# Wireless Sensor Networks and Its Security

Gaurav Rajput[1], Mohan Vishal Gupta[2]
[1]*B.sc. Student, CCSIT, TMU,Moradabad*
[2] *Assistant Professor, CCSIT , TMU,Moradabad*
1gauravchauhan4287@gmail.com
2mohan.computers@tmu.ac.in

*Abstract*— **The confluence of cheap wireless communication, sensing and computation has produced a new group of smart devices and by using thousands of these kind of devices in self-organizing networks has formed a new technology that is called wireless sensor networks (WSNs).**

**WSNs use sensor nodes that placed in open areas or in public places and with a huge number that creates many problems for the researchers and network designer, for giving an appropriate design for the wireless network. The problems are security, routing of data and processing of large amount of data etc.**

**This paper describes the types of WSNs and the possible solutions for tackling the listed problems and solution of many other problems. This paper will deliver the knowledge about the WSN and types with literature review so that a person can get more knowledge about this emerging field.**

***Keywords***— **WSN, Overview of WSN, WSN with Types, WSN Security, RBAC**

## I. INTRODUCTION

WSN has become an emerging field in research and development due to the large number of applications that can become significantly beneficial from such systems and has led to the development of cost effective, not-reusable, tiny, cheap and self-contained battery powered computers, also called sensor nodes. These sensor nodes can accept input from an attached sensor and process the input data gathered from the sensor nodes. After that the process data wirelessly transmits the results to transit network. WSNs are highly dispersed networks of lightweight and small wireless nodes, deployed in huge numbers, to monitor the system or environment by the measurement of physical parameters like pressure, temperature, or relative humidity [1]. China put intelligent information processing and sensor network in priority for 15 years in the “National medium and long term program for science & development (2006-2020)”. WSNs can be applied in industry, agriculture, military defence, environment monitoring, remote control and city management etc. that is why WSNs are becoming more and more popular [2] [3]. WSNs have much more similarity with Mobile Ad-hoc Networks (MANET). WSNs also create network that contains sensor nodes connecting with each other, in an Ad-hoc manner and no proper infrastructure is there for both but WSNs have the collection of data with the sensor nodes but MANET can or cannot use sensor nodes. In this paper, we gave the description of WSNs and its types with literature review, as shown in the WSNs consist of tiny and low power sensor nodes that collect data through tiny sensors, process the data and send to particular location. We also describe the types of WSNs with the research work. We include the flaws of existing technology or in a particular type and how we can cover those open holes by using various techniques, protocols or algorithms.

## II. TYPES OF WSN

### 2.1. Mobile Wireless Sensor Networks (MWSNs)

MWSNs can be defined as a WSN that have mobile sensor nodes as compared to the usually used WSN in which sensor nodes are static. MWSNs have more versatility than the static WSNs because MWSNs can be deployed for any scenario and they can manage with quick topology changes. The normal WSN is simply deployed with static nodes to achieve monitoring missions in the area of interest but due to dynamic changes of hostile environment and events, a pure static WSN may face the following problems:

1- Connectivity of the whole network and complete coverage of the sensing area could not possible in WSN like in the case of robots or aircrafts for hostile region [4].

2-As sensor nodes usually works with battery powered and prone to errors. The node can be dead if the energy of battery ends and this results the communication breakup of sensor network and replacement of new nodes is also a difficult task.

3- For some special applications like tracking applications, the network needs a larger nodes to cover the whole area that ultimately the cost of network is increased.

4- For some applications, there is a need of some sophisticated sensors for performing some specific military tasks that may need camera with every sensor node for image collection that is not feasible to equip every node with separate camera. By introducing mobility, all the listed problems can be overcome and many other problems can be covered. We can enhance the flexibility and capability of WSN by adding mobile nodes. Different missions can be conduct by controlling the movement of mobile sensors [5]. More and more, individuals and communities are using MWSNs and there is no need of pre-deployed network infrastructure when cooperating mobile nodes communicate with each other, in order to achieve various kinds of functions [6]. MWSNs are deployed in an open environment and having more chances of security attacks. Security is one of key issue in MWSNs and need to be solved. The attacks in MWSNs can occur from any side or any direction to any targeted node because MWSNs are consists of mobile wireless nodes that forms the temporary network without any centralized infrastructure [7] [8]. The complex security mechanisms and algorithms cannot be implemented in wireless mobile sensor nodes. The reason of not implementing any security algorithm or mechanism is due to resource constraints regarding bandwidth, computational power and memory size. The traditional security mechanisms are invalid for MWSNs due to the mobility of wireless nodes in network topology and this mobility creates dynamic attributes in topology that results invalidity of security mechanisms. The security attacks (internal or external) can be controlled or minimized by using the cryptography and authentication mechanisms but both techniques can handle the external attacks in WSNs and are unable to handle the internal attacks in MWSNs because the wireless sensor nodes can be easily stolen when deployed in hostile or in an open environment. For this case, the network can be controlled or destroyed by the nodes which have accessed the network [9]. One of the attack in WSN is the node replication attack and number of protocol proposed for tackling these type of attacks but no suitable mechanism is find out for MWSNs. However an appropriate mechanism is described by Deng, Xiong and Chen [10]. They described the mobility property and propose two protocols for mobility assistance for the detection of node replication attacks in MWSNs. First protocol is the Unary Time Location Storage and Exchange (UTLSE) that assigns each observer a task of tracking a particular set of other nodes. All the observers only store one time location entitlement for every tracked node and detect the replication when they come across each other. The second protocol is Multi Time Location Storage and Diffusion (MTLSD) that lets every observer stores multi time location claims for each tracked node. It also introduces more cooperation between the observers to improve the detection performance. Both protocols works as encounter- based because they only sent messages for detecting the replication when two nodes meet or come across each other and due to this way of working, the protocols do not have any need of routing signaling messages. Both protocols can also identify the replication with high detection accuracy as well as with very low communication, computation and storage overheads [10].

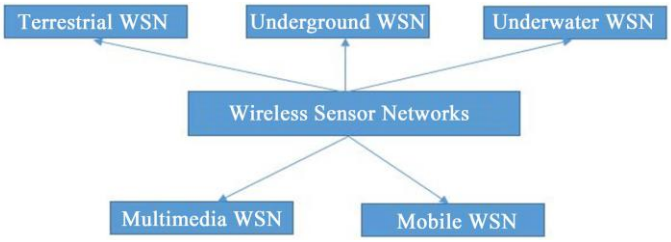

**Figure – 1 .** WSN types .

A three layer architecture for mobile nodes is described, in which all the sensors in MWSNs are organized, by using the architecture. Data collection, data processing and routing table maintenance are placed in different nodes. The complexity of sensors and the cost of construction can be reduced by using Multi-layer MWSNs (M2WSN). SP (Shortest path) routing protocols proposed on the base of new architecture, for adapting sensors to update the network topology. The researchers also include a simulation of SP that reduces the energy utilization and offers a decent solution for node movement in M2WSNs and this simulation shows the better results, as compared to LEACH [11].

### 2.2. Underwater Wireless Sensor Networks (UWSNs)

Underwater wireless communication is one of the major challenge in building UWSN. It has been observed that Radio Frequencies and acoustic waves (having narrow bandwidth) are heavily attenuated and altered in water. An alternative but a feasible solution that can be considered is using optical communication, in case of short range distance. This approach mainly emphasizes on an Optical Physical (PHY) Layer taking into account the features of WLAN (IEEE 802.11) Infrared Physical Layer and the compatibility with the most recent terrestrial Wireless Sensor Network's protocol *i.e.* IEEE 802.15.5. As compared to acoustic communication, if optical communication in green/blue wavelengths (for short distances) are used then they offer high band communication and faster propagation in water. An experimental set up was done and it was noticed that increasing the distance (between a LED and a photodiode) causes a high BER (Bit Error Rate) while water turbidity was also kept in mind [12].

Terrestrial wireless sensor networks are an active area for development and research. Fundamental properties of these networks are low-power, a several number of co-operating small nodes that are capable in observing, detecting, and tracking various objects and events inside a specific environment. This makes these networks very appealing for a number of military and industrial applications. Within the overall wireless sensor network field, underwater wireless sensor networks (UWSN) is an emerging area of research. The number of underwater (M. U. Aftab *et al.* 175) wireless sensor networks-based applications is continually increasing. Most of the UWSN applications can be classified as Seismic, monitoring, assisted control and navigation, location reference points and security applications. While future UWSN includes applications for attack purposes and unmanned submarines. When it comes to UWSN, there are still so many challenges and difficulties to deal with e.g. power-consumption, security, and time synchronization, communication between UWSNs, installation, implementation, power recharging and recovery [13].

### 2.3. Space-Based Wireless Sensor Networks (SB-WSNs)

The wireless sensor networks are networks of integrated micro sensors for monitoring and data gathering for some of the environment conditions *i.e.* temperature, vibration, sound, motion and pressure. While in space, these networks might be used for space weather purposes in (LEO) low Earth Orbit or implementation of wireless sensor networks within a spacecraft in single probe missions or in order to interchange electrical wires, or as very tiny satellite (sensor) nodes flying in compact formations and chemical and physical sensing of the soils, surfaces and atmospheres of other planets. Multipath routing scheme is a perfect nominee for space-based missions

of micro-sensor nodes. WSNs need to be optimized if they are to be used for space or solar system exploration. The modifications should be according to space requirements. Design issues like selection and design of antenna, software and power supply must be completed by thoroughly examining the mission's characteristics [14].

The concept of terrestrial wireless sensor networks (TWSN) can be applied to space *i.e.* satellite sensor network. Grouping the design and enabling technologies for pico-satellite formations. The idea is to use inexpensive constellation of sensor nodes to collect important information instead of doing the same using a large expensive satellite. The research that's been carried out at the Surrey Space

Centre, was mainly aimed at space weather missions in low Earth orbit. Future space-crafts are thought to be miniature, autonomous and distributed. In this regard, flower constellation set is considered to be the best for orbital configuration in nano- and micro- satellite missions. While there are some issues in Flower constellation, related to positioning satellites which can be solved using Inter-satellite communication capability. Communication issues, referring to the Open Systems Interconnection (OSI) networking scheme, of a space based wireless sensor network (SB-WSN) have been ummarized. A system-on-a-chip computing model and platform and the agent middleware for SB-WSNs have been presented. This system architecture focused on the LEON3 soft processor core is targeted at effective hardware support of collaborative processing in these networks, offering several intellectual property cores *i.e.* transceiver core, a hardware accelerated Wi-Fi MAC and a Java co-processor. A new configurable inter-satellite communications component for pico-satellites has also been outlined [15].

### 2.4. Wireless Underground Sensor Networks (WUSNs)

The probabilistic connectivity of the WUSNs has been discussed. WUSNs are one of the unique extension of terrestrial WSNs. WUSNs' heterogeneous network architecture and channel characteristics, the connectivity study is much more complicated than in the ad hoc networks and terrestrial WSNs. This connectivity issue might haven't been addressed previously. Thus, a mathematical model was developed to study and examine the probabilistic connectivity in WUSNs, which gathered the effects of environmental parameters *i.e.* the soil composition and soil moisture, and several system parameters *i.e.* the sensor burial depth, the operating frequency, the density of the sensor devices, the sink antenna height, the number and the mobility of the above-ground sinks and the tolerable latency of the networks. The upper and lower bounds for the connectivity probability are calculated systematically. Simulation and investigation studies were performed, whereas the theoretical bounds were authenticated, and the effects of system parameters and some environmental parameters on the performance were explored [16].

### 2.5. Wireless Multimedia Sensor Networks (WMSNs)

The Wireless Multimedia Sensor Networks (WMSNs) comprise of tiny sensor-nodes that can sense, compute, actuate, communicate, and have control components. Various applications of the Wireless Sensor Multimedia Networks (WMNs) include target trailing, habitation monitoring, traffic management systems and ecological monitoring; these kinds of applications involve efficient communication of event happenings and features in 176 multimedia form *i.e.* image, audio and video [17].

Wireless Multimedia Sensor Network (WMSN) is a novel appliance of Wireless Sensor Networks (WSNs), as Multimedia data needs continuous transmission of data, increased bandwidth, storage and power, and low latency rate so WMSNs requires much attention. So far different routing protocols have been proposed for proficient data communication in WSNs. Usually in WSNs, the routing algorithms designed to route tiny scalar data for comparatively short time interval. The basic ingredients of WSNs routing protocol are use of minimum hops, maximize the available power, achieve low latency rate and less load of traffic, finding more than one path to destination etc. With sensor networks another significant concern is the creation of Holes which is because of the fact that during routing, the nodes nearby the destination are used more frequently so in result the batteries of such nodes gets exhausted in advance. Thus such nodes failed to transmit the sensor information to the base station [18] Hop and Load based Energy Aware Routing protocol (HLEAR) has been developed for WMSNs, to eradicate the above described issues. In HLEAR, the algorithm finds semi disjoint or disjoint paths by hop counts, load of traffic and energy of nodes. As HLEAR is a reactive (On Demand) routing protocol so a compression is made between HLEAR and Tiny Advanced On-demand Distance Vector (AODV), a reactive protocol. The HLEAR protocol found more intelligent in path selection as it chooses such paths which can carry affording traffic rate by having lesser hop distance. Furthermore, due to absorption of energy of nodes, HLEAR also tackles with Hole creation problem [18]. In WMSNs, we mostly comes up with a question that “How and where to Install sensor nodes while having inadequate resources of communication to support all nodes?” Researchers tried to answer this question by making wide theoretical analysis. Its general considerations are less mobile or a static type of networks environment, smooth topology and TDMA based single channel communication to show cross layer design model in which both node admittance to a WMSNs mechanism and the interaction of node with the resource management and link scheduling mechanisms, are examined. Generally interaction of node is originated with two stage optimization problem in which the first step is to increase the total numbers of already acknowledged sensor nodes and the second step is to enlarge the lifetime of the network. The interaction of node can also originates as one stage optimization problem having more complex mathematical logic. The commonality among all described proposals is the segregation of some sort of services, without this segregation the QoS cannot be guaranteed by the WMSNs [19]. As described earlier that WMSNs requires much more recourses like as bandwidth. Spectrum sensing approach is used to reply the request of bandwidth by which the spectrum utilization maximizes. Hence to utilize the spectrum holes and available bands there is a need of reliable, accurate, efficient and real time methods. Previously, in cognitive radio (CR) some methods are introduced to sense the spectrum, among those methods the Multi-Taper Method (MTM) is the most tempting. As MTM is considered very near optimal for wideband signals and also an efficient method for CR so we can assume that for spectrum sensing in WMSNs, MTM can be a superior selection. The existing MTM have some challenges like supplementary resource demand. Therefore, introduced MTM into WMSNs and also present an algorithm to eradicate the previous implementation issues in MTM. The detailed simulations proved that the new approach for wideband signals in WMSNs is more corresponding to the real time values and also provides much less false alarm rate as compare to other methods due to decreased variance. This approach also detects the spectrum holes more efficiently and accurately [20]. For the purpose of optimization of network performance introduced an Energy Efficiency QoS Assurance Routing in Wireless Multimedia Sensor Networks (EEQAR). EEQAR is actually an analysis of social network to improve performance of network. The main idea behind the development of EEQAR is to introduce such routing for wireless multimedia sensor networks which provides energy efficient assurance of QoS. For the selection of most consistent paths, link quality estimators are not used in EEQAR, though it generates an additional load on EEQAR in the process of route discovery to communicate between different clusters. The video quality levels evaluation does not covered by EEQAR [21]. The researchers suggest the concept that for multiple path communication among two nodes, Multipath Data Transfer protocol offers concurrent multiple paths. Their proposed algorithm divides the work between all nodes which equally extends the overall life of WMSNs [17].

### 2.6. Terrestrial Wireless Sensor Networks (TWSNs)

Most generally the Terrestrial WSNs contains hundreds to thousands of cheap wireless sensor nodes which are installed in a specified geographical area. The deployment can be in an ad-hoc network or in pre-planned networks based. In the case of Ad-Hoc networks, the sensor nodes be released from plane and arbitrarily place them into the area of target. In the case of pre-planned, there are four different placements as followed, Grid, Optimal, 2-D and 3-D placement models . The FSO/RF systems in wireless sensor networks are getting much attraction from researcher. A free-space optical(FSO) link used in FSO/RF systems as basic communication medium while a RF (Radio

Frequency) links are also used as backup when LOS for optical communication are not present. As FSO optical communication links results low communication energy than the high data rate broadband optical communications, so the idea of using FSO links in WSNs get heap. The major concern of FSO/RF is weather effects like snow or rain. For terrestrial applications, the comparison of the lifetime performance of hybrid WSNs and FSO/RF WSNs under weather effects of rain and snow shows that by proper threshold selection we can achieve the most favourable practice of power efficient FSO link.

### 2.7. WSN Security and Security Issues

Generally WSNs are used to collect information from various locations of physical world and also they are deployed in controlled and uncontrolled environment [3]. So by their applications and deployment nature Wireless sensor networks are ultimately insecure. These networks have numerous limitations like node (less computational power, less memory, less energy etc.), network (because they are acting as mobile as hoc network) and physical (deployed in different environments like public and hostile) limitations which makes them supplementary vulnerable to various security attacks. Ad hoc nature of sensor networks opens the unique challenges to the reliability and security. Owing to the limited computational and processing constrains traditional security techniques and policies are not suitable in order to maintain confidentiality, Authentication, Availability and Integrity in WSN, s [1].

According to Pfleger there are four different classes of security threads that are common in computational systems and also in sensor networks [24]. These are Interruption, Interception, Modification and Fabrication. In Wireless sensor networks researcher identified several possible security attacks like passive information gathering, node subversion, false node, node malfunction, node outage, message corruption, traffic analysis, routing loops, selective forwarding, sinkhole, Sybil, wormholes, hello flood and DoS etc. These attacks also disturbs WSN layers specifically application, transport, network, data link and physical layers. Different countermeasures and defense techniques are presented by researchers for layered security like malicious node detection and isolation, unique pair wise keys for application layer, limiting connections numbers, client puzzles for transport layer, Key management secure routing, Authentication, Encryption, Redundancy, Probing, monitoring, two way and three authentication and three way handshake for network layer, link layer encryption, rate limitations, error correcting code for data link layer and adaptive antennas, spread spectrum for physical layer. However we need to have a security framework in order to provide countermeasures against security attacks in WSN [24] [25].

Wireless sensor networks (WSNs) are extremely prone and susceptible to external and internal attacks as they consist of numerous devices with constraints for example; less memory, associated low energy and low battery power. The nodes in WSNs communicate with each other through wireless links. Nevertheless, WSNs are being deployed extensively. There are still unsolved problems in WSNs and security is one of the high priority research issues. These networks are implemented in hostile environments. Resource-constraints, communication

overheads involved, and environmental conditions give rise to various security attacks or threats. Securely communication and security among WSN nodes is an important challenge. Authors described the security of M. U. Aftab *et al.* 178 WSNs and attacks that occur at different layered architecture of WSNs and how to prevent them [26]. Secure protocols should be designed and some access control mechanism can be applied to provide a secure network for mobile devices in an organization. Different researchers work on the security and access control mechanisms. Role Based Access Control (RBAC) is one of the most widely used access control model. The main thing in RBAC is the management of large number of permissions with help of Roles. RBAC architectural issues in institution collaborative systems has been highlighted because there is no specific architectural design that had been defined for the institution's security. A system has been proposed that combines the efficiency of both RBAC and Organization Unit (OU). The objective of using OU for the institutional systems is the effective management of users and objects. Proposed system helps in two things: one user management and secondly load sharing of administrator. By applying OU, users can be easily be managed on department level and as well as in a particular department. Also the OU creation would be done on department level. Furthermore, a hierarchical architectural model has been described that can help an institution or IT manager in implementing and deploying of RBAC with the concept of OU thus, making a system more secure and facilitating the users in efficient manner [27].

### 2.8 Security Protocols

In this chapter, TinySec, MiniSec, IEEE 802.15.4, SPINS, L sec, LLSP, LISA, and LISP are described.

*1. TinySec.* Tiny Sec [29] developed by the University of Berkeley is a link layer security architecture that has been included in the Tiny OS version. Its design is based on ease of use andminimal load brought on sensor network. TinySec supports two different security options: encryption with identity authentication and only authentication. In identity authentication encryption, data is encrypted and an identity authentication code (MAC) is added to the package. However, in only authentication method, data is not encrypted bu`t only authentication of the package is realized with a MAC. As it is understood from this, in Tiny Sec, the identity authentication is a must for each package but encrypting the data is an option that can be decided according to the application. In encryption of messages, Skipjack block encryption, 8-bit initialization vector (IV), and code block chaining (CBC) are used. There is no restriction on keying method; in practice, a single key pair (one for the encryption of data and the other for the calculation of MACs) is selected for the whole network according to the desired level of security. TinySec at the tightest security level where identity authentication encryption is used brings 10% extra load on energy, delay, and band width. However, in cases where only authentication is used, this ratio drops to 3%.

*2. SPINS.* SPINS [35], developed by Berkeley University, consists of $\mu$TESLA protocol used in identity authentication broadcasting, SNEP protocol providing confidentiality, identity authentication between two nodes and data freshness, and a routing protocol based on these. SNEP offers the below possibilities:

(i) Semantic security: semantic security, meaning an attacker listening to the network cannot obtain any information about the plain text even if more than one encrypted copy of the same plain text is received, is realized by a counter shared between the receiver and the sender and incremented in each message exchange;

(ii) Identity authentication: the receiving node verifies the identity of the sender with the MAC used;

(iii) Recursion protection: the counter in MAC prevents old messages to be sent again;

(iv) Weak freshness: the counter used between the receiver and sender for semantic security ensures the message received is sent after the previous one;

(v) Low communication overhead: keeping the counter on receiver and sender, not placing it in the message, reduces communication overhead.

In conventional approaches, identity authentication is done by asymmetrical methods. However, hardware restrictions of sensors are highly insufficient for the quite expensive asymmetrical methods. TESL Agives the logic of asymmetry to identity authentication with symmetric methods. The sender creates a MAC for the message packages to be broadcasted by using a key known by only itself and by using a one-way function. It broadcasts the key of the message a certain time after the message is sent. Thus, the possibility of changing the contents of the package is removed. At the receiver end, the package kept in a buffer memory is authenticated by using this key. RC5 is used in encryption. For all this identity authentication process, $\mu$TESLA needs synchronization between the receiver and the sender even if it is loose.

*3. LISP.* LISP aims security solutions in large-scale wireless networks consisting of a large number of nodes with limited resources. To scale networks consisting of a large number of nodes Park and Shin divide them into clusters, select a head for each cluster, and create a key server. LISP [36] (lightweight security protocol) has a new switching mechanism. It uses switching mechanism by using head cluster and key servers. Below are the advantages of this method:

(i) It uses an effective key broadcast which do not need ACKs to be sent;
(ii) It uses check bits created without adding them to the data message;
(iii) It might recover the lost keys;
(iv) It refreshes key without data encryption or decryption. The benefits of LISP in protecting critical information against attacks can be summarized as follows.
(i) Data integrity prevents tampering of data that is sent.
(ii) Access control is achieved by controlling the inputs to the network.
(iii) Key refreshing provides protection against nodes that may jeopardize the network. LISP protocol may combine together with security the other services (routing, data distribution, and location). LISP is a flexible and energy-sensitive protocol. In addition, because it does not need ACK and other control packages, it
is quite strong against DoS [37] attacks.

*4. IEEE 802.15.4.* IEEE 802.15.4 [38, 39] defines medium access and physical layers for wireless private area networks (WPANs). Although this protocol was not developed for WSN, it is used in WSNs because of its low power consumption, low cost, and flexibility. Currently, this protocol works on Micaz, TelosB nodes produced by the company Cross Bow. ZigBee strong encryption AES-128 is used. Zigbee provides freshness. Controlling freshness prevents repeated attacks. Counter is reset when a new key is created. Zigbee provides integrity and prevents an attacker from changing the message. Integrity options are 0, 32, 64, and 128 bit, by default 64 bit. Zigbee provides authentication. Authentication tests whether the right person is reached or not and prevents the attacker showing the device like another one. Authentication is possible at the network and device levels. Authentication at the network level is achieved by using a public network key. Authentication at device level is achieved by using the unique link key between devices. Zigbee provides encryption and prevents an attacker from intercepting and listening. Zigbee uses 128-bit AES encryption. Encryption security is provided at the network and at the device level A public key used at the network level encryption. It prevents attacks because of very low memory usage. Device level encryption uses a common link key. Zigbee uses three types of keys. Master key provides long term security between two devices. Link key provides security between two devices. Network key provides security on the network.

*5. L Sec.* L Sec [40] provides authentication and authorization with simple key exchange scheme. Furthermore, it has protection mechanisms against data confidentiality, breaches, and illegal events. There is variety of security attacks on sensor networks. As examples of Do S, eavesdropping, replay attacks, tempering the message, and malicious nodes can be mentioned. To defend against these types of attacks, L Sec uses data confidentiality, identity authentication, data integrity, defense against intruders, and some security mechanisms. These problems can be solved partially when the communication among the nodes is encrypted but a complete solution requires a strong key exchange and distribution scheme. L Sec provides identity authentication and authorization, simple secure key exchange, defense mechanism against breaches, data privacy, and usage of asymmetrical and symmetrical encryption together. L Sec protocol is simulated on sensor network simulator and emulator (SENSE).There is no application of it.

*6. LISA.* LISA [41] includes security solutions listed below:
(i) Semantic security: the same data is encrypted in different ways by increasing the value of the counter after each data;
(ii) Identity authentication: it ensures that the data is from the right node;
(iii) Protection against replay attacks: it prevents old messages from being repeated;
International Journal of Distributed Sensor Networks

| Security requirements /protocols | TinySec | SPINS | MiniSEC | LSec | LLSP | IEEE 802.15.4 | LISP |
|---|---|---|---|---|---|---|---|
| Data confidentiality | + | + | + | + | + | + | + |
| Data integrity | + | + | - | - | + | + | + |
| Data authentication | + | + | + | + | + | + | + |
| Data freshness | - | + | + | - | + | + | - |
| Data availability | - | - | - | - | - | - | + |
| Implementation | TinyOS (Mica2) | - | TinyOS (Telos B) | - | - | TinyOS (Mica Z, Telos B) | - |

Table 3: Security requirements/protocols.

*7.MiniSec.* MiniSec [42] is implementedonTelos platform. While TinySec provides low security at low power consumption, ZigBee [43] provides high security at high power consumption. According to the authors, MiniSec provides high security at low power consumption. Three techniques are used to achieve this. First, block encryption method is used to provide privacy and authentication. But there is only one pass over the data. Second, initialization vector (or IV) used as a very few bits. Third, basic gaps are used during unicast and broadcast communication. In the unicast mode, the power consumption of radio is reduced bymaking extra computations and using synchronized counters. In the broadcast mode, bloom filter mechanism is used. SkipJack is used as the encryption algorithm and OCB as the encryption mode. It is defenseless against DoS attacks.

*8. LLSP.* LLSP [44] provides minimum cost identity authentication, data integrity, and semantic security by using only symmetric security algorithms. The key mechanism determines key management issues in WSNs. It includes the questions of how the cryptograph keys are distributed, shared, and updated. An appropriate keying mechanism depends on the factors such as the target hazard model, the network communication in practice, security requirements, and ease of use. Keying mechanism is not discussed in the paper.

## III. Conclusions

Networks are shifted from wired to wireless quickly but wireless networks are costly but in wireless networks; WSNs is growing day by day and hot field in the area of research. WSNs are cost effective because it saves the energy by using low power tiny sensor nodes that makes it popular, with the addition of different other features. WSNs have a variety of features and types that can accommodate many problems arising in different scenarios. The only need is the selection of the right approach on the right place, for getting the maximum benefit from the WSN and its types. We have a plan to find out an algorithm or mechanism that improves the performance and security issues, of the WSN. This paper enhances the base for this emerging field and after it we will pick a particular problem in WSN and work for an efficient approach.

## REFERENCES

[1] [1] Sharma, K. and Ghose, M. (2010) Wireless Sensor Networks: An Overview on Its Security Threats. IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs, 42-45.

[2] [2] Li, J.Z. and Hong, G. (2008) Survey on Sensor Network Research. Journal of Computer Research and Development, 45, 1-15.

[3] [3] Ren, F.Y., Lin, G. and Huang, H.N. (2003) Wireless Sensor Networks. Journal of Software, 7.

[4] [4] Dhillon, S.S. and Chakrabarty, K. (2003) Sensor Placement for Effective Coverage and Surveillance in Distributed Sensor Networks. IEEE, 3, 1609-1614.

[5] [5] Rezazadeh, J. (2012) Mobile Wireless Sensor Networks Overview. International Journal of Computer Communications and Networks (IJCCN), 2, 17-22.

[6] [6] Ren, Y. and Boukerche, A. (2008) Modeling and Managing the Trust for Wireless and Mobile Ad Hoc Networks. IEEE International Conference on Communications, 2008. ICC'08, Beijing, 19-23 May 2008, 2129-2133. http://dx.doi.org/10.1109/icc.2008.408

[7] [7] Cho, J.-H., Swami, A. and Chen, R. (2011) A Survey on Trust Management for Mobile Ad Hoc Networks. IEEE Communications

[8] Surveys & Tutorials, 13, 562-583. http://dx.doi.org/10.1109/SURV.2011.092110.00088

[9] [8] Djenouri, D., Khelladi, L. and Badache, N. (2005) A Survey of Security Issues in Mobile Ad Hoc Networks. IEEE Communications Surveys, 7, 2-28.

[10] [9] Duan, J., Qin, Y., Zhang, S., Zheng, T. and Zhang, H. (2011) Issues of Trust Management for Mobile Wireless Sensor Networks. 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Wuhan, 23-25 September 2011, 1-4.

[11] [10] Deng, X.M., Xiong, Y. and Chen, D.P. (2010) Mobility-Assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks. IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Niagara Falls, 11-13 October 2010, 225-232. [11] Duan, Z.-F., Guo, F., Deng, M.-X. and Yu, M. (2009) Shortest Path Routing Protocol for Multi-Layer Mobile Wireless Sensor Networks. International Conference on Networks Security, Wireless Communications and Trusted Computing, NSWCTC’09, Wuhan, 25-26 April 2009, 106-110. http://dx.doi.org/10.1109/NSWCTC.2009.282

[12] [12] Anguita, D., Brizzolara, D. and Parodi, G. (2009) Building an Underwater Wireless Sensor Network Based on Optical: M. U. Aftab et al. 179 Communication: Research Challenges and Current Results. 3rd International Conference on Sensor Technologies and Applications, SENSORCOMM’09, Athens, 18-23 June 2009, 476-479.

[13] http://dx.doi.org/10.1109/SENSORCOMM.2009.79 [13] Davis, A. and Chang, H. (2012) Underwater Wireless Sensor Networks. Oceans, 2012, Hampton Roads, 14-19 October 2012, 1-5. http://dx.doi.org/10.1109/oceans.2012.6405141

[14] [14] Akbulut, A., Patlar, F., Zaim, A. and Yilmaz, G. (2011) Wireless Sensor Networks for Space and Solar-System Missions.

[15] 2011 5th International Conference on Recent Advances in Space Technologies (RAST), Istanbul, 9-11 June 2011, 616-618. http://dx.doi.org/10.1109/RAST.2011.5966912

[16] [15] Vladimirova, T., Bridges, C.P., Paul, J.R., Malik, S.A. and Sweeting, M.N. (2010) Space-Based Wireless Sensor Networks:

[17] Design Issues. IEEE Aerospace Conference, Big Sky, 6-13 March 2010, 1-14.

[18] [16] Sun, Z. and Akyildiz, I.F. (2010) Connectivity in Wireless Underground Sensor Networks. 2010 7th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks (SECON), Boston, 21-25 June 2010, 1-9. http://dx.doi.org/10.1109/secon.2010.5508264

[19] [17] Poojary, S. and Pai, M.M. (2010) Multipath Data Transfer in Wireless Multimedia Sensor Network. 2010 International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), Fukuoka, 4-6 November 2010, 379-383. http://dx.doi.org/10.1109/BWCCA.2010.100

[20] [18] Nayyar, A., Bashir, F. and Hamid, Z. (2011) Intelligent Routing Protocol for Multimedia Sensor Networks. 2011 International

[21] Conference on Information Technology and Multimedia (ICIM), Kuala Lumpur, 14-16 November 2011, 1- 6. http://dx.doi.org/10.1109/icimu.2011.6122747

[22] [19] Phan, K.T., Fan, R., Jiang, H., Vorobyov, S.A. and Tellambura, C. (2009) Network Lifetime Maximization with Node Admission in Wireless Multimedia Sensor Networks. IEEE Transactions on Vehicular Technology, 58, 3640-3646. http://dx.doi.org/10.1109/TVT.2009.2013235

[23] [20] Shafiee, M. and Vakili, V. (2012) MTM-Based Spectrum Sensing in Cognitive Wireless Multimedia Sensor Networks

[24] (C-WMSNs). 2012 6th International Symposium on Telecommunications (IST), Tehran, 6-8 November 2012, 266-270.

[25] http://dx.doi.org/10.1109/ISTEL.2012.6482995

[26] [21] Lin, K., Rodrigues, J.J., Ge, H.W., Xiong, N.X. and Liang, X.D. (2011) Energy Efficiency QoS Assurance Routing in

[27] Wireless Multimedia Sensor Networks. IEEE Systems Journal, 5, 495-505. http://dx.doi.org/10.1109/JSYST.2011.2165599

[28] [22] Akyildiz, I.F., Su, W.L., Sankarasubramaniam, Y. and Cayirci, E. (2002) A Survey on Sensor Networks. IEEE Communications

[29] Magazine, 40, 102-114. http://dx.doi.org/10.1109/MCOM.2002.1024422

[30] [23] Nadeem, F., Leitgeb, E., Awan, M. and Chessa, S. (2009) Comparing the Life Time of Terrestrial Wireless Sensor

[31] Networks by Employing Hybrid FSO/RF and Only RF Access Networks. 5th International Conference on Wireless and Mobile Communications, ICWMC’09, Cannes, 23-29 August 2009, 134-139.

[32] http://dx.doi.org/10.1109/ICWMC.2009.29

[33] [24] Pfleeger, C.P. and Pfleeger, S.L. (2003) Security in Computing. Prentice Hall Professional, Upper Saddle River. [25] Zia, T. and Zomaya, A. (2006) Security Issues in Wireless Sensor Networks. International Conference on Systems and Networks Communications, ICSNC’06, Tahiti, 29 October-3 November 2006, 40-40.

[34] http://dx.doi.org/10.1109/ICSNC.2006.66

[35] [26] Singh, S. and Verma, H.K. (2011) Security for Wireless Sensor Network. International Journal on Computer Science & Engineering, 3, 2393-2399.

[36] [27] Aftab, M.U., Nisar, A., Asif, M., Ashraf, A. and Gill, B. (2013) RBAC Architectural Design Issues in Institutions Collaborative

[37] Environment. International Journal of Computer Science Issues (IJCSI), 10, 216-221.