A Review: QoS Issues in WSN

Zaiba Ishrat[1], Kailash Nath Verma[2], Owais Ahmad Shah [3]
[1]EC, IIMT College Of Engineering, Greater Noida, India, [2]AS, IIMT College Of Engineering, Greater Noida, India, [3] EC, Noida International Unversity, Greater Noida, India

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. Wireless Sensor Networks consist of a large number of pocket- sized sensors deployed in autonomous manner in the area under surveillance. These sensor networks are used in sensitive, unattended and remote environment.WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. This paper studies the security problems of WSN based on its resource restricted design and deployment characteristics and the security requirements for designing a secure WSN. Also, this study documents the well known attacks at the different layers of WSN and some counter measures against those attacks.

Keyword- WSN, Warmhole, Sink hole, Hello flood attack ,Jamming

I. INTRODUCTION

Wireless sensor network (WSN) is made up of a large number of minute sized sensors.These sensors use to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through the network to a main location.[1] There are two types of nodes- sink node and the sensor nodes. The sink node is also called base station. It instructs the sensor nodes about the type of data to be collected from the area under surveillance. The sensing unit of WSN which consists of the sensor nodes gathers the information and reports back to the sink node. The storage and processing of data takes place in the computing unit. The transmission of data occurs through multiple hops and RF band is used for communication[2][3]. The assembly of WSN is shown in Fig 1 and applications in Fig 2.

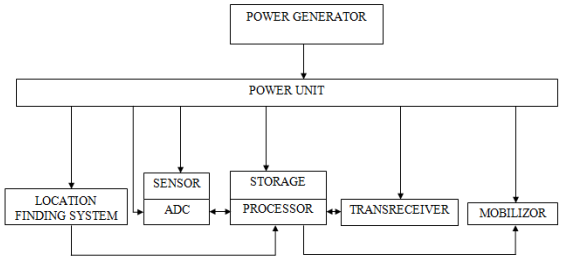


Fig.1: Architecture of Wireless Sensor Networks

WSN is used in many applications from indoor to outdoor [1]. WSNs are expected to be solutions to many applications, such as detecting and tracking the passage of troops and tanks on a battlefield, monitoring environmental pollutants, measuring traffic flows on roads, and tracking the location of personnel in a building. 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.[3]

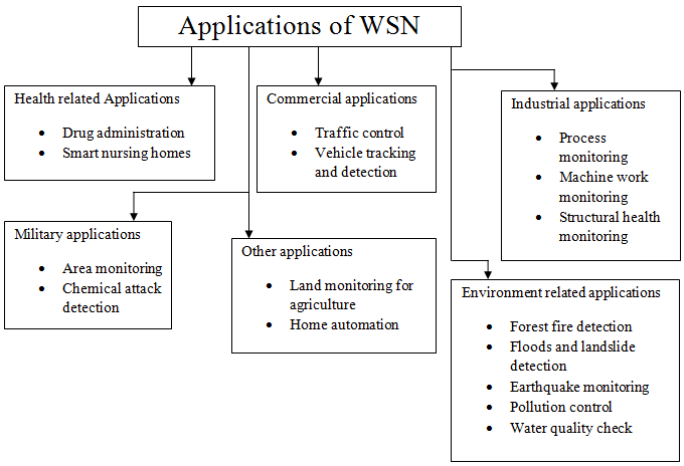


Fig.2: Applications of Wireless Sensor Networks

A. Characteristics of WSN: Power consumption constraints for nodes using batteries or energy harvesting.

a) Ability to cope with node failures (resilience)
b) Mobility of nodes.
c) Heterogeneity of nodes.
d) Scalability to large scale of deployment.
e) Ability to withstand harsh environmental conditions.
f) Ease of use.

B. Constraints in WSN:

a) Energy Consumption

Sensor nodes are equipped with battery that is used as their energy source. The sensor network can be deployed in hazardous condition so it becomes difficult recharging or changing batteries. The energy consumption depends upon major operations of the sensor nodes which are sensing, data processing, communication. The large amount of energy is consumed during communication.[6]

b) Localization

Sensor localization is a fundamental and critical issue for network operations and management. The sensor nodes are deployed in ad-hoc manner so they do not have any information about their position. The problem of determining the physical location of the sensors after they have been deployed is called localization. This problem

can be solved by beacon nodes, GPS, proximity based localization. [5]

c) Coverage

It says how well an area of interest is controlled as traced by the sensor. These Sensor nodes use coverage algorithm to sense data and send them to sink using routing algorithm. For the good coverage, sensor nodes must be selected in such a manner so that whole network should be covered.[4]

d) Clocks

Clock synchronization is a critical service in WSN. The goal of time synchronization is to provide a common timescale for local clocks of nodes in sensor networks. Clocks ought to be synchronized in some applications such as tracking and monitoring. [4,6]

e) Computation

The amount of data proceeds by every node is called computation. The major problem in computation is that it should minimize the use of resources. If the lifetime of base station is more critical then data processing can be completed at every node before sending data to base station. In case when we have few resources at every node then entire computation must be done at sink.

f) Production Cost

As we know, large numbers of nodes are deployed in the sensor networks, so if the cost of a single node will be very high then we can assume the overall cost of the network will also be very high. Eventually, the cost of every sensor node has to be kept low. So cost of each sensor node in the network is a challenging issue. [5]

g) Hardware Design

While designing any hardware of sensor network, it must be energy-efficient. Hardware such as power control, micro-controller, and communication unit should be design in such a way that it consumes less energy.

h) Quality of Service

QOS means data should be delivered within time period. There are some real time sensor applications that are based on time i.e. if data should not be delivered on time to the receiver from the moment it is sensed; data will become useless. There is various quality of service issues in sensor networks such as network topology may change continually and the available state information for routing is constitutionally imprecise.[4,5,6]

1.3 **Security Requirement:**

The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

a) **Data Confidentiality:** Data should not be disclosed to any third-party. Secrecy of the information should be maintained. Unauthorized users should not be able to overhear the information. It should be ensured that information is concealed from the attackers.

b) **Data Integrity:** For secure and reliable communication, data received at the destination node must be same as that sent by the source node. The intermediate nodes must not change the information contained in the packets. Malicious activity should not corrupt the data [7].

c) **Data Authentication:** The attacker can not only alter the information contained in the packets but can also introduce fallacious packets in the network. So verification of sender and receiver identities needs to be carried out as a defensive step against the action of any malicious activity. Data authentication is challenging for WSNs as they are deployed in remote areas where it is very difficult to verify the identity of the sender. Only the authorized users should be able to access the information and the illegitimate users should be denied the access [7,8].

d) **Data Availability:** Availability of data is very vital for proper functioning of the network. Services of the network should be available whenever necessary. Users should be able to use the resources whenever they intend to [9].

e) **Data Freshness:** Data freshness implies that the information received is current and up-to-date. The previous data should not be repeated that is real-time computation must be done. Security protocols must be able to detect and discard the duplicate messages [7,8,9].

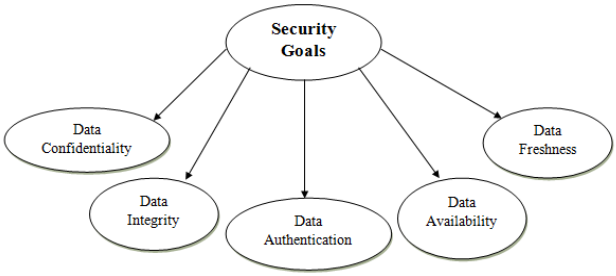
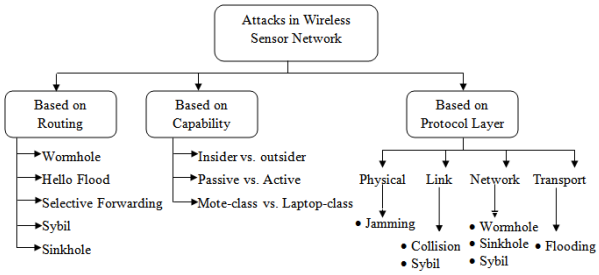


Fig.3: Security Requirement

II. 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. They are roughly categorized as follows:

A) Based on Routing
B) Based on Capability
C) Based on Protocol Layer



A. On the Basis of Routing: In this transmission process, an attacker can steal or modify the information with the help of different attacks. [10][11][13]. Some of the routing attacks are explained below:

B. Wormhole:In this attack, the attacker overhears the communication between two nodes. It then replays information between the nodes located far away physically by giving an illusion that they are very close to each other. This attack occurs at network layer. Fig 4 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 neighbour node B.[12][13][15].

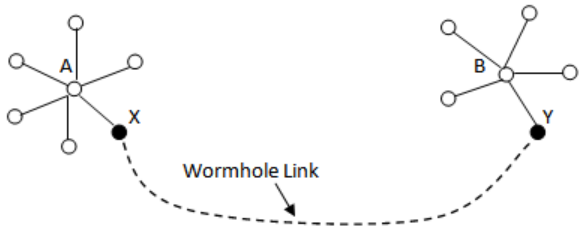


Fig.4: Wormhole attack

C. Hello Flood Attack

Hello packets are broadcasted to the network by the malicious nodes. High power RF transmitters are used. This is done to make the nodes believe that the malicious nodes are the neighbourhood nodes. Thus the unauthorized users have the access to the channel. This results in loss of information as the legitimate user doesn't get the access to the channel. Network layer is affected by the hello packets. As demonstrated in Figure 5 attacker node broadcasts the HELLO packet with high transmission power than the sink. Figure 6 shows that the nodes which receive HELLO packet from attacker node consider it as a neighbour node and send/reply the sensed data packet to the attacker node [13][14]

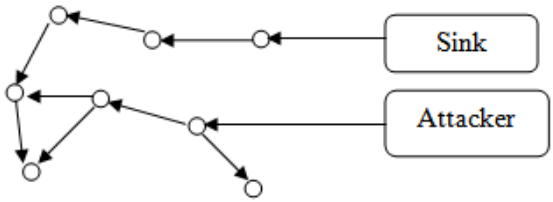


Fig.5: HELLO Flood Attack scenario-Hello Packet send by the Attacker

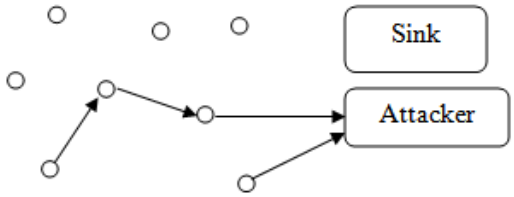


Fig.6: HELLO Flood Attack scenario-Sensor node replying back to the attacker considering it as its neighbor node

D. Selective Forwarding — A significant assumption made in multihop networks is that all nodes in the network will accurately forward received messages. An attacker may create malicious nodes which selectively forward only certain messages and simply drop others . A specific form of this attack is the black hole attack in which a node drops all messages it receives. One defense against selective forwarding attacks is using multiple paths to send data . A second defense is to detect the malicious node or assume it has failed and seek an alternative route. Figure 7 shows a malicious node present between the nodes in network. In this neighboring node unknowingly forwards packets to the malicious node [13][14][16].

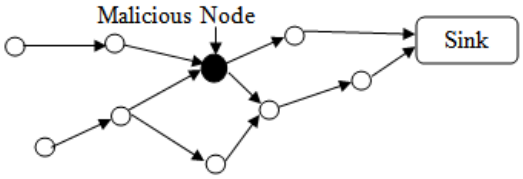


Fig.7: A malicious node in the network

E. Sybil Attack: The Sybil attack is a case where one node presents more than one identity to the network [14,16,17]. Protocols and algorithms which are easily affected include fault-tolerant schemes, distributed storage, and network-topology maintenance. For example, a distributed storage scheme may rely on there being three replicas of the same data to achieve a given level of redundancy. If a compromised node pretends to be two of the three nodes, the algorithms used may conclude that redundancy has been achieved while in reality it has not.

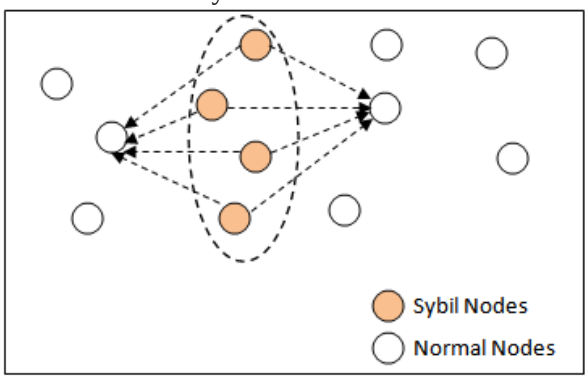


Fig.8: Malicious node with multiple identities

F. Sinkhole attack

In sinkhole attack, a compromised node attracts a large number of traffic of surrounding neighbours by spoofing or replaying an advertisement of high quality route to the base station [18]. The attacker can do any malicious activity with the packets passing through the compromised node.

G. Based on Capability

The level of data access and its damage is different depending upon the type of attack. [19][20] On the basis of capability, attacks are classified as follows:

E. Outsider versus insider attacks: outside attacks are defined as attacks from nodes which do not belong to a WSN; insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways.

F. Passive Vs Active: The attacks can be classified into passive attacks and active attacks. Passive attacker snoops into the network and overhears the contents. Monitoring and Eavesdropping is the most common feature of passive attacks. They eavesdrop the information i.e. the data confidentiality is lost. They are difficult to detect as they are silent and don't make their presence felt. Passive intrusion doesn't hinder the operation of the network. Active attacker alters the message and obstructs the secure and reliable communication. It may harm the network in different ways. It can hinder the performance by not delivering the packets to the authorized and intended user or can mislead the destination node by introducing fallacious packets. Illegitimate user can gain the access to the confidential data and misuse it. A false node can be introduced by the attacker. This node is called malicious or compromised node. This node can alter the message contents; thereby violating the data integrity principle. Wormhole attack, blackhole attack and denial of service attack are some of the active attacks [20].

G. Laptop-class Attacks vs. Mote-class: in mote-class attacks, an adversary attacks a WSN by using a few nodes with similar capabilities to the network nodes; in laptop-class attacks, an adversary can use more powerful devices (e.g., a laptop) to attack a WSN. These devices have greater transmission range, processing power, and energy reserves than the network nodes[21].

H. 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 [19]: 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 [22].

I. **Jamming:** In physical layer, jamming is a common attack that can be easily done by adversaries by only knowing the wireless transmission frequency used in the WSN. [23] Says the attacker transmits radio signal randomly with the same frequency as the sensor nodes are sending signals for communication. This radio signal interferes with other signal sent by a sensor node and the receivers within the range of the attacker cannot receive any message.[19][20]

J. Tampering: In tampering, attacker can tamper the node physically and manipulate the data. Cognizant information like the cryptographic keys can be extracted by the attacker. This may result in loss of important and further higher level of information. This attack occurs at physical layer of OSI. Temper proof physical packaging is one possible defensive strategy against such attacks [20][21].

K. 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,sybil.

L. Collision: When any two nodes undergo concurrent transmissions over similar frequency channels collision can occur. When this happens, there is some change in the packet contents. This results in a mismatch when checksum is computed at the receiving end. As in case of mismatch the packets need to be re-transmitted so this leads to unnecessary energy consumption. Collision occurs at data link layer. To prevent such situation error correcting codes can be used at low collision levels.

M. Network layer attack: The network and routing layer of sensor networks is usually designed according to the following principles [19,20,21]:

a) Power efficiency is an important consideration.
b) Sensor networks are mostly data-centric.
c) An ideal sensor network has attribute-based addressing and location awareness.

Some routing protocol attacks are: wormhole attacks, acknowledgement spoofing, selective forwarding, black holes and so forth.

N. Spoofing: An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network [17,18,19]. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency.

D. Blackhole Attack : In this attack the attacker take hold of the node and reprograms it. The attacker drops the packets and doesn't allow the node to pass the information to subsequent nodes. This results in complete loss of data packets.

E. Acknowledgment Spoofing: Routing algorithms used in sensor networks sometimes require Acknowledgments to be used. An attacking node can spoof the Acknowledgments of overheard packets destined for neighbouring nodes in order to provide false information to those neighboring nodes [22]. An example of such false information is claiming that a node is alive when in fact it is dead.

F. Denial-of-Service Attack: A Denial-of-service (DOS) attack is an attempt to prohibit the genuine user of a service or data. The destination system is overwhelmed with fallacious requests such that it cannot acknowledge the genuine traffic. Thus the services are inaccessible to the authorized users. The efficiency of the system is affected; performance decreases and eventually the network stops functioning. Using the sensor networks in sensitive and critical areas intensifies the likelihood of DOS attacks. This attack drains off the energy of the node and knocks down the network.[21][22]

G. Transport Layer: The transport layer is responsible for managing end-to-end connections [22]. Two possible attacks in this layer, flooding and desynchronization, are discussed in this subsection.

H. Flooding- Whenever a protocol is required to maintain state at either end of a connection it becomes vulnerable to memory exhaustion through flooding [23]. An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored.

I. Desynchronization*:* Desynchronization refers to the disruption of an existing connection [19,20]. An attacker may, forexample, repeatedly spoof messages to an end host, causing

that host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data, thus causing them to instead waste energy by attempting to recover from errors which never really existed.

III. DEFENCE AGAINST SECURITYTHREATS

A. **Cryptography:** Selecting the most appropriate cryptographic method is vital in WSNs because all security services are ensured by cryptography. Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated by code size, data size, processing time, and power consumption. In this section, we focus on the selection of cryptography in WSNs.

B. **Public key cryptography in WSN:**Many researchers believe that the code size, data size, processing time, and power consumption make it undesirable for public key algorithm techniques, such as the Diffie–Hellman key agreement protocol [26] or RSA signatures [25], to be employed in WSNs. Public key algorithms such as RSA are computationally intensive and usually execute thousands or even millions of multiplication instructions to perform a single security operation.

C. **Symmetric key cryptography in WSN:** The constraints on computation and power consumption in sensor nodes limit the application of public key cryptography in WSNs. Thus, most research studies focus on symmetric key cryptography in sensor networks. Popular encryption schemes, RC4 [25], RC5 [26], were evaluated on six different microprocessors ,the execution time and code memory size were measured for each algorithm and platform.

D. **Sybil attack Defence:** Identity verification is the key requirement for countering against Sybil attack. Unlike traditional networks, verification of identity in WSN cannot be done with a single shared symmetric key and public key algorithm because of computational limitation of WSN.

E. **Flooding Defence:** One solution against flooding attack is to limit the number of connections that a node can make. But, this can prevent legitimate nodes to connect to the victim node. A possible solution to this type of attack is to require Authentication of all packets communicated between hosts [18]. Provided that the authentication method is itself secure, an attacker will be unable to send the spoofed messages to the end hosts

F. **Jamming Defence:** Typical defenses against jamming involve variations of spread-spectrum communication such as frequency hopping and code spreading [19,20,21]. Frequency-hopping spread spectrum (FHSS) is a method of transmitting signals by rapidly switching a carrier among many frequency channels using a pseudo random sequence known to both transmitter and receiver. Without being able to follow the frequency selection sequence, an attacker is unable to jam the frequency being used at a given moment in time. However, as the range of possible frequencies is limited, an attacker may instead jam a wide section of the frequency band.

Code spreading is another technique used to defend against jamming attacks and is common in mobile networks. However, this technique requires greater design complexity and energy, thus restricting its use in WSNs. In general, to maintain low cost and low power requirements, sensor devices are limited to single-frequency use and are therefore highly susceptible to jamming attacks.[20]

G. Tampering Defence: One defence against tampering is to tamper-proofing the node's physical package [14]. However, it is usually assumed that the sensor nodes are not tamper-proofed in WSNs due to the additional cost. This indicates that a security scheme must consider the situation in which sensor nodes are compromised.

H. Collision Defence: A typical defence against collisions is the use of error-correcting codes [15]. Most codes work best with low levels of collisions, such as those caused by environmental or probabilistic errors. However, these codes also add additional processing and communication overhead. It is reasonable to assume that an attacker will always be able to corrupt more than what can be corrected. While it is possible to detect these malicious collisions, no complete defenses against them are known at this time.

I. Exahaustion Defence: To avoid the problem of exhaustion is to apply rate limits to the MAC admission control such that the network can ignore excessive requests, thus preventing the energy drain caused by repeated transmissions [17]. A second technique is to use time-division multiplexing where each node is allotted a time slot in which it can transmit [18]. This eliminates the need of arbitration for each frame and can solve the indefinite postponement problem in a back-off algorithm. However, it is still susceptible to collisions.

J. DOS Defence; To avoid the effect of DOS The use of small frames lessens the effect of such attacks by reducing the amount of time an attacker can capture the communication channel. However, this technique often reduces efficiency and is susceptible to further unfairness, for example, when an attacker is trying to retransmit quickly instead of randomly delaying [21].

H. Spoofing Defence: A countermeasure against spoofing and alteration is to append a message authentication code (MAC) after the message. By adding a MAC to the message, the receivers can verify whether the messages have been spoofed or altered. To defend against replayed information, counters or timestamps can be included in the messages [18].

I. hello flood effect Defence:[14]

a) Authentication of the two-way link before acting on the information
b) Cryptographic and non-cryptographic techniques

J. Siink whole effect Defence: [10]

a) Key management
b) Authentication
c) Geographic routing

IV. CONCLUSION

This paper highlights the security issue of the WSN. Security is the big challenge in the sensor network. This paper studies the security threats on the basis of different parameters. To

achieve the security requirements various protocols have been proposed. There are many security solutions or mechanisms that have been proposed for Wireless Sensor Network; some of which are concerned about specific security attacks whereas some are concerned about specific security aspect. There is no standard security mechanism that can provide overall security for WSN. Providing such mechanism is not possible also as WSNs are implemented in various application domains with different level of security requirements. Encryption process is used to make data confidential and MAC is attached to each data packet to provide authenticity. The above mentioned defensive techniques need to be made stronger so as to safeguard the network.

V. REFRENCES

[1]. Padmavathi, Dr G., and Mrs Shanmugapriya (2009), A survey of attacks, security mechanisms and challenges in wireless sensor networks." *arXiv preprint arXiv*:0909.057

[2]. Kavitha, C. (2012), A survey on secured routing protocols for wireless sensor network, *In 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*, pp. 1-8

[3]. Padmavathi, Dr G., and Mrs Shanmugapriya (2009), A survey of attacks, security mechanisms and challenges in wireless sensor networks." *arXiv preprint arXiv*:0909.057

[4]. Jain A, Kant K, Tripathy M (2012) Security solutions for wireless sensor networks in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on IEEE pp: 430-433.

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

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

[7]. Modares, Hero, Rosli Salleh, and Amirhossein Moravejosharieh (2011), Overview of security issues in wireless sensor networks, *In Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on,* pp. 308-311. IEE

[8]. Padmavathi, Dr G., and Mrs Shanmugapriya (2009), A survey of attacks, security mechanisms and challenges in wireless sensor networks." *arXiv preprint arXiv*:0909.057

[9]. Singh, Shio Kumar, M. P. Singh, and D. K. Singh. (2010), A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks, *International Journal of Advanced Networking and Application (IJANA) 2.02* : 570-580

[10]. 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.

[11]. 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.

[12]. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,"

[13]. *Commun. ACM*, vol. 26, no. 1, 1983, pp. 96–99. J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Commun.*, vol. 11, no. 6, Dec. 2004, pp. 6–28.

[14]. 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.

[15]. 4. Patel MM, Aggarwal A (2016) Two phase wormhole detection approach for dynamic wireless sensor networks in Wireless Communications Signal Processing and Networking (WiSPNET), 2016 International Conference on IEEE pp: 2109-2112.

[16]. 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

[17]. Oh, Seo Hyun, Chan O. Hong, and Yoon Hwa Choi (2012), A malicious and malfunctioning node detection scheme for wireless sensor networks. *Wireless Sensor Network 4*, no. 03 pp. 84.

[18]. 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.

[19]. . Mulla RI, Patil R (2016) Review of attacks on wireless sensor network and their classification and security. Imperial J Interdiscipl Res 7: 2.

[20]. 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.

[21]. Ghildiyal, Sunil, Amit Kumar Mishra, Ashish Gupta, and Neha Garg, Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks. *IJRET: International Journal of Research in Engineering and Technology* pp.2319-1163

[22]. 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.

[23]. Yong Wang, Garhan Attebury "A survey of security issue in wireless sensor network" IEEE Communications Surveys, • 2nd Quarter 2006

[24]. I. F. Akyildiz *et al.*, "A Survey on Sensor Setworks," *IEEE Commun. Mag.*, vol. 40, no. 8, Aug. 2002, pp. 102–114.

[25]. W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Info. Theory*, vol. 22, no. 6, Nov. 1976, pp.644–54.

[26]. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Commun. ACM*, vol. 26, no. 1, 1983, pp. 96–99.