International Journal of Electrical, Electronics and Computer Engineering **6**(1): 04-11(2017)

ISSN No. (Online): 2277-2626

Issues, Challenges and Solution for Security in Wireless Sensor Networks: A Review

Prachi Pathak* and Mohd. Amjad Quaz**

**M. Tech. Scholar, Department of Electronics & Communication,*
SISTec, Bhopal, (Madhya Pradesh), INDIA
***Asst. Professor, Department of Electronics & Communication,*
SISTec, Bhopal, (Madhya Pradesh), INDIA

(Corresponding author: Prachi Pathak)

(Received 19 November, 2016 Accepted 15 December, 2016)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The development of sensor network as one of the prevailing innovation drifts in the coming decades has represented several kind difficulties to analysts. These systems are probably going to be made out of hundreds, and a large number of modest sensor nodes, working independently. Though, due to intrinsic resource and computing constraints, security in sensor networks poses different challenges as compared to conventional network security. The undependable communication channel and unattended operation construct the security defenses even harder. It emphasis on the challenges related to the security of Wireless Sensor Network and begins with the concept of WSN. By keeping in mind that the many researchers have instigated to address the challenges of maximizing the processing capabilities and energy reserves of wireless sensor nodes while also securing them adjacent to attackers, while the set of challenges in sensor networks are assorted. In this paper, we present the issues, challenges and solution related to security in WSN.

Keyword: Issues, WSN, Sensor Nodes, Security, Security Mechanism

I. INTRODUCTION

The development of low cost, low power, multifunctional sensor nodes have been possible by developments in wireless communication and electronics. Wireless sensor network (WSN) consists of a set of distributed sensors with sensing, computation and wireless communication capabilities to monitor physical or environmental conditions and pass their data through the network to a Base station [8].

A Wireless Sensor Network (WSN) is a collection of relatively inexpensive computational nodes that measure local environmental conditions like temperature sound, pressure etc. and forward such information to a base station for appropriate processing. Security should be considered because most of sensor networks possess various missions, critical tasks and therefore they need security [14].

The attractive features of the Wireless Sensor Networks attracted many researchers to work on various issues related to these types of networks. However, while the routing strategies and Wireless Sensor Network modelling are getting much preference, the security issues are yet to receive extensive focus. WSNs have the potential to be deployed in mission critical applications such as Military Surveillance or medical applications, e.g. Body Area Network (BAN), [4] where several low cost nodes are attached to the human body to collect data and is periodically transferred to a sink node for further processing. Sink node are also often designed to work as gateways to transfer data to e-Health systems residing in the cloud.

Indeed, WSNs gaining rapid worldwide attention because of their potentially low cost solutions to a variety of real world challenges. Many other favouring factors of WSNs use are self-organizing, self-healing, having dynamic network topology to cope with node malfunctioning and failures, mobility of deployed nodes, unattended operation, ability to withstand bad environmental conditions, heterogeneity of nodes, scalability, at the time of deployment and after deployment as well easy use [14] [5]. The capability of a nodes or distension to discover different compromised nodes allows them to do something, as well disregarding the reconfiguring the network to remove the danger.

In general, WSNs consist of battery operated sensor devices with computing, data processing, and communicating components. The ways the sensors are deployed can either be in a controlled environment where monitoring and surveillance are critical or in an uncontrolled environment.

In the uncontrolled environments, security for sensor networks becomes extremely important [6]. In this paper, we explore the security issues and challenges for next generation wireless sensor networks and discuss the crucial parameters that require extensive investigations. Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensor, consequently the processing power, memory and type of tasks expected from the sensors.

Numerous security plans grant protection so data stay undamaged and communication uninfluenced so little of them compromised [1]. This paper is outlined as follows Section 1 provides the Introduction of WSN and also covers the basic components and architecture of WSN. Section 2 describes various security threats And Issues in WSN.

A. WSN Architecture

In a typical WSN we see following network components [6]:-

(i) Sensor nodes (Field devices):- Each sensor network node has typically several parts, a ratio transceiver with an internal antenna, a microcontroller, an electronic circuit for Interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

(ii) Gateway or Access points–A Gateway enables communication between Host application and field devices.

(iii) Network Manager –A Network Manager is responsible for configuration of the network, scheduling.

The Base stations are one or more distinguished components of the WSN with much more computational, energy and communication resources. They act as a Gateway between Sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables. Many techniques are used to connect to the outside world including mobile phone network, satellite phones, radio modems, high power Wi-Fi links etc. Fig.1. shows the architecture of WSN.

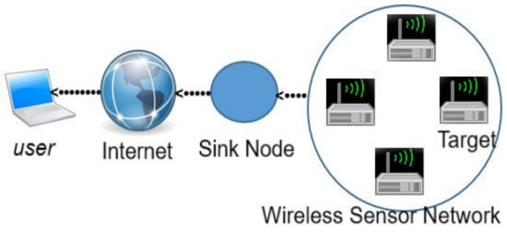

Fig. 1. The Architecture of WSN.

The key components of a node are: a micro sensor, a microprocessor, a memory, a battery, and a transceiver to communicate with rest of the networks. The basic components of sensor nodes are shown in Fig. 2 shows the component of sensor nodes.

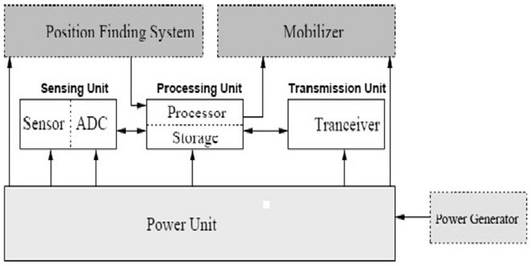

Fig. 2. Components of Sensor Nodes in WSN.

B. Communication Protocol

Wireless Sensor Networks employ layered architecture such as wired network architecture. Traits and actions of every their layers are presented below:

i) Physical layer. Raising the reliability by decreasing path less impact and shadowing is the goal of physical layer. For recognized connection, data rate, modulation, data encryption, signal detection, frequency generation, this layer is reliable.

ii) Data link layer. Data link layer's goal is to provide communication between two nodes. This layer is responsible for recognizing errors and multiplexing. Moreover, to create secure key during network deployment and maintenance. Some scientists suggested the probable use of public key cryptography [4,13] and secure code distribution [10].

iii) Network layer. Providing the best path for effective routing technique is the aim of Network layer. Routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa are in charge of this layer. In WSN , every node works as a router in the network (due to use broadcast method), in order to make secure routing protocol, Encryption and Decryption methods are utilized for secure routing [11, 12 and 9].

iv) Transport layer. For external networks i.e. Sensor Network connected to the internet can use Transport layer setup communication; however it is the main difficult issue in Wireless Sensor Networks.

v) Application layer. Application layer use to display ultimate yield by guarantee smooth information low to lower layers. This layer is in charge of data collection, management and processing of the data by using the application software to obtain trustworthy consequences.

C. Security Needs of Wireless Sensor Network

The major reason of safety services in WSNs is to concern for the in sequence and resources from attacks and misbehavior. The security needs in WSNs comprises the following:[17]

i) Data Confidentiality. Data Confidentiality is also known as privacy of data. Since nodes are sometimes used to manage sensitive information, it is also a set of rules that have the limitations to access the data. Confidentiality is designed to prevent data from reaching the wrong or unauthorized sensor node. The data should not fall into unintended hands.

In many applications nodes communicate highly sensitive data, e.g. key distribution as we want to build a secure communication channel in WSNs. The community sensor information, so that the sensor identities and community keys, be supposed to be encrypted to a number of degree to defend next to traffic analysis attacks.

ii) Data Integrity. The Sensor Data must not be changed in transit. It is the assurance that the information is trustworthy and accurate during the communication process. In WSNs, the issues of integrity have the following requirements:

(i) "A malicious node that present in the WSNs injects false data".

(ii) With the unstable conditions for the wireless channel cause loss of data.

(iii) The nodes in the network should have access to the keys and only an assigned base station should have the privilege to change the keys. This would effectively thwart unauthorized nodes from obtaining knowledge about the keys used and preclude updates from external sources.

(iv) "It protects against an active, intelligent attacker who might attempt to disguise his attack as noise".

iii) Data Authentication. Confirmation guarantees the unwavering quality of the message by distinguishing its root. Assaults in WSNs don't simply include the bundles' adjustment; enemies can likewise infuse extra false parcels. In information validation checked the personality of senders and collectors. Information verification is accomplished through symmetric or deviated components where sending and accepting hubs offer mystery keys.

In 2002, Adrian Perrig *et al.* propose a key-chain dispersion framework for their µTESLA secure telecast convention, the fundamental thought of the µ TESLA framework is to accomplish halter kilter cryptography by deferring the divulgence of the symmetric keys.

iv) Data Freshness. Regardless of the possibility that classification and information uprightness are guaranteed, "there is a need to guarantee the freshness of every message". Casually, information freshness [16] recommends that the information is later, and it guarantees that no old messages have been replayed.

v) Robustness. Wireless sensor networks are highly dynamic and uncertain, including changes in the network topology and the nodes' disappearing or joining. Therefore, the wireless sensor networks under a variety of security attacks should have strong adaptability, and even if a particular attack succeeds, the performance can make the impact minimized.

vi) Access Control: Access control requires the ability to identify the users who access wireless sensor networks to ensure the legitimacy. Access control determines who can access the system, what system resources can be accessed, and how to use these resources.

vii) Secure Localization: Frequently, "the utility of a sensor system will depend on its capacity to precisely and consequently find every sensor in the system". A sensor system intended to find deficiencies will require precise area data so as to pinpoint the area of a shortcoming. In SeRLoc "Secure Range-Independent Localization" is portrayed. "Its oddity is its decentralized, range-autonomous nature. SeRLoc utilizes locators that transmit reference point data". "It is expected that the locators are trusted and can't be traded off. Moreover, every locator is expected to know its own particular area. A sensor registers its area by listening for the signal data sent by every locator". The reference points incorporate the locator's area. Utilizing the greater part of the signals that a sensor hub distinguishes, a hub processes an inexact area in light of the locators' directions. Utilizing a larger part vote plot, the sensor then figures a covering receiving wire locale. "The last processed area is the "focal point of gravity" of the covering radio wire locale. Every sensor additionally imparts a special symmetric key to every locator. This key is likewise pre-stacked on every sensor.

vii) Time Synchronization. Time synchronization objective is to equalizing the local times for all nodes in the network, if required. Since WSNs are limited in computation capability, bandwidth, energy resources, storage capacity. The traditional time synchronization algorithms like Network Time Protocol and Global Positioning System are impractical to synchronize the network.

viii) Self Organization. A remote sensor system is a regularly a specially appointed system, "which requires each sensor hub be free and sufficiently adaptable to act naturally sorting out and self-mending as per diverse circumstances". This characteristic element conveys an extraordinary test to remote sensor system security.

On the off chance that self-association is inadequate in a sensor system, the harm coming about because of an assault or even the hazardous environment may be obliterating.

ix) Backward Secrecy. A joining sensor ought not to have the capacity to peruse any beforehand transmitted message. The security administrations in WSNs are generally based on cryptography. Be that as it may, because of the limitations in WSNs, numerous officially existing secure calculations are not functional for use.

III. SECURITY THREATS AND ISSUES IN WSN

Wireless Sensor Networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Basically attacks are broadly classified in two categories i.e .active attacks and passive attacks. This paper points out both of these attacks in details [6].

A. Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. Some of the more common attacks against sensor privacy are:

Monitor and Eavesdropping. This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents.

Traffic Analysis. Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

Camouflage Adversaries. One can insert their node or compromise the nodes to hide in the sensor network, after that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

B. Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

Routing Attacks in Sensor Networks. The attacks which act on the network layer are called Routing attacks. The following are the attacks that happen while routing the messages.

Attacks on Information in transit. In a sense or network, sensor monitors the changes of specific parameter 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.

Black hole/Sinkhole Attack. In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. In fact, this attack can affect even the nodes those are considerably far from the base stations. Fig. 3 shows the conceptual view of a Black hole/Sinkhole attack.

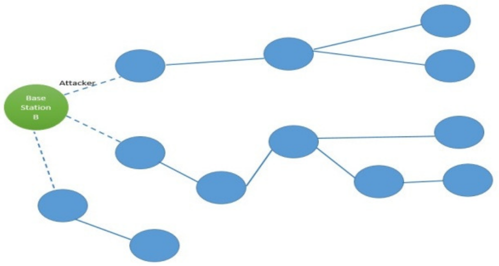

Fig. 3. Conceptual view of Black hole.

Worm holes Attacks. Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location.

HELLO flood Attacks. An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. HELLO flood Attack is a particular kind of DoS. To prevent HELLO flood Attacks, blocking methods can be used.

Denial of Service (DoS). Malicious activity causes Denial of Service through sending extra redundant packets. Various types of DoS attacks in various layers could be presented in WSN as an example at the physical layer the DoS attacks could be jamming and tampering[3].

C. Physical Attacks

Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors or replace them with malicious sensors under the control of the attacker.

D. Message Corruption

Any modification of the content of a message by an attacker compromises its integrity.

Table 1: Denial-of-Service Defence in WSN.

Network layer	**Attack**	**Defences**
Physical layer	Jamming	Spread- spectrum, priority messages.
	Tampering	Tamper-proofing, hiding.
Data link	Collision	Error- correcting code.
	Exhaustion	Rate limit
	Unfairness	Small frames
Network layer	Black holes	Authorization, monitoring, redundancy
	Hello flood	Authentication, packet leashes by using geographical and temporal info.
	Spoofed routing information and selective forwarding.	Egress filtering, authentication, monitoring.
	Sybil	Authorization, monitoring
	Sinkhole	Redundancy
Transport layer	Flooding	Client puzzles, Rate limitation.

IV. SECURITY CHALLENGES IN WSN

The nature of large Ad-hoc, wireless sensor networks present significant challenges in designing security schemes.

A. Wireless Medium

The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks.

B. Ad-Hoc Deployment

The ad-hoc nature of sensor networks means no structure can be statically defined. Nodes may be deployed by airdrop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self configuration. Security schemes must be able to operate within this dynamic environment.

C. Hostile Environment

The next challenging factor is the hostile environment in which sensor nodes function. Motes face the possibility of destruction or capture by attackers. The highly hostile environment represents a serious challenge for security researchers.

D. Immense Scale

The proposed scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tens to hundreds of thousands of nodes has proven to be a substantial task.

V. LITERATURE SURVEY

Many researchers have proposed the mechanism against attacks. The most recent research in field of security in wireless Sensor Network issues, challenges and solution which have been taken help are as follows:

Author/researchers	**Description**
Vikash Kumar, Anshu Jain and PN Barwal [1]	Proposed an attempt has been made to explore the security mechanism widely used to handle those attacks and also describe the classification of attacks in wireless sensor network.
Shahnaz Saleem, Sana Ullah, Hyeong Seon Yoo[5]	Proposed outlined major security requirements and DoS threats in a WBAN. It provided a comprehensive overview of existing security protocols for a WBAN. More efforts which are required to implement and introduce new security levels. AES-CTR,AES-CBC-MAC, and AES-CCM are the security nodes for a WBAN.
B. Sangeetha[2]	Wireless Sensor networks present delightful challenges for the application of distributed control. We have to apply appropriate techniques and metrics in light of new technology opportunities i.e. cheap processing and sensing nodes and limitations i.e. energy constraints. Visualization and Novel debugging technologies designed for the new challenges of sensor networks will be very helpful in testing and maintenance of new algorithms and application.

Author/researchers	**Description**
Dr. G Padmavathi, Mrs. D Shanmugapriya [6]	Proposed the attacks and their classification in wireless sensor networks and also an attempt have been made analyse the security mechanism. This survey explains security mechanism and makes their network safer.
S. Zhu *et al* [15]	Proposed several authentication schemes to prevent false data injection attacks in sensor network. They demonstrated the feasibility of employing their schemes on resource constrained sensor nodes by implementing one of the schemes on the Tiny OS-based Mica 2 motes.
L. Jialiang Valois, F Dohler M, Min You Wu [4]	Showed that the attacks that are popular in a WSN like Hello flood attack, Sink hole attack, Sybil attack and denial of service attack have been simulated in a simulated in a simulator. On Simulation the performance and the efficiency of the network can be analysed.
D. Jing, H. Richard, Shivakant Mishra [11]	Showed in paper the novel secure code propagation protocol for wireless sensor networks that employs private key signing of the root of a joint structure comprised of hash chains for inter page authentication and harsh traces for intrapage authentication.
Ahmad Salehi S., M.A. Razzaque, Parisa Naraei [3]	Concentrate on the threats in WSN security and abstract of threats which present in various layers along with their defense techniques. Specific methods and protocols have been advanced to utilize in WSNs.

VI. SECURITY SOLUTION IN WSN

A. Directional Antennas

The physical layer of a wireless sensor network is in charge of bit-stream transmission/reception over wireless communication channels, performing a series of tasks that includes carrier frequency selection and generation, signal detection, modulation or data encryption. A central role in this context is played by antenna devices which basically transform electric power into electromagnetic waves, or vice versa. In order to be used in WSN nodes, directional antennas have to possess four basic features: they must be small, reasonably priced, consume low power and able to operate in licensed frequency bands: 315 MHz, 433 MHz or 868 MHz in Europe, 915 MHz in North America, 2.45 GHz Industrial-Scientific-Medical (ISM) band or within the millimeter-wave spectrum. These requirements drastically limit the number of directional antenna construction types adaptable for sensor nodes. [18]

Directional antennas can mitigate or even eliminate the risks related to some categories of security attacks on WSNs due to their specific radiation pattern which can be materialized into mechanisms for localization of neighboring or malicious nodes, or can drastically reduce the areas from where an attack can be carried out. The main types of attacks that can be mitigated using directional antennas are: eavesdropping, jamming, Sybil attack and wormhole attack, but similar countermeasures can reduce the risks for traffic analysis, man-in-the-middle attack or node capturing attack.

B. Cryptography

Cryptography and secure routing protocols provides the defense against the security in WSN. Rivest et al. (1998) proposed RC6 block cipher based on RC5 symmetric key approach [19].

Details of RC6: RC6 can encrypt 128-bit data blocks by using 128, 192, or 256 bit keys [19]. RC6 can support various word/key sizes and number of rounds and it can be defined as RC6-w/r/b where w stands for bit size of word, r stands for the number of rounds, and b stands for key size in bytes. The most fundamental difference between RC6 and RC5 is that RC6 uses an extra multiplication operation to perform bit rotations in each word. The operations used in RC6 are defined as followings:

i). A+B integer addition modulo 2w
ii). A-B integer subtraction modulo 2w
iii). A B bitwise exclusive-or of w-bit words
iv). A*B integer multiplication modulo 2w
v). A<<<B rotation of the w-bit word A to the left by the amount given by the least significant lg w bits of B
vi). A>>>B rotation of the w-bit word A to the right by the amount given by the least significant lg w bits of B
vii). f(x) = x(2x+1)mod 2w

Encryption process in RC6 algorithm is described in figure 4 and figure 5. Encryption and Decryption process are vice versa.

```
Input:
Plaintext stored in four w-bit input registers
A, B, C, D
20 rounds
32-bit round keys S [0,…. 43]
Output:
Ciphertext stored in A, B, C, D
Procedure:
B = B + S [0] //Pre-whitening
D = D + S [1]
for i = 1 to 20 do
{
    t = (B x (2B + 1)) <<< 5
    u = (D x (2D + 1)) <<< 5
    A = ((A⊕ t) <<< u) + S[2i]
    C = ((C ⊕u) <<< t) + S[2i+ 1]
    (A, B, C, D) = (B, C, D, A)
}
A = A + S [42] //Post-whitening
```

Fig. 4. RC6 Encryption for AES with RC6-32/20.

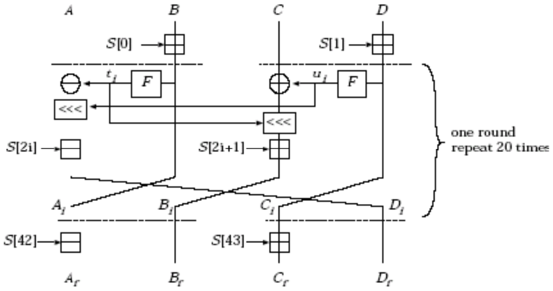

Fig. 5. RC6 AES Encryption Diagram.

C. Key Management Protocol

Key management aims at establishing the key among the nodes in a reliable manner. The entity that controls the generation, re-generation and distribution of keys is called Key Distribution Center (KDC). Localized Encryption and Authentication Protocol (LEAP) is a key management protocol for sensor network. Four types of keys are established for each node:

- An individual key shared with base station (pre-distributed).
- A group of keys shared by all the nodes in the network (pre-distributed).
- Pairwise key shared with immediate neighbour.
- A cluster key shared with multiple neighbour nodes.

D. Defence against DoS Attacks

A defence against DoS attack is the use of error correcting codes [20]. Jamming attack can be defended by frequency hopping and code spreading [21]. A possible solution for energy exhaustion attack is the application of rate limiting MAC admission control.

VII. CONCLUSION

The demand for security in WSNs becomes more obvious during ability growth of WSNs and they are used much more. Security in Wireless Sensor network is vital to the acceptance and use of sensor networks. In particular, Wireless Sensor Network product in industry will not get acceptance unless there is a full proof security to the network. In WSNs the node nature causes limitations like restricted energy, capability of processing and storage capacity. These restrictions create WSNs so destructive from conventional Ad hoc wireless networks. Specific methods and protocols have been advanced to utilize in WSNs. All of the mentioned security dangers including the Hello flood attack, Wormhole attack, Sybil attack, Sinkhole attack, offer one usual goal which is for compromising the integrity of the network they attack.

The security of WSNs has become a major subject since of the different dangers appearing and the significance of data confidentially, although in the past, there was a little concentration on WSNs security. This paper summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks. The challenges of Wireless Sensor Networks are also briefly discussed.

REFERENCES

[1]. Vikash Kumar, Anshu Jain, PN Barwal, "Wireless Sensor Networks". *International Journal of Information and Computation Technology,* Vol. **4** .pp.859-868, 2014.

[2]. B. Sangeetha, "Wireless Sensor Networks: Issues Challenges and Survey of Solutions", *International Journal for Scientific Research and Development,* Vol. **2**, May 2014.

[3]. Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, "Security in Wireless Sensor Networks: Issues and Challenges", *Proc. IEEE International conference on Space Science and Communication,*1-3 July 2013.

[4]. L. Jialing. Valois , F; Dohler M , Min You Wu, "Optimized Data Aggregation in WSNs using Adaptive ARMA, "Sensor Technologies and Applications (SENSORCOMM) 2010 Fourth International Conference on, pp. 115- 120 , 18- 25 July 2010.

[5]. Shahnaz Saleem, Sana Ullah, Hycong Seon Yoo, "On the security issues in Wireless Body Area Networks" *International Journal of Digital Content Technology and its Application*, Sep 2009.

[6]. Dr. G Padmavathi, Mrs. D Shanmugapriya, "A survey of Attacks, Security Machanism and challenges in Wireless Sensor Networks". *International Journal of Computer Science and Information security*, Vol. **4** no. 1 and 2, 2009.

[7]. K. K. Woo, Hwaseong, H.K YONG, H.L. Dong, Implementation and Analysis of New Lightweight Cryptographic Algorithm suitable for Wireless Sensor Networks " Information security and Assurance, 2008.*ISA 2008, International Conference on, 24-26* April 2008, pp.73-76.

[8]. Y. Wang, G Attebury, et al. "A Survey of Security issues in Wireless Sensor networks" *Computer Science and Engineering,* vol. **8**, no 2, 2006.

[9]. A. S. K. Pathan, Hyung-Woo, S.H. Choong, "Security in Wireless Sensor Networks: Issues and challenges, "Advanced Communication Technology, 2006. ICACT 2006, *The 8th International Conference,* vol.**2**, pp.20-22 Feb.2006.

[10]. H.M Kirk. Wong, Z. Yuan, C. Jiannong, W. Schenguei, "A Dynamic user Authentication Scheme for Wireless Sensor Network". *IEEE International Conference on Sensor Networks Ubiquitous and Trustworthy computing (SUTC 06), 2006*

[11]. D. Jing, H. Richard, Shivakant Mishra "Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks", with international conference on Information processing in Sensor networks, pages 292-300, April 19-21,2006

[12]. C. Xiao and Drissi, J., "An efficient key management scheme in hierarchical sensor networks" , Mobile Ad hoc and Sensor Systems Conference,2005. *IEEE International Conference on*, 7.7 Nov2005 pp.846

[13]. G. Gunnar, K. Jens-Peter, S. Berk, "Public Key Cryptography in sensor Networks Revisted", Book Series Lecture Notes in computer Science pages 2-18, 11 January 2005.

[14]. E. Shi and A. Perrig. "Designing Secure Sensor networks". *Wireless communication Mag.,* vol. **11**, no. 6, pp.38-43, Dec. 2004.

[15]. S. Zhu el al , "An Interbaved Hop- by- Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks, "Proc. IEEE Symp , Security and Privacy, Oakland, CA. pp 259-271, May 2004.

[16]. N. S. Fayed, E. M. Daydamoni, and A. Atwan, "Efficient combined security system for wireless sensor network," *Egyptian Informatics Journal.* 2012.

[17]. Parli B. Hari, Shailendra Narayan Singh Security Issues in Wireless Sensor Networks: Current Research and Challenges", IEEE xplore 2016.

[18]. Daniel-Ioan Curiac "Wireless Sensor Network Security Enhancement Using Directional Antennas: State of the Art and Research Challenges", www.mdpi.com/journal/sensors 2016.

[19]. Shailesh N. Sisat, Prof. Shrikant J. Honade "Security and Privacy in Wireless Sensor Network Using RC6 Algorithm", *International Journal of Advanced Engineering Research and Science (IJAERS)* Vol. **3**, Issue-5, May-2016] ISSN: 2349-6495

[20]. A. J. Albarakati, "A Study on Underwater based Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume **119** – No.12, June 2015.

[21]. Dr. S. Mohammadi and H. Jadidoleslamy," A Comparison of Physical Attacks on Wireless Sensor Networks", *International Journal of Peer to Peer Networks* (IJP2P) Vol. **2**, No.2, April 2011.