# Security Issues in Wireless Sensor Network - A Review

**Jitender Grover[1], Shikha Sharma[2]**

[1]*Department of Computer Science & Engineering,*
*M. M. University, Sadopur, Ambala, India*
*jitendergrover0101@gmail.com*
[2]*Member, IEEE, IEEE Delhi Section*
*shikha.vrgo@gmail.com*

***Abstract:*** **Wireless Sensor Networks (WSNs) are formed by deploying as large number of sensor nodes in an area for the surveillance of generally remote locations. A typical sensor node is made up of different components to perform the task of sensing, processing and transmitting data. WSNs are used for many applications in diverse forms from indoor deployment to outdoor deployment. The basic requirement of every application is to use the secured network. Providing security to the sensor network is a very challenging issue along with saving its energy. Many security threats may affect the functioning of these networks. WSNs must be secured to keep an attacker from hindering the delivery of sensor information and from forging sensor information as these networks are build for remote surveillance and unauthorized changes in the sensed data may lead to wrong information to the decision makers. This paper studies the various security issues and security threats in WSNs. Also, gives brief description of some of the protocols used to achieve security in the network. This paper also compares the proposed methodologies analytically and demonstrates the findings in a table. These findings can be used further by other researchers or Network implementers for making the WSN secure by choosing the best security mechanism.**

***Keywords: WSN, Security, Threats, Security Protocols.***

## I. INTRODUCTION

Wireless Sensor Networks (WSNs) are the collectors of information from the physical world in the form of sensed data according to the requirement like temperature, pressure, humidity, level, movement etc [1][2]. This data is available to the sink through gateway. Sensors are deployed in extensive numbers and on account of its wireless nature; it is easily works in any type of environment. Although sensor nodes are deployed in a random manner still it's important to deploy them carefully. [3] Deploying few nodes may raise the issue of coverage and deploying too many nodes may result in an inefficient network because of more collision and interference.

WSN is used in many applications from indoor to outdoor [4]. While transmitting information in the network it is important to provide security. [6] Security is considered to be the most challenging task in WSN as its tough to keep a watch on the sensor nodes/network every time. But it must be secured to prevent an intruder from attacking the transmission of data.

There are lots of constraints with a sensor node specially its size and cost that should be minimum. [5][7] These constraints results in very small size memory, limited energy source and transmission range. [10][12] This ultimately results in no encryption, decryption and authentication that can be actualized on sensor node. Attack and attacker are the most common terms used in the security. Attacker is the one who is an unauthorized to access the data of the network or tries to mislead the information. When an attacker accesses the services of the network is known as attack.

WSN is designed in the form of layers [8][9]. These layers help to protect the sensor from various attacks. Figure 1 shows the layer model of security in wireless sensor networks.

| | |
|---|---|
| SECURITY | APPLICATION |
| | TRANSPORT |
| | NETWORK |
| | LINK |
| | PHYSICAL |

**Fig. 1. Layered Security Model**

[15] Security in the Wireless Sensor Networks has various difficulties, some common are: dynamically changing topology, wireless communication among the sensor nodes, infrastructure-less framework, and limited physical resources like energy source, memory capacity and very low communication bandwidth [11][13]. Numerous analysts proposed so many threats handling models and diverse security protocols for secure data communication and routing in WSN.

## II. SECURITY REQUIREMENTS

Sensor network have to fulfill some requirements for providing a secure communication. General security requirements of [16][17] WSNs are availability, confidentiality, integrity and authentication. [14][18][21] Some other requirements known as secondary requirements are source localization, self organization and data freshness. These requirements gives protection against attacks to the information transmitted over the sensor network [19].

**Data Confidentiality:** In sensor network, data flows from many intermediate nodes and chance of data leak is more [20]. To provide the data confidentiality, an encrypted data is used so that only recipient decrypts the data to its original form.

**Data Integrity:** Data received by the receiver should not be altered or modified is Data Integrity. Original data is changed by intruder or due to harsh environment. The intruder may change the [46][47] data according to its need and sends this new data to the receiver.

**Data Authentication:** It the procedure of confirmation that the communicating node is the one that it claims to be. It is important for receiver node to do verification that the data is received from an authenticate node.

**Data Availability:** Data Availability means that the services are available all the time even in case of some attacks such as Denial of service.

**Source Localization:** For data transmission some applications use location information of the sink node. It is important to give security to the location information. Non-secured data can be controlled by the malicious node by sending false signal strengths or replaying signals.

**Self-Organization:** [19] In WSN no fixed infrastructure exists, hence, every node is independent having properties of adaptation to the different situations and maintains self organizing and self healing properties. This is a great challenge for security in WSN.

**Data Freshness:** Data freshness means that each message transmitted over the channel is new and fresh. It guarantees that the old messages cannot be replayed by any node. This can be solved by adding some time related counter to check the freshness of the data.

## III. CLASSIFICATION OF SECURITY THREATS

WSNs are vulnerable against so many attacks. Attackers can attack the radio transmission; add their own data bits to the channel, replay old packets and any other type of attack. A secure network ought to support all security properties. [22][23] Attackers may deploy some malicious nodes in the network with similar capabilities as of normal node or may overwrite the memory of normal deployed node by capturing them. Attacks in wireless sensor network are shown in Figure 2. They are roughly categorized as follows:

A) Based on Routing

B) Based on Capability

C) Based on Protocol Layer

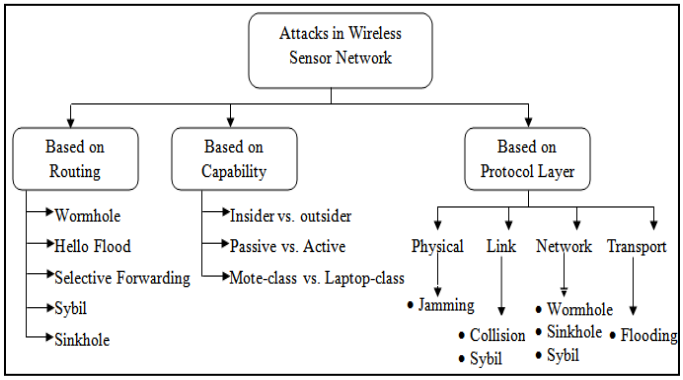


**Fig. 2. Attacks Classification in WSN**

### A) On the Basis of Routing

There are lots of routing protocols proposed for transmitting the data in the network from source to sink. In this transmission process, an attacker can steal or modify the information with the help of different attacks. [24][25] Some of the routing attacks are explained below:

#### a) Wormhole Attacks

In this attack there are two or more malicious nodes present in the network at different locations. When sender node sends information then one malicious node tunnels the information to another malicious node. The receiving malicious node then sends information to its neighbor nodes. In this way, attacker convince the sender and receiver nodes that they are situated at a distance of one or two hops but actual distance between these two are multiple hops and usually both are out of range. Mostly wormhole attack and selective forwarding both are used in combination. If it is used in combination with Sybil attack then detection of attack is difficult [26].

Figure 3 shows that the node X and node Y are nodes which are maintaining the wormhole link in the network and they are the two malicious nodes. There is a shortcut link between both malicious nodes known as wormhole link. Node A sends message which is received by node X. Node X sends message to Node Y through wormhole link which further sends it to its neighbor node B.

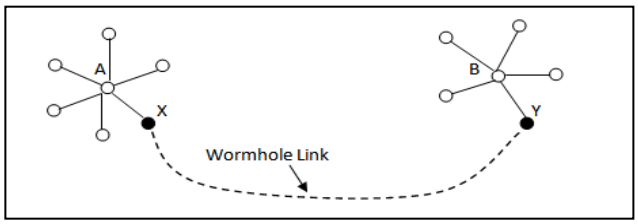


**Fig. 3. Wormhole Attack**

#### b) HELLO Flood Attacks

In a sensor network to discover the neighbors HELLO message is broadcasted by the nodes. The receiver node considers that

the source node is in the range of data tranmission and sends its sensed data to the broadcaster. In a HELLO Flood Attack, HELLO message is broadcast with high transmission power by the attacker. [27][29] The nodes which receive this HELLO message send the data packets to the attacker node. Attacker may change or modify the data packet or may drop the packet. In this way, a lot of energy is wasted and also network congestion occurs. This attack is one of the least difficult attacks in WSN. As demonstrated in Figure 4 attacker node broadcasts the HELLO packet with high transmission power than the sink. Figure 5 shows that the nodes which receive HELLO packet from attacker node consider it as a neighbor node and send/reply the sensed data packet to the attacker node.

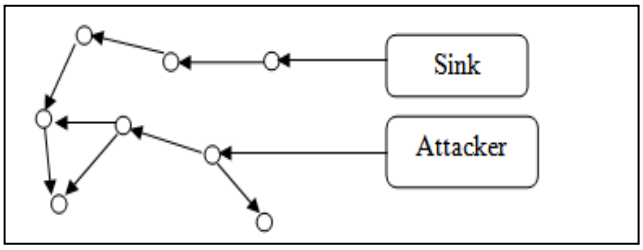


**Fig. 4. HELLO Flood Attack scenario-Hello Packet send by the Attacker**

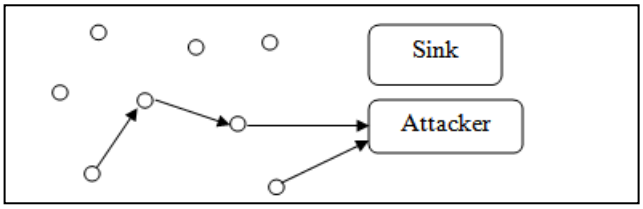


**Fig. 5. HELLO Flood Attack scenario-Sensor node replying back to the attacker considering it as its neighbor node**

### *c) Selective Forwarding Attack*

In this attack, a malicious node in the network interrupts the communication process. There may be the case of multiple malicious nodes in the network that depends upon the attacker. [28] This node selectively forwards some of the received packets. This malicious node can also be referred as a black hole as it may drop all the received packets. In such case, neighboring nodes assumes that this has failed and starts searching for another route. This attack is easy to detect if it acts as a black hole and drop all the received packets but is complicated if it forwards packet selectively. On the off chance that an attacker included externally to the path then selective forwarding attacks are more viable. On the premise of packets drops, it is divided into two categories:

- Drops packets of some specified nodes
- Drops packets of some specified types

Figure 6 shows a malicious node present between the nodes in network. In this neighboring node unknowingly forwards packets to the malicious node.

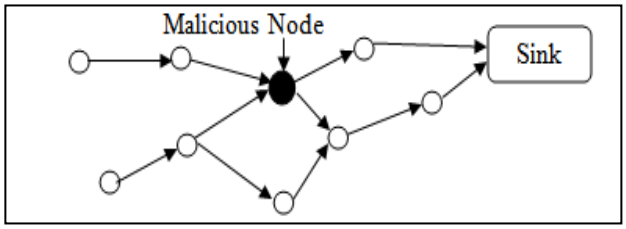


**Fig. 6. A malicious node in the network**

### d) Sybil Attack

In Sybil Attack, a single attacker makes and presents different identities to the other nodes in the sensor network. It can also be considered that "It can be in more than one place at once" [33]. Malicious nodes are known as Sybil nodes. This attack is used against redundancy mechanism of distributed systems. In WSNs, Sybil attack is generally used to attack several types of protocols [30]. This is a serious threat to a location based protocols in which location information is exchanged for efficient routing. Figure 7 shows a Sybil attack in a network.

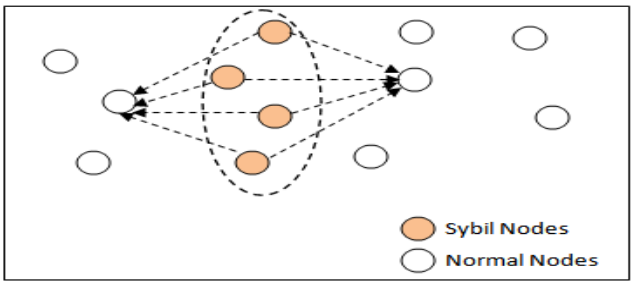


**Fig. 7. Malicious node with multiple identities**

### e) Sinkhole Attack

In sinkhole attack, a malicious node advertises fake routing information to attract the network traffic [31]. WSNs are vulnerable to this type of attack because communication happens in many to one form i.e. many sensor nodes to a single BS. Wormhole attack can also be used in combination with this attack. In Figure 8, malicious node has more power than other nodes in the network and connects with the sink node using single hop. It claims and displays to have the shortest possible path to the sink so that more network traffic is attracted towards it. Most of the routing algorithms select the shortest path for data transfer.

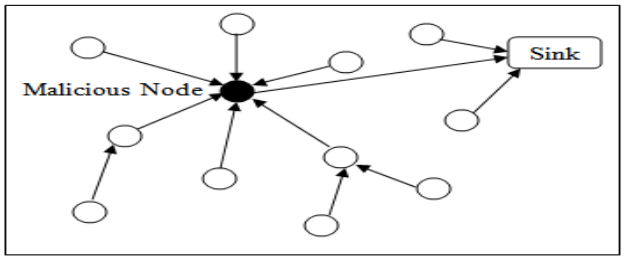


**Fig. 8. Sinkhole Attack**

### B. Based on Capability

The level of data access and its damage is different depending upon the type of attack. [32][34] On the basis of capability, attacks are classified as follows:

#### a) Insider vs. Outsider Attacks

**Outcast attacks** are the type of attacks in which attacker finds no extraordinary access of the deployed sensor network yet wants to harm the network. These are also known as external attacks [36]. The attacker nodes which participate and execute this type of attack are not the part of network but still authorize themselves to harm the network. In **insider attack**, a node situated in the network is malicious. This surmises attacks from inside are generated by the network nodes rather than from outside nodes, and they are truly a part of the sensor system. These type of attacks are more dangerous than that of outside attacks as the insider knows critical and riddle information, and have all type of access rights.

#### b) Passive vs. Active Attacks

These attacks are divided on the basis of level of damage or level at which attacker can access the network. In passive attacks, no interruption takes place in the actual communication. An attacker can monitor the traffic or access the data without modifying it. Only the sensitive data is collected by the attacker. This exploits the confidentiality and privacy requirement. Interception, traffic monitoring and analysis are the examples of passive attacks. In active attacks, attacker interrupts the actual communication by modifying the data. Attacker can add some faulty data in the actual data stream. It affects the performance of the network. Denial of service, impersonating, modification and message replay are examples of active attack.

#### c) Laptop-class Attacks vs. Mote-class

In a mote-class attacks, an attacker attack the few nodes having the same capabilities as that of the normal network node. The attackers have at least one authorized node in the sensor network to stole the key or code. Hence, it is also known as insider attack. Other type of attack is called laptop-class attack in which the attacker does not have any special access to the network. An attacker has the access to more effective and powerful devices having more battery power, powerful radio transmission, more capable CPU, sensitive antenna etc. These are also known as outsider attacks. For example: laptop or its equivalent. It can do much more harm to a network in comparison to an ordinary malicious sensor node. A standard sensor node may just have the capacity to disturb its nearby network, while a portable workstation like laptop class attacker may have the capacity to stick the whole sensor network utilizing its stronger transmitter.

### C) Based on Protocol Layer

WSN is divided into different layers. The working of each layer is different. The attacks on the basis of protocol layers are explained below [35]:

#### a) Physical Layer

Physical layer is used for transmitting information in raw bits over the wireless or wired medium. It is easy to jam a common radio signal. In general, physical layer attacks are categorized as: Eavesdropping, Tampering and Jamming [37]. In eavesdropping attack, an unauthorized receiver reads the messages. Jamming attack implements under DoS attack. It is the interference with the radio frequency used by the network nodes. This completely changes the working of network.

#### b) Link Layer

Data link layer is utilized to ensure the proper communication on physical layer between nodes. This layer is in charge of multiplexing, error detection, packets collision prevention, repeated transmission of data and so on. Link-layer threats include collisions, interrogation, and packet replay. Error detection and correcting codes can be used to decrease the number of collisions but due to this the routing overhead in the network is increased. Another connection layer danger to WSNs is the denial-of-sleep attack, in which node is unable to go to into the sleep mode. This decreases the whole network lifetime.

#### c) Network Layer

For the data routing between nodes, nodes to sink, node to BS, node to CH, and vice versa [14], this layer is responsible [5]. A direct attack on Routing protocols by the attackers can have impact on network data traffic, indulge themselves into the data path between the source and destination, and by this control the data flow. This infers that effective and powerful routing protocols are required to manage node failure and security attacks. Some routing protocol attacks are: wormhole attacks, acknowledgement spoofing, selective forwarding, black holes and so forth.

#### d) Transport Layer

Transport Layer is utilized to build up a communication link for outer sensor network joined with the internet. This can be considered as the most complex issue in WSNs. [40] Attacks of the transport layer protocol are flooding and de-synchronization. Flooding attack is used to deplete the node's memory by sending numerous requests for connection

establishment. In the de-synchronization attack, the attacker node forges packets to at least one or both ends of a connection using different sequence numbers on the packets. In this way, host requests for retransmission of the missed packet frames.

## IV. SECURITY PROTOCOLS IN SENSOR NETWORKS

Cryptography is a basic technique to achieve the security in a network. This establishes a secure relationship between two end points. In this, sender encrypts the original data and receiver decrypts the received data to obtain an original data. Different types of keys are used in the process of cryptography. The various protocols [38] that are proposed by different authors for solving the security issue in WSN are:

### a) SPINs

SPIN (Sensor Protocols for Information via Negotiation) protocol works in three steps. First, a node advertises the ADV packet containing the metadata. If the received node is interested in the data then it sends the request for data using REQ packet. Finally, [11][9] the advertiser node after receiving request sends the DATA packet to the requestor node. It performs best in small size networks because of its efficiency and high latency properties [39]. Typical SPIN consists of two secure building blocks named as μTESLA (Timed Efficient Stream Loss-tolerant Authentication) and SNEP (Sensor Network Encryption Protocol).

SNEP provides confidentiality, authentication and integrity. It uses the concept of encryption. To authenticate the data, MAC (Message authentication Code) is used. It adds 8 bytes to the message [41]. To reduce the communication overhead, SNEP uses a shared counter between sender node and receiver node. After each block counter gets incremented. Counter helps in identifying the freshness of data.

In TESLA, digital signatures are used to authenticate the data packet. Sink node computes a MAC on the packet after receiving the packet with the secret key to send an authenticated packet back to source. After receiving a packet, node confirms that the sink does not disclose the computed MAC key to other nodes. With this, receiving node assures that data packet is original and no alterations are done in the packet.

### b) LEAP

LEAP (Localized Encryption and Authentication Protocol) is a protocol with key management scheme that is very efficient with its security mechanisms used for large scale distributed sensor networks. It generally supports for inside network processing such as data aggregation. In-network processing results in reduction of the energy consumption in network. To provide the confidentiality and authentication to the data packet, LEAP uses multiple keys mechanism. For each node four keys are used known as individual, pair wise, cluster and group key. [13] All are symmetric keys and use as follows:

- Individual Key: It is the unique key used for the communication between source node and the sink node.
- Pair wise Key: It is shared with another sensor nodes.
- Cluster Key: It is used for locally broadcast messages and shares it between the node and all its surrounding neighboring nodes.
- Group Key: globally shared key used by all the network nodes

These keys can also be used by other non-secured protocols to increase the network security. LEAP is satisfies several security and performance requirements of WSN. LEAP is used to defend against HELLO Floods Attack, Sybil Attack and Wormhole Attack [42].

### c) TINYSEC

TINYSEC is link layer security architecture for WSNs. It is a lightweight protocol. It supports integrity, confidentiality and authentication. To achieve confidentiality, encryption is done by using CBC (Cipher-block chaining) mode with cipher text stealing, and authentication is done using CBC-MAC [43]. No counters are used in TINYSEC. Hence, it doesn't check the data freshness. Authorized senders and receivers share a secret key to compute a MAC. TINYSEC has two different security options. One is for authenticated and encrypted messages (TinySec-AE) and another is for authenticated messages (TinySec-Auth). In TinySec-AE, the data payload is encrypted and the received data packet is authenticated with a MAC. In TinySec-Auth mode, the entire packet is authenticated with a MAC, but on the other hand the data payload is not encrypted.

In CBC, Initialization Vector (IV) is used to achieve semantic security. Some of the messages are same with only little variation. In that case IV adds the variation to the encrypted process. To decrypt the message receiver must use the IV. IVs are not secret and are included in the same packet with the encrypted data.

### d) ZIGBEE

ZIGBEE is a typical wireless communication technology [7]. [45] It is used in various applications such as military security, home automation and environment monitoring. IEEE 802.15.4 is a standard used for ZIGBEE. It supports data confidentiality and integrity. To implement the security mechanism ZIGBEE uses 128 bit keys. A trust center is used in ZIGBEE which authenticates and allows other devices/nodes to join the network and also distribute the keys. Generally, ZIGBEE coordinator performs this function. Three different roles in ZIGBEE are:

- Trust Manager: It authenticates the devices which are requesting to join the network.

- Network Manager: It manages the network keys and helps to maintain and distribute the network keys.
- Configuration Manager: It configures the security mechanism and enables end-to-end security between devices.

It works in two different modes: Residential mode and Commercial mode. In the residential mode less security is needed hence, no keys are used while the commercial mode needs high security and thus, maintains the keys and counter.

Table 1 shows the comparison between the security protocols on the basis of service provided [43][44]. This table shows the type of services offered by the existing protocols.

**TABLE 1: Comparison between Security Protocols**

| Protocols | Confidentiality | Freshness | Integrity | Availability | Authentication | Implicit Authentication | Key Agreement |
|---|---|---|---|---|---|---|---|
| SPIN | Yes | Yes | Yes | No | No | Yes | Symmetric Delayed |
| LEAP | Yes | No | No | No | No | Yes | Pre Delayed |
| TINYSEC | Yes | No | No | --- | Yes | Yes | Any |
| ZIGBEE | Yes | Yes | Yes | No | Yes | Yes | Trust Centre |

## V. CONCLUSION

This paper highlights the security issue of the WSN. Security is the big challenge in the sensor network. Some applications such as military need a secure communications. For a secure communication network must fulfill some security requirements. This paper studies the security threats on the basis of different parameters. To achieve the security requirements various protocols have been proposed. Encryption process is used to make data confidential and MAC is attached to each data packet to provide authenticity.

## REFERENCES


[1] Xiangwu Gong, Hang Long, Feihong Dong, Qing Yao, "Cooperative security communications design with imperfect channel state information in wireless sensor networks", IET Wireless Sensor Systems, Vol. 6, Issue: 2, pp. 35-41, 2016.

[2] Agnihotri, Ram Bhushan, Ajay Vikram Singh, and Shekhar Verma. "Challenges in wireless sensor networks with different performance metrics in routing protocols." In Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on, pp. 1-5. IEEE, 2015.

[3] Jun Wu, Kaoru Ota, Mianxiong Dong, Chunxiao Li, "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities", IEEE Access, Vol. 4, pp. 416-424, 2016.

[4] Goutam Mali, Sudip Misra, "TRAST: Trust-Based Distributed Topology Management for Wireless Multimedia Sensor Networks", IEEE Transactions on Computers, Vol. 65, Issue: 6, pp. 1978-1991, 2015.

[5] Jitender Grover and Anjali, "Wireless Sensor Network in Railway Signalling System", The IEEE International Conference on Communication Systems and Network Technologies (CSNT-2015), Shri Ram Group of Institutes, Gwalior, DOI-10.1109/CSNT.2015.28, pp. 308-313, April 04-06, 2015.

[6] Renu Sharma and Jitender Grover, "Mitigation of Byzantine attack using Enhanced Cooperative Bait Detection and Prevention Scheme (ECBDPS)", 4th IEEE International Conference on Reliability, Infocom Technologies and Optimization (ICRITO-2015), Amity University, Noida, DOI: 10.1109/ICRITO.2015.7359296, pp. 1-6, September 2-4, 2015.

[7] Jitender Grover & Reena Rani, "Probabilistic Density Based Adaptive Clustering Scheme to Improve Network Survivability in WSN", IEEE Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT 2014), Hefei, Anhui, China, DOI: 10.1109/ICCCNT.2014.6963132, pp. 1-7, July 11-13, 2014.

[8] Heejung Byun, Jungmin So, "Node Scheduling Control Inspired by Epidemic Theory for Data Dissemination in Wireless Sensor-Actuator Networks With Delay Constraints", IEEE Transactions on Wireless Communications, Vol.15, Issue: 3, pp. 1794-1807, 2015.

[9] Jitender Grover, Shikha Sharma and Mohit Sharma, "Optimized GAF in Wireless Sensor Network", IEEE 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO 2014), Amity University, Noida, DOI: 10.1109/ICRITO.2014.7014686, pp. 01-06, October 8-10, 2014.

[10] Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song, "Privacy Protection for Wireless Medical Sensor Data", IEEE Transactions on Dependable and Secure Computing, Vol. 13, Issue: 3, pp. 369-380, 2015.

[11] Jitender Grover, Shikha and Mohit Sharma, "Location Based Protocols in Wireless Sensor Network – A Review", IEEE Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT 2014), Hefei, Anhui, China, DOI: 10.1109/ICCCNT.2014.6962990, pp. 1-5, July 11-13, 2014.

[12] Hosein Marzi, Arash Marzi, "A security model for wireless sensor networks", 2014 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), Ottawa, ON, pp. 64-69, 2014.

[13] Jitender Grover, Shikha Sharma and Mohit Sharma, "Reliable SPIN in Wireless Sensor Network", IEEE 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO 2014), Amity University, Noida, DOI: 10.1109/ICRITO.2014.7014694, pp. 01-06, October 8-10, 2014.

[14] Pankaj Pardesi and Jitender Grover, "Improved Multiple Sink Placement Strategy in Wireless Sensor Networks", 2015 IEEE International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (A-BLAZE), Amity University, Greater Noida, Uttar Pradesh, India, DOI: 10.1109/ABLAZE.2015.7155032, pp. 418-424, 25-27 Feb, 2015.

[15] Heena Rathore, Venkataramana Badarla, Sushmita Jha, Anupam Gupta, "Novel approach for security in Wireless Sensor Network using bio-inspirations", 2014 Sixth International Conference on

Communication Systems and Networks (COMSNETS), Bangalore, pp. 1-8, 2014.

[16] Eirini Karapistoli, Anastasios A. Economides, "Wireless sensor network security visualization", 2012 4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 850-856, 2012.

[17] Virendra Pal Singh, Sweta Jain and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", International Journal of Computer Science Issues (IJCSI), Volume 7, Issue 3, No 11, pp. 23-27, May 2010.

[18] Jitender Grover, Shikha Sharma and Mohit Sharma, "Reliable SPIN in Wireless Sensor Network: A Review", IOSR Journal of Computer Engineering (IOSR-JCE), ISSN: 2278-0661, Vol. 16, Issue 6(III), DOI: 10.9790/0661-16637983, pp. 79-83, Nov.-Dec. 2014.

[19] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi, "Security Issues and Attacks in Wireless Sensor Network", World Applied Sciences Journal, Volume 30, Issue 10, pp. 1224-1227, November 2014.

[20] Chinyang Henry Tseng, Shiau-Huey Wang, Woei-Jiunn Tsaur, "Hierarchical and Dynamic Elliptic Curve Cryptosystem Based Self-Certified Public Key Scheme for Medical Data Protection", IEEE Transactions on Reliability, Vol. 64, Issue: 3, pp. 1078 - 1085, 2015.

[21] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security (IJCSIS), Volume 4, Issue 1 & 2, pp. 1-9, August 2009.

[22] Daniel E. Burgner, Luay A. Wahsheh, "Security of Wireless Sensor Networks", 2011 Eighth International Conference on Information Technology: New Generations (ITNG), Las Vegas, NV, pp. 315-320, 2011.

[23] Heena Rathore, Sushmita Jha, "Bio-inspired machine learning based Wireless Sensor Network security", 2013 World Congress on Nature and Biologically Inspired Computing (NaBIC), Fargo, ND, pp. 140-146, 2013.

[24] Lukman Sharif and Munir Ahmed, "The Wormhole Routing Attack in Wireless Sensor Networks (WSN)", Journal of Information Processing Systems, Volume 6, Issue 2, pp. 177-184, June 2010.

[25] Kyung-Ah Shim, "A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, Vol. 18, Issue: 1, pp. 577-601, 2015.

[26] Banta Singh Jangra and Vijeta Kumawat, "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 3, pp. 291-296, September 2012.

[27] Leela Krishna Bysani and Ashok Kumar Turuk, "A Survey on Selective Forwarding Attack in Wireless Sensor Networks", IEEE International Conference on Devices and Communications (ICDeCom), pp. 1-5, February 2011.

[28] Gurudatt Kulkarni, Rupali Shelk, Kiran Gaikwad, Vikas Solanke, Sangita Gujar, Prasad Khatawkar, "Wireless sensor network security threats", Fifth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2013), Bangalore, pp. 131-135, 2013.

[29] Yulong Zou, Gongpu Wang, "Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack", IEEE Transactions on Industrial Informatics, Vol. 12, Issue: 2, pp. 780-787, 2015.

[30] Gagandeep and Aashima, "Study on Sinkhole Attacks in Wireless Adhoc Network", International Journal on Computer Science and Engineering, ISSN: 0975-3397, Volume 4, Issue 06, pp. 1078-1085, June 2012.

[31] Jyoti Ahlawat, Mukesh Chawla and Kavita Sharma, "Attacks and Countermeasures in Wireless Sensor Network", International Journal of Computer Science and Communication Engineering (IJCSCE), pp. 66-69. 2012.

[32] Manju.V.C, "A Survey on Wireless Sensor Network Attacks", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 2, pp. 23-28, August 2012.

[33] Peng Zhou, Siwei Jiang, Athirai Irissappane, Jie Zhang, Jianying Zhou, Joseph Chee Ming Teo, "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs", IEEE Transactions on Information Forensics and Security, Vol. 10, Issue: 3, pp. 613-625, 2015.

[34] S. Som, S. Sinha, R. Kataria (2016) "STUDY ON SQL INJECTION ATTACKS: MODE, DETECTION AND PREVENTION", International Journal of Engineering Applied Sciences and Technology, Indexed in Google Scholar, ISI etc., Impact Factor: 1.494, Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 23-29, June - July 2016.

[35] Abhishek Pandey and R.C.Tripathi, "A survey on Wireless Sensor Networks Security", International Journal of Computer Applications, Volume 3, Issue 2, pp. 43-49, June 2010.

[36] Kalpana Sharma and M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on Mobile Ad-hoc Networks (MANETs), Volume 1, Issue 8, pp.42-45, 2010.

[37] Lina Nachabe, Marc Girod-Genet, Bachar El Hassan, "Unified Data Model for Wireless Sensor Network", IEEE Sensors Journal, Vol. 15, Issue: 7, pp. 3657-3667, 2015.

[38] Rajat Gupta, Kaushal Sultania, Pallavi Singh, Archit Gupta, "Security for wireless sensor networks in military operations", Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, pp. 1-6, 2013.

[39] S.V.Annlin Jeba, B. Paramasivan and D.Usha, "Security Threats and its Countermeasures in Wireless Sensor Networks: An Overview", International Journal of Computer Applications, Volume 29, Issue 6, pp. 15-22, September 2011. [B17

[40] T.C. Aseri and N. Singla, "Enhanced Security Protocol in Wireless Sensor Networks", International Journal of Computers, Communications & Control, Volume 6, Issue 2, pp. 214-221, June 2011.

[41] Ching-Tsung Hsueh, Chih-Yu Wen, Yen-Chieh Ouyang, "A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks", IEEE Sensors Journal, Vol. 15, Issue: 6, pp. 3590-3602, 2015.

[42] Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks", 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, Langkawi, pp. 308-311, 2011.

[43] Sencun Zhu, Sanjeev Setia and Sushil Jajodia, "LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks", 10th ACM Conference on Computer and Communications Security (CCS 03), pp. 62-72, October 2010.

[44] Binod Kumar Mishra, Mohan C. Nikam, Prashant Lakkadwala, "Security against Black Hole Attack in Wireless Sensor Network - A Review", 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, pp. 615-620, 2014.

[45] Daojing He, Sammy Chan, Mohsen Guizani, Haomiao Yang, Boyang Zhou, " Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 26, Issue: 4, pp. 1129-1139, 2014.

[46] Sneha Ghormare, Vaishali Sahare, "Implementation of data confidentiality for providing high security in Wireless Sensor Network", International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, pp. 1-5, 2015.

[47] Singh, Ajay Vikram, and Moushumi Chattopadhyaya. "Mitigation of DoS attacks by using multiple encryptions in MANETs." In Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on, pp. 1-6. IEEE, 2015.

[48] Ajay Vikram Singh, Bani Singh, M. Afshar Alam, “Issues and Challenges associated with Secure QoS aware Routing in MANETs”, International Journal of Research and Reviews in Ad Hoc Networks (IJRRAN), Vol. 1, No. 3, pp. 73-76,ISSN: 2046-5106, Science Academy Publisher, United Kingdom, September 2011.