I.J. Wireless and Microwave Technologies, **2018, 6, 15-39**
Published Online November 2018 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2018.06.02

***Available online at** http://www.mecs-press.net/ijwmt*

Classification of Attacks on Wireless Sensor Networks: A Survey

Muhammad Noman Riaz[a], Attaullah Buriro[b], Athar Mahboob[b]

[a]*Department of Computer Science, Virtual University of Pakistan, Lahore, 54000*
[b]*Department of Computer Science, Khwaja Fareed University of Engineering & Information Technology Rahim Yar Khan, 64200*

Received: 13 May 2018; Accepted: 05 July 2018; Published: 08 November 2018

Abstract

Wireless Sensor Networks (WSN) is one of the fastest rising emerging technologies that find widespread use in various applications comprising of military, health, agriculture, habitat etc. Seen as sensor network deployed at sites which can be considered as remote and hostile, the technology is seriously faced with challenges to the network and functional security at the cost of their inherent limitations in energy capacity and computing power. In this paper we have delved upon and summarized earlier research on security challenges poised to WSNs, classified the threats and then presented a generic WSN security model keeping in line with the intended security targets to be met. We have also tried to give a realistic theoretical analysis of our WSN security model against these threats.

Index Terms: Wireless Sensor Networks, Security Goals, WSN Threat Model Security Attacks, Security Classification

1. Introduction

Wireless Sensor Network constitutes several sensing nodes that interact wirelessly among each other, are arranged in spatial way in order to intelligently monitor record and relay information on any physical/environmental phenomenon. Basically, a WSN is a group of wireless sensor nodes which have the capability of self-configuration, as and when required. A classic example of WSN is shown in Figure 1 below:-

A classic wireless sensor node consists of four fundamental parts (as shown below in Figure 2), namely: a Sensor Module (which senses the physical phenomenon), a Processing & Memory module (which processes the sensed data), a Transceiver Module (which receives and transmits the data) and a Power Unit (which

* Corresponding author. Tel.: +92-333-3083304
E-mail address: mnriaz@cae.nust.edu.pk

distributes and regulates the power requirement of the whole WSN node).

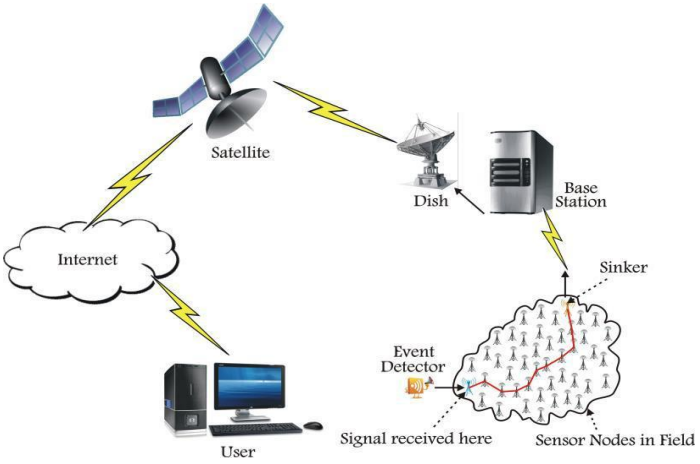

Fig.1. A Classic Example of Wireless Sensor Network [1]

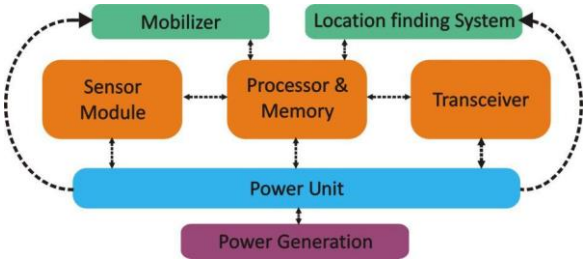

Fig.2. A Typical WSN Node [2]

The Wireless Sensor Networks have a significant role in military due to surveillance requirements in very difficult to reach terrains. WSN technology has also found useful applications in health, industrial, computational and commercial arena. Due to hostile nature of deployment scenarios for WSN, the security concern is of prime importance. Researchers have proposed several security mechanisms, but the common draw back in most of these models is that they are not capable of handling a wide variety of WSN security attacks rather are oriented towards a particular vulnerability (e.g. SPINS, Ariadne etc). Another issue is that these security mechanisms consume a significant amount of energy and consequently reduce the lifespan of a typical node. Thus, in order to develop a robust, resilient, secure and energy efficient WSN protocol, a thorough understanding of different types of security attacks on WSN is mandatory. This paper tries to summarize different WSN attacks (up to 52) according to the latest research along with elaborating and identifying the Security Challenges of WSN, Security Goals of WSN, Security Threats of WSN, Classification of WSN attacks, and it's Security Threat Model.

2. Contribution of the Paper

During the past few years, a relatively large number of research works has been done on the security aspect of WSNs. This paper is an effort to comprehensively analyze the maximum number of security attack on WSNs. The objectives and goals of this survey paper can be summarized as follows: (1) To build a huge audience aware of the existence of a number of security attacks on WSNs; (2) To facilitate the readers and provide a

sound framework through a in depth taxonomy of WSN security attacks; (3) To help protocol designers identify and select appropriate strategies by knowing the nature of WSN security attacks by providing them a complete WSN attack model. This survey is different from earlier surveys in that it covers majority (fifty two) of the WSN attacks till date and presents a detailed taxonomy of WSN attacks based on different layers of communication protocol stack. To the best knowledge of the authors, no such work on this magnitude exists before.

3. Structure of the Paper

The paper is further structured in seven sections as mentioned. Section 4 describes related work, section 5 deals with the Security Challenges of WSN, section 6 discusses Security Goals of WSN, section 7 elaborates Security Threat Model of WSN, section 8 gives the classification of WSN attacks of different layers of communication protocol stack, section 9 summarizes the discussion and the conclusions are presented in section 10.

4. Literature Survey

During the past few years many researchers have contributed in analyzing the security attacks of WSN. Most of these papers have not touched upon Security Challenges of WSN, Security Goals of WSN, Security Threats of WSN, Classification of WSN attacks, and Security Threat Model in more detail, thereby unable to clearly draft a wholesome picture of WSN Security model. A brief description of these related works is given in Table 1:-

Table 1. Summary of Previous Surveys on Attacks on Wireless Sensor and Adhoc Networks

Year	Authors	Literature	Main Contributions
2010	Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S. Ali and Prof.J.S. Deshpande	"A Survey of Mobile Ad-Hoc Network Attacks"	• Discussion on 28 WSN security attacks on the basis of communication protocol stack • Discussion on five major security goals
2009	N. Shanti, Dr. Lganesan and Dr. K. Ramar,	"Study of Different Attacks on Multicast Mobile Ad Hoc Network"	• Simulation of two most common WSN attacks • Discussion on issues in secure multicast routing
2009	Dr. G. Padmavathi and Mrs. D. Shanmugapriya,	"A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks"	• Classification of security attacks, security mechanisms and challenges in WSN • Detailed information about the security goals in WSN
2010	Abhishek Pandey and R.C. Tripathi	"A Survey on Wireless Sensor Networks Security"	• Discussion on layered architecture of WSN • Elaborated six different attacks on WSN along with their mitigation techniques • A brief overview of WSN simulators is presented

2012	Dr. Yudhvir Singh, Dheer Dhwaj Barak, Vikas Siwach and Prabha Rani	"Attacks on Wireless Sensor Networks : A Survey"	• Discussion related to security issues of WSN • Elaborated eight different security attacks in WSN
2010	Kalpana Sharma and M.K. Ghose	"Wireless Sensor Networks : An Overview on its Security Threats"	• Discussion on overview of the general security needs for WSN • Critical security challenges are also elaborated • A detailed coverage of different internal attacks of WSN
2012	Rajkumar , Sunitha K. R. , Dr. H.G. Chandrakanth	"A Survey on Security Attacks in Wireless Sensor Network"	• Discussion on applications of WSN • Elaborated eight different types of WSN attacks which are followed by counter measures of these security attacks
2011	Shio Kumar Singh, M.P. Singh and D.K. Singh	"A Survey on Network Security and Attacks Defense Mechanism for Wireless Sensor Networks"	• Discussion on constraints in WSN, Security Requirements in WSN • Elaborated Security Goals in WSN, Security Challenges, Security Attacks in WSN and Future Trends • The authors have discussed 18 security attacks of WSN
2012	Jyoti Ahlawat, Mukesh Chawla and Kavita Sharma	"Attacks and Countermeasures in Wireless Sensor Networks"	• Discussion on critical security issues in WSN • Described attacks on WSN, and have given a review on the related work pertaining to security in WSN. The authors have discussed five security attacks of WSN in detail
2006	John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary	"Wireless Sensor Network Security : A Survey"	• Discussion on security issues in WSN • Limitations of WSN • Classification of attacks based on the capacity of adversary and attacks on WSN. The survey paper includes nine security attacks

5. Security Challenges of WSN

The WSN faces a significant number of security challenges some of which are mentioned below:-

(a) **Wireless Medium**. The passive attacks like eavesdropping is quite simple to launch due to the fact that WSN uses wireless medium for communication purposes which is inherently less secure [5]. The adversary can very easily intercept, alter or replay the transmission when desired [5].

(b) **Ad-Hoc Deployment**. The Ad-Hoc communication environment of WSN demands the security solution to facilitate the uninterrupted operation of sensor nodes in case of node failure, addition or mobility. The security solutions must have the potential to support self-configuration in case a node fails or is replaced by some adversary [5].

(c) **Hostile Environment**. The sensor nodes of WSN are most likely to be deployed in unattended and hostile environment that creates a possibility that an attacker or adversary can get physical access to these devices. These nodes can be physically captured by an adversary for retrieving important security parameters like cryptographic keys by an attacker [5].
(d) **Resource Scarcity**. As the nodes of WSN can be deployed in remote and hostile environment without further attendance, the importance of energy conservation and hardware resource utilization increases manifold. The security solution for WSN must be efficient in terms of bandwidth consumption, computational capability, memory utilization and energy consumed for secure communication protocol (transmission and reception) to achieve these WSN targets [5].
(e) **Immense Scale Deployment**. Scalability is a major requirement of WSN and nodes number can range from few dozens to thousands. However, where scalability can be major requirement the security model for such a huge network has to be designed thoughtfully, such that with scalability the WSN is able to achieve high computation and communication efficiency [5].

6. Security in Wireless Sensor Networks (WSN)

The security design of WSN needs to be robust and effective for which it has to cover WSN security goals, security threats and security classes.

(a) **Security Threat**. An event that has the potential to adversely affect the systems' performance by virtue of security breach is known as security threat [11].
(b) **Security Threat Classification**. The attacks on WSN can be largely classified as interception, interruption, modification and fabrication [13].

- **Interception**. A type of an attack that can harm the confidentiality by attempting to have unauthorized access of the sensor node and its stored data/keys [11].
- **Interruption** A type of an attack that prevents the legitimate communication between the communicating parties. Interruption can harm the availability of the network [11], by corrupting messages, injection of malicious code or physically capturing of nodes etc.
- **Modification** A type of an attack that harms the integrity of the network. In this attack the adversary not only attempts to have an access of the data but also attempts to tamper it, for example the adversary can alter the contents of the data that is in transition [11].
- **Fabrication** harms the authentication of the data that is being transmitted as the adversary injects the false data packets into the network [11].

(c) **Security Goals.** It is well known fact that a sensor network has the ability to operate both in an Adhoc fashion as well as in normal network manner thus the security goals encompasses both, for conventional networks known as "Primary Goals" and goals appropriate to distinctive constraints of wireless sensor networks known as "Secondary Goals" [14]. The primary goals are Data Confidentiality, Data Integrity, Node Authentication, and Node/Network Availability [15]. Whereas, the secondary goals are Optimal Power Consumption, Self Organization, Data Originality Freshness, Secure Localization and Time Synchronization, and [16]. These are explained in detail in the subsequent paragraphs.

A. Primary Goals

Data Confidentiality

Data Confidentiality refers to a concealment of messages in transition so that the messages communicated or transmitted via sensor nodes and networks remain aloof or confidential from the passive attacker. It is much

more difficult to ensure data confidentiality in Wireless Sensor Network than a wired network, since in WSN neighbouring nodes of a transmitting node also listen to the communication not intended for them, and therefore can easily accomplish eavesdropping on the information being routed.

Data Integrity

Data Integrity refers to the message being transmitted to remain unaltered. Data Integrity in sensor network is critical because the messages from source node to destination node must pass through intermediate nodes and despite the confidentiality measures there is still a probability of compromise by alterations [14]. The attacks on integrity of the network are further categorized as follows:-

- **Non-Repudiation** refers to condition in which both sending and receiving parties must not deny that they have not sent/received the data message/control message. The WSNs are the most vulnerable networks to these types of attacks because they lack centralized controlling infrastructure. Such type of attacks can easily be initiated by impersonating any network node or by injecting a new unauthorized node into the network. These illegitimate nodes may deny the fact that they received any of the valid messages.
- **Modifications**. After intercepting or accessing information, the attacker modifies the information to make it beneficial to itself.
- **Masquerading**. Masquerading or spoofing happens when the attacker impersonates somebody else.
- **Replaying.** In this attack, the attacker acquires a copy or duplicate of the message transmitted by the node and afterward tries to replay that message.

Data Authentication

Data Authentication relates to the identification of the sending origin of the received message and also its reliability [14]. The Wireless Sensor Networks involve both modification of packets attack and insertion of additional or false packets attack [18]. As the communication medium of WSN is wireless in nature and sensor networks are generally deployed in hostile or unattended environment. Thus, it becomes very difficult to guarantee data authentication [19].

Node or Network Availability

Node Availability means that whether the node has the capability to operate its assets and/or the accessibility of network is ensured for the communicating nodes [14]. There should be an assurance of availability of the node/network under any critical situation like DoS attacks. On the MAC and Physical layers the attackers may use jamming techniques to interfere with wireless communication [20]. By launching DoS attack the attacker can also disrupt the routing protocol on network layer [21]. Also, the high level services can also be brought down by the attacker on higher layers [15].

Access Control

Access Control means that only legitimate and authorized users have a right to access the services of the node.

B. Secondary Goals

Data Freshness

The freshness of each and every data packet needs to be ensured even the confidentiality and integrity of data has been assured.[16]. Informally speaking, data freshness depicts that the data is latest, as well as data freshness must ensure that no previous messages will be replayed [17].

Route Freshness

Even if we ensure the data freshness there is still a need to ensure freshness of the network route. As we know that the nodes of WSNs are inherently facing resource scarcity in terms of limited processing, storage, and energy capacities [22], an attacker could impersonate nodes and restrict them to update their routing tables. Therefore, the routing protocols should be flexible and adaptive as to counter the topology changes and ensure freshness of the route.

Self-Organization

A WSN is a typical form of an ad-hoc network which has no fixed or centralized infrastructure exists for the reason of network management [16]. This inherent constraint in the network architecture of WSN poses an immense challenge to its security aspect. In order to successfully counter the limitation of decentralized (peer to peer) infrastructure every sensor node of the network should self-organize and self-heal independently and flexibly as the situation dictates. If the nodes lack self-organization and self-healing capability then the damage resulting from an attack or from a natural calamity could be catastrophic.

Time Synchronization

The wireless sensor network is a distributed system, and in such distributed systems each node has its own clock and own time domain [23]. However, a common scale among sensor nodes is important to identify causal relationship between events in the physical world, and to support the elimination of redundant sensor data [23]. Furthermore, the packet's end-to-end delay may be computed with two pair-wise communicating sensor nodes [16].For tracking applications, a group synchronization is required in sensor network which must be collaborative [14].

Secure Localization

Localization is the task of determining the physical coordinates of sensor nodes (or a group of sensor nodes) or spatial relationship among objects [24]. The utility of a wireless sensor network depends on the ability of its sensor nodes to accurately, precisely and automatically determine/trace the current location of the intended senor nodes to which it wants to communicate. Localization is of utmost importance whether the sensor network is deployed for the purpose of surveillance, tracking, and detection or otherwise. Unfortunately, location of sensor node can effortlessly be manipulated by adversary through reporting of fake signal strengths, or message replays [16].

Power Management

The power consumption of a WSN is of key concern due to inherent energy constraints of sensor nodes [25] as they are generally operated with batteries and it may be impractical to change the depleted batteries in deployed area. It is pertinent to mention here that those attacks launched to exhaust the power of the nodes' batteries can adversely affect the performance of the entire setup if the attacker launches this attack on the "critical node" i.e. a node to which different nodes are connected and which serves as a gateway to other nodes. The attacker can put the target node into undesired routing updates, irrelevant computations or sending unnecessary control messages. Eventually, the node's battery gets depleted resulting in DoS.

The following figure classifies and compares WSN attacks based on security threats (confidentiality, integrity, availability and authenticity) and security classes (interruption, modification and fabrication) as shown in figure 3:-

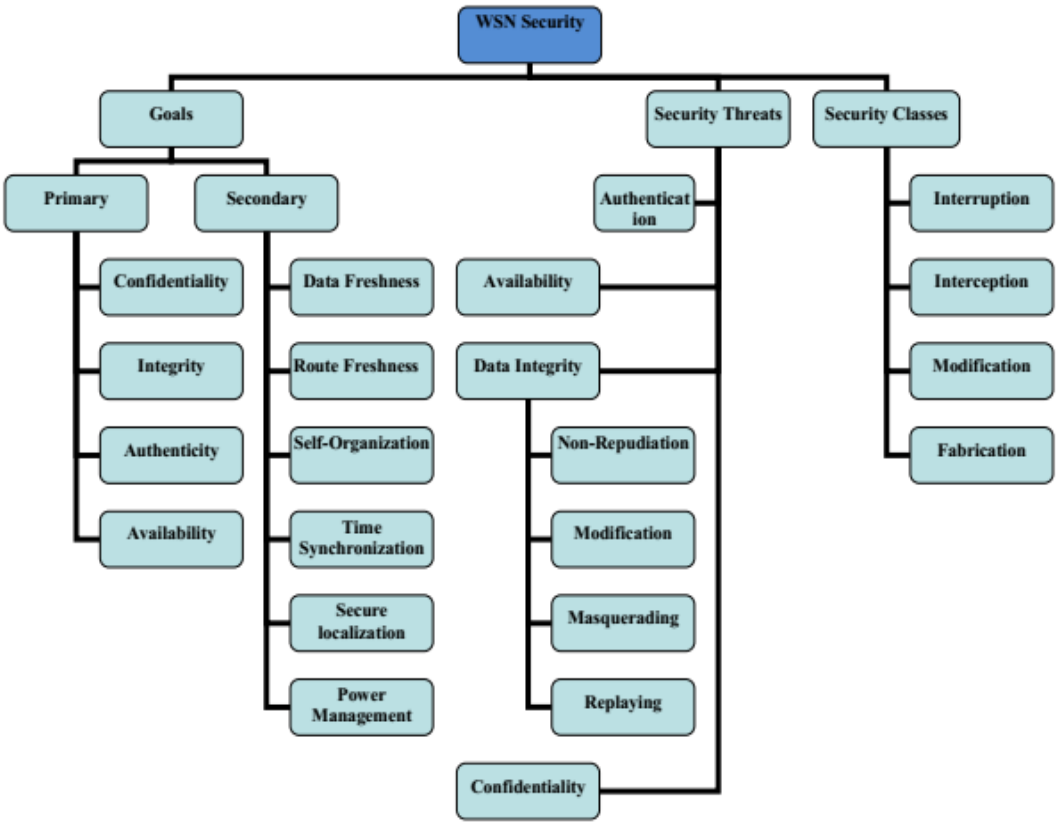

Fig.3. Security in WSN

7. Threat Model in WSN

There are various classes of wireless sensor networks attacks based on the objectives and nature of the adversaries or attackers [43]. The threat models will be discussed in this section.

Attack Based on Damage/Access Level

In this subsection of the paper, the classifications of wireless sensor networks attacks are based on their access level or damage level is presented, these include:

Active Attacker

An active attack is launched by the attacker to upset the regular operation of a network by altering and/or destroying the data being communicated in the network [16]. These attacks, whether performed by inner adversary or internally compromised node involves actions such as:

- Inserting fake or faulty data into wireless sensor network [16]
- Impersonating [57, 58]
- Modification of data packet [59]
- Unauthorized access monitors, eavesdropping and modifying data stream and resources[16]

- Generate opening in security protocol [60]
- Overfilling the wireless sensor network [56]

Some of the objectives and impacts of these attacks are [56]:

- Disruption in operation of wireless sensor network
- Degradation of performance in wireless sensor network
- Destruction of sensor nodes
- Alteration or modification in data
- Services of wireless sensor networks cannot be used optimally
- Restricting certain nodes from communicating with their neighbouring nodes

Passive Attacker

A passive attacker has no capability to disturb the typical function of the network and he makes no alterations in the messages travelling among the nodes. In passive attack the integrity of the data is not compromised but the confidentiality of the data is compromised. Therefore, it becomes extremely difficult to detect the passive attack. The following functions may be performed by the passive attacker [56]:

- A passive attacker is like a normal node which collects information from wireless sensor networks
- eavesdropping and monitoring of data [61] from communication channel by authorized attackers or adversaries

The objectives and impacts of such type of attacker contain:

- Eavesdropping on data, information stealing and gathering [56]
- Confidentiality and privacy necessities will be compromised [56]
- Selfish node stores energy and it refrains itself from cooperation [56]
- Degradation in the functionality of wireless sensor network
- A network partition may occur due to non-cooperative behaviour of nodes in operations [26]

Attacker Location Based Attack

Attackers can be deployed within or outside the perimeter of wireless sensor networks. This subsection presents and classifies WSN attacks based on attacker's location.

External Attacker (Outsider)

If the attacker launches an attack by using the malicious node(s) outside of the network that was not a part of the network when the network was initially deployed then this type of attack is termed as external attack. While launching the external attack the aim of the adversary is to effect traffic congestion, disseminate bogus routing information or disturb nodes from extending desired services [16].

Some salient features of outsider attacks include:

- The adversary or attacker exists outside the perimeter of the network i.e. does not fall within range of wireless sensor networks[61]
- illegal or unauthorized parties execute this attack [57]
- Attacks are initiated before being authenticated [56]

Few general effects of outsider attacks are [56]:

- The complete communication of WSN is jammed
- The resources of WSN consumed aggressively
- DoS attacks activated

Internal Attacker (Insider)

If an adversary launches an attack by using or impersonating one of the actual node of the network that was originally the part of the network at the time of its deployment then this type of attack is termed as internal attack [16].

Some of the goals of these attacks are [56]:

- The adversary has got a right to cryptographic keys or other codes of wireless sensor network
- Partial or total degradation
- secret keys disclosed

Attacking Devices Based Attack

Adversaries can use diverse types of devices to attach with wireless sensor networks to launch attacks; such devices may contain dissimilar powers, antenna and other relevant capabilities [43]. The most general categories of these attacks include:

Mote-Class Attack

The mote-class attack [56] is an attack in which devices comparable to WSN sensor nodes to be attacked. This depicts that this attack:

- Occurs within the perimeter of wireless sensor networks
- Uses compromised sensor nodes or granted access to alike motes/nodes (which contain comparable functional capability as wireless sensor network's motes/nodes) [62]
- Ensures the execution of programs of malicious nature [63]

An attacker of Mote-Class may have many objectives, which include:

- To ensure the jamming of radio link [56]
- To paved way for the stealing of cryptographic keys [56]

Laptop-Class Attack

Laptop-class attack [56] is an attack which utilizes extra powerful devices as compare to ordinary wireless sensor nodes, to achieve the following:

- Injection of unwanted traffic [57]
- eavesdropping of the entire wireless sensor networks data will be carried out by a device which belongs to a laptop-class[59]

Attackers of laptop-class have many effects on wireless sensor networks [56], for instance:

- more grave attacks will be launched which may then lead to more severe damage [56]
- Possesses the capability to provide way in to low latency communication channel and high bandwidth [56]

Attack Based on Function (Operation)

These types of attacks have been classified in three types, based on their core functionality, which encompasses: secrecy, availability and stealth (this kind of attack is in service stealthily on the communication channel) [64].

8. Classification of Wireless Sensor Network Attacks

Now, we will discuss different types of attacks that can be launched on 5 different layers of communication protocol stack. We, here divide these attacks as active and passive attacks.

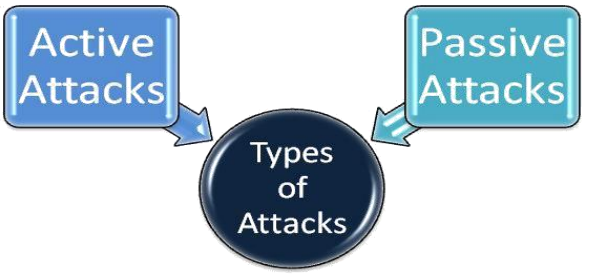

Fig.4. Types of Security Attack

Active Attacks

The active attacks can be initiated on 5 different layers of communication protocol stack are discussed below:

A. Physical Layer Attacks

The attacks are hardware oriented at the physical layer and though simple to perform, need access to some sort of hardware to become effective [16]. These attacks are fairly simple and do not need complete information of the technology [17, 18].

Physical Layer Jamming Attack

Jamming attack can be launched by an attacker both externally and internally. In order to launch a jamming attack he uses a high power transmitter, generating a signal(s) that will be strong enough to interfere with the legitimate wireless communication. Thus, the result could be either to prevent a real source from transmitting packet, or denying the reception of legitimate packets [16]. Random noise and pulse is the most common type of signal jamming. For the adversary, jamming attack is quite difficult to launch due to dynamic network topology or frequent position changing of sensor nodes.

Physical Attacks

WSNs are usually operated in hostile and remote environmental conditions. In these environments, the distributed and unattended nature of WSNs deployment makes them vulnerable to physical attacks. The attacker can destruct the node physically, hamper with the associated circuitry, extort cryptographic assets, amend coding in the sensors or substitute the codes with the sensors that lie within the range and control of the invaders [29]. Such type of physical attacks destroys sensor nodes eternally, so the losses are permanent [16].

Node Subversion

If an adversary captures a node either physically or electronically the information residing in the node may be revealed including the cryptographic keys and eventually the entire sensor network will be compromised. [30].

Passive Information Gathering

In wireless sensor networks there is a possibility that an invader may gather critical information from the wireless sensor network, provided the information is unencrypted, using powerful algorithms [16]. A hacker with a well designed antenna and powerful receiver can easily invade the data stream [15]. This enables them to intercept messages including the physical location of the sensor nodes that permits invader to find those nodes and demolish them [31]. Besides the location of the sensor node, opponent can examine the application specific message contents containing message IDs, time stamps and other fields of interest [31].

Device Tampering Attack

The nodes in WSNs are typically soft, compact in nature unlike nodes in a wired network. Control messages initiated by a node should be validated as well as signed by a receiver node which is in the process of route discovery [15]. Hence, the route discovery impedes anti-authenticating attack, for example, generating routing loops, as no node is able to generate and mark a data packet in the name of invented or spoofed node [15].

Message Corruption

The integrity of the message can be compromised if an adversary amends the contents of the message. [32].

B. Medium Access Control Layer Attacks

As we know that the attacks can be categorized depending on the performance delivered by a node. The improper behaviour of the node can be malicious intent or merely selfish interest [29].

Selfish Misbehaviour of Nodes

- **Manipulation of Protocol Parameters of 802.11**

The manipulation of the parameters of protocol 802.11 is also of an attack which can be launched by an adversary e.g. (oversized NAV, shorter DIFS, Back-Off manipulation) [26]. Such attacks will unavoidably give unjustified benefit to the selfish node in terms of unwarranted access to bandwidth or channel [26].

- **Selfish Nodes' Refusal to Forward Packets**

A selfish node usually refuses to participate in the process of forwarding packets or start dropping the packets purposely to preserve its own assets or resources [26] which will disturb the usual function of the network.

Nodes Malicious Behaviour

These types of attacks are essentially intended to interrupt the standard functioning of the network like availability of network resources, throughput and consequently obstruct the other legal users from communicating with each other [26]. The attacks examined in such scenarios are mainly Denial of Service (DoS) attacks as discussed below:

- **Back-off Interval Manipulation**

In this type of attack [33,34], the sender has the capability to select smaller intervals if he has an intention of initiating a Denial of Service [26]. This attack capitalizes the vulnerability of 802.11 protocols [35].

- **Jelly Fish Attacks**

In case of Jelly Fish attack [36] the mischievous node obeys the protocol but silently disorders, delays or drops packets periodically [39]. Such an attack is hard to identify as the node functions fine a large amount of time and hence any monitoring mechanism is unable to invalidate the trust level of such nodes [36].

- **Intelligent Cheater Attacks[37]**

These attacks are comparable to Jelly Fish Attacks [26] where the nodes behave fine nearly all of the time and behave badly occasionally [37]. The damage potential of such threats is difficult to detect since such intelligent and smart nodes keep their trust rating within certain threshold limit [37].

- **Link Layer Jamming Attacks**

These attacks focus on disrupting a normal operation among sensor nodes about the jammer [51]. This attack exploits the weaknesses of a few link layer protocols [52].

- **Collisions**

An enemy or adversary node may purposefully originate collisions in explicit packets such as acknowledgment (ACK) messages [51]. This results in expensive exponential back-off in few medium access control protocols [51].

C. Network Layer Attacks

The idea related to the network layer attack is to inject control by the node itself into the sender and receiver path, and hence divert the flow of network traffic [26]. The invader may attain these aims and objectives by attacking any routing protocol. Different network layer attacks will be discussed in the ensuing paragraphs.

Flooding Attack

The objective of flooding attacks is to drain the network assets like computational and battery power, bandwidth and thus consuming the node's resources or to interrupt a routing function to originate strict deprivation in the operation of network [38]. As a consequence network bandwidth, and node battery power will be utilized and could be lead to DoS [39].

Blackhole Attack

This attack has two distinctive characteristics [26]. First, the node makes use of routing protocols, such as Ad-hoc On-demand Distance Vector (AODV), to announce itself having route from source node to destination node even the path is amended, with the objective of packets interception [15]. After that, an invader uses the intercepted packets for its own purpose, without forwarding them [15].

Greyhole Attack

McDonald and Pirzada have talked about dissimilarity in blackhole attack, called Greyhole attack .In Grayhole attack, the node does not drop all the packets which are passing through it but it keeps itself selective i.e. drops only few packets.

Wormhole Attack

This attack considers as one of the most devastating and complicated attacks in WSN [41]. An invader keeps record of packets at one position in the network and makes a tunnel with another node of the network and thus the packets passes through this tunnel [42]. Such tunnelling between these two colluding attack paths is called wormhole [43].

Rushing Attack

The colluding invaders use tunnel procedure to form a wormhole. The packets that tunnelled through a wormhole can disseminate more rapidly than any usual multi-hop route, if a speedy transmission route is available between two ends of a wormhole. Such an attack is called rushing attack [44].

Link Withholding Attack

In Link Withholding Attack, the wicked node cannot not propagate the information related to the links to particular nodes, which may cause loss of the links to these nodes [26].

Link Spoofing Attack

In this type of attack, a malicious node propagates bogus links with other nodes except neighbouring nodes to interrupt the routing operations [45].

Byzantine Attack

In Byzantine attack, an intermediate node that has become compromised or a group of compromised nodes work in agreement and initiate attacks like packet forwarding through non-optimal paths, creating routing loops, hence causes degradation and/or disruption of the routing activities.

Colluding Misrelay Attack

In this type of attack, numerous invaders try in agreement to drop and/or change the routing packet(s) to interrupt the routing operation in wireless sensor network. Such an attack is hard to identify by means of the conventional or usual methods like Pathrater and Watchdog[46].

Replay Attack

In WSN, the network topology keeps on changing regularly owing to the mobility of sensor nodes, which depicts that the present network topology will not stay alive for a large period of time. In such an attack, a sensing node keeps record of valid control messages of some other node and retransmits them later on [47]. This is one of the reasons that other sensing nodes have to keep record of their routing tables [26].

Position Disclosure Attack

The invader gathers the information about the structure of the network or position of a desired node.It collects the information of node, such as route map to plan attack scenario.

Resource Consumption Attack

A Resource Consumption Attack is also recognized as Sleep Deprivation Attack. The invader can make an effort to utilize battery of node by forwarding packets, or by requesting excessive route discovery of victim node.

IP Spoofing Attack

In case of conflict detection allocation, a fresh node elects the random address (call X) and propagates a packet (conflict-detection) in sensor network. Any rejection from a node will impede it utilizing such address. If the victim node at all times imitates an associate which has taken an identical IP address and replies with “rejections”, this is known as IP Spoofing attack as depicted below [15]:

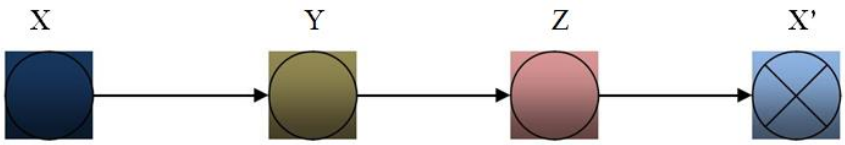

Fig.5. IP Spoofing Attack

State Pollution Attack

In such an attack, a malicious sensing node gives false parameters in response e.g. in finest effort location, malicious allocators can at all times allocate the fresh node an occupied address that directs to repetitive broadcast of Duplication Address Detection message all over the sensor network and cancellation of fresh node[15].

Neighbour Attack

An intermediate node includes its ID in the packet prior to disseminating the packet to the next node upon receiving a packet. In case, an invader just forwards the packet devoid of mentioning its ID in that particular packet, the nodes consider they are neighbours even they are not within the communication range of each other.

Packet Dropping Attack [15]

Using the packet dropping attacks, routing messages can be interrupted directly. In a typical attack of this type, an attacker can collaborate as typical in the route discovery process and initiates the packet dropping attacks on regular basis, if it is mentioned as an intermediate node.

Sleep Deprivation Torture Attack

The thought behind this Sleep Deprivation Torture Attack is to ask for the services offered by a node again and again. So that the node can enter into power idle or preserving state. Thus, preventing it to take its sleep (thus the name).

Sinkhole Attack

In Sinkhole, main objective of attacker is to draw attention the entire traffic from a specific area by virtue of a compromised node. This process of gathering traffic is called sinkhole attack [48].

Sybil Attack

In such an attack, a malicious sensing node shows various IDs to other nodes that are component of the network. This attack makes target fault tolerant schemes like multi-path routing, distributed storage [48].

False Node Attack

A false sensing node includes incrementing of a sensing node by an opponent and initiates the insertion of malicious data. An intruder might insert a node to the network which injects false data or impedes the channel of correct data [49]. A malicious code injected into the network could reach to all the nodes, potentially annihilating the entire network, or capture the network on behalf of an adversary [49].

Acknowledgement Spoofing Attack

The attacking node may spoof the acknowledgements of overheard packets which are intended for neighbouring sensing nodes to give fake information to these neighbouring sensing nodes [51]. The fake or false acknowledgement can persuade the sending node that a disabled or dead node is alive or a weak node is strong. Thus, the selective forwarding attacks will be generated by the target nodes while sending information by utilizing strong false links.

De-synchronization Attack

This type of an attack causes disruption in the present connection. An attacker may maliciously force the end host start the start the retransmission of lost frames. If the timing is correct, the attacker may impede or degrade the capacity of the end host(s) to efficiently exchange or share the data. It is a scenario of disruption of a presently available connection. An invader may force an end host for a retransmission of lost or missed frames. Hence, in this way the nodes start to waste their energies in the efforts to recover from those errors actually do not exist in reality [51].

Hello Flood Attack

The invader sends HELLO packets from one node to some other node again and again with more energy. This attack makes use of s HELLO packets as a “stick” to flood sensors in wireless sensor network [16]. In this

attack, an invader uses high processing power and transmission range and transmits HELLO packets to several sensor nodes which are inaccessible with in wireless sensor network [51]. These sensors infer that the invader is their neighbour. As a result suffered nodes try to go through the invader while transmitting the information to the base station as they are aware of their neighbours and are eventually spoofed by the invader [48].

Selective Forwarding Attack

It is very crucial that all sensing nodes in a multi hop network will accurately and faithfully forward the received message(s) to next node [51]. But a few compromised nodes might deny forwarding packets; however, neighbours might initiate using other node [48].

Routing Table Overflow Attack

In this type of attack, invader tries to make routes to the nodes which do not exist. The main objective of this attempt is to generate enough routes to stop fresh routes from being formed, thus overwhelming the implementation of protocol [15].

Routing Table Poisoning Attack

In Routing Table Poisoning Attack, the compromised node(s) in the network modify the genuine route or send the fictitious routing updates to other uncompromised nodes called routing table poisoning attack. This routing table poisoning will creates congestion in parts or portions of the network or result in sub-optimal routing [15].

Packet Replication Attack

In Packet Replication Attack compromised node replicates old packets which utilizes extra bandwidth resources and battery power of the nodes and becomes cause of needless uncertainty in the routing processes.

Route Cache Poisoning Attack

Every node keeps a route cache that maintains information about the routes that have been recognized by the nodes in the recent past in case of reactive routing protocols like AODV etc. An invader may also disrupt the route cache to attain related goals like routing table poisoning [15].

D. Transport Layer Attacks

SYN Flooding Attack

The invader initiates a great number of half-opened TCP connections with a suffered node, but cannot completely performs handshake to open the connection. It's a Denial of Service attack.

Session Hijacking Attack

In this type of attack, the invader spoofs the IP address of victim node, finds out a proper sequence numbers which is anticipated by the target node , and subsequently carries out the Denial of Service attack on the victimized node [16].

E. Application Layer Attacks

The Application layer like other layers is also susceptible in terms of security compared with other layers of communication protocol stack. The application layer supports various protocols such as FTP, TELNET, HTTP and SMTP comprises of user data which offers many access points and vulnerabilities for the invaders [26]. The application layer attacks on sensor networks are discussed below:

Malicious Code Attack

Malicious codes such as worms, virus, Trojan Horses and spywares, can attack both user application and

OS()[50]. These malicious programs usually damage or cause to slow computer system and networks [50].

Repudiation Attack

The term Repudiation refers to a denial of partial or complete contribution in communication. For example, a selfish person can refuse to conduct credit card purchasing operation, which is with reference to commercial system, considers as a repudiation attack.

False Data Filtering Attack

The energy restricted Wireless sensor networks usually utilize in-network data aggregation [51]. The end-to-end cryptography becomes impracticable because of the requirements of data aggregation [56]. An attack on a point of aggregation gives permission to the attacker to alter or damage entire amount data coming from the down-stream nodes as well as the overall data aggregation consequence experienced at the base station and consequently the attacker can critically impede sensing applications [51].

Clock Synchronization Attack

Time synchronization is a vital building block in wireless sensor networks [23]. Time desynchronization can interrupt sleep schedule [23]. An invader node can transmit the fallacious synchronization message to its adjacent nodes throughout the period of time exchange, and thus make other nodes to evaluate an erroneous skew and phase offset [51].

False Data Injection Attack

The nature of in-network aggregation is susceptible to fictitious data injection. Attacker may initiate an external attack by transmitting its personal data packets in order to inject false data. This attack can also be initiated by first compromising the internal, the then exploit such compromised nodes to insert false data into the network [51].

Passive Attacks

The listening and monitoring of communication channel by unauthorized invaders is termed as passive attacks. The passive attacks are discussed below:

Monitoring and Eavesdropping

Attacker can easily find out the communication by snooping to data, for example, in case the traffic transmits the control information of wireless sensor network, the eavesdropper can potentially acquire more information than available by virtue of a server [16].

Traffic Analysis

Even in the transmission of encrypted messages, possibility of analysis of WSN communication patterns is still possible [16]. Sensor communication activities can inherently disclose sufficient information to allow an opponent to facilitate damage to the sensor network.

Camouflaged Adversaries

The attacker can compromise or hide desired number of nodes in wireless sensor network. Subsequently, such nodes can imitate as a regular node to draw the packets, then misroute these packets and eventually conduct a privacy analysis [16].

Packet-tracing

An equipped attacker may notify the position of immediate sender of overheard packet in packet tracing attack [54]. The Attacker is competent to implement hop-by-hop tracing in the direction of the original data source, which becomes cause of revealing the privacy of source[51].

9. Discussions

In this section, the comparison of the attacks on five layers of communication protocol stack is presented, based on; capabilities and nature of attackers nature and wireless sensor network threat model, as mentioned in the table below:

Table 2. Wireless Sensor Networks Attacks Classification

S.No	Attack	Security Class	Layer	Attack Threat	Threat Model		
					Attacker Location	Attacking Device	Active / Passive
1	Jamming Attack	Modification	Physical	Availability/ Integrity	Both	Both	Active
2	Physical Attack	Modification	Physical	Integrity/ Availability	External	Both	Active
3	Node Subversion	Modification	Physical	Integrity/ Availability	Both	Both	Active
4	Passive Information Gathering	Modification/ Interception	Physical	Confidentiality/ Integrity/ Availability	Both	Both	Active
5	Device Tampering Attack	Modification/ Fabrication	Physical	Confidentiality/ Integrity/ Availability	Internal	Laptop	Active
6	Message Corruption	Modification	Physical	Integrity	Both	Laptop	Active
7	Manipulation of Protocol Parameters of 802.11	Interruption	MAC	Availability	Internal	Both	Active
8	Selfish Nodes' Refusal to Forward Packets	Interruption	MAC	Availability	Internal	Both	Active
9	Back-off Interval Manipulation	Interruption	MAC	Availability	Internal	Both	Active
10	Jellyfish Attack	Interruption	MAC	Availability	Internal	Node	Active
11	Intelligent Cheater Attack	Interruption	MAC	Availability	Internal	Node	Active
12	Link Layer Jamming Attack	Modification	MAC	Integrity/ Availability	Both	Both	Active
13	Packet-tracing	Interception	MAC	Confidentiality	Internal	Both	Passive
14	Collisions	Interruption	MAC	Availability	Internal	Both	Active
15	Flooding Attack	Interruption	Network	Availability	Internal	Both	Active

16	Blackhole Attack	Interception/ Interruption	Network	Confidentiality/ Availability/ Authenticity	Internal	Both	Active
17	Greyhole Attack	Interception/ Interruption	Network	Confidentiality/ Availability/ Authenticity	Internal	Both	Active
18	Wormhole Attack	Fabrication/ Interception	Network	Confidentiality/ Authenticity	External	Both	Active
19	Rushing Attack	Interruption/ Interception	Network	Availability/ Authenticity	Internal	Both	Active
20	Link Withholding Attack	Interruption	Network	Availability	Internal	Both	Active
21	Link Spoofing Attack	Interruption	Network	Confidentiality/ Availability	internal	Both	Active
22	Byzantine Attack	Interruption	Network	Availability	Internal	Both	Active
23	Colluding Misrelay Attack	Modification/ Interception/ Interruption	Network	Confidentiality/ Integrity/ Availability	Both	Both	Active
24	Replay Attack	Interruption/ Interception	Network	Confidentiality/ Availability	Internal	Both	Active
25	Location Disclosure Attack	Modification/ Interception/ Interruption	Network	Integrity/ Confidentiality	External	Both	Active
26	Resource Consumption Attack	Interruption	Network	Availability	Both	Both	Active
27	IP Spoofing Attack	Fabrication	Network	Authenticity	Internal	Both	Active
28	State Pollution Attack	Interruption/ Fabrication	Network	Availability/ Authenticity	Internal	Both	Active
29	Neighbor Attack	Fabrication	Network	Authenticity	Internal	Both	Active
30	Packet Dropping Attack	Interruption	Network	Availability	Internal	Node	Active
31	Sleep Deprivation Torture	Interruption	Network	Availability	Internal	Both	Active
32	Sinkhole Attack	Modification/ Fabrication	Network	Confidentiality/ Integrity/ Availability	Both	Both	Active
33	Sybil Attack	Interruption/ Fabrication	Network	Availability/ Authenticity	Internal	Both	Active
34	False Node Attack	Interruption/ Interception	Network	Availability/ Confidentiality	Internal	Both	Active
35	Acknowledgement Spoofing Attack	Interruption/ Interception	Network	Authenticity/ Availability	Internal	Both	Active

36	Desynchronization Attack	Fabrication/ Modification	Network	Availability/ Authenticity	Both	Both	Active
37	Hello Flood Attack	Interruption	Network	Authenticity/ Availability	Both	Both	Active
38	Selective Forwarding Attack	Interruption/ Interception	Network	Confidentiality/ Availability	Internal	Node	Active
39	Routing Table Overflow Attack	Fabrication/ Interruption	Network	Availability	Both	Both	Active
40	Routing Table Poisoning Attack	Fabrication/ Interruption	Network	Availability	Both	Both	Active
41	Packet Replication Attack	Interruption	Network	Integrity/ Availability	Both	Both	Active
42	Route Cache Poisoning Attack	Fabrication/ Interruption	Network	Availability	Both	Both	Active
43	SYN Flooding Attack	Interruption	Transport	Availability	Internal	Both	Active
44	Session Hijacking Attack	Interruption/ Interception	Transport	Availability	Both	Both	Active
45	Malicious Code Attack	Interruption	Application	Availability	Both	Both	Active
46	Repudiation Attack	Interruption	Application	Integrity	Internal	Both	Active
47	False Data Filtering Attack	Interruption/ Modification	Application	Integrity/ Availability	Internal	Node	Active
48	Clock Synchronization Attack	Interruption	Application	Availability	Internal	Both	Active
49	False Data Injection Attack	Interruption/ Fabrication	Application	Authenticity/ Availability	Both	Both	Active
50	Monitoring & Eavesdropping	Interception	Network	Confidentiality	Both	Both	Passive
51	Traffic Analysis	Interception	Network	Confidentiality	Both	Both	Passive
52	Camouflaged Adversaries	Interception/ Fabrication	Network	Confidentiality/ Availability	Both	Node	Passive

10. Conclusions

During the past few years a substantial amount of work has been done in the WSN security domain as security has become a key focus for energy constrained WSN due to diverse critical security applications. Keeping in view this fact, the key objective of our work is to encompass several security facets of WSN that can be helpful in analyzing the nature and complexities of WSN security attacks on different routing protocols [66] that can be originated from five layers of communication protocol stack. This paper will hopefully encourage the researchers to bring more efficient and robust security mechanisms and build the future sensor networks, safe and secure.

References

[1] Muhammad R Ahmad, Xu Huang and Dharmendra Sharma, " A Taxonomy of Internal Attacks in Wireless Sensor Networks", World Academy of Science, Engineering and Technology, page 427 - 430,year 2012.

[2] www.research.ee.port.ac.uk

[3] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S. Ali and Prof.J.S. Deshpande, " A Survey of Mobile Ad-Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol.2(9), 2010, 4063-4071.

[4] N. Shanti, Dr. Lganesan and Dr. K. Ramar, " Study of Different Attacks on Multicast Mobile Ad Hoc Network", Journal of Theoretical and Applied Information Technology, page 45-49, year 2009.

[5] Dr. G. Padmavathi and Mrs. D. Shanmugapriya, " A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol.4, No. 1 & 2, year 2009.

[6] Abhishek Pandey and R.C. Tripathi, " A Survey on Wireless Sensor Networks Security", International Journal of Computer Applications (0975-8887), Vol. 3 –No. 2, June 2010.

[7] Dr. Yudhvir Singh, Dheer Dhwaj Barak, Vikas Siwach and Prabha Rani, " Attacks on Wireless Sensor Networks : A Survey", International Journal of Computer Science and Management Studies, Vol. 12, Issue 03, Sept 2012.

[8] Kalpana Sharma and M.K. Ghose, " Wireless Sensor Networks : An Overview on its Security Threats", IJCA Special Issue on " Mobile Ad-hoc Networks", year 2010.

[9] Rajkumar , Sunitha K. R. , Dr. H.G. Chandrakanth, " A Survey on Security Attacks in Wireless Sensor Network", International Journal Engineering Research and Applications, Vol. 2, Issue 4, July-August 2012, pp. 1684-1691.

[10] Shio Kumar Singh, M.P. Singh and D.K. Singh, " A Survey on Network Security and Attacks Defense

[11] Mechanism for Wireless Sensor Networks", International Journal of Computer Trends and Technology- May to June Issue 2011.

[12] Jyoti Ahlawat, Mukesh Chawla and Kavita Sharma, " Attacks and Countermeasures in Wireless Sensor Networks", International Journal of Computer Science and Communication Engineering, Special issue on "Emerging Trends in Engineering", year 2012.

[13] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, " Wireless Sensor Network Security : A Survey", Security in Distributed, Grid and Pervasive ComputingYang Xiao (Eds), page 3-5, 10-15, year 2006.

[14] William Stallings, " Cryptography and Network Security Principles and Practise", Cryptography Book, 2nd Edition, Prentice-Hall, 2000,0-13-869017-0.

[15] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006

[16] Pradip M. Jawandhiya, Mangesh M Ghonge, Dr. M.S Ali, Prof.J.S. Deshpande," A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), page 4063- 4071, year 2010.

[17] Dr. G. Padmavathi, Mrs. Dr. Shanmugapriya," A survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, year 2009.

[18] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002

[19] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2-23, year 2006
[20] Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 - 40, year 2006
[21] J.T. Chiang and Y. C. Hu, "Dynamic jamming mitigation for wireless broadcast networks", in Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM), April 13–18, 2008, pp. 1211–1219, Phoenix, AZ, USA.
[22] S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, October 2002.
[23] Waltenegus Dargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", chapter # 7, year 2010.
[24] Waltenegus Dargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", chapter # 9, year 2010.
[25] Waltenegus Dargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", chapter # 10, year 2010.
[26] Waltenegus Dargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", chapter # 8, year 2010.
[27] Vikrant Gokhle,S.K. Ghosh and Arobinda Gupta," Security of Self organizing Networks", chapter # 9, year 2010.
[28] I. Aad, J. Hubaux, and E. W. Knightly, "Denial of service resilience in ad hoc networks", in Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom 2004), September 26–October 11, 2004, pp. 202–215, ACM Press, Philadelphia, PA, USA.
[29] P. Kyasanur and N. H. Vaidya, "Selfish MAC layer misbehavior in wireless networks", IEEE Transactions on Mobile Computing, 2005, 4(5).
[30] Waltenegus Dargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", chapter # 11, year 2010.
[31] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006
[32] Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. "Security for sensor networks". In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, year 2002 http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf
[33] Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 - L. Guang and C. Assi, "On the resiliency of mobile ad hoc networks to MAC layer misbehavior", in Proceedings of the 2nd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, October 10–13, 2005, Montreal, QC, Canada.
[34] L. Guang, C. Assi, and Y. Ye, "DREAM: A system for detection and reaction against MAC layer Misbehavior in ad hoc networks", Computer Communications, 2007, 30(8).
[35] IEEE802.11 wireless LAN media access control (MAC) and physical layer (PHY) specifications, IEEE, 1999. http://standards.ieee.org/getieee802/802.11.html.
[36] I. Aad, J. Hubaux, and E. W. Knightly, "Denial of service resilience in ad hoc networks", in Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom 2004), September 26–October 11, 2004, pp. 202–215, ACM Press, Philadelphia, PA, USA.
[37] L. Guang and C. Assi, "On the resiliency of mobile ad hoc networks to MAC layer misbehavior", in Proceedings of the 2nd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, October 10–13, 2005, Montreal, QC, Canada.
[38] P. Yi, et al., A new routing attack in mobile ad hoc networks, Int. J. Info. Tech., 2005, 11(2).
[39] R. V. Boppana and S. Desilva, "Evaluation of a statistical technique to mitigate malicious control packets in ad hoc networks", in Proceedings of the 2006 International Symposium onWorld of Wireless, Mobile and Multimedia Networks, 2006.

[40] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks", in Proceedings of the 27th Australasian Conference on Computer Science, 2004, Vol. 26, pp. 47–54, Dunedin, New Zealand.
[41] Y. C. Hu, A. Perrig, and D. B. Johnson, Packet leashes: "A defense against wormhole attacks in wireless networks", in Proceedings of Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, March 30–April 3, 2003, Vol. 3.
[42] Y. C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks", Selected Areas in Communications, 2006, 24(2).
[43] R. Maheshwari, J. GAO, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information", in Proceedings of 26th IEEE International Conference on Computer Communications, May 6–12, pp. 107–115, Anchorage, AK, USA.
[44] Y. C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols", in Proceedings of the 2nd ACM Workshop on Wireless Security, September 19, 2003, San Diego, CA, USA.
[45] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for Security", in 2nd OLSR Interop/Workshop, Palaiseau, France, July 28–29, 2005.
[46] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks",in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, 2000, Boston, MA, USA.
[47] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for Security", in Proceedings of 2nd OLSR Interop /Workshop, July 28–29, 2005, pp. 1–7, Palaiseau, France.
[48] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Adhoc Networks (elsevier), Page: 299-302, year 2003
[49] G. Athanasiou, L. Tassiulas, and G. S. Yovanof, "Overcoming misbehavior in mobile ad hoc networks:An overview", ACM Crossroads 11.4: Mobile and Wireless Networking, 2005.
[50] M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenker, "DDoS defense by offense", in Proceedings of the SIGCOMM 2006, September 11–15, 2006, Pisa, Italy.
[51] Qinghua Wang and Tingting Zhang, "Security in RFID and Sensor Networks", chapter # 14, year 2010.
[52] Y. Law, P. Hartel, J. Hartog, and P. Havinga, "Link-layer jamming attacks on S-MAC", Technical Paper, University of Twente, the Netherlands, 2005.
[53] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sen- sor networks", in Proc. Cerate Net Conference on Security and Privacy in Communication Networks (SecureComm), 2005.
[54] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source location privacy in sensor network routing", in Proc. 25th IEEE International Conference on Distributed Computing Systems (ICDCS), 2005.
[55] E. Sabbah, A. Majeed, K. Kang, K. Liu, and N. AbuGhazaleh, "An application driven perspective on wireless sensor network security", in Proc. 2nd ACM Workshop on QoS and Security for Wireless and Mobile Networks, Torremolinos, (Malaga), Spain, Oct. 2-6, 2006.
[56] Dr. Shahriar Mohammadi and Hossein Jadidoleslamy, "A Comparison of link layer attacks on Wireless sensor networks", International Journal on applications of graph theory in wireless adhoc and sensor networks", (GRAPH-HOC) Vol.3, No.1, March 2011.
[57] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA, Special Issue on Mobile Ad-hoc Networks MANETs; CSE Department, SMIT, Sikkim, India; 2010.
[58] J. Yick, B. Mukherjee and D. Ghosal, "Wireless Sensor Network Survey", Elsevier's Computer Networks Journal 52 (2292-2330), Department of Computer Science, University of California, 2008.
[59] Y. Zhou, Y. Fang and Y. Zhang, "Security Wireless Sensor Networks: A Survey", IEEE Communication Surveys, 2008.
[60] Y. Wang, G. Attebury and B. Ramamurthy," A Survey of Security Issues in Wireless Sensor Networks", IEEE Communication Surveys; 2006.

[61] K. Sharma and M. K. Ghose, “Wireless Sensor Networks: An Overview on its Security Threats”, IJCA, Special Issue on “Mobile Ad-hoc Networks MANETs”, CSE Department, SMIT, Sikkim, India,2010.
[62] A. Dimitrievski, V. Pejovska and D. Davcev, “Security Issues and Approaches in WSN”, Department of computer science, Faculty of Electrical Engineering and Information Technology, Skopje, Republic of Macedonia.
[63] J. Yick, B. Mukherjee and D. Ghosal, “Wireless Sensor Network Survey”, Elsevier's Computer Networks Journal 52 (2292-2330), Department of Computer Science, University of California, 2008.
[64] Y. Wang, G. Attebury and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks”, IEEE Communication Surveys, 2006.
[65] Muhammad Noman Riaz, " Clustering Algorithms of Wireless Sensor Networks: A Survey", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.8, No.4, pp. 40-53, 2018.DOI: 10.5815/ijwmt.2018.04.03.
[66] Muhammad Noman Riaz, " Clustering Algorithms of Wireless Sensor Networks: A Survey", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.8, No.4, pp. 40-53, 2018.DOI: 10.5815/ijwmt.2018.04.03

Authors’ Profiles

M Noman Riaz was born in September, 1982 at Karachi. He completed his B.S. in Electronic Engineering from Sir Syed University of Engineering & Technology, Karachi in 2006. He then joined government owned organization as an engineering officer and since then worked in different capacities that include Simulator Maintenance Manager, Manager (Telecom and Computer Networks), Manager (Training & Development), Senior Technical Manager (Air Field Electronics & Communication). Besides having professional experience in engineering domain, he had been affiliated with National University of Sciences & Technology, Islamabad as an Assistant Professor & Training coordinator from April 2014 till October, 2017. He did his M.E. in Telecomm Engineering in 2010. Also, he completed his M.S. degrees in Project Management and Software Engineering in 2017 and 2018, respectively. Currently, he is pursuing PhD in Computer Software Engineering from National University of Computer & Emerging Sciences, Islamabad, M.S. in Financial Engineering from World Quant University, Louisiana and MicroMasters in Data, Economics & Development Policy from MITx.

Engr. Dr. Attaullah Buriro is presently affiliated with Khawaja Fareed University of Engineering & Information Technology, Rahim Yar Khan and performing his duties as HoD Information Securty Department. He completed his PhD and Post Doctorate in Informationan & Communication Technologies from University of Trento, Itlay. I was also associated wtih Mohammad Ali Jinnah University, Karachi, and Federal Urdu University of Science, Arts and Technology, Karachi , as visiting faculty.He has published 20 research papers in reputable internanational conferences and journals. His research interests include behavioral biometrics, machine learning, smartphones user authentication, artificial intelligence, network security and data mining.

Engr. Prof. Dr. Athar Mahboob, TI is an academic leader par excellence. He is the Vice Chancellor of Khawaja Fareed University of Engineering & Information Technology, Rahim Yar Khan. Earlier he had been a Professor and Dean at the DHA Suffa University, Karachi (2012-15). He obtained his PhD in Electrical Engineering from National University of Sciences & Technology, Pakistan in 2005 and obtained BS and MS degrees in Electrical Engineering both from Florida State University, Tallahassee, Florida, USA (1992,1995). He has over 25 years of teaching, research and industrial experience in various prestigious universities and organizations in Pakistan and abroad. In addition to teaching and research, over the last 25 years Dr. Athar Mahboob has performed IT Consultancy assignments for many reputable organizations in the public and private sectors. His consultancy assignments have included PTCL, Pakistan Security Printing Corporation, Peoples' Steel Mills, Institute of Bankers, Pakistan, EFU General Insurance, Dubai Chamber of Commerce and Industry and many others. In addition, Dr. Athar Mahboob founded Ibn Khaldun Systems in 2005 and has undertaken more than 100 industrial projects in the financial, manufacturing, services and defence sectors.

How to cite this paper: Muhammad Noman Riaz, Attaullah Buriro, Athar Mahboob, "Classification of Attacks on Wireless Sensor Networks: A Survey", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.8, No.6, pp. 15-39, 2018.DOI: 10.5815/ijwmt.2018.06.02