IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Security in Wireless Sensor Networks: Attacks and Solutions

Swati Bartariya[1], Ashutosh Rastogi[2]

M. Tech Scholar, Department of Electronics and Communication, Babu Banarasi Das University, Lucknow, India[1]

Assistant Professor, Department of Electronics and Communication, Babu Banarasi Das University, Lucknow,India[2]

Abstract: To many thought provoking problems, Wireless Sensor Networks have become a feasible solution. However, the deployment of new technology without security has often proved to be immoderately dangerous. WSN have recently attracted a lot of interest to the researchers due to wide range of applications. In this paper, we identify the security threats and attacks in WSN. Security solutions are also discussed and we also provide a brief discussion on the future research direction in WSN security.

Keywords: Wireless Sensor Network, Security, Sybil, Wormhole, Sinkhole.

I. INTRODUCTION

Since WSNs provide potentially low cost solutions to a variety of real world challenges they are quickly gaining popularity [1]. WSNs are emerging as a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management and security [2], [3], [4].

Sensors are tiny devices that have capability of sensing parameters and communicating with other devices, over a specific geographic area for specific purposes like target tracking, environmental monitoring etc.

Some of the applications of WSN are:

- Area monitoring application-In this a WSN is deployed in a region where a particular activity is to be monitored.
- Environmental application: For detection of pollution, floods, forest fire etc.
- Health applications: For drug administration, patient monitoring, telemonitoring of human physiological data etc.
- Other applications: Home automation, monitoring of car theft etc. [5].

Sensors are low powered devices and are capable of observing, measuring and communicating data in the network [6]. Due to the various hardware limitations network nodes are prone to different attacks like eavesdropping, sinkhole attack, wormhole attack, Sybil attack, Hello flood attack Sensors can also monitor humidity, pressure, noise levels, temperature, lightning conditions, the presence and absence of various objects and substances and various other properties[7]. The security properties of sensors must be completely apprehended before their deployment in different infrastructures.

However, while the routing strategies and modelling of wireless sensor networks are getting preference, the security issues are yet to receive extensive focus.

Power and lack of data storage are the two main obstacles to the implementation of traditional computer security techniques in WSN [8].

Challenges in sensor network security-

- Because of wireless communication characteristics of WSN traditional wired based security schemes may become impractical.
- Link attacks ranging from passive eavesdropping to active interfering.
- Trade-off between resource consumption minimization and security maximization.

Some of the limitations of sensor network are described below-

- Node limitations: A typical sensor node processor is of 4-8 MHz, 128 KB flash, 4KB RAM and 916 MHz of radio frequency.
- Network limitations: Lack of physical infrastructure and dependence on wireless media.
- Physical limitations: Their deployment in public and hostile environment make them vulnerable to vandalism (malicious mischief).

Physical security increases the node cost [9].

The rest of the paper is organised as follows: Section 2 describes the architecture of a sensor node. Section 3 includes types of sensor network. Section 4 describes issues of wireless sensor network. Section 5 gives an overview of security constraints. Section 6 describes security threats and attacks in WSN. Section 7 describes security solution. Section 8 describes the future research area and in Section 9 we conclude the paper.

II. ARCHITECTURE OF A SENSOR NODE

A sensor node comprises of five main parts as shown in Figure 1:

- Sensor
- Battery
- Control Unit
- Memory
- Communication module

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

The task of sensors is to gather information from the environment.

Battery supplies energy to all parts and the transceiver communicates with the environment.

The function of control unit which is in the form of microprocessor is to manage the tasks.

The purpose of memory is to store temporary data or data which is created during processing [10].

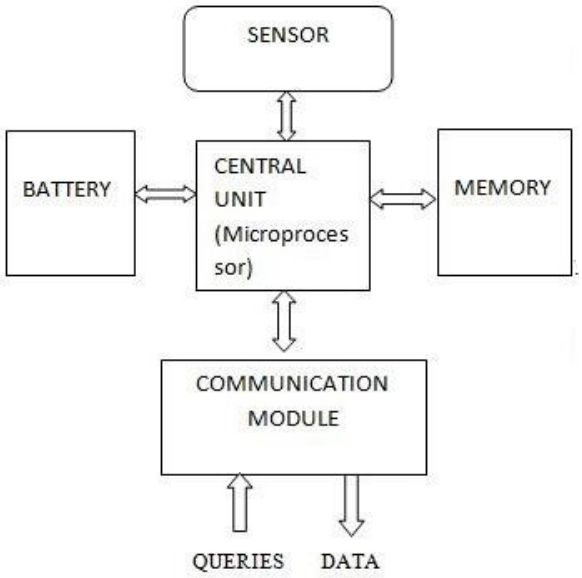


Figure 1: Architecture of a sensor node

III. TYPES OF SENSOR NETWORK

There are five type of wireless sensor networks:

A. Terrestrial WSNs

It consists of hundreds to thousands of wireless sensor nodes deployed in a particular area and the deployment can be in an adhoc or planned manner [11].

In adhoc manner the nodes are dropped from plane and are deployed randomly in the target area [12].

On the other hand in pre-planned deployment there are grid placement, optical placement, 2-d and 3-d placement models.

These networks are different from generic wireless adhoc networks, in that the traffic is not created by the nodes, but by the environment in which they exist [13].

B. Underground WSNs

It consists of a large number of sensor nodes buried underground to monitor underground conditions.

In this some additional sink nodes are placed above ground to relay information from sensor nodes to base station.

The idea of underground utilization of WSN prove to be benefited from rapid deployment [14].

C. Underwater WSNs

Sound has better distinctiveness, making it the appropriate technology for underwater communication [15]. Underwater wireless communication are established through transmission of acoustic waves.

D. Multimedia WSNs

Wireless Multimedia Sensor Networks is a network of devices that are connected wirelessly and allow retrieving audio and video streams, scalar data and still images [16].

E. Mobile WSNs

In mobile WSNs sensor nodes can move on their own and have capability to sense and communicate like static nodes. In mobile WSN the nodes have ability to organize themselves in the network. A node can communicate information to the other nodes when they are within range of each other.

IV. ISSUES OF WIRELESS SENSOR NETWORK

The issues of wireless sensor network can be categorized as:

- Design issues
- Architectural issues

Design Issues-

A. Energy Consumption

Batteries are used as energy source for WSNs. Because of deployment of sensor network in hazardous environment it becomes difficult to replace and recharge batteries.

During communication large amount of energy is consumed therefore efficient routing must be used at each layer [17].

B. Reliability

In a WSN a node may fail due to various reasons but the failure of node should not affect the performance of WSN [18]. Reliability of WSN is the ability to maintain the functionality of the network due to node failure.

By Poisson distribution the reliability is modelled to capture the probability of not having node failure during time interval (0, t) [19].

$$Rk(t) = e^{-\lambda kt}$$

Where,
λk = failure rate of sensor node k.
t= time period.

C. Scalability

Based on the application or requirement of WSN the number of nodes can be increased or decreased. In WSN the reliability and scalability are inversely coupled [20].

D. Localization

Localization is defined as the problem of determining the position of nodes. It can be solved by:

- GPS
- Beacon nodes
- Proximity based localization

E. Topology Control

Various factors are affected by topology of a network like latency, capacity and robustness [19].

There are 3 phases of topology control:

DOI 10.17148/IJARCCE.2016.5352

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

- Predeployment and development phase- Sensors can be deployed by-
  - Dropping from a plane
  - Throwing by a catapult
  - .Placing in factory
  - Delivering in rocket
  - Placing one by one human or robot
- Post deployment phase- There may be a change in topology due to position, malfunction or available energy.
- Redeployment of additional node phase- Additional nodes can be redeployed due to malfunctioning or task dynamics [18].

F. Hardware Constraints

The hardware constraints are –

- Nodes should be power efficient because their power resource determines network lifetime.
- Radio range should be around 2-5 km.
- Memory chips (flash memory) is required as they are non-volatile [21].

G. Data Gathering

The task of collecting data from different sensors by removing redundant data is called data gathering.

The information must be delivered to sink node without any loss or delay.

H. Query Processing

It is the task of answering query from sink by the information that is gathered from other node. The storage node gathers the data from other nodes and replies the query from sink and hence it is a 2-tier architecture in which storage node act as an intermediate node [18].

I. Production cost

The cost of each sensor node has to low as large number of sensors are deployed in a network [17].

J. Coverage , Clock and Computation-

- Coverage: To ensure good coverage sensor nodes must be selected in such a way that the entire network is covered [17].
- Clock: Time synchronization is required to provide a common time scale for clocks of nodes in network [17].
- Computation: Computation is defined as the amount of data proceeds by each node.

The major issue of computation is that it should minimize the use of resources.

K. Scheduling

It determines that at which time period a sensor will be in which mode: sleep, active or standby mode [18].

L. Security

A sensor network must achieve all security goals:

- Availability
- Authentication
- Freshness
- Authorization
- Integrity
- Non-repudiation[18]

Architectural Issues-

A. Network layer issues

Various issues are:

- A very important criterion is energy efficiency as it affects the network lifetime
- Multipath design techniques should be incorporated. Multipath is referred to protocols that set multiple paths so that a path among them can be utilized when the primary path fails.
- Fault tolerance is also desirable.
- Heterogeneity should be there that is each node is different in terms of power, computation and communication.

Various routing protocols are:

Sensor Protocol for Information via Negotiation (SPIN), Low Energy Adaptive Clustering Hierarchy, Threshold Sensitive Energy Efficiency Sensor Network Protocol (TEEN), Geographic and Energy Aware Routing (GEAR) and others [22].

B. Transport layer issues

The transport layer maintains the data flow if the application requires it [23]. The issues are:

- Orderly transmission of fragmented packets should be ensured.
- Protocol should be reliable to deliver data to large group of sensors.
- When data flow from source to sink, the loss of data is tolerable but when data flows from sinks to source it is very sensitive to data loss.

Pump Slowly Fetch Quickly (PSFQ) is one of transport layer protocols [22]

C. Physical layer issues

It accomplishes different tasks like:

- Signal detection
- Modulation
- Data encryption
- Carrier frequency generation
- Frequency selection[24]

D. Application layer issues

It provides software for the translation of data in an understandable form and also send queries to obtain information. It is also responsible for traffic management[24]

E. Data link layer issues

It is responsible for:

- Data frame selection
- Multiplexing data
- MAC
- Error control
- Reliability

Errors and unreliability are result of:

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

➢ Co-channel interference at MAC layer and this problem is mitigated by MAC protocol.
➢ Multipath fading at physical layer.

MAC layer-

- It avoids collision. When more than one packets is received by the receiver at the same time it is called as collided packets and it leads to higher energy consumption.
- It avoids over emitting. It is a condition when a destination node is not ready to receive a message
- It also avoids overhearing which is a condition when a node picks up packet which is not destined to them.

Popular MAC protocols are:
S-MAC, B-MAC, Z-MAC, Time MAC, Wise MAC

V. OVERVIEW OF SECURITY CONSTRAINTS IN WSN

In order to acquire useful security mechanisms it is mandatory to understand the following constraints first-

A. Memory and power limitations

Since a sensor is a tiny device which possesses a small storage space for the code, it is necessary to limit the size of the code of the security algorithm. Sensor Energy is also a major concern to WSNs and it is not very easy to replace the nodes because of high operating cost.

B. Unreliable communication

Network security depends on the defined protocol which in turn depends on communication.

C. Security requirements

The security requirements [25, 26] of a WSN are-

1) *Data Confidentiality:* Information should only be revealed to authorized entities; any other entity should not be able to discover the information from eavesdropping or from reading memories.
2) *Data Integrity:* The receiver of information wants to be sure that it is not modified in transit, either intentionally or by accident.
3) *Availability:* Legitimate entities should be able to access certain information and to enjoy proper operation.
4) *Authentication:* Data authenticity means assurance of the identities of communicating nodes. Authentication is necessary for the exchange of information in the network.
5) *Data Freshness:* Data should be recent and it must be ensured that no old messages have been replayed. The outdated information can cause problems to the applications deployed in WSN.

VI. SECURITY THREATS AND ATTACKS

A. Security Threats

According to capability of attackers, threats can be classified as-

➢ External vs Internal Attacks-

External Attacks- External attack does not belong to the network and does not possess any internal information about the network such as cryptographic information. Common features of this attack are:

- External to the network
- Committed by illegitimate parties.
- Commence attack without being authenticated [27].

Internal Attacks- When a legitimate node acts in an illicit way, we consider it as an internal attack. Goals of an internal attacker are:

- To provide threat to efficiency of network.
- To reveal secret keys.
- Entrance to WSN nodes [27].

➢ Passive vs Active Attacks-

Passive Attacks- Passive attack does not have any direct influence on the network as it is outside the network. Passive attacks are in the form of eavesdropping or monitoring of packets exchanged within WSN. Eavesdropping is a kind of passive attack in which an eavesdropper monitors the communication channel between two nodes and collects information without affecting the communication [28]. Goals of passive attacker are:

- Eavesdropping
- Gathering
- Stealing information
- Functionality degradation
- Network partitioning [29].

Active Attacks- Attacker can hinder the normal functionality of the network. It can also modify the original data and can change the information. Active attacker performs operation like:

- Packet modification
- Impersonation
- Overloading
- Injecting faulty data [29].

B. Security Attacks

These can be classified as-

- Interruption- It is an attack on availability of the network. Its main purpose is to launch DoS attacks.
- Interception- It is an attack on confidentiality of the network. In this an adversary can gain unauthorised access to sensor node.
- Modification- It is an attack on integrity of the network. In this the authorised entity not only access data but also fiddles it.
- Fabrication- It is an attack on authentication. In this the adversary injects false data and ruins the authenticity of the information.

C. Layering Based Attacks

The attacks on physical layer can be classified as-

- Jamming-It is a popular DoS attack. In this, the attacker jams the frequency used for communication. An attacker needs only a few nodes to disseminate a large network. It disturbs the radio channel by sending useless information and jamming can be temporary, intermittent or permanent [30].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

- Tampering- Here, the adversary can extract cryptographic keys from the node captured, alter its circuitry, modify the codes or even replace it. In order to acquire information a tampering attacker may damage or replace the node. A defence to the attack is tamper proofing the physical package of node [31].

The attacks on link layer can be classified as-

- Collision- It is a DoS attack. In this the node induces a collision and due to this the packet will fail the checksum check and hence the receiver node will ask for retransmission of the packet.
- Exhaustion- In this the malicious node repeatedly conducts collision attacks and as a result the power supply of the communicating nodes gets exhausted.
- Denial of Service- DoS [32, 33] is caused by unintentional failure of node. Since, sensor nodes are very energy sensitive they are vulnerable to DoS attack.

The network layer attacks are discussed as follows-

- Sybil Attack: To accomplish a certain task nodes in a wireless sensor network need to work together. Hence, they distribute subtasks. In such a condition, a node can pretend to be more than one node using the identities of other nodes. Hence, Sybil Attack is a attack where a node forges the identity of more than one node as shown in Figure 2 [34, 35].

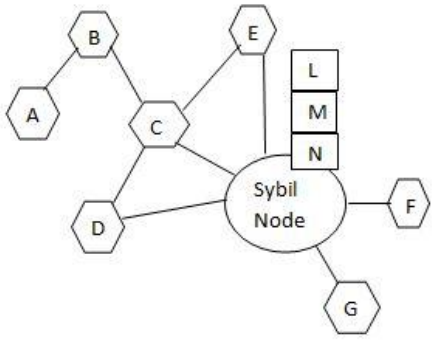


Figure 2: Sybil Attack

- Black hole/Sinkhole Attack- Here, a malicious node acts as a black hole [36] and attracts all the traffic as shown in Figure 3.

The attacker listens to request for routes and then replies that it contains the shortest path to the base station. Once the malicious device inserts itself between the sink and the sensor node it can do anything with the packets passing between them.

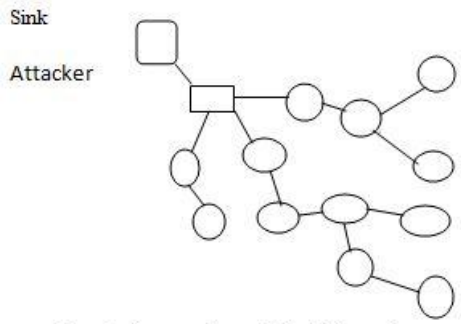


Figure 3: Conceptual view of Black hole attack.

- Wormhole attack- In wormhole attack [37], the attacker records the packet at one location and tunnels it to another location.

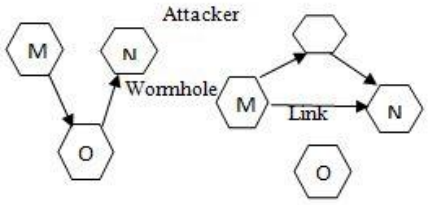


Figure 4: Wormhole Attack

When a node M broadcasts the packet the attacker node receives it and replays it in its neighbourhood as shown in Figure 4. As a result, each neighbour node considers itself to be in the range of node M. Hence, even if the victim node is multi-hop apart from M, the attacker convinces them that it is a single-hop away from them.

The transport layer attacks are –

- Flooding- In this the attacker repeatedly makes new connection requests until the resource required by each connection are completely exhausted or reach the maximum limit.
- De-synchronization- It refers to interruption in an existing connection [38].

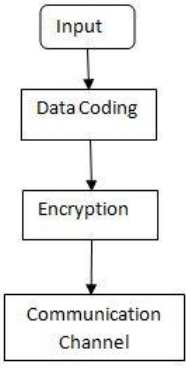
Some other attacks are energy drain attack, homing and node replication attacks.

VII. SECURITY SOLUTIONS FOR WSN

A. *Cryptography*

In order to achieve security in WSNs, performing cryptographic operations including encryption, authentication and so on is very important. Due to severe constraints in processing power and supply of energy it becomes difficult to apply data security in some applications because the process of data encryption and decryption consumes a lot of time and power.

Here, two techniques of data encryption are discussed: Figure 5(a) i.e. traditional encryption and Figure 5(b) i.e. selective key encryption. In traditional encryption, whole information is encrypted which is not important in case of image snapshot. In selective key encryption the encryption is performed on only a portion of compressed data. Selective key encryption encodes a set of blocks of sensed images [40].



(a)

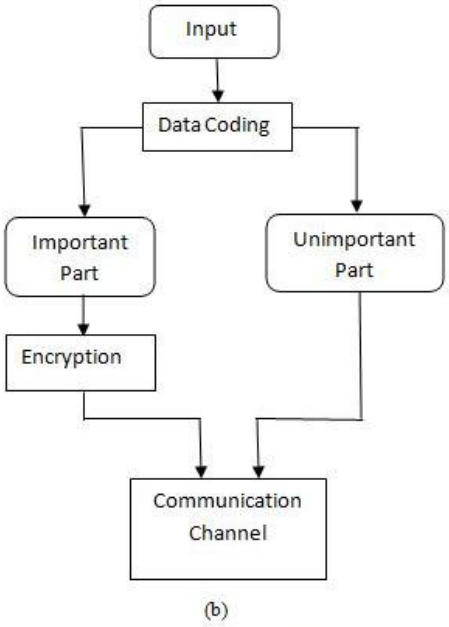


Figure 5: Cryptography Paradigms: (a) traditional encryption (b) selective encryption

Asymmetric cryptography is too expensive for many applications. It is more efficient to use symmetric cryptographic alternative. Sensor Protocol for Information via Negotiation (SPIN) was proposed. Two secure building blocks of SPIN are Sensor Network Encryption Protocol (SNEP) and µTESLA.

SNEP (Secure Network Encryption Protocol) provides data confidentiality, data authentication and data freshness. It secures channels for confidentiality by making the use of authentication. µTESLA (Micro timed, efficient, and streaming, loss tolerant, authentication protocol) provides authentication broad cast for resource limited environment. It uses asymmetric authenticated broadcast to provide authentication [39].

B. 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.

C. Defence against DoS Attacks

A defence against DoS attack is the use of error correcting codes [15]. Jamming attack can be defended by frequency hopping and code spreading [38].

A possible solution for energy exhaustion attack is the application of rate limiting MAC admission control.

VIII. FUTURE RESEARCH AREA

Although many efforts have been made on key management cryptography and defence against DoS attack, some challenges are still need to be addressed. The current cryptographic mechanisms detect and defend against node compromise but there are still some compromise activities that cannot be detected immediately.

IX. CONCLUSION

We have described the following aspects of security in WSN: Security constraints, attacks and threats and security solution. Our aim is to provide a general idea of the existing WSN security approaches.

Many issues will remain open and we would like to see more research activities on these topics in the future.

REFERENCES

[1] A .Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, June 2004/Vol. 47, No. 6.

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

[3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey",Computer Networks, 38, 2002, pp. 393-422.

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

[5] H. Chawla, "Some issues and challenges of Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering 4(7), July - 2014, pp. 236-239.

[6] D. Cariac, M. Plastoi, O. Banias, C. Volosencu, R. Tandoroin, D. Pescaru, "Software Development for Malicious Nodes Discovery in WSN Security", Proceedings of Fourth International Conference on Sensor Technologies and Applications,2010,pp. 402-407.

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

[8] M. K. Jain, "Wireless sensor networks: security issues & challenges", IJCIT, vol. 2, no. 1, **(2011)**, pp. 62-67.

[9] G. Kulkarni, R. Shelk, K. Gaikwal, V. Solanke, S. Gujar, P. Khatawkar," Wirelesss Sensor Network Security Threats".

[10] G. Sasikumar, H.V. Ramamoorthy, S.N. Mohamed, "An Analysis on Animal Tracking System using Wireless Sensors", International Journal of Advanced Research in Computer Science and Software Engineering 4(9), September - 2014, pp. 155-162.

[11] Rajkumar, Vani B A, K. Jadhav, Vidya S, "Wireless Sensor Networks Issues and Applications", Int.J.Computer Technology & Applications, Vol 3 (5), 1667-1673.

[12] Indu, S. Dixit, "Wireless Sensor Networks: Issues & Challenges" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014, pg. 681-685.

[13] S. Toumpis, L. Tassiulas, "Optical Deployment of Large Wireless Sensor Networks", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 52, NO. 7, JULY 2006.

[14] T.A. Kadi, Z.A. Tuwaijri, A.A. Omran, " Wireless Sensor Networks for Leakage Detection in Underground Pipelines: A Survey Paper", Procedia Computer Science 21 (2013) 491 – 498.

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

[16] I.F. Akyildiz, T. Melodia, K.R. Chowdhury,"A survey on wireless multimedia sensor networks", Computer Networks 51 (2007) 921–960.

[17] K. Kaur, P. Kaur, S. Singh," Wireless Sensor Network: Architecture ,Design Issues and Applications", International Journal of Scientific

Engineering and Research (IJSER), ISSN (Online): 2347-3878Volume 2 Issue 11, November 2014.

[18] G. Singh, H. Arora,"Design and Architectural Issues in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering (1), January - 2013, pp. 28-32.

[19] S. Kalantary, S. Tagjipour," A survey on architectures, protocols, applications and management in wireless sensor networks",Journal of Advanced Computer Science & Technology, 3 (1) (2014) 1-11, Science Publishing Corporation,www.sciencepubco.com/index.php/JACST.

[20] S. Muthukarpagan, V. Niveditta, S. Neduncheliyan, "Design issues, Topology issues, Quality of Service Support for Wireless Sensor Networks: Survey and Research Challenges", 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 6.

[21] K. Gupta, V. Sikka, "Design Issues and Challenges in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 112 – No 4, February 2015.

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

[23] A.A. Alhameed Alkhatib, G.S. Baicher," Wireless Sensor Network Architecture",2012 International Conference on Computer Networks and Communication Systems (CNCS 2012) IPCSIT vol.35(2012) © (2012) IACSIT Press, Singapore.

[24] G. Bianchi, "A comparative study of the various security approaches used in wireless sensor networks," International journal of advanced science and technology, vol. 17, (2010) April, pp. 31-44.

[25] T. A. Zia, "A Security Framework for Wireless Sensor Networks", SAS 2006 – IEEE Sensors Applications Symposium Houston, Texas USA, 7-9 February 2006.

[26] N. Fatima and R. Brad ," ATTACKS AND COUNTERATTACKS ON WIRELESS SENSOR NETWORKS", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.4, No.6, December 2013.

[27] Chun-Ta Li," Security of Wireless Sensor Networks: Current Status and Key Issues".

[28] S. Mohammadi, R.E. Atani, H. Jadidoleslamy," A Comparison of Link Layer Attacks on Wireless Sensor Networks", Journal of Information Security, 2011, 2, 69-84.

[29] M.L. Messai," Classification of Attacks in Wireless Sensor Networks", International Congress on Telecommunication and Application'14 University of A.MIRA Bejaia, Algeria, 23-24 APRIL 2014.

[30] M. Panda ,"Security Threats at Each Layer of Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering 3(11), November - 2013, pp. 61-67.

[31] M. Sharifnejad, M. Shari, M. Ghiasabadi and S. Beheshti, "A Survey on Wireless Sensor Networks Security", SETIT 2007 ,4th International Conference: **S**ciences of **E**lectronic, **T**echnologies of **I**nformation and **T**elecommunications March 25-29, 2007 – TUNISIA.

[32] B. T. Wang and H. Schulzrinne, "An IP Traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, vol. 2, (2004) May 2-5, pp. 901-904.

[33] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).

[34] J. Newsome, E. Shi, D. Song, A. Perrig," The Sybil attack in sensor networks: Analysis & Defences", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[35] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

[36] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defence against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies.IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

[37] A. D. Wood and J. Stankovic, "Denial of service in sensor network", IEEE Computer Magazine, vol. 35, no. 10, (2002) October, pp. 54-62.

[38] 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.

[39] Danilo de Oliveira Gonçalves and D.G. Costa, "A Survey of Image Security in Wireless Sensor Networks", J. Imaging 2015, 1.