IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 4, Ser. 2 (Jul. – Aug. 2024), PP 01-07
www.iosrjournals.org

Wireless Sensor Networks: Current State and Security Issues

Chukwu Jeremiah[1*], Igwe Sylvester Agbo[1] and Ugwu, G.E.[1]
Department of Computer Science, Ebonyi State University
Abakaliki, Nigeria
**chukwu.jeremiah@ebsu.edu.ng*

Abstract— *Wireless Sensor Network (WSN) is an emergent and fast growing technology that proves great in the future age of computing applications. WSNs are employed in various areas of human endeavour and high risk environments such as health sectors in monitoring patient medical history, military force applications deployed in battleground, environmental or ecological monitoring in oil and gas industries, factory monitoring and agricultural or farming monitoring. Because of the sensitive nature of message or information that these applications are meant to monitor such as tracking of adversary in battleground or monitoring of patient in health care, security is then vital in Wireless Sensor Networks. WSNs struggle with lot of constraint in computation capability, low memory capacity, limited power resources, vulnerability to physical seizure, and enclosure of wireless communication device also incurs many kinds of security threats. In this paper, security requirements/goal, sensor network security challenges, wireless sensor networks security threat model were discussed. Also, WSNs threat model based on attacker tools, sensor network protocol stack attacks and countermeasures in wireless sensor networks were covered.*

Keywords- *Wireless Sensor Network, WSN, Security, Threat, Challenges, Countermeasures*

Date of Submission: 01-07-2024 Date of Acceptance: 11-07-2024

I. INTRODUCTION

Owing to the recent advancement in wireless network systems and digital electronics communication, network systems are gaining more interest both in academia, government and professional bodies because of their attributes such as low-priced, low energy consumption, limited bandwidth as well as diverse sensors applications nature with no human attendant. These wireless sensors are miniature in size, capable of sensing, capturing and processing data and also communicating with all others over a radio frequency [1]. These sensor networks are patterned to perceive, collect data from the immediate surroundings and based on their intelligence, they are able to communicate the sensed information to the users.

Wireless Sensor networks proffer self-supporting responses for a diversity of applications. For instance, deployment in military operation such as tracking of terrorist, and civilian like factory instrumentation monitoring, detection of industrial level of pollution, highways and major roads traffic. Other applications include habitat and ecosystem monitoring, seismic monitoring, health monitoring, emergency service, monitoring of industrial processing, surveillance and security and weather control [2]. These networks exhibit some attribute of ad hoc wireless network, but also have features that give it unique nature when compared with ad hoc or mesh network. These characteristics are sensor network deployment pattern, which is either crowded or sparse deployment, waning owing to topology change at regular basis and low energy consumption, low transmission power, etc [3]. Sensor networks are designed for mission-critical tasks and therefore require security consideration.

Based on the wide range variety of application areas of wireless sensor network, there is need for thorough research on Wireless Sensors Networks (WSNs) concerning hardware and software architecture, information management system, distributed algorithms and security. Currently, WSN is threatened by issues of security as this was previously seen as insignificant at the early stage of development [4]. However, its security has grown into a pertinent issue in different WSN applications because of its deployment in mission-critical areas.

In this research work, we discuss security requirements/goal, challenges facing sensor network in terms of security and consider also WSNs security threat model and tools used by the attackers. Finally, we considered Security countermeasures against attacks and conclude.

II. SECURITY REQUIREMENTS/GOAL

The aim of security services in Wireless Sensor Networks is to guard the data or information and resources from

attacks either from insiders or outsiders and misconduct. The security requirements in Wireless Sensor Networks comprise [5]:

- Availability of service: This service ensures availability of Network/system even if security issues raises via denial of Service attacks. This will be determined by appropriate management and control of network resources, access control and other security services.
- Authorization: This ensures that information provided to the network services are only accessed by authorized sensors
- Authentication: This ensures that the transmission from one sensor node to another sensor node is authentic. This is to avoid a malicious node from masquerading themselves as a trusted sensor network node

Sponsored by Ebonyi State University TETFUND Project

- Confidentiality, which ensures the secrecy of the message, that is to say, any given message can only be accessed by anticipated recipient
- Integrity: This ensures that message transmitted from one sensor node to another are not altered or modified by malicious intermediate sensor nodes at the course of transmission
- Non-repudiation: This prevents any form of denial either from the sending node or receiving node of transmitting a message.

- Freshness: This denotes that the information or data is new and as a result no enemy can rerun old messages

Furthermore, it is recommended that forward and backward confidentiality be considered as new sensor devices are developed and deployed and also as older sensor devices failed.

- Forward secrecy: A wireless sensor device should not be capable of interpreting any communication or message once it has left the network
- Backward secrecy: Any wireless sensor joining the topology or network ought not to read any earlier message broadcast.

The wireless sensor networks (WSNs) security services mostly focus on cryptography. Though, because of restriction in WSNs, secure algorithms existing in many are unusable.

III. SENSOR NETWORK SECURITY CHALLENGES

Wireless Sensor Networks (WSNs) are associated with a sole security challenge because its security architecture is quite different from conventional networks; as a result the same security procedure for traditional network cannot be used [6]. WSNs are limited in their power as it is supplied by a battery, sensing capabilities, transmission and computation capabilities. Other security challenges in WSNs are mode of operations, that is, they operate in real-time mode, have ability to change topology dynamically, the entire actions of all sensor nodes is relevant as against a wired network where all the nodes are also important, deployment location for sensor networks are critical, when compare to wired network that are site independent and WSNs make use of actuators and sensors as nodes interfaces. Also WSNs transmit information wirelessly connecting electronic devices, are self-organizing, adaptive and heterogeneous in nature and deployed in an ad-hoc manner [4], [7].

More particularly, the characteristics of wireless sensor networks present several related challenges: The issue of coverage is of essence when assessing the effectiveness of the WSN in a designated area. Coverage exposes how the deployed nodes can oversee a set of target area. Target tracking application may have need of higher degree of coverage for adequate tracking of the target correctly while environmental application can accept a lower degree of coverage and mobility in WSNs, which the distance of the nodes are capable of occupy within a given time [8], [9].

These attributes contain quite a lot of vulnerabilities of wireless sensor networks, which can result to threat and when this threat occurs, they are seen as attacks.

IV. WIRELESS SENSOR NETWORKS SECURITY THREAT MODEL

Wireless sensor networks are vulnerable to security threats and attacks because of the deployment of these sensor nodes in a critical environment and their wireless nature of communication channel or medium [10]. Furthermore, WSNs hackers can induce a malicious node with comparable hardware competences or capabilities as the genuine sensor node and also the adversary can manipulate legitimate sensor nodes to act as threat agents. The attackers can instill false messages, which will result to waste of sensor networks memory or resource. Therefore, security threat in WSNs needs an attention. In this section, we propose to discuss classifications of security attacks, which include: insider or misfeasor, masquerader/imposter or outsider and Clandestine or secret users and we consider security threat models in WSNs application.

A. WSNs Threat Model Based on Attacker Tools

Security Attackers are people who attempt to gain unauthorized access to secured system or network by taking advantage of a security flaws. They security attacks can be classified as in [11], [12].

- **Insiders:** are node attackers that are given legitimate access to sensor network and also have right to one or more organizational asset structure but accesses nodes resources for which such access is not authorized. These insiders sometimes are people who abuse or misuse access right by impersonating privileged high ranking officer. An insider is also known as misfeasors.
- **Outsider or masquerader:** these are node attacker that takes access privileges of authorized WSNs user and pose as that WSNs user to attack the sensor network.
- **Secret or Clandestine User:** These WSNs node attacker are either insiders or outsiders who gain their individual separate unauthorized WSNs access to a node. For instance, hackers who gain administrative privilege to a node long enough to generate their individual user accounts.
- **Passive attacks:** involves node attacker monitoring or eavesdropping on sensitive information that is being transmitted with a WSNs.
- **Active attacks**: is the act of node attackers modifying some of the data stream or fabrication of a false stream.
- **Mote-Class Attacks:** The attacker attacks a wireless sensor networks by using a few sensor nodes with comparable capabilities to the nodes.
- **Laptop-Class Attacks:** The adversary attacks the nodes using more powerful electronic devices, with high transmission range, energy reservation, sensitive antenna such as laptop, iPad, etc to bout WSN nodes.

B. Evaluation

The appropriateness of any security implementation in Wireless Sensor Networks needs to be based on evaluation metrics suggested below

- Security: security requirement outlined above has to be met.
- Resiliency: security scheme have to be capable of protecting another node in the event of compromise in any of the nodes.
- Energy efficiency: The security schemes have to be effective in maximizing the energy in the node and sustain the sensor network life cycle. In other words, energy-efficient nodes must be considered while planning, designing, installing and deployment of wireless sensor networks.
- Flexibility: flexibility in key management is essential to allow for diverse network deployment approaches.
- Scalability: the security plan should be in such a way that increases in the number of nodes does not compromise the security requirements.
- Fault-tolerance: sensor nodes should be able to provide adequate security services even in the midst of compromised nodes.
- Self-Organizing: sensor nodes should be capable of utilizing their self-organizing functionality to maintain security level in case of failed node or power depletion in the node.
- Assurance: is the ability to broadcast diverse information at different levels to nodes with guarantee that each node claims is right. Network performance criteria is of essence in security scheme with respect to availability, utilization, latency, response time, etc

C. Sensor Network Protocol Stack Attacks Most Wireless Sensor Networks architecture follows the OSI Model. We will discuss attacks on the first four network architecture [13].

1) Physical Layer attack: Most Wireless Sensor Networks, when compared with traditional networks are more susceptible to threats in physical layer because of the wireless medium of communication and non-tamper resistant wireless sensor networks node [12]. The two common attacks in the Physical layer are jamming and tampering [13].

Jamming**:** Jamming occurs when an attacker or adversary block or interfere with the radio frequencies (RF) signals or bypass the MAC layer protocol that legitimate network nodes are using [14]. If the attackers succeeded in disrupting the whole network, then denial of service of either transmission or reception node functionalities will occur. In this case, the jamming resource or source is termed to be powerful. Also when the jamming sources are distributed haphazardly in the network nodes even with lesser powered jamming resources such as injecting immaterial or irrelevant information, the attackers have the potential to interrupt the entire or whole network. The defense against physical layer jamming involves the use of spread spectrum. This makes it complex for capturing and jamming to occur and also provides enhanced reception [11].

There are difference spread spectrum communication technique for defense against jamming such as frequency- hopping spread spectrum (FHSS) and Code Spreading [15]. FHSS is the type of spread spectrum in which the signals are transmitted or broadcast by quickly switching the carrier frequency between many channels at fixed intervals known to both receiver and transmitter. Without the frequency channel following a given selection sequence, an attack is incapable of jamming the frequency channel used in the transmission at any given fixed interval and also when a part of the sensor network is affected by jamming, a sensor network with jamming resistant could conquer the attack by sensing the jamming, mapping the region affected, and then routing around the jammed region [6]. However, frequency band limitation is a challenge because an attacker may decide to jam a wide unit.

Code spreading on the other hand is a spread spectrum communication technique used to protect against jamming attacks in mobile networks. The use of this technique is restricted in Wireless Sensor Networks because of its high design complication and energy or power requirement. Wireless sensor devices are restricted to single frequency usage, since it has to maintain low energy and cost requirement. Hence, making it highly vulnerable to jamming attacks [13], [15].

Tampering: Sensor nodes are vulnerable to physical tampering, especially when involved in a network that covers a massive or large environment. A physical tampering attacker may possibly impair a sensor, alter the node, replace the whole node or change hardware component of the nodes. In addition, an attacker or adversary can access sensitive data such as shared cryptographic keys and other information on communication protocol layers. The standard defense to tampering attack is to implement tamper proofing on the sensor node [12].

2) Data Link Layer: The data link layer is the second layer of the Wireless Sensor Network OSI layers. This layer is accountable for the multiplexing data streams, medium access control, detection of data frame, and control of errors, ensures dependability in a network communication such as point-to-point, point-to-multipoint connection [3]. There are three major types of attacks associated with data link layer such as collisions, exhaustion and unfairness [13].

Collision: Collisions are type of jamming in data link layer. It happens when two sensor nodes tries to transmit signals concurrently on the frequency channel resulting to packet collision. This packet collision can cause change in any portion of the data or corrupt the signal transmission, thereby causing a mismatch in the checksum at the receiver's end and disruption of the entire packets. An adversary or intruder may tactically cause collisions in particular packets such as Acknowledgement (ACK) control messages leading to costly exponential back-off in specific MAC (media access control) protocols. Furthermore, an intruder may possibly deny access to a frequency channel deliberately because of compromised node [13], [16].

Xiangqian, *et al* [17] recommend using error-correcting codes, code detection mechanism and time division multiple access as a defense against collision attack in link jamming even though it has limitation in its defense mechanism.

Exhaustion: This is another form of attack in link layer where attacker aimed at exhausting the power or battery resources of the node by keeping the channel busy. This happens when an attacker implement a naïve link layer in the node to retransmit corrupt packet [17]. A difference or variation of this type of attack is when a self- sacrificing sensor node unceasingly asks for access to a channel, compelling its neighbors to act in response to a 'clear to send message' [12], [4].

The standard solution to exhaustion attack is to set rate boundary or limit to the Media Access Control admission control such that the sensor network can overlook too much requests, thereby preventing the power depletion caused by frequent transmissions and next technique is the use of time division multiplexing to resolve frame intercession and also handle indefinite delay issue in a back-off algorithm.

Unfairness: occurs when there is degradation in the network performance because of abuse of the MAC priority schemes or disruption in line with the application requirements [4]. In the form of attack, the attacker does not prevent access to the sensor network service completely but instead uses degradation of service to gain an advantage leading to loss of real time communication deadlines. Small frames are ideal for defense against this attack

3) Network layer: This layer is responsible for protocol routing involving sensor node to sensor node, sensor node to sink node via network and also act as pathfinder for effectual routing mechanism [24]. The network layer has many challenges such as power saving, memory limitation, and buffers. This is different from computer networks with internet protocol and routing device for controlling. The threats and attacks associated with this layer are spoofing, alteration or replayed information; Sybil attacks; sinkhole attacks; selective forwarding; hello flood attacks; wormholes; and acknowledgement spoofing [13].

Spoofed, altered or replayed routing information: Most attack on routing protocol in any sensor network is achieved by aiming the routing information being exchanged or swapped between nodes. Here, the adversary can interrupt the network traffic [17] by creating routing loops, magnetizing or repulsing traffic from choice nodes, generating fake error messages, shortening or extending source paths/routes or partitioning the

network partition, and increasing of latency at end-to-end nodes.

A standard defense against spoofed, altered, or replayed routing information is to add a message authentication code after the message. This will help the sensor node receivers to authenticate the message for spoof or alteration. Counters or timestamps can be involved in the message to defend against replayed routing information [18].

Selective Forwarding: In selective forwarding, it is presumed that the participating nodes in multi-hop networks will reliably forward receive messages. The adversary nodes may decide not to forward certain message or packets but selectively forward only some message and drop others and in some cases, it might decide to drop all the received packet, thereby [17] causing routing black holes within the network [4].

Sinkhole Attacks: This another form of attack on the network layer of sensor network protocol stacks. This attack is aim at baiting traffic to a compromise node. This is achieved by making a compromise or malicious node look alluring to it surrounding nodes by falsifying routing packet [4, 14]. The malicious node publicize a high quality (or low latency) routes and deceived genuine neighbor nodes into forwarding their packets meant for the base station to the lying or deceitful node. This creates a sinkhole in the sensor network. This attack is possible because of their communication patterns, multi- hopping nature of transmission and it also simplify selective forwarding attacks in the network as the whole packet intended for the base station flows via the malicious nodes [11].

Sybil Attack: In Sybil Attack, the malicious node poses manifold identities to the network nodes [19], thereby confusing routing protocols of the network applications as the adversary appear in multiple site at once [4]. This attack aimed at reducing fault tolerant schemes effectiveness such as distributed storage, disparity, multipath routing, and network topology maintenance [13].

Wormhole Attacks: In this type of attack, the adversary channels information accepted in one part of the network over a high quality (low latency) link for the message to be replayed in another part of the network. This form of attack arises when a malicious node is forwarding or transmitting packet between two genuine nodes. Also wormhole attack persuades remote node that they are neighbors, therefore causing rapidly depletion of their energy resources via routing. For example, wormhole attacker that is near base station (BS) to can convince legitimate node that are many hops away that they are couple of away from the BS. When this attack is jointed with Sybil and selective forwarding, it will be very difficult to detect. [4], 13]

Hello flood attacks: In these form of attack, the adversary nodes uses hello packet in many routing protocol to broadcast their presence to their surrounding environment or neighbors. A node receiving such a package or message can presume that the node transmitting the message is within its span. An adversary with a high powered antenna can convince nodes of being neighbors in the same network and also with advertising or publicizing high quality route to the BS (Base Station); it can trick nodes to forward messages to it. Routing protocol that rely on limited data exchange connecting neighboring nodes for topology maintenance are victim of this attacks [20].

Acknowledgement Spoofing: Wireless Sensor Networks that uses routing protocol algorithms depend on understanding of the data link layer acknowledgement. An intruder or adversary can spoof the acknowledgements for eavesdropped packets addressed to adjacent node, thereby convincing the transmitting node that a feeble link is strong or that a dead node is active or alive. This attack is seen when protocols chooses the next hop based on reliability link [13].

4) Transport layer: This layer is responsible for overseeing end to end connection. There are two forms of attacks that are possible in the transport layer, flooding and desychronization [17].

Flooding: each time there is need for a protocol to maintain state at each connection end, it will turn out to be susceptible to memory depletion or exhaustion via flooding [wood]. An adversary may possibly make fresh or new connection demands frequently in an attempt to exhaust each connection resource making the node unresponsive to legitimate requests by ignoring the traffic. Flooding is similar to TCP Synchronize (SYN) attacks where an adversary sends a lot of connection establishment demand or request, thereby depleting memory resources of the victim [21].

The defense against flooding demands that clients demonstrate the allegiance of their individual resources to every connection by solving client puzzles [22].

De-synchronization: is the disruption of existing connection between two end points. In this form of attack, the adversary falsifies information between transmitter or sender and receiver, altering control flags and sequence numbers in the packet header. If the attackers timing is right, then the sender and receiver might be restricted from ever interchanging information, causing that host to request the retransmission of missed or invalid frames. Countermeasure to this attack is to authenticate packet before transmission including all control flags/fields in the protocol header [17], [4].

V. COUNTERMEASURES

At the present, we have the background description of the vulnerabilities and security threats of

wireless sensor networks. Here, we will discuss some countermeasures to the security threats [14].

Jamming: There are a lot of shortfalls solutions to the problem of physical jamming. The use of spread spectrum communication may be an impermanent countermeasure pending when the jammers find out the follow the hopping sequence or how to block a broaden part of the frequency range.

Code spreading: This problem of code spreading can be resolved by applying comparable principle in mobile phone. That is to say, code spreading similar to the one used in mobile phone system may solve the problem but then, it will need extra design effort, energy and cost. Changing or altering the communication mode to optical or infra-red may work nevertheless is expensive or costly. There is also need for nodes under jamming attacks to notify other surrounding nodes during the jamming gap especially the base station about the situation [13].

Tampering: The model countermeasure to tampering is to provide tamper resistant packaging [13]. This method is implemented during design time and is quite expensive, if to be considered. Camouflaging of sensor nodes is also another way of programming the sensor nodes in such a way as to erase sensitive data upon captured [23].

Collision: For defense against collision attacks, the following are the likely solution: error correcting codes, collision detection, diversity and cyclic redundancy checks [23].

Unfairness: The countermeasure is to use small frames to prevent the transmission channel from being attacked or captured for a long period of time. An adversary can trick other nodes by responding quickly when requiring access whereas other sensor nodes delay [23, 17].

Exhaustion attack can be prevented using time division multiplexing (TDM) to resolve the issue of indefinite delay or postponement that occurs during collisions [23]. Also, Media Access Control admission control use is in the link layer to ignore too much requests without sending packet [7].

Spoofed, altered or replayed data: To defend against message spoofing, altering or replaying, encryption and authentication of link layer is required. Also, resending of failed packet through different routes can work [17].

Other countermeasures are summarized in the table I below

TABLE I
SENSOR NETWORK LAYERS AND DoS DEFENSES [12].

Network	**Attacks**	**Defense**
Network and Routing	Spoofed, altered or replayed data	Egress filtering, authentication, monitoring
	Selective forwarding	Redundancy, probing
	Sinkhole	Authentication, monitoring, redundancy
	Sybil	Authentication, probing
	Wormholes	Authentication, packet leashes by using geographic and temporal information
	Hello flood attacks	Authentication, verify the bidirectional link
	Acknowledgment spoofing	Authentication
Transport	Flooding	Client puzzles
	Desynchronization	Authentication

VI. CONCLUSION

This survey work provides a good understanding of the security challenges facing deployment of Wireless Sensor Network in different application areas and the dire need to begin implementing security at design time in sensor networks. This paper introduce wireless sensor network, the security requirements/goal, sensor network security challenges, wireless sensor networks security threat model and also discuss WSNs threat model based on attacker tools. Classifications of attacks based on sensor network protocol stack model were touched. We covered countermeasures in wireless sensor networks and defense against those attacks. Although, countermeasures have been implemented to combat the issues of vulnerabilities in Wireless Sensor Networks but no particular measure dealt with all the attacks and threats. Hence, the need to design and implement a single protocol such as enhanced, improved IPSec and SSL to handle the entire security challenges as in the case of wired networks.

REFERENCES

[1]. M. Haenggi, Opportunities and challenges of wireless sensor network. In: Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, USA: CRC Press LLC, 2005.

[2]. C.F. García-Hernández, P.H. Ibarguengoytia-Gonzalez, J. García-Hernández and J.A. Pérez-Díaz, "Wireless sensor networks and applications: A survey", IJCSNS International Journal of Computer Science and Network Security," vol. 7, no. 3, pp.264-273, 2007.

[3]. Y. W. Law, S. Dulman, S. Etalle, and P. Havinga, Assessing security-critical energy efficient sensor networks. In: Sensor network operations. Canada: Wiley & Sons, Inc., 2006.

[4]. K. Koffka, G. Wayne, and R. Diana "Security in Wireless Sensor Networks," Global Journal of Computer Science and Technology Network, Web & Security, vol. 11, no. 16, pp. 43 -50,2012.

[5]. S. William, Network Security Essentials: Applications and Standards. 4th edn. USA: Pearson Education, Inc., 2011

[6]. Sora, "Security Issues in Wireless Sensor Networks," International Journal of Online Engineering (iJOE), vol. 6, no. 4, pp. 26-30, 2010.

[7]. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," In Communications of the ACM (CACM), vol. 47, no. 6, June 2004.

[8]. J. H. Li and M. Yu, "Sensor coverage in wireless ad hoc sensor networks", International Journal of Sensor Networks, Vol. 2, Nos.3/4, pp. 218 - 229, 2007.

[9]. X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated coverage and connectivity configuration in wireless sensor networks", in: Proceedings of the First International Conference on Embedded Networked Sensor Systems (Sensys), Los Angeles, CA, 2003.

[10]. A.K. Pathan, H. Lee, and C.S. Hong, "Security in wireless sensor networks: Issues and challenges", Advanced Communication Technology, 2006. ICACT 2006. the 8th International Conference, IEEE, paper 6, pp.1048, 2006.

[11]. W. Stallings, Network security essentials: Applications and standards. 4th ed., USA: Pearson Prentice Hall, 2011.

[12]. W. Yong, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks", Communications Surveys & Tutorials, IEEE, vol. 8, no. 2, pp.2-23, 2006.

[13]. S. Kaplantzis, N. Mani, M. Palaniswanmi, and G. Egan, "Security models for wireless sensor networks", PhD Conversion Report, Centre of Telecommunications and Information Engineering, Monash University, Australia, pp. 1- 41, 2006.

[14]. S. Singh, and H.K. Verma, "Security For Wireless Sensor Network", International Journal on Computer Science and Engineering (IJCSE), vol. 3, no. 6, pp. 2393 – 2399, 2011.

[15]. R. Roman, J. Zhou, and J. Lopez, On the security of wireless sensor networks, in International Conference on Computational Science and Its Applications – ICCSA 2005, Lecture Notes in Computer Science. Springer Verlag, Heidelberg, D-69121, Germany, 2005, vol. 3482, pp. 681–690.

[16]. S. Yan-qiang, and W. Xiao-dong, Jamming attacks and countermeasures in wireless sensor networks, in Anonymous Handbook of research on developments and trends in wireless sensor networks: From principle to practice, IGI Global. pp. 334-352, n.d.

[17]. C. Xiangqian, M. Kia, Y. Kang, and P. Niki, "Sensor Network Security: A Survey", IEEE Communications Surveys & Tutorials, vol. 11, no. 2, pp52-73, 2009.

[18]. Koubaa, M. Alves, and E. Tovar, "Lower Protocol Layers for Wireless Sensor Networks: A Survey", IPPHURRAY Technical Report, HURRAY-TR-051101, 2005.

[19]. Hamid, and C.S. Hong, "Defense against lap-top class attacker in wireless sensor network", Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, IEEE, paper 5, pp. 318, 2006.

[20]. C.L. Schuba, I.V. Krsul, M.G. Kuhn, E.H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on TCP", Security and Privacy, Proceedings., 2007 IEEE Symposium on, IEEE, p208-223.

[21]. Y. Jennifer, M. Biswanath, and G. Dipak, "Wireless sensor network survey", Computer Networks, vol. 52, no. 12, pp. 2292- 2330, August 2008

[22]. H.K. Kalita, and A. Kar, "Wireless sensor network security analysis", International Journal of Next-Generation Networks (IJNGN), vol. 1, no. 1, pp.1-10, 2009.

[23]. A.S. Sastry, S. Sulthana, and S. Vagdevi, "Security threats in Wireless Sensor Networks in each Layer", International Journal of Advanced Networking and Applications, vol. 4, no. 4, pp.1657- 1661, 2013.