue growth of wireless sensor networks, the need for more effective security mechanisms is also increasing. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. In this paper we tried to discuss various issues concern with the security of WSNs along with the research challenges. There are many ways to provide security, one is cryptography. Selecting the appropriate cryptography method for sensor nodes is fundamental to provide security services in WSNs. Public Key based cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches. In the future work, we tend to study various attacks on WSNs along their various countermeasures proposed .

## VII. REFERENCES

[1]. Matt Welsh, Dan Myung, Mark Gaynor, and Steve Moulton "Resuscitation monitoring with a wireless sensor network", in Supplement to Circulation: Journal of the American Heart Association, October 2003.

[2]. E.Shi and A.Perrig, "Designing Secure Sensor Networks", Wireless Commun. Mag., Vol. 11, No. 6, pp.38-43, Dec 2004.

[3]. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Sean Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. ICACT 2006, Volume 1, 20-22, pp. 1043-1048, Feb. 2006.

[4]. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[5]. Shahnaz Saleem, Sana Ullah, Hyeong Seon Yoo, "on the Security Issues in Wireless Body Area Networks", International Journal of Digital Content Technology and its Applications Vol. 3, No. 3, Sep. 2009.

[6]. Chelli, Kahina. "Security issues in wireless sensor networks: attacks and countermeasures." Proceedings of the World Congress on Engineering. Vol. 1. 2015.

[7]. K.Akkaya and M.Younis,A survey on routing protocols for wireless sensor networks,Ad Hoc Networks,3(2005),325-349.

[8]. Singh, Rupinder, Jatinder Singh, and Ravinder Singh. "Security challenges in wireless sensor networks." Int. J. Comput. Sci. Inf. Technol. Secur. IJCSITS 6 (2016): 1-6.

[9]. Kalpana Sharma. M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on Mobile Adhoc Networks 2010.

[10]. David Martins, and Herve Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", 2010 IEEE.

[11]. Anitha S.Sastry, Shazia Sulthana and Dr.S Vagdevi, "Security Threats in Wireless Sensor Networks in Each Layer", International Journal of Advanced Networking and Applications, Vol. 04 Issue 04, pp. 1657-1661, 2013.

[12]. Kaplantzis, S., "Security Models for Wireless Sensor Networks", 2006, http://members.iinet.com.au/~souvla/transferfinal-rev.pdf.

[13]. Y Xiao, VK Rayi, B Sun, X Du, F Hu, M Galloway, "A survey of key management schemes in wireless sensor networks", Computer Communications 30(11-12), 2314–2341, 2007.

[14]. Ketu File white papers, "Symmetric vs Asymmetric Encryption", a division of Midwest Research Corporation.

[15]. S Zhu, S Setia, S Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks", Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), 62–72, Oct. 2003.

[16]. R Anderson, H Chan, A Perrig, "Key infection: Smart trust for smart dust", Proceedings of the 12thIEEE International IEEE International Conference on Network Protocols (ICNP '04), 206–215, October 2004.

[17]. Ning P, Wang R and Du W (2005), "An efficient scheme for authenticating public keys in sensor networks", Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, Chicago, IL, USA, pp. 58-67.

[18]. RSA Security (2004), "Cryptography ", Available at: http://www.rsasecurity.com/rsalabs/node.asp?id=2152.

[19]. IAN F.Akyildiz, Weilian Su, YogeshSankarasaubramaniam,ArdialCayirci,"A Survey on Sensor Networks",IEEE Communications Magazine,August 2002,pages 102-114.

[20]. B. Arazi, I. Elhanany, O. Arazi, and H. Qi, Revisiting public-key cryptography for wireless sensor networks, Computer, 38 (2005),103–105.

[21]. A. Liu and P. Ning, TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks, in Proc. of the International Conference on Information Processing in Sensor Networks (IPSN '08), St. Louis, MO, 2008, 245–256.

[22]. Arazi,B.,Elhanany,L.,Arazi,O.,Qi,H.,2005:Revising public – key cryptography for wireless sensor networks. IEEE Computer,38(11):103-105.

[23]. David J. Malan, Matt Welsh, Michael D. Smith, "A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography", Division of Engineering and Applied Sciences, Harvard University, Dec 2007.