Security Attacks, challenges and Mechanisms for security in Wireless Sensor Network: A survey

[*]Priyanka R

[*]*Assistant Professor, Department of Information Science and Engineering, CMRIT, Bangalore (India)*

ARTICLE DETAILS

Article History

Published Online: 06 January 2018

Keywords

Wireless Sensors Network, security, structured, unstructured, CIA, active attack, passive attack

[*]**Corresponding Author**

Email: priyanka.r.89@gmail.com

ABSTRACT

The main objective of the paper is to discuss about different types of Security attacks and challenges on WSN, we also present the effect of the attack and the defense mechanisms in Wireless sensor networks which are prone to attacks due to its characteristics. Security attacks are identified and classified based on attacker location, based on transmission of information, based on different protocols etc.. and the different security measures that can be applied to defend against different attacks. This survey paper focuses on various aspects of different security attacks, their effects and defense mechanisms corresponding to each attack etc. So this paper helps researchers to have an idea about the security issues, existing attacks and they can also use the ideas and concepts to build more secure wireless sensor network system in future. A direction can be obtained to develop new security mechanisms to protect new possible attacks along with existing ones.

INTRODUCTION

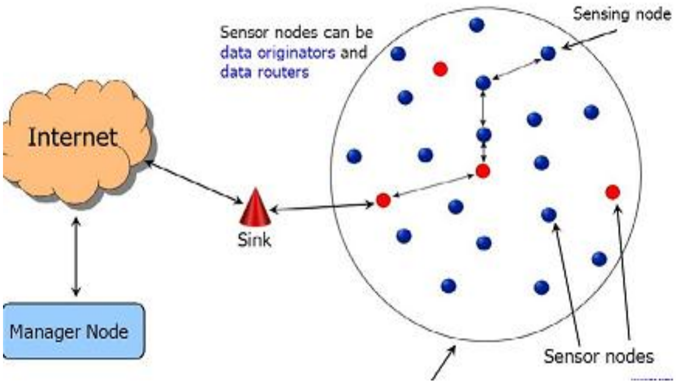


Fig 1: Architecture of WSN

Components of smart sensor nodes are one or more sensors, a processor, memory, a power supply, a radio, and an actuator. Battery is the main power source of a sensor node. A WSN consists of a number of sensor nodes.

Not only a sensor node [2] collects data but also have additional functionality like in-network analysis, correlation and combination of its own sensor data and data that are coming from other sensor nodes. Many sensors cooperatively monitor large physical environments with help of a wireless sensor network (WSN). Sensor nodes communicates with each other and with a base station (BS) with the help of their wireless radios and it allows them for spreading their sensor data for the requirement of remote processing, analysis, and storage systems in the network. The figure above shows the architecture of WSN.

An Unstructured WSN is one that composed of a dense collection of sensor nodes. The network [3] of this kind is homogeneous in nature with respect to node type without physical hierarchy that means that they are physically and architecturally equal. In a Structured WSN, all or some of the sensor nodes are implemented in a pre-structured manner.

The advantage of a Structured network is that only few nodes can be implemented with lower network maintenance and management cost.

SECURE NETWORK GOALS

Computer and network security [2] is composed of all policies, mechanisms, and services that require a computer system or network protecting unauthorized access or unintended uses. Most security mechanisms must provide three well-known services that are in the CIA (Confidentiality Integrity and Availability) security model.

Primary Goals

Confidentiality: Security mechanisms ensure that only the intended receiver can receive a message correctly and that unauthorized access and usage of the message is prevented.

Integrity: Modification of a message must be restricted which is being propagated from the sender to the receiver.

Availability: A system or network must be able to do their tasks at any time without interruption. The mechanism takes care of this.

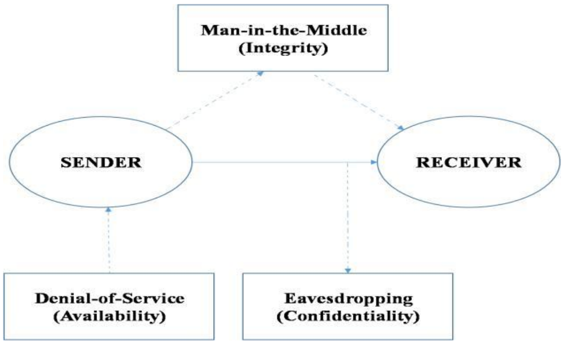

Man-in-the-Middle (Integrity)
SENDER
RECEIVER
Denial-of-Service (Availability)
Eavesdropping (Confidentiality)

Fig 2: CIA model and attacks [2]

Secondary Goals [4]

Data Freshness:

Data freshness identifies that the data is recent and no old packets have been replayed. There are two types of data freshness: Weak Freshness, which is applicable for sensor

Synchronization of time:

Most sensor network applications depend on some form of time synchronization. Sensors can compute the end-to-end delay of a packet, at the time of travelling a packet between two pair wise sensors.

Secure Organization:

The sensor network must have the ability to accurately and automatically locate each sensor in the network.

SECURITY CHALLENGES IN WIRELESSSENSOR NETWORKS

WSNs possesses a variety of unique challenges [2] that must be considered for the security concerns that may be present in sensor network applications.

Resource constraints:

Security mechanisms i.e. traditional with high overheads are not suitable for resource-constrained WSNs.

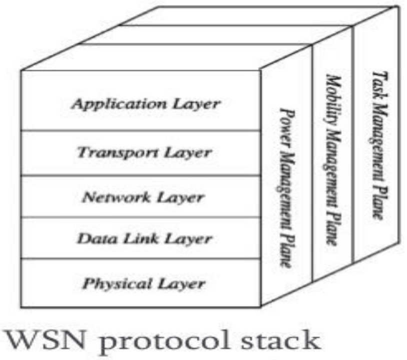
Remote location:

The first line of defense against security attacks is to provide only controlled physical access to a sensor node.

Lack of central control:

It is often infeasible to have a central point of control in sensor networks, for example, because of their large scale network size, resource constraints, and network dynamics.

SECURITY ATTACKS IN SENSOR NETWORKS



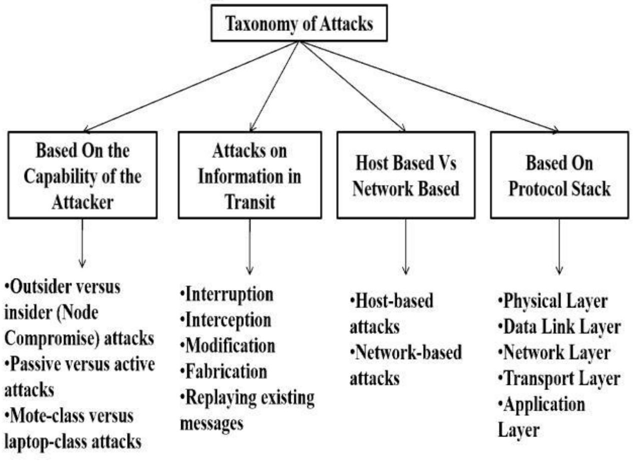

Taxonomy of Attacks
Based On the Capability of the Attacker
Attacks on Information in Transit
Host Based Vs Network Based
Based On Protocol Stack
•Outsider versus insider (Node Compromise) attacks
•Passive versus active attacks
•Mote-class versus laptop-class attacks
•Interruption
•Interception
•Modification
•Fabrication
•Replaying existing messages
•Host-based attacks
•Network-based attacks
•Physical Layer
•Data Link Layer
•Network Layer
•Transport Layer
•Application Layer

Fig 3: Taxonomy of attacks [5]

Based on the capability of the attacker

Outsider vs. Insider attack [4]:

In an outsider attack, a malicious node harms WSN without being part of it. In contrast, in an insider attack the malicious node harms the WSN as (authorized) participant of the WSN. The following section shows different types of active and passive attacks [4] [6] [7] [8] [9] [10].

Active attacks [11]:

Active attacks: The unauthorized attacker monitors, listens to and modifies the data stream in the packet exchange within the network including routing attacks, eavesdropping and creation of a false stream etc. Active Attacker [12] does operations, such as addition of faulty data into the WSN, impersonating, modification of packets.

Examples of Active attacks:

- ✓ *Routing attacks:* The network layer attacks are also known as routing attacks. The following are the attacks that happen while routing the messages.

- ✓ *Spoofed and Altered or Replayed Routing Information:* To make disturbance to the traffic, an adversary may alter, spoof or replay routing information in the network.
- ✓ Selective Forwarding: The malicious nodes forward selectively only certain messages and simply discard others.

- ✓ *Sybil Attacks*: The Sybil Attacks target the fault tolerant schemes like multipath routing, topology maintenance and distributed storage.

- ✓ *Wormhole Attacks:* An attacker collects packets of data at one particular location in the network, transfers them to some other location and then resends them into the network.

- ✓ *HELLO flood attacks*: A malicious node sends or re-plays the routing protocol HELLO packets from one node to another with abnormally high transmission power.

- ✓ *Sinkhole Attack*: Traffic from a particular region is attracted by the adversary. The adversary may advertise a false optimal path with sufficient available power and bandwidth. There are two types of attackers may launch sinkhole attack [13]. They are known as malicious insider and resourceful outsider. Malicious insider, the attacker uses a node to launch the attack advertising a route to deceive neighbors. Resourceful outsider, the laptop-class adversary announce a single-hop route from its neighbors to BS and the neighbors are convinced by the route and forward all traffic through it.

- ✓ *Black-hole Attack*: A malicious node advertises the wrong paths as good paths to the destination node during the path finding process. In a black hole attack, the adversary receives but does not forward all the received messages. Location plays an important role influencing the network, when adversary is nearer to BS, all traffic to BS, may go through the adversary. If the attacking node location is at edge of the WSN, there is a possibility of very few sensor nodes may communicate with each other. As a result, the harm can be very limited.

- ✓ *Acknowledgement Spoofing:* The acknowledgements of overheard packets can be spoofed by an adversary for particular nodes for providing false information to the neighboring nodes. In this type of attack [14], node C wants to send data to node D where node D is not alive. At link layer, suppose a malicious node N eavesdrop the message and give acknowledgement falsely to node C. According to the acknowledgement that is spoofed, node C sends its messages through node N to the base station. Now node N can drop packets or can modify the packet's content.

- ✓ *Misdirection:* A malicious node sends the packets in the wrong direction from that point the destination is not reachable. Throughput and network life time are reduced and the delay [15] is increased by the effect of this attack.

- ✓ *Internet Smurf Attack:* The attacker may falsify the network and the address of victim and broadcasts multiple messages in the network. This may flood a victim intentionally with hundreds of responses for every request.

- ✓ *Homing:* To achieve DoS an attacker detects traffic pattern and target nodes with special responsibilities, such as cluster heads or cryptographic key managers by destroying these key network nodes.

- ✓ *Denial of service attacks:* This attack is posed by malicious action of some nodes or sudden failure of the nodes in the sensor networks.

- ✓ *Node Subversion:* A normal node capture is done by some attacker node and the attacker may disclose its security information like cryptographic keys and thus affects the whole security mechanism of the WSN.

- ✓ *Node Outage*: As in node outage problem, when a cluster head stops its function, then the WSN protocols must be robust enough to handle this by using some other routes that are suitable.

- ✓ *Physical Attacks:* WSN is implemented in an open environment so they are easily vulnerable to several types of physical attacks i.e. physical node destruction causes a threat.

- ✓ *Node Replication Attacks:* A malicious node is added by attacker in the sensor network with same node-id as of a normal sensor node.

- ✓ *Passive Information Gathering*: If sensor node is not encrypted, information can be collected by any opponent with powerful resources from the sensor networks.

- ✓ *False Node:* In this situation, a false node is added by an attacker injecting malicious data in the network.

Passive attacks [11]

The monitoring and eavesdropping on the packet exchange by unauthorized attackers within a WSN are known as passive attack. Passive attacker [12] as a normal node may do several functions like collects information from the WSN and unauthorized attackers monitor and eavesdroppers from communication channel. Examples of Passive attacks:

Attacks against Privacy: Passive Attacks are also called as attacks against privacy.

Monitor and Eavesdropping: With the help of snooping to the data, the adversary could easily find the communication contents.

Traffic Analysis: If the encrypted message which is transferred then also there is risk of malicious harm.

Camouflage Adversaries: Intruder injects their node or compromises the nodes to hide and it can copy as a normal node to attract the packets.

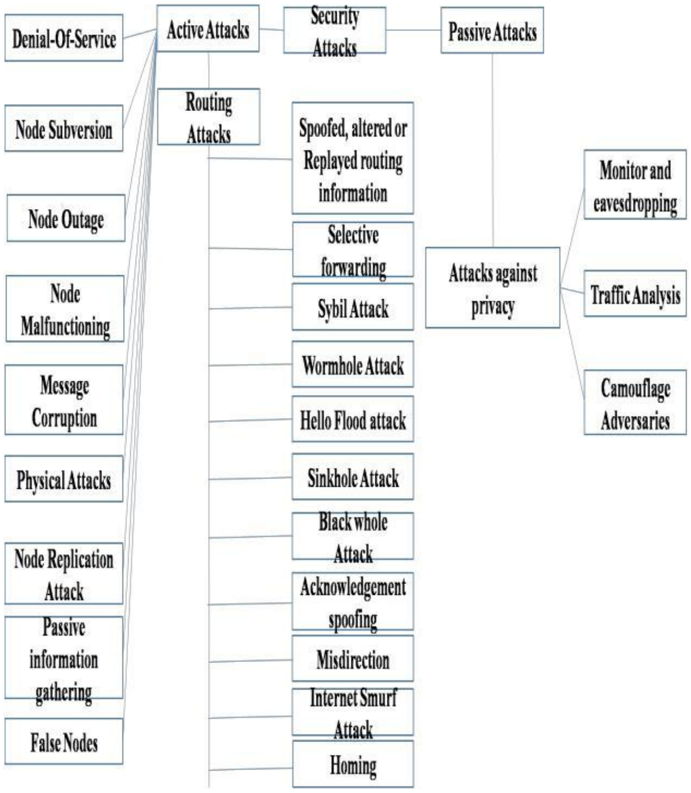


Fig 3: Active and passive attacks

Attacks on information in transit

Interruption:

It is an attack [17] on the availability of the network, for example physical nodes capturing, corruption of message, malicious code insertion etc. The main purpose [4] is to launch denial-of-service (DoS) attacks.

Interception:

It is an attack [17] on confidentiality. An adversary can compromise the sensor network to get unauthorized access to sensor node or data stored within it. The main purpose [4] is to eavesdrop on the information carried in the messages.

Modification:

It means [17] that a party without any authorization, not only accesses the data but tampers the data. This threatens message integrity. The main [4] purpose is to create confusion of mislead the parties involved in the communication protocol. This is usually aimed at the network layer and the application layer.

Fabrication:

It is an attack on authentication [17]. This [5] gives threats to message authenticity.

Host based vs. network based attacks

Host based attacks:

It is further divided into three categories [5]: User compromise: The users of a WSN are compromised e.g. the users are forced revealing information such as passwords or keys about the sensor nodes.

Hardware compromise: This is associated with tampering of the hardware to extract the program code, data and keys stored within a sensor node.

Software compromise: This aids in breaking the software running on the sensor nodes. The operating system and/or the applications running in a sensor node are exposed to popular exploits such as buffer overflows.

Network based attacks:

It has two orthogonal perspectives [5]: layer-specific compromises, and protocol-specific compromises. This includes all the attacks on information at the time of transmission. Network-based denial-of-service [18] attacks are one of the easiest types of attacks. Mainly DoS attacks try to send huge amount of false packets in the network.

- ✓ *Ping of death:* Oversized ICMP datagram's (encapsulated in IP packets) is sent to the victim node by the ping of death attack. The Ping command using the ICMP echo request and echo reply messages and it is commonly used to check if the remote host is alive.

- ✓ *Teardrop attack:* Data [19] is divided into smaller fragments i.e. data packets in the source system and reassembled at destination system. In this type of attack, the target systems fails to reassemble the data packets, due to the overlapping value of the OFFSET field in the TCP header part of the data packets sent by attacker and the target system crashes, hangs or reboot.

- ✓ *SYN - flood attack:* In SYN flooding attack, several SYN packets that are consist of invalid source IP address, are sent to the target host. When these SYN packets are received by the target system, it make a try to respond to each system with the help of a SYN/ACK packet but as all the source IP addresses are invalid the target system enters into wait state for Smurf attack: It Broadcasts ICMP packets containing victim's spoofed source IP and causes all hosts on the network to reply to the ICMP request, results significant traffic to the victim's node.

SECURITY MECHANISM

The main motive [46] behind the security mechanisms is to detect, prevent and recover from the security attacks and also provides a pseudo idea to protect from different kind of security attacks.

Low level security mechanism

Key establishment and trust setup:

The establishment [46] of cryptographic keys is the primary requirement to setting up the sensor network. Key-establishment [47] techniques need to scale to networks with hundreds or thousands of nodes. The disadvantage of this mechanism [46] is that the attacker may compromise the sensor nodes and most of them could be rebuild the complete key pool and easily break the security scheme. Prior knowledge of nodes and secure node-to-node communication are needed for good key distribution or establishment and management schemes [48].

Privacy:

Like other traditional networks, the sensor networks have also force privacy concerns [47]. Initially the sensor networks [46]are deployed for legitimate purpose might subsequently be used in unanticipated ways. The main privacy problem [50], in reality much information from sensor networks could be gathered using direct site surveillance.

Robustness to communication denial of service an adversary [47] attempts to disrupt the network's operation broadcasting a signal that is a high energy signal.

Secure routing:

Routing and data forwarding [47], is a crucial service for enabling communication in sensor networks. Adversaries [51] can severely limit the availability of the resources wireless sensor network by DoS attacks.

Resilience to node capture:

In Resiliency against [47] node capture, in most of the applications, sensor nodes are to be deployed on different locations that are easily accessible to the attackers. Attacker can capture the sensor node to extract secrets of the cryptographic, modify their programs and may replace them with malicious nodes under the control of the attacker. Algorithmic [51] solutions to the problem of node capture are preferable. Tamper-resistant packaging may be a defense but it is expensive.

High level security mechanism

Secure group management:

Data aggregation and analysis [28] can be performed by groups of nodes in wireless sensor networks and secure protocols for group management are required, securely admitting new group members and supporting secure group communication.

Secure data aggregation:

To avoid excess amounts of traffic, the sensed values [47] must be aggregated back to the base station. As for example the system may calculate the average the temperature of a geographic region. With the help of removing redundant data, data aggregation [52] can greatly help to reduce energy consumption. In general [53], when designing a secure data aggregation protocol, the primary objective is to devise a secure aggregation function that computes the data aggregates securely and the secondary objective is to ensure that other than the sink and the sources, intermediate nodes should not have any knowledge of the raw data or the aggregation result.

Intrusion detection:

Intrusion detection [47] as it applies to detecting attacks on the sensor network itself. Wireless sensor networks are vulnerable to many forms of intrusion.

CONCLUSION

Most of the attacks and challenges and defense mechanisms that exist in wireless sensor network are represented in this paper. Security Attacks are categorized based on different layering of network where the attack exists. Some of security attacks are common in different layers of protocol stack but defense mechanisms may not always be same. The defense mechanisms are explained clearly for different layers. The study of various defense mechanisms is very much important for future research study of several security attacks. This paper of survey may help researchers to explore new and unknown types of security attacks with the help of the knowledge about existing attacks. It may also guide to develop new security schemes for wireless sensor network.

REFERENCES

[1] Yuck, J., Mukherjee, B., & Ghosal, D. "Wireless sensor network survey", Computer networks, 52(12), 2292-2330 (2008).

[2] Dargie, Waltenegus W., and Christian Poellabauer, "Fundamentals of wireless sensor networks: theory and practice". John Wiley & Sons, (2010).

[3] Methley, Steve, "Essentials of wireless mesh networking", Cambridge University Press, 2009.

[4] Virmani, Deepali, et al., "Routing Attacks in Wireless Sensor Networks: A Survey", arXiv preprint arXiv: 1407.3987 (2014).

[5] Kavitha, T., and D. Sridharan, "Security vulnerabilities in wireless sensor networks: A survey", Journal of information Assurance and Security 5.1 (2010): 31-44.

[6] D. Singla, C. Diwaker, "Analysis of Security Attacks in Wireless Sensor Networks", International Journal of Software and Web Sciences (IJSWS), ISSN (Print): 2279-0063, ISSN (Online): 2279-0071

[7] Prabu, M., et al., "DOS Attacks and Defenses at the Network Layer in AD-HOC and Sensor Wireless Networks, Wireless AD-HOC Sensor Networks: A Short Survey", Middle-East Journal of Scientific Research 23.5 (2015): 779-784.

[8] Mohanty, Prabhudutta, et al., "SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY", Journal of Theoretical & Applied Information Technology 13 (2010).

[9] Dhara, Buch, and Jinwala Devesh., "Denial of Service Attacks in Wireless Sensor Networks", NUiCone 2010. 2010.

[10] Mohammadi, Shahriar, and HosseinJadidoleslamy, "A comparison of physical attacks on wireless sensor networks", International Journal of Peer to Peer Networks 2.2 (2011): 24-42.

[11] Butani, Bhavana, Piyush Kumar Shukla, and Sanjay Silakari, "An Exhaustive Survey on Physical Node Capture Attack in WSN", International Journal of Computer Applications 95.3 (2014).

[12] Mohammadi, Shahriar, and HosseinJadidoleslamy, "A comparison of link layer attacks on wireless sensor networks", arXiv preprint arXiv:1103.5589 (2011).

[13] Shafiei, Hosein, et al. "Detection and mitigation of sinkhole attacks in wireless sensor networks", Journal of Computer and System Sciences 80.3 (2014): 644-653.

[14] Rawat, Danda B., ed. "Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications", IGI Global, 2013.

[15] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Wormhole attacks in wireless networks", Selected Areas in Communications, IEEE Journal on 24.2 (2006): 370-380.

[16] Kellner, Ansgar, Omar Alfandi, and Dieter Hogrefe, "A survey on measures for secure routing in wireless sensor networks", International Journal of Sensor Networks and Data Communications 1 (2012): 1-17.

[17] Singh, Shio Kumar, M. P. Singh, and D. K. Singh, "A survey on network security and attack defense mechanism for wireless sensor networks", International Journal of Computer Trends and Technology 1.2 (2011): 9-17.

[18] Malik, Monika, and Yudhvir Singh, "A Review: DoS and DDoS Attacks" (2015).

[19] [19] Korgaonkar, Prachi, Ashish Patil, and Nilesh Khochare, "NetSHIELD: Countermeasure Tool for Network Layer Attacks", International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) 1.8 (2012): 91-94.

[20] Maidamwar, Priya, and NekitaChavhan, "A Survey On Security Issues to Detect Wormhole Attack in Wireless sensor Network", International Journal on Ad hoc Networking Systems 2.4 (2012).

[21] Sen, Jaydip, "A survey on wireless sensor network security", arXiv preprint arXiv:1011.1529 (2010).

[22] Ghildiyal, Sunil, et al., "Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks", IJRET: International Journal of Research in Engineering and Technology: 2319-1163.

[23] Anil M. Hingmire, "Enhancing Security of Wireless Sensor Network", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013

[24] Raymond, David R., and Scott F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses", Pervasive Computing, IEEE 7.1 (2008): 74-81.

[25] Murthy, C. Siva Ram, and B. S. Manoj, "Ad hoc wireless networks: Architectures and protocols". Pearson education, 2004.

[26] Zhang, Linyuan, et al., "Byzantine Attack and Defense in Cognitive Radio Networks: A Survey" (2015).

[27] Khan, Shafiullah, and Al-Sakib Khan Pathan, "Wireless Networks and Security: Issues, Challenges and Research Trends", Springer Science & Business Media, 2013.

[28] Pathan, Al-Sakib Khan, ed., "The State of the Art in Intrusion Prevention and Detection", CRC Press, 2014.

[29] Elçi, Atilla, ed., "Theory and Practice of Cryptography Solutions for Secure Information Systems", IGI Global, 2013.

[30] Isha, Arun Malik, and Gaurav Raj., "DOS Attacks on TCP/IP Layers in WSN".

[31] Karmakar, Gour, and Laurence S. Dooley., "Mobile multimedia communications: Concepts, applications, and challenges", Information Science Reference, 2008.

[32] Zhang, Yan, Jun Zheng, and Miao Ma, eds. "Handbook of research on wireless security", IGI Global, (2008).

[33] Rahman, Nabila, Matthew Wright, and Donggang Liu., "Fast and energy-efficient technique for jammed region

mapping in wireless sensor networks", arXiv preprint arXiv:1401.7002 (2014).

[34] Wireless Technologies: Concepts, Methodologies, Tools and Applications:Volume 1, Management Association, Information Resources, IGI Global, 31-Aug, (2011).

[35] Zhu, Yanmin, Xiangpeng Li, and Bo Li, "Optimal Adaptive Antijamming in Wireless Sensor Networks", International Journal of Distributed Sensor Networks 2012 (2012).

[36] Nielsen, Hanne Riis, and Dieter Gollmann, eds., "Secure IT Systems": 18th Nordic Conference, NordSec, Ilulissat, Greenland, October 18-21, Proceedings. Vol. 8208. Springer, (2013).

[37] Zurawski, Richard, ed., "Embedded systems design and verification", CRC Press, (2009).

[38] Guo, Qin, et al., "Secure network coding against wiretapping and Byzantine attacks", EURASIP Journal on Wireless Communications and Networking 2010 (2010): 17.

[39] Kai Xing, ShyaamSundharRajamadam Srinivasan, Manny Rivera, Jiang Li, Xiuzhen Cheng, "Attacks and Countermeasures in Sensor Networks: A Survey", Springer, (2005).

[40] Kuorilehto, Mauri, et al., "Ultra-low energy wireless sensor networks in practice: Theory, realization and deployment", John Wiley & Sons, (2008).

[41] Basagni, Stefano, et al., eds., "Mobile Ad Hoc networking: the cutting edge directions", Vol. 35. John Wiley & Sons, (2013).

[42] Pareek, Anamika, and Mayank Sharma, "Detection and Prevention of Sybil Attack in MANET using MAC Address", International Journal of Computer Applications 122.21 (2015).

[43] Yang Xiao, Hui Chen, Frank Haizhon Li , "Handbook on sensor networks", Singapore:: World Scientific, 2010.

[44] R Sowmya1, Mrs. Shoba, Detection and Prevention of Misdirection Attack by Third Party Monitoring in WSN, International Journal of Research In Science & Engineering, Volume: 1 Special Issue: 2.

[45] Wood, Anthony D., and John Stankovic, "Denial of service in sensor networks", Computer 35.10 (2002):54-62.

[46] Wahid, Abdul, and Pavan Kumar, "A Survey on Attacks, Challenges and Security Mechanisms in Wireless Sensor Network", International Journal for Innovative Research in Science and Technology 1.8 (2015): 189-196.

[47] Rathod, Vishal, and Mrudang Mehta, "Security in wireless sensor network: a survey", Ganpat University Journal of Engineering & Tech., 1.1 (2011): 35-44.

[48] Chaudhari, Ms Nimisha Chunilal, "Key Management in Wireless Sensor Network A Survey", International Journal of Application or Innovation in Engineering & Management (IJAIEM).

[49] S. Dhawale, Dr. B.G. Hogade, "Node Authentication for Wireless Sensor Network Security", ", Volume 5, Issue 3, International Journal of Advanced Research in Computer Science and Software Engineering, (2015).