Comparative Study of Security Attacks on Wireless Sensor Networks

Muhammad Ahsan Raza[1], Binish Raza[2] and Anum Aftab[3]

[1]Institute of Computing, Bahauddin Zakariya University, Multan, Pakistan
[2]Department of Electrical Engineering, Pakistan Institute of Engineering and Technology, Multan, Pakistan
[3]Department of Computer Science and Engineering, UET, Lahore, Pakistan
ahsan_0136@yahoo.com[1], binish155@yahoo.com[2], anumafab772@gmail.com[3]

***Abstract*– Today, the growing interest for usage of ubiquitous services is a call for advanced researches in the emergence of 'Wireless sensor network (WSN)'. This is the key tool that supports various ultramodern applications. In every network security is the main challenge. The security measure for WSN is important dispute due to its unmonitored deployment nature and its inherent resources limitation. Wireless Sensor Network is sometime used in very sensitive fields such as healthcare, military and airports. Therefore the addressing of security issues of network is most challenging task. Due to limited resources of sensor nodes, the security in Wireless Sensor Network is more difficult to implement as compared to other traditional networks. Today huge research is going on in the field of security. Various techniques are now deployed to resolve the security issues. But still there is no appropriate corrected solution against some of them. This paper provides a comprehensive study of linked but seemly unlinked security issues, requirements, attacks on WSN and also present a simple yet effective salt based encryption methodology with perfect blend of randomness to achieve security in wireless sensor network.**

***Keywords*– Wireless Sensor Network, Security and Encryption**

I. INTRODUCTION

Wireless Sensor Network (WSN) [1] is considered to be the key technology to support the various current and future technologies. WSN is a gigantic area of dynamic research including data management, distributed algorithms, programming models, hardware and system design networking and security and social factors [2]. It is more valuable in several applications because it give a very low cost solution to many problems in real life. Due to deployment in hostile and unmonitored environment, it is highly susceptible to security attacks than simple wireless and other traditional wired infrastructure networks.

The susceptible variety of security attacks includes denial of services, physical tampering, altering and capturing of data by eavesdropper during transmission of data between sensor nodes. These susceptible attacks lead to the research challenges in the field of security. Most applications of wireless required same security as the traditional networks require. Cryptography is the standard method to provide security, which also used in WSN. But for WSN success the conventional security methods cannot be useful, because of sensor's limitations and restrictions in its resources. Without effective security techniques WSN gives undesirable and disaster results. Although the great progress in security fields, the security problem is still remaining. Such as the key management techniques provide confidentiality and integrity at one layer but security can breach at any layer in network during communication [3].To completely secure the WSN security must be applied on each node in the network.

In this section we describe a brief introduction to WSN and its security. In next section II we preset the model of WSN. In section III we discuss the numerous issues relating to security and its challenges in WSN and give a comparative overview of several security attacks that are susceptible to WSN. In section IV we mapped various security attacks on different layers on WSN protocol stack. In next section V, we present our simple propose algorithm to implement security in WSN. In last section VI, we conclude our result.

II. WIRELESS SENSOR NETWORK

A wireless sensor environment constitutes a huge figure of sensor nodes that are scattered in a network fashion. WSN is used for numerous mechanisms in which sensing is involved. Sensor nodes are low cost and small size devices that are used for sensing the surrounding environment [4]. These sensor nodes can sense many parameters such as light, humidity, vibration, etc. Its low cost and low power energy consumption facilitate its deployment in various types of surroundings and areas. Example including terrestrial, underground, underwater, military sensing and tracking, patient monitoring and healthcare centres [5].

The network design of these nodes are according to the requirement of application and environment ,but the key challenges of network design is its limited resources such as limited memory capacity, computation ability, energy source and communication bandwidth . Reporting about data collection of earthshaking, environmental observation and forecast system, sensing fault in building construction or automobile and aircraft and a range of smart and intelligent systems are different applications of sensor networks.

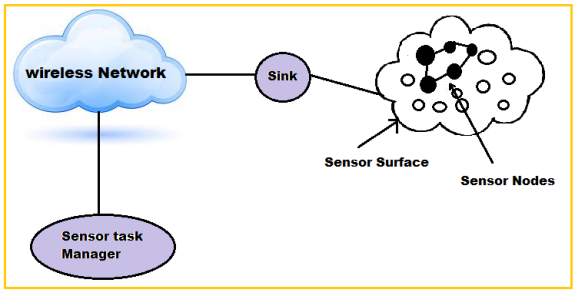

Fig. 1. Sensor Network Design

III. SECURITY OF WIRELESS SENSOR NETWORK

WSN are more susceptible to security attacks due to its deployment in unmonitored environment and its broadcast nature. The security issues, requirement and attacks are discussed as follows:

A. *Security Issues*

WSN are deployment in unmonitored environment therefore the sensor nodes are more vulnerable and physically open to attack. As the amount of nodes installed in an area is enormous on one side implies that they must be low cost but this feature on other side create complexity for manufactures to build nodes able to tolerate ruthless environment. Hence sensor nodes are exposed to the attacker to take over the control untraceably and cryptographic keys are compromised.

The security issues for WSN are as follows [6]:

Limited Resources

A certain amount of data memory and battery energy are needed, to implement all types of security algorithms in sensor devices .the resources limitation can be categories as:

- *Limited memory size*

Sensor nodes have very short memory to implement a security algorithm; therefore it is important to restrict the size of the algorithm for effective security. Due to limited size it lacks the ability to create unique keys for each other node in the network.

- *Limited power*

Power consumption is the critical constraint to WSN. The limited power usage and computation is undesirable for public key algorithms. The power is conserved in deployed environment by first extended every sensor node lifetime and then whole wireless sensor environment.

There is no public-key cryptography due to the extraordinary cost of the public-key algorithms for applying on sensor nodes in the cases of energy and storage.

Unmonitored Environment

The sensor nodes are deployed in unmonitored environment therefore these are physically open to attack.WSN are broadcast in nature so it is more vulnerable to attacks such as bad weather and bushfires.

Protection on Multi-Layer

The network model consists on multiple layers so security on each layer is most important. To protect the network security must be implemented on each layer individually, because the security can breach at any level during transmission and prone to attack [7].

Different layers can be a victim of attacks for example DOS can attack on every layer because these layers are directly or indirectly exposed to different types of attacks.

Randomly deployed sensor networks imply the lack of beforehand knowledge of communication range of nodes with each other. If the deployment of nodes is done by hand, the pre-determination of the location of each node makes it expensive.

B. *Security Requirements*

To attain security for WSN these issues governed following requirements:

Confidentiality

Securing data during the transmission from one node to another node or denial of unauthorized access is a way of maintaining confidentiality of data. Illegal access to sensitive data and eavesdropping should be blocked by using encryption techniques [8].The nodes in the network should not depict their confidential data to its acquaintance. For example in forces application extremely sensitive information is transferred between nodes which can be secured by developing a specific channel for security between senders and receivers.

Routing of high sensitive data can occur by passing through many nodes before the destination point. This highlights the need of encryption of data thought out the transmission extended with the encryption of public sensor identities to protect from traffic analysis attack.

Integrity

Integrity involves affirmation that data or readings which are transferred cannot be modified by opponent. Integrity provides protection against masquerade, replay and modification of message attacks. Data integrity is fulfilled by Machine authentication code (MAC). MAC is verified on the receivers end satisfying the sender is originator of this particular message, establishes a protection against masquerade attack [7].

Authenticity

WSN has broadcasting nature of communication so the attacker instead of changing message contents can add futile packets in the original packet stream. To defend from this technique of attacker the receiver node should have an ability to control access by detecting which node is legal and which is unauthorized. And let the message of legal one come and stops the message of illegal source. Digital signature is a way to authenticate the node [9].

Data Freshness

In shared key cryptography in which keys are refreshed after a time period to provide assurance that data received is

fresh. This assures that there is no replay attack in which attacker capture a unit of data and retransmits it to create illegal access [8]. Protection from this type of attack can be attained by attaching a timestamp with the message. Comparison of clock of the receiver node and timestamp is done to identify that data received is fresh or not.

Availability

Potential of communication and computation is limited in sensor nodes so computation more than its capability results in the extra usage of energy but if there is no more energy there will be no more availability of data. Breakdown of a single node can affect the accessibility of network. Attacker can launch a energy or resource utilization attack, DOS attack and node compromise attack. Sensor nodes can use their energy in an intelligent way by acquiring a sleep mode when there is a constant state for a long time and reserve energy for cases in which more than usual computation is required.

Self-Organizing

Sensor nodes should have self-healing and self-organizing ability to adjust in their self when environment changes [9]. So, they can overcome the failure of a single node in such a way that surrounding nodes control that condition. Sensor nodes has requirement to be flexible or ductile that they can be attuned to unusual situations.

Time Synchronization

Time synchronization is required when communication takes place between two nodes. It is possible for a sensor radio to be in off state for reserving energy. So, group synchronization is essential requirement for sensor network to be more collaborative in detecting application.

Secure Localization

Different attacks are accomplished by finding the exact location of nodes in network. A search of packet headers and protocol layer data can be made by opponent. So secure positioning of nodes is required. Sensor nodes should be positioned in an accurate way by which every node in network can automatically locate the other node in wireless sensor network and point-out the exact location of fault in the whole network [10].

C. Security Attacks

WSN are exposed to various security threats, because of its broadcast feature, limited computational resources and highly constrained on energy and power. These limitations give a broad scope for attackers to attack. Attacks has two types first is passive attacks and second is active attacks.

The first type of attack can be future categories as eavesdropping on, and observing of information during transmission. The aim of opponent is to examine the whole traffic or information that is being transmitted. Active attacks can be of two types, analysis of traffic between nodes and release of message contents. In active attacks the attacker or opponent has change the contents of the message and transmitted the fake or modified message instead of original message. It can be divided into four subcategories: *masquerade, replay, modification of messages, and denial of service* [11].To secure WSNs multiple layer security is applied on each layer of networking stack. Various DOS attacks are discuss here.

Physical Attack

The physical attack is occurs on physical layer. Due to unmonitored deployment of sensor nodes it is more susceptible to physical attacks. The attackers can access the source code which gives the information about the network. Attacker can change this source code according to its attacks requirements and can enter into network. By this way the attacker can destroy the sensor nodes physically that is a nonreversible process. The main physical attacks can be spoofing, eavesdropping, jamming, node replication attack etc [12].

Jamming

Jamming attacks can be described as the radio signal that interfere the communication and attempting to interrupt in physical layer [13]. There are two types of jamming .Constant jamming influence the whole network, while in intermittent jamming the sensor not can communicate by exchanging data periodically but not constantly. Attackers can capture the source code and then alter its content and get the permission for entrance to the system. After getting access to system the attacker could take the position of authenticate node by using false or illegal identity that negotiating the entire network.

Collision

Collision can happen when two communicating nodes exchange the data simultaneously at the same frequency. This type of attacks decreases the efficiency of network. An attacker can attacks by colliding certain packets during the transmission. The lost packets are transmitted again which cause decreases in network efficiency by increases the time and energy cost of transmission. The collision attack is occurring on data link layer [13].

Exhaustion

In this attack the attacker nodes transmitting messages again and again even if no or delayed collision occurs. This takes over the energy resources and decreases the efficiency. This attack takes place on link layer of network [14].

Negelct and Selective Forwarding Attack

In WSN multi-hop transmission is commonly used. During the transmission between the two nodes, there are number of nodes between them through which the packet is passing before reach to destination. During this transmission some packets become lost and dropped, or selective packets forward by mysterious party to a wrong node. This attack causes problem for the nodes who received wrong messages, or waiting for messages. This attack is taking place on network layer [15], [16].

Attacks on Homing Network

The attacker examine the load of traffic on network at network layer to identify the critical nodes .then the attacker apply some other security attacks on the critical nodes that completely destroy it physically which also damages the network [14] .

Alteration of Information (Spoofing)

This is the most common attack on network layer. The attacks modify the information transmitted between sensor nodes. The modified information is related to routing decision. The information is adversely effected by modifying or replaying the message contents.WSN is susceptible to eavesdropping, therefore the opponent can easily analyze the transmission and can modify or interrupt the traffic. Due to this modification false information is transmitted to communicating nodes. One attacker adverse several sensor nodes at the same time due to limited resources and short range transmission of sensor nodes. These type of attacks create new routing paths, produce new false messages, repel or attract the traffic of network, increase or decrease the routing paths, shorten or lengthen the latency time [15].

Sink or Black Holes Attack

This attack is occurring in network layer. The attacker attracts the transmission load towards the susceptible node. This node is usually placed at the centre of traffic area. Mostly this node is placed near to the base station so that it can be seemed as a base station. These malicious nodes attract the traffic by showing zero-cost for routing to neighbour nodes or by convincing that traffic has a short link to base station .the nodes that collide to the malicious node causes destruction of message.

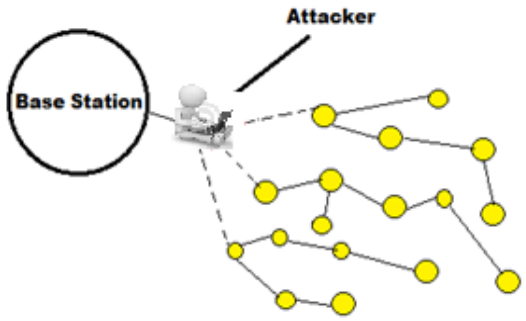

Fig. 2. Sink or Black holes Attack

This attack can be avoided by using unique key to initiate the frequency hopping and spread spectrum communication [17].

Sybil Attack

In this attack the attacker create multiple fake identities of nodes, either by stealing or producing the identities of legal nodes. By using these fake identities the attacker take position on multiple locations on the network at the same time. The attack can commonly occur on network layer [18]. This type of attack is pose important threat to the geographical routing protocols such as location aware routing protocol. In this

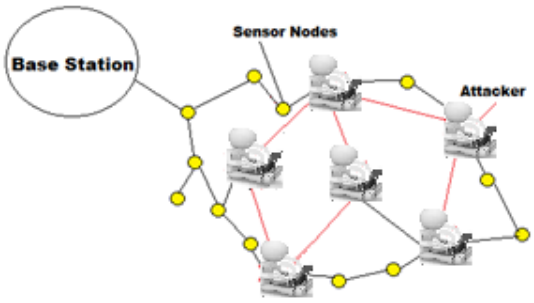

Fig. 3. Sybil Attack

protocol the communication nodes exchange information about their coordinates to design the network. So it is supposed that one node present one set of coordinates, but due to this attack multiple set of coordinates are achieved from fraud nodes.

The attack could be avoided through proper authentication.

Wormhole Attack

A low latency intersecting node among two segments of network is known as a Wormhole. The attacker firstly locates this wormhole on network layer for attack [18]. This attack is done by convincing the communicating nodes that malicious node is more close to the base station via the wormhole. In this attack the attacker node receive messages from one segment to the other segment of network. This creates a fake transmission between the legitimate nodes. The opponent that is placed near to base station can destroy routing by locating wormhole in sound place. When this attack is combined with Sybil and selective forwarding it is difficult to identify. Even if the routing is encrypted and authenticated this attack still effects the transmission.

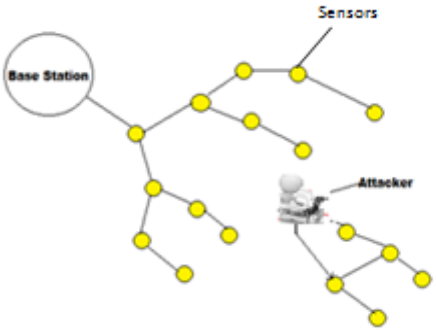

Fig. 4. Wormhole Attack

This attack can be avoided by using clock synchronization and verification of actual location.

Flood Attack by Hello Messages

This attack is occurs on network layer. In some network protocols the nodes broadcast a hello message to the network to advertise themselves to the neighbour nodes. The nodes

which receive this message may suppose that it is within the limits of sender nodes.

This Hello attack is done by the attacker convincing the other nodes that he/she is the nearest neighbour of that node towards the BS. The sensor node send packets to BS, the message pass through this malicious node that captures its required information. This effects the network efficiency and cause difficulties in the flow of data [14], [19].

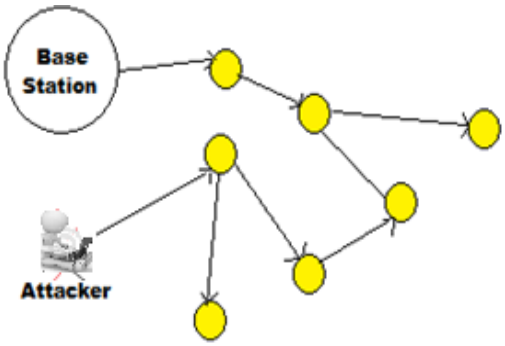

Fig. 5. Flood Attack by Hello Messages

Node Replication Attacks

The compromised node copied the legitimate node identity that is already located in the existing network. The message packets that passed through this copied identity node can be dropped, changed or misrouted. This leads to the loss of information, drop of connection and increase end-to-end suspension. These attacker nodes can get access to the more important and dedicated information which can damage the network [14].

Data Aggregation Attack

Data aggregation in sensor network is more susceptible to security attacks. The sensor nodes aggregate their data at one base station to avoid the overhead of traffic load. This aggregated data is more vulnerable to security attacks. The attacker can generate the false report or modify the data contents or affecting the whole network efficiency [20].

IV. MAPPING OF SECURITY ATTACKS ON PROTOCOL STACK

We describe mapping of each attack on different layers of wireless protocol stack in the form of Table 1.

V. PROPOSED ALGORITHM

Solution to security problem in WSN routing is to use a simple protocol with the ability of encrypting data with private key. For this little modification will need to be made to existing packet structure. This technique can be used with any kind of existing routing protocol as it only involves modification to the user data part.

Assumptions

It is assume that every node of the network is running some OS with same encryption method. All the nodes are known by the base station. All nodes receive some kind of programming before being deployed. Data for one node is not used in processing in some other node but only in base station. All the nodes can easily be uniquely identified wither by a MAC address, an IP or some serial number. This unique ID is transmitted in every packet.

Table 1: Mapping of Security Attacks on Layers of Protocol Stack

Layers of Protocol Stack	Attacks	Protection measures
Physical Layer	Jamming, Node Replication	Temper-proofing, Spread Spectrum, hiding, Duty cycle region mapping.
Data Link Layer	Jamming, Collision, Exhaustion	Tiny Sec, Error-correcting code, Link Layer Encryption, Distributed MD (mediation device) protocol.
Network Layer	Neglect or Selective forwarding, Sybil, Wormhole, Spoofing, Homing, Sink or Black holes, Hello-Flooding	TIK based upon symmetric cryptography, Multipath Routing, REWARD algorithm, SNEP.
Application Layer	Data Aggregation, De-synchronization	SDAP, Aggregate commit-prove Framework.

Procedure

We program each node with a number of "Good Encryption keys" which is any variable number of secret keys known not duplicated in same node with variable number being greater than 0. These keys are also stored in every base node along with the unique ID of the mote.

User data part of every packet is modified with 8 bits is reserved for this protocol security procedure and remaining bits are used for user data.

All the user data in packet is encrypted using a randomly selected key from the good encryption key. First bit of the 8 security bits tells the base station whether the packet data is encrypted or not i.e., if the first bit is 1 then the packet is encrypted or reverse of this technology. Any salt based encryption method like AES can be used as encryption/decryption algorithm. If the user information is to be encrypted then a special 7-bit pattern is also encrypted

using the same key. This pattern is known to both base station and mote and this pattern can be unique to each mote. This pattern can be all 1s (111111) or all 0s (0000000) or any combination of 1s and 0s. This small pattern is use to minimize data decryption overhead at the base station as decrypting large data will take more processing time and computing powers.

The data is forwarded using normal routing methods. At the receiving base station the base station first check if the packet is encrypted or not based upon the first bit of user data. If it is encrypted then base station check the unique ID of the sender and select all its keys from database else if it is not encrypted then the base station proceeds as normal. In Encrypted packet the next 7 bit pattern is decrypted using all the keys and decrypted string is matched against stored bit pattern and a match is found then by using resulting secret key the rest of the packets are decrypted.

Algorithm

ENCRYPTION PROCEDURE

1. let good_keys = {x>0| x belong to unique secret keys}
2. let bit_pattren = unique 7 bit pattern
3. secret_key = random(good_keys)
4. encrypted_pattren = encrypt(bit_pattren, secret_key) so that length(encrypted_pattren) = 7 and decrypt(encrypted_pattren, secret_key) = bit_pattren while decrypt(encrypted_pattren, wrong_key) != bit_pattren
5. encrypted_data = encrypt(data, secret_key)
6. make and send packet
7. exit

DECRYPTION PROCEDURE

1. let good_keys = {x>0| x belong to unique secret keys}
2. let bit_pattren = unique 7 bit pattern
3. secret_key = get_next_secret_key(unique ID of sender)
4. decrypted_pattren = decrypt(encrypted_pattren, secret_key)
5. if decrypted_pattren = null then drop packet and exit
6. if decrypted_pattren = bit_pattren then goto step 7 else goto step 4.
7. data = decrypt(encrypted_data, secret_key)
8. process data
9. exit

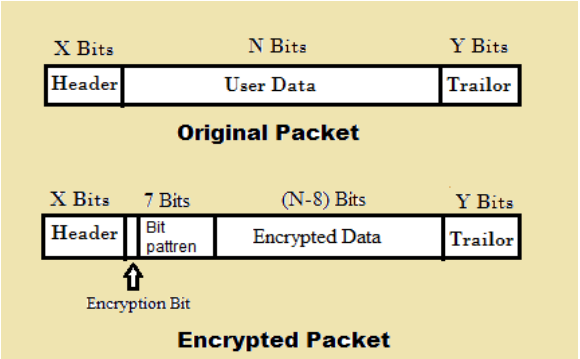

Fig. 6. Difference in Packet Structure

VI. CONCLUSION

The WSN security has been important challenge due to its unmonitored deployment nature and its inherent resources limitation. Due to limited resources of sensor nodes, the security in Wireless Sensor Network has become more difficult to implement as compared to other traditional networks. Various techniques had deployed to resolve the security issues. In this paper, in a very comprehensive way, we scrutinized all the limitations existing in the WSNs. In this paper different requirements for WSNs are grasped which are necessary to be considered to accomplish the goal of security. A confined comparative analysis of attacks on all layers of WSN protocol stack has shown in this paper. The mapping of security attacks on each protocol layer has been presented in the form of table. The algorithm presented here is a step toward solving this security problem with simple salt based encryption.

It can support both encrypted and non encrypted data packets and it does not require any modification to header or trailer. It is designed to use minimum extra power and low processing overhead at base station. The small bit pattern helps in this regard while also speeding up the whole procedure.

Advance research in security measures proposed many solutions to resolve security issues but still some WSNs are exposed to security attacks because of no proper countermeasure developed against these security attacks.

REFERENCES

[1] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, pp. 53-57, 2004.

[2] A.-S. K. P. and, H.-W. L. and, and C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges," *CoRR*, vol. abs/0712.4169, p. 1043, 2007.

[3] D. B. and and T. Newe, "Securing Wireless Sensor Networks: Security Architectures," *JNW*, vol. 3, pp. 65-77, 2008.

[4] M. R. K. Amin Reza Sedghi, "Data Security via Public-Key Cryptography in Wireless Sensor Network," *International Journal on Cybernetics & Informatics (IJCI)* vol. 2, 2013.

[5] A. Singla and R. Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks," *International Journal*, vol. 3, 2013.

[6] Q. I. Sarhana, "Security Attacks and Countermeasures for Wireless Sensor Networks: Survey," *International Journal of Current Engineering and Technology*, vol. 3, 2013.

[7] Y. Hao, L. Haiyun, Y. Fan, L. Songwu, and Z. Lixia, "Security in mobile ad hoc networks: challenges and solutions," *Wireless Communications, IEEE*, vol. 11, pp. 38-47, 2004.
[8] M. Saraogi, "SECURITY IN WIRELESS SENSOR NETWORKS," presented at the SenSys - Conference On Embedded Networked Sensor Systems.
[9] M. K. Jain, "Wireless sensor networks: Security issues and challenges," *International Journal of Computer and Information Technology*, vol. 2, pp. 62-67, 2011.
[10] S. Capkun and J. P. Hubaux, "Secure positioning in wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, pp. 221-232, 2006.
[11] W. Stallings, *Cryptography and Network Security: Principles and Practice*: Prentice Hall Press, 2010.
[12] X. Wang, W. Gu, K. Schosek, S. Chellappan, and D. Xuan, "Sensor Network Configuration Under Physical Attacks," in *Networking and Mobile Computing*. vol. 3619, X. Lu and W. Zhao, Eds., ed: Springer Berlin Heidelberg, 2005, pp. 23-32.
[13] Anthony D. Wood and J. A. Stankovic., "Denial of service in sensor networks," *Computer*, vol. 35, pp. 54-62, 2002.
[14] M. Y. Malik, "An Outline of Security in Wireless Sensor Networks: Threats,Countermeasures and Implementations," *CoRR*, vol. abs/1301.3022, 2013.
[15] J. Sen, "Security and Privacy Challenges in Cognitive Wireless Sensor Networks," in *Cognitive Radio Technology Applications for Wireless and Mobile Ad Hoc Networks*, ed: IGI Global, 2013, pp. 194-232.
[16] S. P. Prabhudutta Mohanty, Nityananda Sarma, Siddhartha Sankar Satapathy, "SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY.," *Journal of Theoretical & Applied Information Technology*, vol. 13, pp. 14-27, 2010.
[17] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, 2003, pp. 113-127.
[18] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," presented at the Proceedings of the 3rd international symposium on Information processing in sensor networks, Berkeley, California, USA, 2004.
[19] M. Pooja , Dr. Yudhvir Singh, "Security Issues and Sybil Attack in Wireless Sensor Networks," *International Journal of P2P Network Trends and Technology*, vol. 3, 2013.
[20] A. Jain, K. Kant, and M. R. Tripathy, "Security Solutions for Wireless Sensor Networks," presented at the Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies, 2012.