 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

All Possible Security Concern and Solutions of WSN: A Comprehensive Study

[1]Hassan Ali, [2]Abdullah Al Mamun, [3]Sultan Anwar
[1,2,3]King Fahd University of Petroleums and Minerals Dhahran, Saudi Arabia

Abstract
Wireless sensor networks are used in many fields such as military, hospitals, environment monitoring and so on. The nodes used in these networks are resource limited that use open public channels to communicate with each other. Due to this reason these networks are highly susceptible to attacks. In this survey we have identify the security issues and challenges in these networks. We also describe basic security fundamental techniques and their feasibility in WSNs. The basic security requirements of these networks are also discussed in detail. The paper includes classification of almost every kind of attack that can occur on these networks and security schemes and algorithms in correspondence with such attacks.

Keywords
Sensor Networks, Security, Solutions, Survey, Taxonomy, Classification

I. Introduction

Wireless sensor networks consist of small or tiny nodes which forward or pass data among each other thus forming a network. These sensing nodes consist of small and inexpensive battery powered devices along with wireless transmitters which are deployed in a scattered way to form a wireless ad-hoc network. The networks can be deployed in various environments to collect data for several purposes such as property protection, assisted living, climatic data collection, enemy monitoring, and criminality control, protection of natural resources from exploitation, factory instrumentation, environmental monitoring, building safety, military applications, safety applications, medical monitoring, weather, pollution, traffic control, and healthcare, disaster relief operations, seismic data collection, monitoring wildlife, target tracking, surveillance, and many others [1-3]. Hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors are the areas of research of WSNs [4]. There are some of the factors that affect the designing of this network such as unattended operation, the self-organization and the scalability. The most appropriate reasons of its adaptability are wireless communication and processing power. Wireless sensor networks are very useful in above mentioned applications but they have certain limitations of resources and other elements. These limitations include: Low memory, limited time of battery, less processing capacity, low bandwidth, weather and people's action vulnerabilities. Due to these limitations wireless sensor networks are much susceptible to security threats and attacks. In our survey we have provided a complete detail of security attacks, security challenges and security schemes that can be used against particular attacks in WSNs. We have described in section II the basic fundamental security schemes for any kind of network and their adaptability in WSNs. We explore almost all issues and challenges that a WSN can have in section III. WSNs security requirements are discussed in Section IV. Section V reviews classification and description of all possible attacks that can occur in the network. Finally section VI concludes the paper by providing security schemes against particular attacks.

II. Basic Fundamental Security Techniques

A. Cryptography

The security techniques related to encryption decryption used for conventional wired networks are not viable for the wireless sensor networks. The nodes used in wireless sensor networks have very limited resources such as energy, processing power and memory etc. These resources are critical for implementation of security in these networks [5]. Extra bits are required in implementation of encryption that's why more energy, more processing power and more memory is required. Also, traditional encryption schemes offer packet loss, delay and jitter in wireless sensor networks [5]. The critical security issues such as alteration, packet injection or eavesdropping need to abstain in wireless sensor networks. Data cryptography specially designed for wireless sensor networks can be used to provide protection against these security issues.
Symmetric cryptography is being used now days but the problem with this scheme is, for example if only one node in the entire network is compromised than whole network will suffer because due to the compromised node the shared secrets among other nodes will not remain secret. On the other hand shared key can also be used and the network will require n-1 keys, where 'n' is the number of nodes. Shared key scheme has a biggest disadvantage that the network will no longer be scalable after deployment which is very big issue in wireless sensor networks where extra nodes are required all the time. Public curve cryptography scheme is used in which to implement 80 bits security; the parameter size of 160 bits is required which will provide as much security level as provided by 1024 bits in RSA. Public key cryptography is another scheme but as we have very limited resources in WSNs so it will be expensive to implement. Langendorfer and Piotrowski [6] studied and explained various parameters viable public key cryptography for WSNs. These parameters are related to time of processing, memory usage and energy etc. Also there are certain architectures [7] that are used to run public key cryptography. But there is no option to implement cryptography in wireless sensor networks without using secure key distribution schemes. It needs simple key setup in the large WSN networks. That's why cryptography in WSNs depends on implementation of keys [8].

B. Steganography

In cryptography, the message or the content of message is hiding while in steganography we try to hide the whole message [9]. Steganography is a security fundamental where the entire message hides by embedding the message into any video, sound or image bit stream. Steganography aims to hide the message bits into these multimedia bit streams [10] by changing the carrier in such a way that it remains undetectable. Steganography is used when there is a need to hide private data to send publicly or when there is a need to send data by disclosing sender's identity. But steganography in wireless sensor networks is not feasible because there is no such data like multimedia which travels across this network with such incapable resources. So steganography is verydifficult to implement and still it is a research issue in security field [11].

C. Secure Physical Layer Access

Frequency hopping is used to provide secure access of physical layer in wireless sensor networks. There are three parameters which ensure frequency hopping by consuming fewer resources like energy, processing power and memory.

1. **Hopping set:** It includes all the available frequencies used for hopping.
2. **Hopping Pattern:** Order of frequencies which are available in hopping set.
3. **Dwell Time:** Time taken by one hope.

Efficient design is very important in secure access of physical layer and sender and receiver synchronization is required to change the hopping sequence in less time than that of discovering it. There can be two techniques [12] that specify secure access of physical layer, either by developing secret keys over open channels or by designing intelligent coding strategies transmission without the need of secret key.

III. Security Issues and Challenges

Security schemes in wireless sensor networks solely depend on sensors sizes, memory usage, processing power and tasks needed from sensing nodes. These challenges are very critical in deploying and measuring the efficiency of securityschemes. Below are some of the major challenges that are being faced to implement security schemes in wireless sensor networks [34].

A. Resource Constraint

Resource constraint is one of the major issues which exist in wireless sensor nodes. WSN is created through such sensor nodes in which maximum of them are resource restricted. They are not able to do heavy computations and communication due to less processing power, short energy time, less memory storage and short range etc. Energy is one of the most critical issues in WSN nodes. There are several energy consumption classification parts in sensor nodes that consume energy and computation power [13]. It is some timemuch difficult to implement security schemes due to the scarcity of such resources. The security schemes or security algorithms require extra processing power and extra storage capacity which is difficult to provide by the nodes with less resources. These schemes and algorithms will consume more processing power, which utilizes more energy and thus the wireless node will no longer be alive because of no continuous energy resource [14]. So it is very crucial to be aware of these restrictions to employ security schemes in WSNs [15].

B. Wireless Communication

Wireless communication is also very big challenge for security implementation in WSNs. There are public accessible wireless channels to be used in WSNs so data privacy is a big issue because same frequency radio interface can participate into the communication. Trust gaining is difficult in such wireless environment because WSNs users are very acute to recognize others personal information. Unguided transmission medium is always considered to be vulnerable for security issues. So there is always a temptation for attack such as eavesdropping over the private data stream in wireless networks. Due to this fact they can be unpractical to use without strong security mechanisms.

C. Threats Susceptibility

WSNs are more susceptible to threats and risks than that of wired networks. WSNs are employed in such hostile environments so there are high chances for an adversary to compromise a sensing node. Very sensitive issues such as embedding wrong messages in network, message snooping, alteration, data integrity and destroying the network resources are very crucial to take into account. There are different mechanisms and protocols [16] for communication of nodes in wireless networks and most of the communication protocols do not have security implementation.

D. Dense and large WSNs

Usually WSNs comprises of large networks with so many nodes. According to experts, one should deploy 40 nodes if he wants 20 nodes in his network to minimize the probability of failure of the network. In this situation it is difficult and challenging to design and implement security schemes for such large, dense and dynamic network. The scalability is also a critical aspect to be considered to design security schemes. Usually, WSNs are deployed in hostile environment where the nodes are always in danger. In order to deploy more replacing nodes if needed, the security schemes must be flexible enough to cover the scalable network.

E. Network Topology Before Deployment

Most of the time WSNs are deployed in such areas where human access is difficult such as around volcano, in zoo caves, in war areas etc. so the nodes are deployed randomly in such areas. It is up to the nodes which topology they used after deployment. As nodes can use various topologies depending on their current physical location so it is also a challenge to design such security schemes or protocols that are feasible for such vast variety of topologies for wireless sensing nodes.

F. Hostile Environments

WSNs are usually used in hostile and sensitive environments where adversary can easily damage the nodes. There are such adverse conditions in these environments where any node can easily be compromised. The severe conditions include:

1. **Army War Zone:** where army needs todeploy sensing node in order to detect or inspect enemy movements. If anyone of the nodes is compromised than whole network becomes fragile or enemy may have control over whole network which may cause wrong interpretations that can do severe damage.
2. **Open Environment:** The nodes if deployed in open environment may face harsh weather as well. The nodes may face heavy rain fall, severe cold and hot environments, storms and blizzards etc.
3. **Remote Area:** As mentioned above, sensing nodes are deployed where human access is difficult. There is a critical issue of energy resource constraint for nodes. Wireless nodes with limited energy power in remote areas are difficult to implement because of no human interaction.
4. **Animal's Area:** Node may be deployed in animal caves in zoo where, there is a need to monitor animal positions or movements etc. So the node is always in danger of physical attack and energy constraint.

IV. Security Requirements

A. Authentication

Different application in wireless sensor network significantly require authentication of message. Administrative duties such as duty cycle control of a sensor node and reprogramming of the network require authentication. Attackers can easily inject the wrong messages if authentication is not there in the network. Authentication ensures genuine end to end communication [17].

Thus authentication discovers illegitimate entities that try to inject malicious messages in network. Actual nodes should also be capable to discover these messages which originate from false entities. In this way every node must check the authenticity of message even it is received from the legitimate node. An authentication code [18] can be applied to ensure message authentication in WSNs.

B. Authorization

Authorization is necessary to provide security of entire network. The unauthorized node can spread malicious messages mostly the routing messages which change the routing protocols in the network and thus incorrect routing table establishes in each node.

C. Availability

Availability ensures that the information delivering or service providing node is available or accessible whenever is required. Services in network can be restricted by originating radio interference, using different tricky methods to consume energy of nodes and by interruption of various network protocols [18-22]. However, Network services need to be available all the time even if there is a severe attack such as denial of service [23]. There are various encryption schemes in wireless sensor networks but they are costly enough to implement. Some of the approaches reuse the same code by modification, some attempt to build extra communication to achieve similar goals and some of them use 'central point scheme' to limit the access of data, which is inappropriate. These approaches reduce the availability of node as well as availability of network because additional computations and communications rapidly consume the energy and power of node and if the node is dead due to power consumption than it will be no longer available in network. 'Central point scheme' severely affects the availability of the network because it not only affects the function of the network but also nodes can be crashed by its implementation [24].

D. Confidentiality

Confidentiality ensures that the contents of message or the message itself transmitted by any sensing node can only be understood by authorized or trusted receiver and thus ensures secrecy and privacy of data transmission within the network. The security service i.e. confidentiality hides the information from illegal or unwanted entities [17]. Secret key is used to hide the crucial data by encryption and thus provide confidentiality. The similar decryption keys first determine the type of data such as packets, headers or payload and then apply encryption [19-20]. The content of messages are encrypted at the transmitter side and decrypted at receiver side in order to keep attackers to access important information.

E. Integrity

Data during transmission can be changed by the attackers named as alteration thus can do severe damage by manipulating the information. Integrity ensures that the exchanged message between two nodes is not altered by other odes. Cyclic redundancy check can be used to detect random errors in the whole transmission of packets. In the same way authentication [20] and keyed checksum can also be used to prevent changes in packets to provide data integrity [19, 21-22, 25].

F. Non Repudiation

In non-repudiation the transmission of messages cannot be rejected by either a sending or receiving node. A node cannot refuse to send the message which has already been sent if the resources are less. Only the entities which are authorized can allocate specific resources in access control.

G. Freshness of data

One of the security requirements is that old packets should not travel within the network that is why freshness of every message [17] is also required. Old packets either by default or by adversaries not only consume extra resources but also can create hurdles in transmission of new information. Old messages can be eliminated and data freshness can be achieved by embedding timestamp with every packet.

H. Forward secrecy

If a sensing node is compromised and other nodes are forcing it to leave the network then it should leave the network permanently. The node may be able to take information of network away with it and can be utilized by the adversary. Forward secrecy is required to ensure that no leaving node inthe network can access any future information.

I. Backward secrecy

If a node joins a network then it should not be able to read any preceding information that has gone through the network. The node trying to become a part of network may be supplied by an adversary to get the information of network.

V. Classifications of Attacks

A. According to types

1. Denial of Service

The most severe attack created by unexpected crash of nodes due to malicious action. Redundant and unwanted packets are injected in network to consume accessible resources in order to restrict authorized entities to access these resources and services [26]. Network resources and services provide necessary functions to perform specific tasks. When these services are attacked, whole network suffers and becomes fragile, thus legitimate entities cannot access to resources and services whenever they are required [27]. These services are restricted by initiating certain events to perform any task to reduce the ability of whole network [28]. Denial of service attack can be of different kinds related to different layers. The attacks related to physical layer can be tempering or jamming. Exhaustion, collision and unfairness can occur on data link layer. Homing, black holes, misdirection, neglect and greed may occur on network layer. De-synchronization and malicious flooding are related to transport layer [29]. All of these attacks and their subsequent layers, security schemes and type of adversaries are listed in Table 1.

2. Attacks on Information in Transit

Sensing nodes keep tracks of various values and parameters and whenever they change, they inform sink node about these values. When these sensing nodes send this sort of information or any routing information to sink node, there is always a threat that this information in transit may diminish, changed, spoofed or play back again and again through tampering, eavesdropping, fraud or replay routing information. The attacker observes the flow of

traffic and can manufacture [30] or intervene into the traffic to provide wrong information to base station. These types of attacks are initiated during transmission by a laptop class adversary to change original information. With the help of extra processing power and higher range of communication, the attacker attacks on various sensors at the same time to manipulate or interrupt the information.

3. Sybil Attack

In most of the cases various sensors in a Wireless sensor network are grouped together to fulfill certain tasks by dividing subtasks and redundancy of information to each other. In this way, one node from a group claims to have a same identity [31] like the other legal nodes of that group (Fig 1). Distributed, de-concentrated and peer to peer systems are especially vulnerable to Sybil attack. An attacker can get this proportionality big impact to affect peer to peer network by making a large number of artificial entities [32].

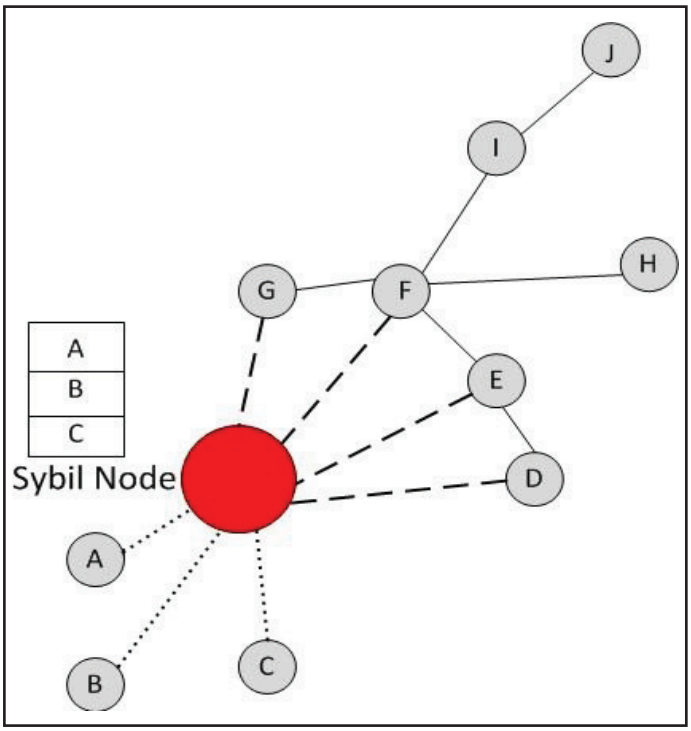

Fig. 1: Sybil Attack

These peer to peer networks can come up with security problems from defective or unfriendly outside or distant computing elements. The protocols and algorithms such as storage allocation, fault tolerant procedures and topology makers are highly susceptible to these attacks. An efficient utilization of resources, secure access of resources and integrity of data are well managed by distributed algorithms but may be humiliated by Sybil attacks. Detection of misbehavior, efficient allocation of resources, voting, data aggregation, fair storage allocation and routing procedures can also be the victims of Sybil attack [32]. Efficient protocols can be used to restrict these attacks as all wireless networks have gateways or base stations. As Sybil attacks are always likely to happen if there is no centralized authority presents [33]. On the other hand the detection of Sybil nodes is also very difficult but with the help of radio resource testing, the probability of presence of a Sybil node can be calculated [32]. There are some methods such as encryption and authentication that can restrict to initiate an outsider Sybil attack in a network. Insider Sybil attack can be restricted with the help of public key cryptography but is expensive for a resource limited network [17]. Matchless symmetric key is another solution if there is a relied base station is present in the network. There are certain algorithms that can be applied to detect repetition of declaration which a node makes to have same identity as of the other group nodes in order to prevent the Sybil attack [34].

4. Blackhole/ Sinkhole Attack

A vindictive node tries to tempt all traffic towards itself and becomes a blackhole in sensor networks [35]. The main focus of this attack is to point out the routing algorithms [36] and nodes that can be compromised. Attacker sends its own messages instead of original messages to receiving nodes that it has a best shortest path to reach other nodes and base station. If vindictive node becomes able to put itself into the route of other nodes and base station then it can do anything with the information which will pass through it. This attack can also affect the distant nodes from base station. Sinkhole is similar to black hole in which an attacker first gains a control over a node and then put it into the network to make a sinkhole at base station [37]. An adversary belongs to the laptop class can render prime routes with the help of high power radio transmitter to gain access of most of the network [38]. Fig. 2 shows an imaginary view of Black hole attack.

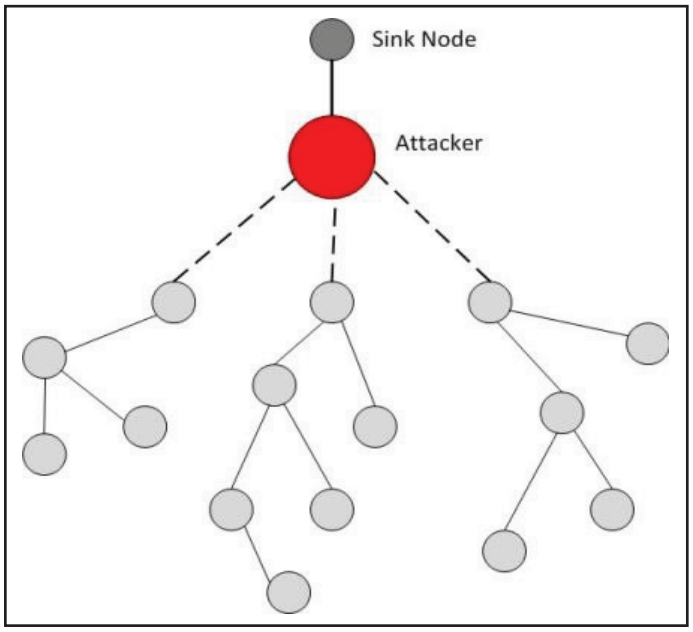

Fig. 2: Sinkhole Attack

5. Hello Flood Attack

This attack belongs to the network layer in which an attacker sends hello messages to other nodes in the beginning of network deployment [39]. Through these hello messages the attacker persuades other nodes that it is their neighbor and in consequence, other nodes enter this attacker node in their routing table. This attack is initiated by a laptop class adversary having high processing power and high range of radio transmission [39]. Once attacker is succeeded to make itself as a part of routing table of other nodes which are spoofed to falsely declare the compromised node as their neighbor, then victim nodes send their information to base station through this malicious node. In this way malicious node can do anything with this information and can create congestion within the network. Blocking methods [40], Authentication, Geographical packet leash, Bidirectional verification, multi-path multi-base station routing schemes can be used to prevent these attacks.

6. Wormhole Attack

This serious attack [29] [35] also belongs to the network layer in which attacker stores the messages (packets) in a location within the network and supply that information to another location. This attack occurs in the beginning of network when all nodes try to detect its neighboring nodes. The attacker takes the benefit of low latency between two parts of a network [42] to establish a connection. Wormhole attack is same as sinkhole which attacks the nodes near to base station as shown in fig. 3 (a,b). Whenever a base station initiates a routing request, the attacker captures the message and delivers to its neighboring nodes. Each node after receiving this message analyzes that it is in the range of base station thus making sure that base station is its parent node. But originally the victim nodes are at many hopes distance from the base station thus creates a wormhole in the network.

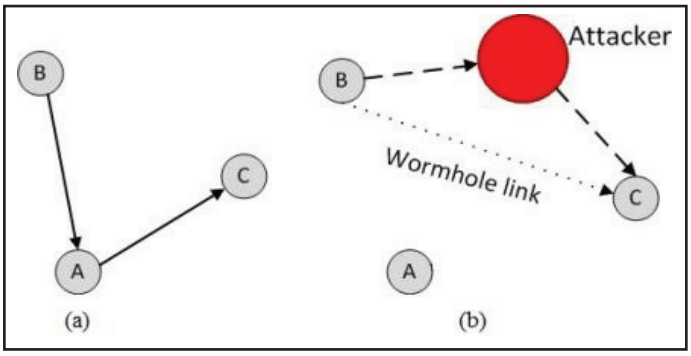

Fig. 3: Wormhole Attack

7. Selective Forwarding

The main responsibility of a routing node is to forward packets or messages but a vindictive node can intend to drop or forward selective packets. It is usually presumed by the multihop network that the transmission will be lucid from transmitter to receiver but a compromised node can reject to transmit or discard certain packets in the network. A framework [43] is used to detect this attack in which it is suggested that the number of receiving and transmitting packets must be equal and these numbers are monitored by a routing sensor. But each and every sensor has to work with integrity so it can catch the communication of neighboring nodes [44]. Neighbors do communication with each other and gather the information about malicious node, in this way based on data collected they can declare a node as a malicious one. Neighbor of a malicious node can also discover the surpassing threshold of malicious node which it uses to send extra amount of packets which failed to transmit by malicious nodes [44-45].

8. Response to Deceive

A large amount of routing protocols depends on the response of data link layer. So an attacker can deceive the response of data link layer by manipulating the packets of neighboring nodes. In this attack the attacker deceives the targets to achieve real efficiency of a link which is monitored by sender or to monitor the effective nodes which are illegal or expelled.

B. According to Adversaries

1. Active Attacks

Active attacks are those attacks which change the information such as modification, addition or deletion of transmission of data stream on the channel. These changes among the information are critical attacks to authenticity, data integrity and confidentiality. Particularly the security holes are tapped by an active attacker to initiate severe attacks such as replay packets, alteration and packets injection.

2. Passive Attacks

The motive of an attacker in passive attack is to get the information un detectively and covertly because it does not leave any evidences or proves. Eavesdropping and observing the transferring of packets are well known passive attacks in which attacker stays restrained to show its existence. The attacker can also detect the communication protocols among different nodes to take part into the communication.

3. Outsider Attacks

The attack is initiated by the node which does not belong to the network in which an outsider node is not authorized to enter. The wireless sensor networks are mostly run by only one authority and the other nodes in the network perform their tasks with lucidity and integrity. In this attack, attackers launch all the attacks from outside of the network because they don't have any access to network. These sorts of attacks such as data aggregation are limited and cannot do much harm to the networks as they cannot reach to the information transmitting inside the network.

4. Insider Attacks

Unlike the outsider attacks an adversary is managed to get the access to the network and damage the network by reaching to the critical information which is flowing in the network. These attacks are severe innature because attacker deploys some vindictive and malicious nodes inside the networks which keep tracks of the useful information of network. Moreover an attacker can also take control of existing node by making it compromised to access the control over entire network. The legal nodes of the network become suspected or unauthorized when an attacker gains control over them by running malicious codes or by stealing key materials.

5. Mote Class Attacks

Mote class attack is a same sort of insider attack in which attacker gain access to some of the nodes of network with the similar abilities to network nodes. Wormhole attack is a type of mote class in which motes are captured and compromised to do specific tasks with them.

6. Laptop Class Attacks

This type of attack is the most common attack used by an adversary to target the resource constrained networks with high power devices. These attacks are very effective as attacker attacks the network by considering the weakest ability of such resource limited networks. These devices have greater abilities than the nodes of network. An adversary can use a laptop device to deploy high power radio and antennas [46] for large communication range. Laptop class attackers with the help of high computing capabilities and energy reserves can destroy whole network within a short period of time.

C. According to Layers

Just like wired networks, wireless sensor networks also operate under layered architecture. There are various tasks which are performed by each layer in the network. As we are discussing only the security aspects we will not go deep in the layers. So as these layers exist in the wireless sensor networks, we can study the attacks related to different layers.

1. Physical Layer

Physical layer increases reliability by decreasing shadowing and path loss effect. The parameters such as data rate signal detection, modulation and encryption deal with physical layer due to its reliability. Several attacks may occur on physical layer to damage these parameters. A known attack on physical layer is jamming which interferes to radio frequency of legal nodes. Packets injection is another reason for jamming to consume extra energy of both transmitting and receiving nodes [47]. There are four various kinds of jamming attacks [48] to jam the wireless network. Packet delivery can detect congestion but cannot detect that the congestion is general or by attack. Tempering is another attack on physical layer in which nodes are damaged or tempered physically [49] to reduce the ability of a network.

2. Data Link Layer

The layer's responsibility is to ensure end to end reliable communication, flow control and error control. Data link layer is also susceptible to attacks in which the attacker sends extra messages to create collision for breaking communication protocol. Collision cause retransferring which ultimately reduce the power and energy of node to be alive in the network [50]. Tiny Sec [51] security scheme has been proposed for data link layer security. Zigbee [52] has been proposed for symmetric key encryption related to hardware. Distribution of secure code [53] and Public key cryptography [54] has been indicated to develop secure key at the time of maintenance or deployment of network.

3. Network Layer

Network layer provides efficient routing among various entities of the network such as nodes, sink node, clusters and base station. Each node in a network works as a router and may get advantage of multi hopping to reject certain route messages of the neighbors which labels route through malicious nodes to make them disable to transfer messages [50]. Network layer is susceptible to active and passive attacks. Active attacks such as denial of service [55], Blackhole attacks [56], and routing attacks [57] can disrupt the packets of routing which ultimately futile routing table. Passive attacks can also occur on network layer that can detect information and eavesdrop on the flow of traffic. Hash functions or encryption and decryption schemes [58] i.e. key management is used for secure routing, data integrity and authentication. Public key cryptography with Certificate Authority is used for security purpose of WSN nodes [49].

4. Transport Layer

Transport layer is used where it is necessary to connect wireless sensor network to an outside network such as internet. The attacks which may occur on transport layer can be flooding or resource exhaustion etc. Many connection requests are generated in case of flooding to a susceptible node to exhaust its resources [50]. However efficient allocation of sender must be there to manage such connection requests.

5. Application Layer

Application layer's responsibility is to ensure reliable flow of information to lower layers. Aggregation based attacks may occur on application layer. Several applications software is used by transport layer to provide trustworthy data processing, management and data collection.

VI. Security Schemes and Solutions

A. Encryption

As most of the wireless sensor networks use unsecure public wireless channels for transmission over a large area so they are more amenable to packet injection or eavesdropping attacks [24]. Symmetric key encryption schemes such as TIK [41], public cryptography infrastructure [59] and message authentication protocols such as mu-TESLA [60] can be used to prevent these attacks.

B. Data aggregation security

Denial of service is one of severe attacks occur in data aggregation based sensor networks. As the flow of data increases inside the network, sensing nodes aggregate certain measures before transferring to base station to reduce network traffic and overhead [61]. This aggregated data is very attractive to adversary and an attacker may attack to erupt its credibility or may generate false report by taking control over aggregating node. Reliable functions must be used to detect and report false reports with the help of data authentication [24]. Structurefree, structure-based, distance and time-based data aggregation protocols [62] are other solutions to prevent application layer active attacks on aggregated data in WSNs.

C. Security Protocols and Algorithms

Various security protocols [63] have been devised for wireless and resource limited networks. These protocols offer less overhead in communication, authenticity, semantic security and replay defense. Similarly there are various security algorithms that are used in WSNs.

1. ILS

This algorithm [2] is used to obtain correct localization on the bases of signal strength and time. The position of a node is estimated by gathering certain measures such as RSSI, TOA and TDOA of a signal by reference nodes. The system estimates the location, based on continuous circles with the help of translated measures. These algorithms have not exact remedy for attenuation as they have value of reported attenuation different then measured one between different nodes.

2. PADS

The embedding algorithm [64] measures a MAC which is inserted inside the data to develop a secret key based time synced key. This time synced key is then used between two communicating nodes. Attackers could also use certain algorithms to detect and extract the embedded part but in order to the break this encryption the attacker needs to betime synced with the sensor network

3. RC5

Block cipher based RC5 algorithms [65] have been proposed that implements security in hash functions using cryptography. The algorithm is used to establish and authenticate MACs and derivation of keys that belong to location binding. Base station starts the chain of sequence numbers that encrypt the plaintext with the help of random key. Ciphers keep creating other cyphers until all required keys are created [66].

4. SOWSN

To mention distance between points or angles SOWSN algorithm is used which is based on range. This algorithm may be used

to target locations and announcing alerts for certain detections with high frequency. It can also be used as a MDR (multifactor dimensionality reduction) algorithm to allow nodes to send messages or alerts through intermediate nodes towards base station [67].

5. Protected Grouping

Several nodes in wireless sensor networks do certain tasks by making a group together. These automated and compact nodes need to communicate securely among their group. There have not been much security schemes to protect the whole group however, exceptions can be the solutions in which high power nodes can be assigned to protect the groups.

6. Architecture for link layer Security

A common security package in wireless sensor networks is TinySec [51]. This is a light package that can be found with Tiny OS. There are two security mechanisms in TinySec. The first one is authentication-only which authenticate the MAC along with whole packet but the payload remains unencrypted. The second is Authenticated-encryption which authenticate the MAC along with whole packet and it encrypts the data payload as well [63].

D. Shared Keys

Key management is the area that has received much attention for wireless sensor networks security [68]. Security can be provided to a resource constrained sensor networks by just applying regular key schemes. Certain key protocols are used to establish key mechanisms. Key is private information which allows access to only authorized users by ensuring authenticity and integrity.

There are two major types of cryptographic keys. Asymmetric key uses different kind of shared keys where symmetric key uses same kind of shared keys. Attacker can identify the key scheme being used inside the network due to repetition of messages. That is why communicating nodes must keep changing the keys time to time. WSNs key management schemes [69] are as follows:

1. Single Network-Wide Key

This is a simple technique for key establishment in which the key is loaded among each node of a network at initialization. Later on all the nodes use this key for cryptography.

2. Pair Wise Key Establishment

The key offer authenticity and prevention for replaying. Each node is loaded with a unique key to communicate with the nodes under its range. It provides authentication and verification of identity of other communicating node. This scheme also provides resilience to reveal information if a node is captured.

3. Trusted Base Station

This scheme is also called distributed centralized key in which base station transfers session keys to various nodes. This scheme is also resilient for a node to reveal information but does not offer scalability.

4. Public Key Schemes

Public key schemes offer more flexibility than that of nonpublic schemes. Regular cryptography techniques are not essential in resource constrained networks as mentioned in the start. But public key encryption such as elliptic curve cryptography [70] and RSA are in testation phase. ECC has more computing power, less memory usage and small keys than RSA. They both can be enhanced in terms of efficiency by providing extra processing power.

5. Key Pre distribution Schemes

Keys are loaded into the nodes of a network before deployment. Then after deployment nodes look for a mechanism to establish share keys for secure interaction [71]. The properties of various sub key predistribution schemes are as follows:

- Polynomial Pool Based: Two nodes can communicate with each other in the presence of malicious nodes by establishing pairwise keys.
- Grid based key: PP based scheme which ensures pair wise key establishment between non compromised nodes
- Q-Composite random key: Random keys are picked and every node has to locate common shared keys.
- Hypercube key: Nodes are able to communicate even in the presence of compromised nodes in the network [72].
- Random key: Keys are randomly distributed and after initialization nodes detect common keys for communication.
- Random subset key: Random keys and their polynomial are selected from a large pool and then assigned to the nodes.
- Multipath key reinforcement: to provide the link among to sensing nodes where security is more critical than power and bandwidth [73].

E. Other Security Schemes

- JAM- This technique [74] is used to prevent jamming attack in general wireless sensor networks. With the help of adjacent neighboring nodes, it avoids jammed areas in the network.
- Wormhole based Security- The networks that have both infrastructures such as wired and wireless (Hybrid) use this technique to provide security against jamming attack. Wormhole based security mechanism [75] uses wormholes to restrict wormhole attack.
- Statistical En-route filtering- This technique [76] is suitable for large and dense WSNs. It restricts spoofing attack on information and diminishes false reports between forwarding process.
- Multi-path multi-base station routing (MPMBSR) and Bidirectional Verification- MPMBSR [63] has been proposed for general WSNs in which secret sharing scheme is used. With the help of multi-path multi-base station routing and bidirectional verification, it prevents hello flood attacks.
- On communication security- This technique [77] is used in traditional WSNs that detects and prevents spoofing attack on information and data. Due to efficient resource allocation and management it secures the remaining part of the network even if one part becomes malicious or compromised.
- REWARD- This technique [78] uses geographic routing and prevents black hole attacks by keeping tracks of neighboring nodes and their communications. Traditional WSNs use this approach to overcome miss directions, homing and other network layer attacks.
- Priority Messages and tamper proofing- To cope with physical layer active attacks such as denial of service and tampering, these schemes are used.
- Error correcting codes- This is used to prevent data link layer attacks. The attacks related to active adversary such as jamming and collision is tackled by this technique.
- Identity certificates and authorization- These approaches [32] are used to restrict network layer attacks such as flooding,

sinkhole attack, wormhole attack and Sybil attack.

- Spread spectrum- Spread spectrum technique provides defense against jamming attacks at physical layer.
- Rate limit- Rate limit eliminates exhaustion at data link layer.
- Small frames- This is used to prevent unfairness of resource allocation.
- Authentication and packet leashes- Prevents hello flood attacks that occur on network layer and belong to the laptop class adversary.
- Client puzzles- They tackle with flooding attacks associated to transport layer.
- Black listing and channel hopping- They are used to prevent physical layer attacks such as jamming and interference.
- Information and Network ID protection- These techniques are utilized to avoid exhaustion and to protect Network ID. They are also used to protect critical information that is used to join different network devices.
- Synchronization- Synchronization is used to prevent De-synchronization using various neighboring nodes. Synchronization is used to maintain time synchronization among nodes.
- Protection and Inspection- To protect the network physically and to protect specific data link network ID as well. Inspection is used to monitor the attacks on network layer.
- Source route monitoring- Regular detects and monitors selective forwarding attack associated with network layer with the help of source routing. Source routing also helps in physical and regular network monitoring.

Table 1: Attaks and Solutions

Attacks	Sub categories	Solutions	Layer Associated	Type of Adversary
Denial of Service	Tempering	Tamper Proofing, Priority Messages, Hiding, Encryption Protection,Changing of key.	Physical	Active
	Jamming	Spread-spectrum, Priority Messages, JAM, Error correcting codes, Channel hopping and blacklisting, wormhole based.		
	Interference	Channel Hopping, Black listing		
	Collision	Error Correcting Codes, CRC, Time diversity	Datalink	
	Exhaustion	Rate limit, Network ID and information protection		
	Unfairness	Small frames		
	Neglect and greed, Homing, Miss directions, Black holes	Authorization, monitoring, redundancy, REWARD, Network ID and information protection	Network	
	Malicious Flooding	Client puzzles, Rate limitation, Redundancy, Probing, Authorization, Monitoring	Transport	
	DE-synchronization	structure-free, structure-based, distance and time-based data aggregation, Time synchronization	Application	
Attacks on Information in transit	Eavesdropping	Session key	Data link, Network	Passive Laptop
	Replay Information	SNEP and TESLA, TinySec	Network	
	Spoofing	Random key Predistribution, Key management, Statistical EnRoute Filtering, Communication security, Different message sending paths	Data link, Network	
	Alteration	Random key predistribution	Network	
Sybil Attack	Data aggregation	Radio resource testing, Random key pre distribution, Physical protection	Data link	Outsider
	Routing mechanism	Authorization, monitoring, Public key cryptography, matchless symmetric key, Random key predistribution, Changing of session keys	Network, Routing	Insider
Sinkhole attack	Flooding based protocol	Redundancy, Identity certificate, Probing, Authorization, Monitoring	Network	Laptop
Hello Flood attack		Blocking methods, Authentication, Geographical packet leash, Bidirectional verification, multi-path multi-base station routing	Network	Laptop
Wormhole attack		TIK, Geographical packet leash, Authorization, Physical monitoring, Source route monitoring	Network	Passive, Mote
Selective forwarding attack		Egress filtering, authentication, monitoring, Network monitoring using source routing	Network	Laptop
Response to deceive		Egress filtering, authentication, monitoring	Data link	Active
Aggregation based attacks		Aggregate commit prove framework	Application	Active

Table 1 shows all major types of attacks and their sub categories. Where the adversaries in correspondence with these sub categories are also shown. As Wireless Sensor Networks are comprise of layered architecture that is why the layers associated with each major and sub types of attacks are also shown. As this survey is based on the classification of attacks according to various types and their security solution, algorithms and schemes. So all the possible security solutions against different kinds of attacks are shown and suggested in the table. The security schemes can be more than one for a single attack or there can be only one solution for several kind of attacks. All of these relationships are shown in Table 1.

VII. Conclusion

Wireless Sensor Networks are the need of a day and their applications are increasing everyday in almost every field but on the other hand they are associated with deep security concerns due to resource constraint. In our survey we studied the basic security fundamental techniques. Some of them can be used in these networks while some of them cannot. We made a relationship of all of the attacks, their corresponding security techniques, the type of adversaries and their associated layers in our comprehensive survey. But as new attacks are being invented day by day and new security schemes are being deployed and analyzed. This survey paper will not enough for security in WSNs in coming days. This survey paper can be updated in future in order to accommodate and identify all incoming attacks and security solutions.

References

[1] Silva, F.,"Industrial Wireless Sensor Networks: Applications, Protocols, and Standards [Book News]." Industrial Electronics Magazine, IEEE 8.4 (2014): pp. 67-68.

[2] Paradells, Josep, Jordi Vilaseca, Jordi Casademont, "Improving security applications using indoor location systems on wireless sensor networks," Proceedings of the International Conference on Advances in Computing, Communication and Control. ACM, 2009.

[3] Pathan, Al-Sakib Khan, et al.,"A framework for providing e-services to the rural areas using wireless ad hoc and sensor networks," arXiv preprint arXiv:0712.4168 (2007).

[4] Dai, Shijin, Xiaorong Jing, Lemin Li.,"Research and analysis on routing protocols for wireless sensor networks," Communications, Circuits and Systems, Proceedings, International Conference on. Vol. 1. IEEE, 2005.

[5] Rahman, Musfiq, Srinivas Sampalli,"A hybrid key management protocol for wireless sensor networks," Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.

[6] Saleh, Mohammad, Iyad Al Khatib,"Throughput analysis of WEP security in ad hoc sensor networks," Proc. The Second International Conference on Innovations in Information Technology (IIT05), September. 2005.

[7] Peter, Steffen, Peter Langendorfer, Krzysztof Piotrowski, "Public key cryptography empowered smart dust is affordable," International Journal of Sensor Networks 4.1 (2008): pp. 130-143.

[8] Modares, Hero.,"A scalar multiplication in elliptic curve cryptography with binary polynomial operations in Galois Field," 2009.

[9] Akhtar, Nadeem, Shahbaaz Khan, Pragati Johri,"An improved inverted LSB image steganography," Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on. IEEE, 2014.

[10] Mane, Smita P. Bansod Vanita M., Leena R. Ragha,"Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity," International Conference on Communication, Information and Computing Technology. 2012.

[11] Rustamov, Anar,"Measurement of QoS in wireless sensor networks with single multimedia traffic-class," Problems of Cybernetics and Informatics (PCI), 2012 IV International Conference. IEEE, 2012.

[12] Mukherjee, Amitav, et al.,"Principles of physical layer security in multiuser wireless networks: A survey," 2010: 1-24.

[13] J. Ben-Othman, B. Yahya. "c." Journal of Parallel and Distributed Computing 70(8), pp. 849-857, 2010.

[14] Bashir, Adil, and Ajaz Hussain Mir.,"An energy efficient and dynamic security protocol for wireless sensor network," Advanced Electronic Systems (ICAES), 2013 International Conference on. IEEE, 2013.

[15] Modares, Hero, Rosli Salleh, Amirhossein Moravejosharieh, "Overview of security issues in wireless sensor networks," Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on. IEEE, 2011.

[16] K. Akkaya, M. Younis,"A survey on routing protocols for wireless sensor networks," Ad hoc networks 3(3), pp. 325-349, 2005.

[17] Mayank Saraogi,"Security in Wireless Sensor Networks ", University of Tennessee, Knoxville.

[18] N. Wang, N. Zhang, et al.,"Wireless sensors in agriculture and food industryRecent development and future perspective," Computers and Electronics in Agriculture 50(1), pp. 1-14, 2006.

[19] H. Alemdar, C. Ersoy,"Wireless sensor networks for healthcare: A survey," Computer Networks 54(15), pp. 2688-2710, 2010.

[20] K. Ren, S. Yu, et al.,"Multi-user broadcast authentication in wireless sensor networks," Vehicular Technology, IEEE Transactions on 58(8), pp. 4554-4564, 2009.

[21] C. Gomez, J. Paradells,"Wireless home automation networks: A survey of architectures and technologies." Communications Magazine, IEEE 48(6), pp. 92-101, 2010

[22] L. B. Oliveira, D. F. Aranha, et al.,"TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," Computer communications 34(3), pp. 485-493, 2011.

[23] Hung, X, L, et al.,"An Energy-Efficient Secure Routing and Key Management Scheme for Mobile Sinks in Wireless Sensor Networks Using Deployment Knowledge, Sensors," Vol. 8, pp. 7753-7782, 2008.

[24] Kalpana Sharma, M.K. Ghose, Deepak Kumar, Raja Peeyush Kumar Singh,Vikas Kumar Pandey,"A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks. In IJAST, Vol. 7, April 2010.

[25] K. Sunitha, H. Chandrakanth,"A Survey on Security Attacks in Wireless Sensor Network", International Journal of Engineering Research and Applications (IJERA) 2(4), pp.1684-1691, 2012.

[26] Yuntao, Zhao, et al.,"Research and analysis of denial of service performance based on service-oriented architecture." Control and Decision Conference (2014 CCDC), The 26th

Chinese. IEEE, 2014.
[27] Zargar, Saman Taghavi, James Joshi, David Tipper,"A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." Communications Surveys and Tutorials, IEEE 15.4 (2013): pp. 2046-2069.
[28] M. Dohler. "Wireless sensor networks: the biggest cross-community design exercise to-date." Bentham Recent Patents on Computer Science 1(1). 2008, pp. 9-25.
[29] Kalpana Sharma, M K Ghose. Wireless Sensor Networks: An Overview on its Security Threats. IJCA Special Issue on Mobile Ad-hoc Networks 2010.
[30] Zhou, Lingjing, Zhengdao Zhang,"A secure data transmission scheme for wireless sensor networks based on digital watermarking," Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on. IEEE, 2012.
[31] M. Al-Ameen, J. Liu, et al.,"Security and privacy issues in wireless sensor networks for healthcare applications," Journal of Medical Systems 8(December) 2010, pp. 1988-1988.
[32] Sinha, Somnath, Aditi Paul, Sarit Pal,"The Sybil attack in mobile adhoc network: Analysis and detection," pp. 458-466, 2013.
[33] Khan, Muhammad Sajid, Naima Iltaf, Adnan Rashdi, "Collusionresistant Sybil attack detection scheme in mobile ad hoc networks," Software Engineering Conference (NSEC), 2014 National. IEEE, 2014.
[34] Pal, S., A. Mukhopadhyay, et al.,"Defending Mechanisms Against Sybil Attack in Next Generation Mobile Ad Hoc Networks," IETE Technical Review 25(4), pp. 209-220, 2008.
[35] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong,"Security in Wireless Sensor Networks: Issues and Challenges", Proc. ICACT 2006, Vol. 1, 20-22 Feb, 2006, pp. 1043-1048.
[36] H. A. Farooqi, F. A. Khan,"A survey of Intrusion Detection Systems for Wireless Sensor Networks," International Journal of Ad Hoc and Ubiquitous Computing 9(2). 2012, pp. 69-83.
[37] F. Bao, R. Chen, et al.,"Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," Network and Service Management, IEEE Transactions on 9(2). pp. 169-183, 2012.
[38] A. G. Fragkiadakis, E. Z. Tragos, et al.,"Design and performance evaluation of a lightweight wireless early warning intrusion detection prototype," EURASIP Journal on Wireless Communications and Networking 2012(1).
[39] Magotra, Shikha, Krishan Kumar,"Detection of HELLO flood attack on LEACH protocol," Advance Computing Conference (IACC), 2014 IEEE International. IEEE, 2014.
[40] Y. Zhang, X. Li, et al.,"A Hierarchy-based Dynamic Key Management for Clustered Wireless Sensor Network," Energy Procedia 13, pp. 7967-7974, 2011.
[41] Hu, Y.-C., Perrig, A., Johnson, D.B.,"Packet leashes: A defense against wormhole attacks in wireless networks, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976-1986.
[42] P. Yi, Y. Wu, et al.,"A survey on security in wireless mesh networks." IETE Technical Review 27(1). 2010.
[43] K. Li, C. F. Lai, et al.,"Energy efficiency routing with node compromised resistance in wireless sensor networks." Mobile Networks and Applications 17(1), pp. 75-89, 2012.
[44] X. Zhang, J. He, et al.,"Secure and Energy-Efficient Routing for Wireless Sensor Networks," Journal of Networks 6 (9). 2011, pp. 1288-1295.
[45] B. Xiao, B. Yu, et al.,"CHEMAS: Identify suspect nodes in selective forwarding attacks," Journal of Parallel and Distributed Computing 67(11). 2007, pp. 1218-1230.
[46] P. Apostolos, "Cryptography and Security in Wireless Sensor Networks," FRONTS 2nd Winterschool Braunschweig, Germany, 2009.
[47] H.-J. Kim, et al.,"A method to support multiple interfaces mobile nodes in PMIPv6 domain," presented at the Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea, 2009.
[48] W. Xu, et al.,"The feasibility of launching and detecting jamming attacks in wireless networks," 2005, pp. 46-57.
[49] P. B. Jeon,"A pheromone-aided multipath QoS routing protocol and its applications in MANETs," Citeseer, 2006.
[50] J. P. Walters, et al.,"Wireless sensor network security: A survey," Security in distributed, grid, mobile, and pervasive computing, pp. 367, 2007.
[51] K. Chris, S. Naveen, W. David, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, Proceedings of 2nd international conference on Embedded networked sensor systems, November 3-5, 2004, pp. 162-172, Baltimore, Maryland, USA.
[52] S. Naveen, W. David, Security Consideration for IEEE802.15.4 Networks, WiSE04, October 1, 2004 Philadelphia, Pennsylvania,USA.
[53] D. Jing, H. Richard, Shivakant Mishra, Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks, 5th international conference on Information processing in sensor networks, April 19-21, 2006, pp. 292-300.
[54] H. M. Kirk. Wong, Z. Yuan, C. Jiannong, W. Shengwei, A Dynamic User Authentication Scheme for Wireless Sensor Networks, IEEE International Conference on Sensor Networks Ubiquitous and Trustworthy Computing (SUTC06), 2006.
[55] W. Enck, et al.,"Exploiting open functionality in SMS-capable cellular networks", 2005, pp. 393-404.
[56] Mishra, Binod Kumar, Mohan C. Nikam, Prashant Lakkadwala,"Security against Black Hole Attack in Wireless Sensor Network-A Review," Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on. IEEE, 2014.
[57] Durrani, Nouman M., et al.,"Secure multi-hop routing protocols in Wireless Sensor Networks: Requirements, challenges and solutions," Digital Information Management (ICDIM), 2013 Eighth International Conference on. IEEE, 2013.
[58] K. K. Woo, L. Hwaseong, H. K. Yong, H. L. Dong, "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks," Information Security and Assurance, 2008. ISA
[59] Kim, Daehee, Sunshin An,"Efficient and scalable public key infrastructure for wireless sensor networks," Networks, Computers and Communications, The 2014 International Symposium on. IEEE, 2014.

[60] Li, Xiang, et al.,"Efficient and enhanced broadcast authentication protocols based on multilevel TESLA," Performance Computing and Communications Conference (IPCCC), 2014 IEEE International. IEEE, 2014.
[61] Feng, Hailin, Guanghui Li, Guoying Wang,"Efficient secure innetwork data aggregation in wireless sensor networks," Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on. Vol. 1. IEEE, 2010.
[62] Bala Krishna, M., Noble Vashishta,"Energy efficient data aggregation techniques in wireless sensor networks," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on. IEEE, 2013.
[63] Hamid, Md Abdul, Md Mamun-Or-Rashid, Choong Seon Hong,"Routing security in sensor network: Hello flood attack and defense," IEEE ICNEWS (2006), pp. 2-4.
[64] Albath, Julia, Sanjay Madria,"Practical algorithm for data security (PADS) in wireless sensor networks," Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access. ACM, 2007.
[65] Tajeddine, Ayman, et al.,"Authentication schemes for wireless sensor networks,"Mediterranean Electrotechnical Conference (MELECON), 2014 17th IEEE. IEEE, 2014.
[66] Minglin, Yao, Ma Junshuang,"Stream Ciphers on Wireless Sensor Networks," Measuring Technology and Mechatronics Automation (ICMTMA), 2011 Third International Conference on. Vol. 3. IEEE, 2011.
[67] Boudriga, Noureddine, Mourad Baghdadi, Mohammad S. Obaidat.,"A new scheme for mobility, sensing, and security management in wireless ad hoc sensor networks." Proceedings of the 39th annual Symposium on Simulation. IEEE Computer Society, 2006.
[68] Raazi, S. Muhammad K., Zeeshan Pervez, Sungyoung Lee, "Key management schemes of wireless sensor networks: A survey," Department of Computer Engineering, Kyung Hee University, Global Campus, Korea, 2011.
[69] Xiao, Yang, et al.,"A survey of key management schemes in wireless sensor networks," Computer communications 30.11, 2007, pp. 2314-2341.
[70] Mungara, Rajasekhar, K. VenkateswaraRao, Venkatasubba-reddy Pallamreddy,"A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks."
[71] Kazienko, Juliano F., N. Clio Vinicius,"Secure Secret Key Distribution and Storage in Wireless Sensor Networks," CIT. 2010.
[72] Liu, Donggang, Peng Ning, Rongfang Li.,"Establishing pairwise keys in distributed sensor networks," ACM Transactions on Information and System Security (TISSEC) 8.1, pp. 41-77, 2005.
[73] Deng, Jing, Yunghsiang S. Han,"Multipath key establishment for wireless sensor networks using just-enough redundancy transmission," Dependable and Secure Computing, IEEE Transactions on 5.3 (2008), pp. 177-190.
[74] Wood, A., John A. Stankovic, Sang H. Son,"JAM: A jammed-area mapping service for sensor networks," Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE. IEEE, 2003.
[75] Hubaux, Jean-Pierre,"Wormhole-Based Anti-Jamming Techniques in Sensor Networks," 2005.
[76] Ye, Fan, et al.,"Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal on 23.4, pp. 839-850, 2005.
[77] Slijepcevic, Sasha, et al.,"On communication security in wireless ad-hoc sensor networks," Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on. IEEE, 2002.
[78] Karakehayov, Zdravko,"Using REWARD to detect team black-hole attacks in wireless sensor networks," Wksp. Real-World Wireless Sensor Networks, pp. 20-21, 2005.

Hassan Ali received his B.S. degree in Computer Engineering from COMSATS Institute of Information Technology, Islamabad, Pakistan, in 2013 and continuing the M.S. degree in Computer Networks form King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. He was in faculty of Electrical Engineering department in Govt. College of Technology, Lahore, Pakistan in 2014. His research interests include Distributed Systems, Heterogeneous communications and Real time publish subscribe Operating systems and software. At present, He is engaged in Smart Grid communication interoperability and its standards.

Abdullah Al Mamun received his B.S. degree in Computer Science & Engineering from Dhaka University of Engineering & Technology, Bangladesh, in 2012, the M.S. degree in Computer Engineering from King Fahd University of Petroleum and Minerals, in 2016 (possible date). He was a Part time Research Assistant, with Department of Renewable Energy, Research Institute, KUPM in 2015, 2016 respectively. His research interests include Bigdata Analysis and Machine Leering. At present, He is studying MS in Computer Engineering in KFUPM.

Sultan Anwar received his B.S. degree in Computer Engineering from COMSATS Institute of Information Technology, Islamabad, Pakistan, in 2013 and continuing the M.S. degree in Computer Networks form King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. He was an assistant DCO in Pakistan Telecommunication Co. Limited. He is a research assistant with faculty of College of Computer Science and Engineering King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. His research interests include Wireless Sensor Networks, Network Security schemes, and Geographical Information Systems. At present, He is engaged in Pipeline leak detection techniques using wireless sensing nodes.