*Journal of Information Security*, 2011, 2, 69-84
doi:10.4236/jis.2011.22007 Published Online April 2011 (http://www.scirp.org/journal/jis)

# A Comparison of Link Layer Attacks on Wireless Sensor Networks

**Shahriar Mohammadi[1], Reza Ebrahimi Atani[2], Hossein Jadidoleslamy[3]**
[1]*Department of Industrial Engineering, K. N. Tossi University of Technology, Tehran, Iran*
[2]*Department of Computer Engineering, University of Guilan, Rasht, Iran*
[3]*Department of Information Technology, Anzali International Branch, The University of Guilan, Rasht, Iran*
*Email*: *smohammadi40@yahoo.com, rebrahimi@guilan.ac.ir, tanha.hossein@gmail.com*
*Received December* 12, 2010; *revised January* 10, 2011; *accepted February* 26, 2011

## Abstract

Wireless sensor networks (WSNs) have many potential applications [1,2] and unique challenges. They usually consist of hundreds or thousands of small sensor nodes such as MICA2, which operate autonomously; conditions such as cost, invisible deployment and many application domains, lead to small size and resource limited sensors [3]. WSNs are susceptible to many types of link layer attacks [1] and most of traditional network security techniques are unusable on WSNs [3]; This is due to wireless and shared nature of communication channel, untrusted transmissions, deployment in open environments, unattended nature and limited resources [1]. Therefore security is a vital requirement for these networks; but we have to design a proper security mechanism that attends to WSN's constraints and requirements. In this paper, we focus on security of WSNs, divide it (the WSNs security) into four categories and will consider them, include: an overview of WSNs, security in WSNs, the threat model on WSNs, a wide variety of WSNs' link layer attacks and a comparison of them. This work enables us to identify the purpose and capabilities of the attackers; furthermore, the goal and effects of the link layer attacks on WSNs are introduced. Also, this paper discusses known approaches of security detection and defensive mechanisms against the link layer attacks; this would enable IT security managers to manage the link layer attacks of WSNs more effectively.

**Keywords:** Wireless Sensor Network, Security, Link Layer, Attacks, Detection, Defensive Mechanism

## 1. Introduction

Advances in wireless communications have enabled the development of low-cost and low-power WSNs [1]. WSNs have many potential applications [1,2] and unique challenges. They usually are heterogeneous systems contain many small devices, called sensor nodes, that monitoring different environments in cooperative; *i.e*. sensors cooperate to each other and compose their local data to reach a global view of the environment; sensor nodes also can operate autonomously. In WSNs there are two other components, called "aggregation points" and "base stations" [4], which have more powerful resources than normal sensors. As shown in **Figure 1**, aggregation points collect information from their nearby sensors, integrate them and then forward to the base stations to process gathered data. Limitations such as cost, invisible deployment and variety of application domains, lead to requiring small size and resource limited (like energy, storage and processing) sensors [3]. WSNs are vulnerable to many types of attacks and due to unsafe and unprotected nature of communication channel [5-7], untrusted and broadcast transmission media, deployment in hostile environments [1,2], automated nature and limited resources, most of security techniques of traditional networks are impossible in WSNs; therefore, security is a vital and complex requirement for these networks. It is necessary to design an appropriate security mechanism for these networks [2,8], which attending to be WSN's constraints. This security mechanism should cover different security dimension of WSNs, include confidentiality, integrity, availability and authenticity. The main purpose of this paper is presenting an overview of different link layer attacks on WSNs and comparing them together. In this paper, we focus on security of WSNs and classify it into four categories, as follows:

- An overview of WSNs,
- Security in WSNs include security goals, security

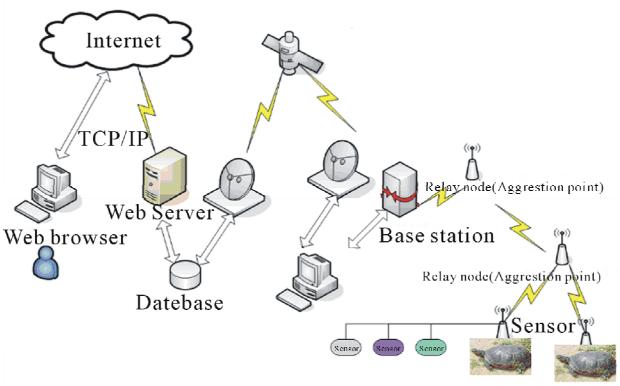



**Figure 1. WSN's architecture.**

obstacles and security requirements of WSNs.

- The threat model on WSNs,
- A wide variety of WSN's link layer attacks and comparing them to each other, include classification of WSN's link layer attacks based on threat model and compare them to each other based on their goals, results, strategies, detection and defensive mechanisms;

This work makes us enable to identify the purpose and capabilities of the attackers; also, the goal, final result and effects of the attacks on the WSNs. We also state some available approaches of security detection and defensive mechanisms against these attacks to handle them. The rest of this paper is organized as follows: in Section 2 an overview of WSNs is presented. Section 3 is mainly focused on the security issues in WSNs. Section 4 considers the threat model in WSNs. Section 5 includes definitions, strategies and effects of link layer attacks on WSNs. WSNs' link layer attacks is considered in Section 6 and finally conclusion are drawn in Section 7.

## 2. Overview of WSNs

In this section, we present an outline of different aspects of WSNs, such as definition, characteristics, applications, constraints and challenges.

### 2.1. Definition and Suppositions of WSNs

A WSN is a heterogeneous system consisting of hundreds or thousands of low-cost and low-power tiny sensors to monitor and gather real-time information from deployment environment [8-10]. Common functionality of WSNs are broadcasting and multicasting, routing, forwarding and route maintenance. The sensor's components are: sensor unit, processing unit, storage/memory unit, power supply unit and wireless radio transceiver; these units are communicating to each other, as shown in **Figure 2**. The existing components on WSN's architecture

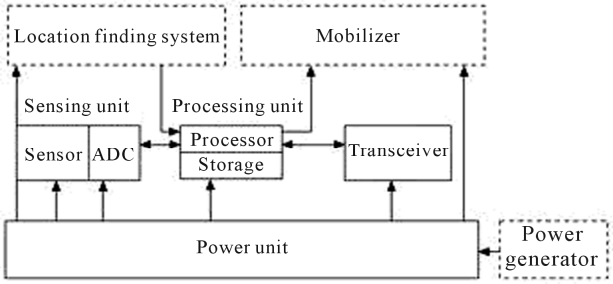



**Figure 2. WSN's node architecture.**

include sensor nodes (motes or field devices that are sensing data), network manager, security manager, aggregation points, base stations (access point or gateway) and user/human interface. Besides, there are two approaches in WSN's communication models containing hierarchical WSN versus distributed [8] and homogeneous WSN versus heterogeneous [8]. Some of the common suppositions of these networks are:

- Insecure radio links [6,10,11],
- Packet injection and replay [6,10],
- Non tamper resistant [11],
- Many normal sensor nodes (high-density) and low malicious nodes,
- Powerful attackers (laptop-class) [11,12].

### 2.2. WSNs Characteristics and Weakness

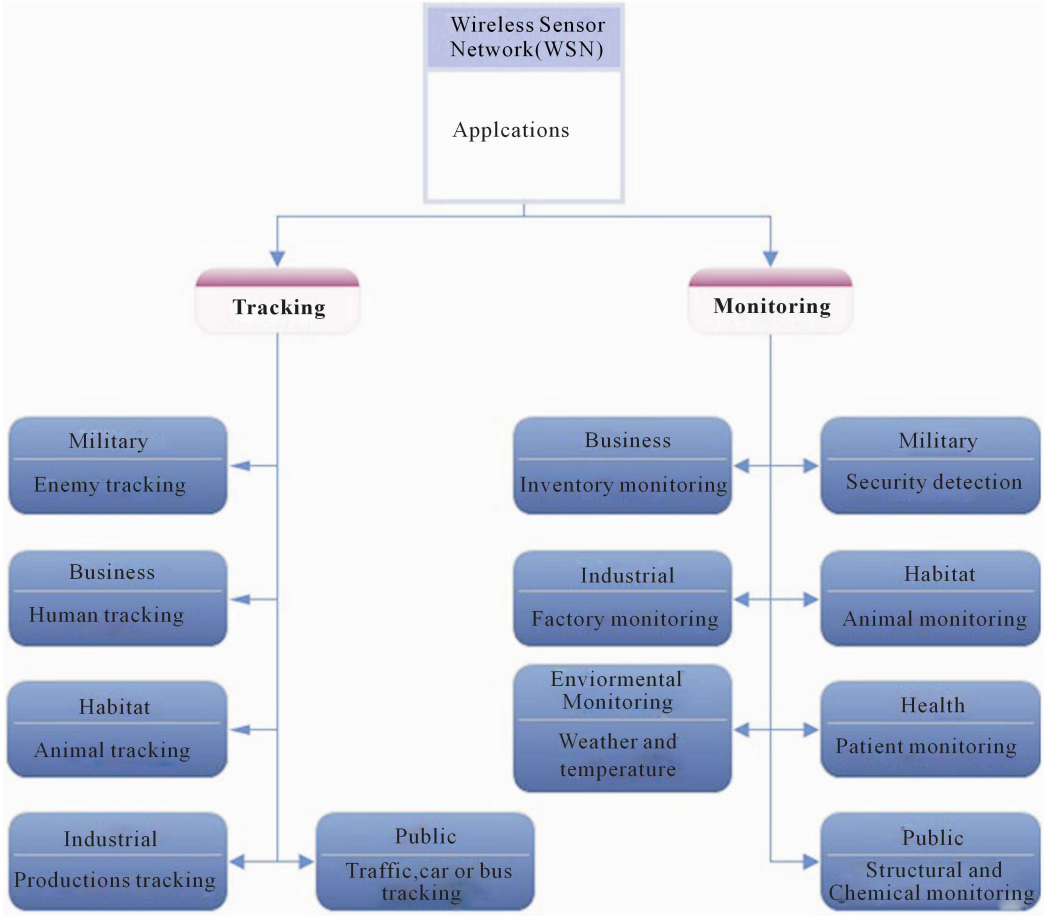
Most important characteristics of WSNs are:

- Constant or mobile sensors (mobility).
- Resource limited sensors [5,13] (limited range radio communication, energy, computational capabilities [5]), low reliability, wireless communication [5] and immunity.
- Dynamic/unpredictable WSN's topology and self-organization [5,14].
- Ad-hoc based networks [10,15] and hop-by-hop communication (multi-hop routing) [14,16,17].
- Non-central management, autonomously and infrastructure-less [10].
- Open/hostile-environment nature [10,11] and high density.

### 2.3. WSN's Applications

In general, there are two kinds of applications for WSNs: monitoring and tracking [10]. Therefore, some of the most common applications of these networks are: military, medical, environmental monitoring [3,8,10], industrial, infrastructure protection [3,10], disaster detection and recovery, agriculture, intelligent buildings, law enforcement, transportation and space discovery (as shown in **Figure 3(a)** and **3(b)**).




(a)


(b)

**Figure 3. WSN's applications.**

### 2.4. Vulnerabilities and Challenges of WSN

WSNs are vulnerable to many kinds of attacks; some of the most important reasons are:

- Theft (reengineering, compromising and replicating),
- Limited capabilities [18,19] (DoS attacks risks, constraint in using encryption),
- Random deployment (hard preconfiguration) [18, 7].
- Unattended nature [7,14,15,18].

In continue this section states most common challenges and constraints in WSNs; include:

- Deployment on open/dynamic/hostile environments [7,12,15] (physical access, capture and node des-truction);
- Insider attacks;
- Inapplicable/unusable traditional security techni-ques [3,7,19] (due to limited devices/resources, deploying in open environments and interaction with physical environment);
- Ad-hoc based deployment [12,15] (dynamic structure and topology, self-organization);
- Resource scarcity/hungry [5,7,20] (low and expensive communication/computation/processing resources);
- Devices with limited capabilities [21,22], pervasi-veness (privacy worries), wireless (medium) [5,7, 18] and mobility;
- Unreliable communication [5,7] (connectionless packet-based routing ⇨ unreliable transfer, channel broadcast nature ⇨ conflicts, multi-hop routing and network congestion and node processing ⇨ Latency);
- Unattended operation [6,12] (Exposure of physical
- attacks, managed remotely, no central management point);
- Increased attacks' risks and vulnerabilities [7], new attacks, increased tiny/embedded devices, multihopping routing (selfish) [14];
- Immense/large scale (high density, scalable security mechanism requirement);
- Redesigning security architectures (distributed and self-organized);

## 3. Security in WSNs

Now, intrusion techniques in WSNs are increasing; also there are many methods to disrupt these networks. In WSNs, data accuracy and network health are necessary; because these networks usually use on confidential and sensitive environments. There are three security key points on WSNs, including system (integrity, availability), source (authentication, authorization) and data (integrity, confidentiality). Necessities of security in WSNs are:

- Correctness of network functionality;
- Unusable typical networks protocols [3,15];
- Limited resources [5,7,23];
- Untrusted nodes [5,12,15];
- Requiring trusted center for key management [15], to authenticate nodes to each other [24], preventing from existing attacks and selfishness [23,25] and extending collaboration;

### 3.1. Why Security in WSNs?

Security in WSNs is an important, critical issue, necessa-ry and vital requirement, due to:

- WSNs are vulnerable against security attacks [7, 26] (broadcast and wireless nature of transmission medium);
- Nodes deploy on hostile environments [7,12,15] (unsafe physically);
- Unattended nature of WSNs [6,12];

### 3.2. Security Issues

This section states the most important discussions on WSNs; it is including key establishment, secrecy, authentication, privacy, robustness to DoS attacks, secure routing and node capture [18,15].

### 3.3. Security Services

There are many security services on WSNs; but some of their common are including encryption and data link layer authentication [12,15,20,23], multi-path routing [15,14, 23,24], identity verification, bidirectional link verification [14,15,24] and authenticated broadcasts. As **Figure 4** shows, the most important dimensions of security in WSNs are including security goals, obstacles, constraints, security threats, security mechanisms and security classes; however, this paper considers only star spangled parts/ blocks to classify and compare WSNs' link layer attacks based on them; *i.e.* security threats (including availability, authenticity, integrity and confidentiality) and security classes (containing interruption, interception, modification and fabrication); as shown in **Table 1**.

## 4. Threat Model in WSNs

There are many classes of WSNs' attacks based on nature and goals of attacks or attackers; but, in this section we present and compare their most important classes (called threat model of WSNs).

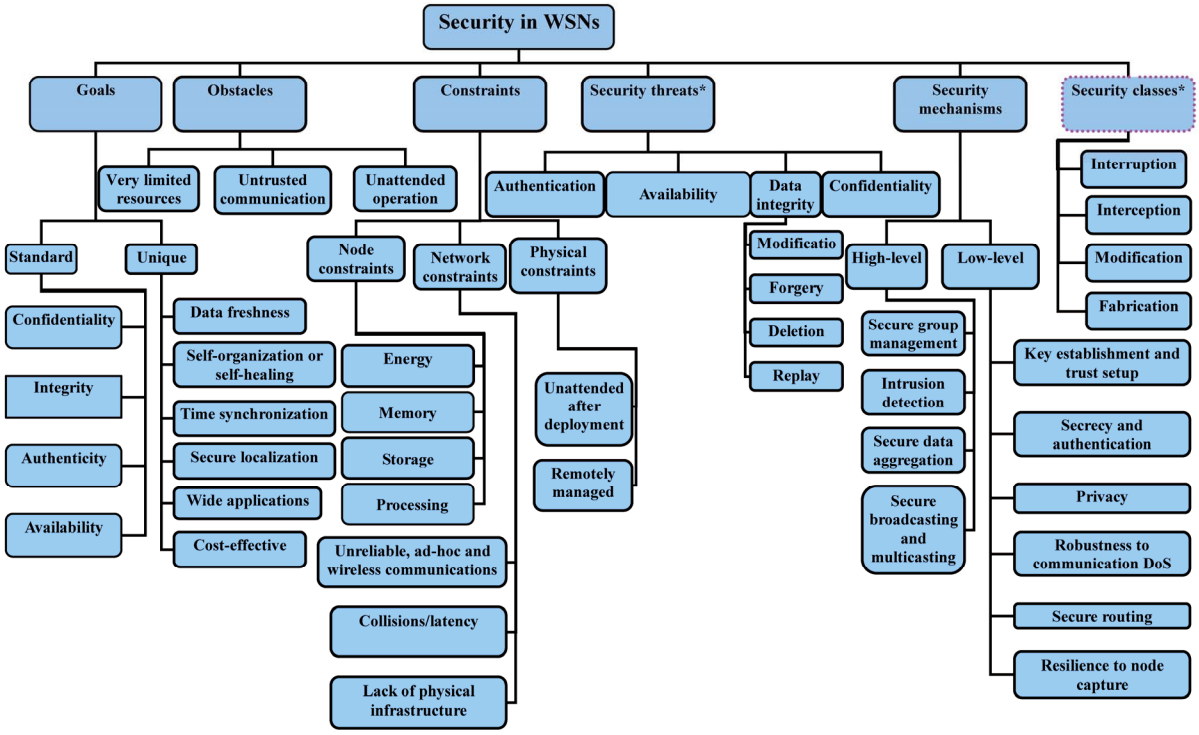



**Figure 4. Security in WSNs.**

**Table 1. WSN's link layer attacks classification based on WSNs' threat model.**

| Attacks/features | Security class[1] | Attack threat[2] | Threat model[3] | | |
|---|---|---|---|---|---|
| | | | Attacker location | Attacking device | Attacks on WSN's protocols |
| **Node outage** | Modification | Availability, integrity | External | Both | Active |
| **Link layer jamming** | Modification | Availability, integrity | External | Both | Active |
| **Collision** | Modification | Availability, integrity | External | Both | Active |
| **Resource Exhaustion** | Modification | Availability, integrity | External | Both | Active |
| **Traffic manipulation** | Modification | Availability, integrity | External | Both | Active |
| **Unfairness** | Modification | Availability, integrity | External | Both | Active |
| **Acknowledge spoofing** | Fabrication, modification | Integrity, authenticity | Both | Both | Active |
| **Sinkhole** | Modification, fabrication | Availability, integrity, authen-ticity | Both | Both | Active |
| **Eavesdropping** | Interception | Confidentiality | External | Both | Passive |
| **Impersonation** | Interception, fabrication, modification, | Availability, integrity, confi-dentiality, authenticity | External | Both | Active |
| **Wormholes** | Fabrication, interception | Confidentiality, authenticity | External | Both | Active |
| **Desynchronization** | Modification, fabrication | Availability, authenticity | External | Both | Active |
| **Denial of Service (DoS) attacks** | Interruption, interception, modification, fabrication | Availability, integrity, confi-dentiality, authenticity | Both | Both | Active |

[1]Security class: the nature of attacks; include interruption, interception, modification and fabrication;
[2]Attack threat: security service attacked; threaten/affected security dimension; include confidentiality, integrity, authenticity and availability;
[3]Threat model: based on attacker location or access level (internal/insider or external/outsider), based on attacking devices (mote-class or laptop-class and based on damage/attacks on WSN protocols include active attacks (availability (packet drop or resource consumption), integrity (information modification) and authenticity (fabrication)), passive attacks (confidentiality (interception));

## 4.1. Attacks based on Damage/Access Level

In this subsection is presented the classifications of WSNs' link layer attacks based on their damage level or attacker's access level, including:

### 4.1.1. Active Attacker

This kind of attacker does operations, such as:

- Injecting faulty data into the WSN;
- Impersonating [3,10];
- Packet modification [15];
- Unauthorized access, monitor, eavesdrop and modify resources and data stream;
- Creating hole in security protocols [12];
- Overloading the WSN;

Some of the goals and effects of these attacks are:

- The WSN functionality disruption;
- The WSN performance degradation;
- Sensor nodes destruction;
- Data alteration;
- Inability in use the WSN's services;
- Obstructing the operations or to cut off certain nodes from their neighbors;

### 4.1.2. Passive Attacker

Passive attacker may do the following functions;

- Attacker is similar to a normal node and gathers information from the WSN;
- Monitoring and eavesdropping [3,12] from communication channel by unauthorized attackers;
- Naturally against privacy;

The goals and effects of this kind of attacker include:

- Eavesdropping, gathering and stealing information;
- Compromised privacy and confidentiality requirements;
- Storing energy by selfish node and to avoid from cooperation;
- The WSN functionality degradation;
- Network partition by non-cooperate in operations;

## 4.2. Attacks based on Attacker Location

Attacker can be deployed inside or outside the WSN; if the attacker be into the WSN's range, called insider (internal), and if the attacker is deployed out of the WSN's range, called outsider (external). This subsection presented and classified the WSNs' link layer attacks based on attackers' location, including:

### 4.2.1. External Attacker (Outsider)

Some of the most common features of this type of attacks are:

- External to the network [3,15] (from out of the WSN range);
- Device: Mote/Laptop class;
- Committed by illegally parties [3,9];
- Initiating attacks without even being authenticated;

Some of the common effects of these attacks are:

- Jamming the entire communication of the WSN;
- WSN's resources consumption;
- Triggering DoS attacks;

### 4.2.2. Internal Attacker (Insider)

The meaning of insider attacker is:

- Main challenge in WSNs;
- Sourced from inside of the WSN and access to all other nodes within its range [2,3,9];
- Authorized node in the WSN is malicious/compromised;
- Executing malicious data or use of cryptography contents of the legitimate nodes [12,15];
- Legitimate entity (authenticated) compromising a number of WSN's nodes;

Some of most important goals of these attacks type are:

- Access to cryptography keys or other WSN codes;
- Revealing secret keys;
- A high threat to the functional efficiency of the whole collective;
- Partial/total degradation/disruption;

## 4.3. Attacks based on Attacking Devices

Attackers can use different types of devices to attack to the WSNs; these devices have different power, radio antenna and other capabilities. There are two common categories of them, including:

### 4.3.1. Mote-class Attacker

Mote-class attacker is every one that using devices similar to common sensor nodes; this means,

- Occurring from inside the WSN;
- Using WSN's nodes (compromised sensor nodes) or access to similar nodes/motes (which have similar functionality as the WSN's nodes) [9,10];
- Executing malicious codes/programs;

Mote-class attacker has many goals, such as:

- Jamming radio link;
- Stealing and access to cryptography keys;

### 4.3.2. Laptop-class Attacker

Laptop-class attacker is every one that using more powerful devices than common sensor nodes, including:

- Main challenge in WSNs;
- Using more powerful devices by attacker, thus access to high bandwidth and low-latency communication channel;
- Traffic injection [3];

- Passive eavesdrop [15] on the entire WSN by a single laptop-class device;
- Replacing legitimate nodes;

Laptop-class attackers have many effects on WSNs, for example:

- Launching more serious attacks and then lead to more serious damage;
- Jamming radio links on the WSN entirely (by using more powerful transmitter);
- Access to high bandwidth and low-latency communication channel;

### 4.4. Attacks based on Function (Operation)

Link layer attacks in WSNs have been classified into three types, based on their main functionality; this subsection presented them, include:

#### 4.4.1. Secrecy

Its definition and techniques are:

- Operating stealthy on the communication channel;
- Eavesdropping [5,12];
- Packet replay, spoofing or modification;
- Injecting false data into the WSN [2,8];
- Cryptography standard techniques can prevent from these attacks;

Goals and effects of this kind of attacks are:

- Passive eavesdrop;
- Packet replication, spoofing or modification;

#### 4.4.2. Availability

This class of attacks known as Denial of Services (DoS) attacks; which leads to WSNs' unavailability, degrade the WSNs' performance or broken it. Some of the most common goals and effects of this attacks' category are including:

- Performance degradation;
- The WSN's services destruction/disruption;
- The WSN useless/unavailable;

#### 4.4.3. Stealthy

This kind of attacks is operating stealthy on the communication channel; such as:

- Eavesdropping [3,10,12];
- False data injection into the WSN;

The most important effects of these attacks are including:

- Partial/entire degradation/disruption the WSN's services and functionality;

As shown in **Table 2**, damage level of link layer attacks on WSNs can be high (serious effect on the WSN) or low (limited effect on the WSN); besides, the attackers identification can be easy (possible), medium or hard (impossible), depending on that kind of attack; also the attackers' presence or attacks' effects can be explicit (serious damage) or implicit (for example, eavesdropping).

## 5. Definitions, Strategies and Effects of Link Layer Attacks on WSNs

WSNs are designed in layered form; this layered architecture makes these networks susceptible and lead to da-mage against many kinds of attacks. For each layer, there are some attacks and defensive mechanisms. Thus, WSNs are vulnerable against different link layer attacks, such as DoS attacks, Collision, unfairness and other attacks to link layer protocols [3,15]; WSNs are susceptible to link layer attacks. Attackers can gain access to transmission media, create radio interference, prevent from legitimate sensor nodes to communicate/transmit (access to the com-munication channel) or launch DoS attacks against link layer. Now, in **Table 3** is presented the definitions of link layer attacks on WSNs, and then it classified and compared them to each others based on their strategies and effects.

## 6. Comparison Link Layer Attacks on WSNs

WSNs are vulnerable against link layer attacks. Therefore, we have to use some techniques to protect data accuracy, network functionality and its availability. As a result, we require establishing security in WSNs with attention to requirements and limitations of these networks.

**Table 2. Threat model of WSNs.**

| Attack category/ features | Types | Damage level[4] | Ease of identify[5] | Attacker presence[6] |
|---|---|---|---|---|
| **Based on damage level** | Active attacker | High | Easy | Explicit |
| | Passive attacker | Low | Hard | Implicit |
| **Based on attacker location** | External (outsider) | Low | Medium | Implicit |
| | Internal (insider) | High | Hard | Implicit |
| **Based on attacking devices** | Mote-class attacker | Low | Hard | Implicit |
| | Laptop-class attacker | High | Easy | Explicit |
| **Based on attack function** | Secrecy | High | Hard | Implicit |
| | Availability | High | Hard | Both |
| | Stealthy | High | Hard | Implicit |

[4]Damage level: high (serious or more damage than other type) and low (limitary);
[5]Ease of identify attackers: easy (possible), medium (depending on attack type) and hard (impossible or not as easy to prevent as other ones);
[6]Attacker presence or attack's effect: explicit (more powerful attacker, then more serious damage/harm) and implicit;

**Table 3. Link layer attacks on WSNs (classification and comparison based on strategies and effects).**

| Attack/criteria | Attack definition | Attack techniques | Attack effects |
|---|---|---|---|
| **Node outage** | • Stopping the functionality of WSN's components, such as a sensor node or a cluster-leader; | • Physically ;<br>• Logical; | • Stop nodes' services;<br>• Take over/compromise the partial/entire the WSN and prevent from some communication;<br>• Impossibility reading gathered information;<br>• Launching other attacks; |
| **Link layer jamming** | • Finding data packet and to jam it[1]; | • Looking at the probability distribution of the inter-arrival times between all types of packets;<br>• This attack can be applied on S-MAC, B-MAC and L-MAC protocols [1]; | • Colliding packets during transmission;<br>• Exhausting nodes' resources;<br>• Confusion; |
| **Collision** | • Message transmission by two nodes on a same frequency [1,5], simultaneously;<br>• There are 2 types collision: environmental and probabilistic collision; | • Environmental collision;<br>• Probabilistic collision;<br>• Verifying and isolate radio transmissions;<br>• Change packet's fields;<br>• Alter the ack message; | • Interferences [1];<br>• Data/control packets corruption/cripple [1];<br>• Discarding packets;<br>• Energy exhaustion;<br>• Cost effective; |
| **Resource Exhaustion** | • Repeated collisions and continuous retransmission until the sensor node death [1]; | • Continuously retransmission;<br>• Interrogation attack (RTS/CTS);<br>• Message modification;<br>• Ack corruption/change; | • Resources exhaustion;<br>• Compromise availability; |
| **Traffic manipulation** | • Regular monitoring transmissions and computing some parameters based on affected MAC protocol carefully ⇨ time adjustment ⇨ transmitting messages just at the moment when normal nodes do so;<br>• Similar to Collision attack; | • Regular monitoring the communication channel and computing require parameters;<br>• Misusing from the wireless nature of communications in WSNs;<br>• Disobeying the coordination rules of MAC schemes in use;<br>• Collision attack techniques;<br>• Unfairness attack techniques;<br>• Continuously collisions and unfairness; | • Excessive packet collisions;<br>• Artificially increased contention;<br>• Decreasing signal quality and network availability;<br>• Aggressively competition for channel usage;<br>• Break the protocols' operations;<br>• Unfair bandwidth usage;<br>• Degradation of the WSN performance;<br>• Traffic distortion;<br>• Effects of collision and unfairness attacks;<br>• Confusion; |
| **Unfairness** | • Partial DoS attack;<br>• Using other attacks such as collision and exhaustion continuously; | • Intermittent application of collision and exhaustion attacks;<br>• Misusing/abusing a cooperative MAC-layer priority mechanism;<br>• Continuously request to access to channel by attacker; | • Decrease utility and efficiency of services;<br>• Nodes' hungry to channel access;<br>• Limiting access to channel and undermine communication channel capacity; |
| **Acknowledge spoofing** | • An adversary can spoof link layer acknowledgements (ACKs) of overheard packets [11]; | • ACKs replication;<br>• Forging/spoofing link layer ACKs of neighbor nodes; | • False view/information of the WSN;<br>• Launch selective forwarding attack;<br>• Packet loss/corruption; |
| **Sinkhole** | • A special selective forwarding attack;<br>• More complex than blackhole attack;<br>• Attracting [5,6] or draw the all possible network traffic to a compromised node by placing a malicious node closer to the base station [17] and enabling selective forwarding;<br>• Centralizing traffic into the malicious node [13];<br>• Possible designing another attack during this attack;<br>• Sinkhole detection is very hard; | • Luring [3] or compromising nodes [11];<br>• Tamper with application data along the packet flow path (selective forwarding);<br>• Receiving traffic and altering or fabricating information [17];<br>• Identity spoofing for a short time;<br>• Using the communication pattern;<br>• Creating a large sphere of influence;<br>• Based on used routing protocol: MintRoute or MultiHopLQI protocol; | • Luring and to attract almost all the traffic;<br>• Triggering other attacks, such as eavesdropping, trivial selective forwarding, blackhole and wormhole;<br>• Usurp the base station's position;<br>• Message modification;<br>• Information fabrication and packet dropping;<br>• Suppressed messages in a certain area;<br>• Routing information modification/fake;<br>• Resource exhaustion; |

| | | | |
|---|---|---|---|
| **Eavesdroping**[7] | • Detecting the contents of communication by overhearing/stealthy attempt to data; | • Interception;<br>• Abusing of wireless nature of WSNs' transmission medium;<br>• Using powerful resources and strong devices, such as powerful receivers and well designed antennas; | • Launching other attacks (wormhole, black-hole);<br>• Extracting sensitive WSN information;<br>• Delete the privacy protection and reducing data confidentiality; |
| **Impersonaion**[8] | • Malicious node impersonates a cluster leader and lures nodes to a wrong position;<br>• Impersonating a node within the path of the data flow of attacker's interest by modifying routing data or implying itself as a trustworthy communication partner to neighboring nodes in parallel; | • The WSN reconfiguration;<br>• Access to encryption keys and authentication information;<br>• Man-in-the-middle attack and fake MAC addresses;<br>• Node replication [26];<br>• Physical access to the WSN;<br>• False or malicious node attack techniques;<br>• Sybil attacks techniques;<br>• Misdirection/misrouting;<br>• Modifying routing information;<br>• Luring/convince nodes; | • Routing information modification;<br>• False sensor readings;<br>• Making network congestion or collapse;<br>• Disclose secret keys;<br>• Network partition;<br>• False and misleading messages generated;<br>• Resources exhaustion;<br>• Degrade the WSN performance;<br>• Invasion;<br>• Carrying out further attacks to disrupt operation of the WSN;<br>• Confusion and taken over the entire WSN; |
| **Wormholes** | • Tunneling [5,11] and replicating messages from one location to another through alternative low-latency links [1,3], that connect two or more points (nodes) of the WSN with fast communication medium [14] (such as Ethernet cable, wireless communication or optical fiber), by colluding two active nodes (laptop-class attackers [3]) in the WSN, by using more powerful communication resources than normal nodes [4,21] and establishing better real communication channels (tunnel);<br>• Wormhole nodes operate fully invisible [21]; | • Compromising/luring nodes [3] with false and forged routing information;<br>• An attacker locates between two nodes and forwards messages between them;<br>• Using out-of-band or high-bandwidth fast [14] channel;<br>• Wormholes may be used along with Sybil attack;<br>• This attack may combines with selective forwarding or eavesdropping; | • Routing disruption/disorder (false routes, misdirection and forged routing);<br>• False/forged routing information;<br>• Confusion and WSN disruption;<br>• Enable other attacks;<br>• Exploiting the routing race conditions;<br>• Change the network topology;<br>• Prevention of path detection protocol;<br>• Packet destruction/alteration by wormhole nodes;<br>• Changing normal messages stream; |
| **De-synchroniz ation** | • Disrupting the established connections between two legitimate nodes by re-synchronizing their transmission[6]; | • Sending repeatedly forged or false messages;<br>• Re-synchronizing transmissions; | • Disrupt communication;<br>• Go out the synchronization;<br>• Resource exhaustion; |
| **Denial of Serice (DoS) attacks** | • A general attack includes several types other attacks in different layers of WSN, simultaneously [27];<br>• Reducing WSN's availability [15,27] | • Physical layer, link layer, routing layer, transport layer and application layer attacks techniques; | • Effects of physical layer, link layer, routing layer, transport layer and application layer attacks; |

## 6.1. Link Layer Attacks Classification based on Threat Model of WSNs

In this subsection, we have tried to compare the link layer attacks of WSNs based on attacks' nature and effects, attackers' nature and capabilities, and WSN's threat model; as shown in **Table 1**.

**Table 1** shows the most important known attacks on WSNs; this table has three columns, including security class, attack threat and WSNs' threat model. Our purpose of security class is the nature of attacks, includes interruption, interception, modification and fabrication. Attack threat shows which security service attacked or security dimension affected, includes confidentiality, integrity, authenticity and availability. The threat model of WSNs has three sub-columns, that they are presenting attackers' features and capabilities, including based on attacker location (internal/insider or external/outsider), based on attacking devices (mote-class or laptop-class) and based on attacks on WSN's protocols, include active

[7]Also called passive information gathering attack; a threat for data confidentiality; the most common attack against privacy; an adversary with powerful resources (powerful receiver and well designed antenna) can gather the data stream from the WSN, if they are not encrypted;
[8]Also called identity spoofing or node replication [26] or multiple identity attacks; identity spoofing and play the role of other one [26]; the attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes;
[9]In link layer: using different neighbors to time synchronization; In transport layer: an established connection between two end points can be disrupted by de-synchronization;

attacks and passive attacks; active attacks are targeting availability (packet drop or resource consumption), integrity (information modification) and authenticity (fabrication); passive attacks are aiming confidentiality (interception).

According to **Table 1**, **Figure 5** shows the percentages of security classes' different parameters associated to the nature of WSNs' link layer attacks; it compares these attacks based on their nature by presents the percentage of WSNs' link layer attacks which based on interruption, interception, modification or/and fabrication; so, it represents the importance of the security classes' parameters. As a result, the nature of the most of these attacks is modification (almost 85 percent of them) and interruption-based attacks have lowest effect/importance on this layer (7.6 percent).

The diagram of **Figure 6** shows a comparison of WSNs' link layer attacks based on their security threats factors including confidentiality, integrity, authenticity and availability, in percentage; for example, it presents almost 31 percent of security threat of WSNs' link layer attacks is confidentiality and the nature of 38.4 percent of them is fabrication (fabricating data or identity). As shown in **Figure 6**, the aim of the most WSNs' link layer attacks is attacking integrity and availability.

**Figure 7** shows a comparison link layer attacks based on the threat model of WSNs; As shown **Figure 7**, the occurred percentage of WSNs' link layer attacks, in attacker location, are 23 percent internal and 100 percent external; *i.e.* most of WSNs' link layer attacks are occurring from out of WSNs' range and attackers can trigger them by mote-class or laptop-class devices. Also, it presents most of link layer attacks on WSNs are active, except eavesdropping; *i.e.* almost 92 percent of WSNs' link layer attacks are active. Besides, **Figure 7** shows least attacks on link layer of WSNs are internal attacks.

## 6.2. Link Layer Attacks Comparison based on Their Goals and Results

In link layer, attacker can disrupt the WSN's functionality by tampering with link layer services such as modifying MAC (Media Access Control) protocol, interference in communication channel and replicating/altering data frames. As shown in **Table 4**, it categorizes the link layer attacks of WSNs, based on their goals, effects and results. Also **Table 4** compares WSNs' link layer attacks based on attack or attacker purpose (including passive eavesdrop, disrupt communication, unfairness, authorization and authentication), requirements technical capabilities (such as radio, battery, powerful receiver/antenna and other high-tech and strong attacking devices), vulnerabilities, main target and final result of attacks. Besides, the contributors of all following link layer attacks (shown in **Table 4**) are one or many compromised motes, pc or laptop devices on WSNs. The vulnerabilities of these attacks can be physical (hardware), logical or their both; Attacks' main target may be physical (hardware),

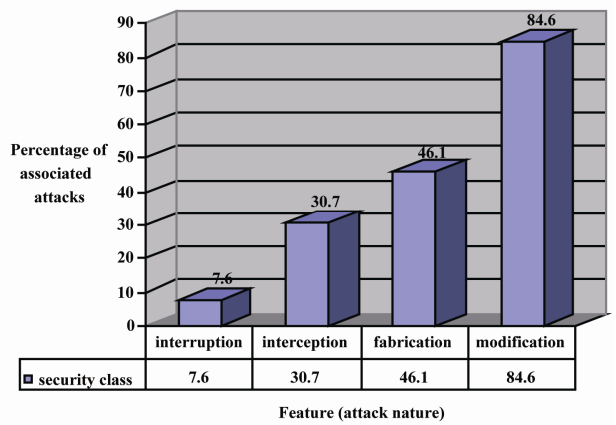



**Figure 5. Comparison link layer attacks based on their nature.**

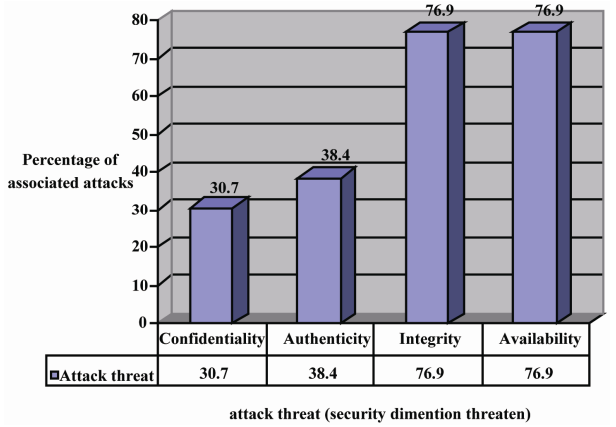



**Figure 6. Comparison link layer attacks based on affected/ threaten security dimension.**

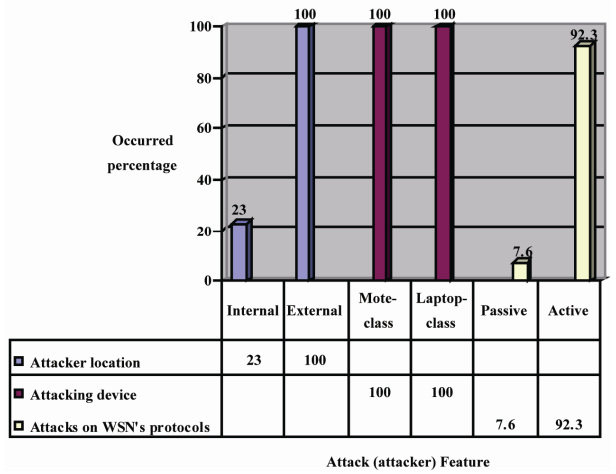



**Figure 7. Comparison link layer attacks based on WSN's threat model.**

logical (lis: logical-internal services or lps: logical-provided services) or their both. Final result of these attacks is inclu- ding passive damage, partial degradation of the WSN functionality and total broken of the WSN's services or functionality.

**Figure 8** shows that how much percentage of WSNs' link layer attacks are happened by targeting the fairness, confidentiality, authentication, authorization and disrupt communication on WSNs' functionalities, services and resources; for example, almost 85 percent of these attacks are aiming the fairness of WSNs, and then they lead to unfairness.

**Figure 9** is presenting the percentage of every one of kinds of link layer attacks vulnerabilities and their main target on WSNs, including: 15.4 percent of them are attacking the WSNs' hardware, 61.5 percent of them are aiming the WSNs' logical-internal services (lis) and 92.3 percent are targeting the logical-provided services (lps) by WSNs. Thus, most link layer attacks on WSNs have logical vulnerabilities and only almost 15.4 percent of them have physical harm/effects.

## 6.3. Detection and Defensive Strategies of WSNs' Link Layer Attacks

In **Table 5** a classification and comparison of detection and defensive techniques on WSNs' link layer attacks is presented.

**Table 4. Link layer attacks comparison based on attacks' goals and their results.**

| Attacks/ features | Purpose[10] | Technical capability | Vulnerability[11] | Main target[12] | Final result[13] |
|---|---|---|---|---|---|
| **Node outage** | Unfairness | - | Logical | lis; lps | PTDB[14] |
| **Link layer jamming [1]** | Disrupt communication | Radio | Logical | lps | PTDB |
| **Collision [1]** | Unfairness | - | Logical | lis; lps | PTDB |
| **Resource Exhaustion [1]** | Unfairness | - | Logical | lis; lps | PTDB |
| **Traffic manipulation** | Unfairness | - | Logical | lis; lps | PTDB |
| **Unfairness** | Unfairness | - | Logical | lis; lps | PTDB |
| **Acknowledge spoofing** | Unfairness | - | Logical | lps | PTDB |
| **Sinkhole [1]** | Unfairness | - | Logical | lps | PTDB |
| **Eavesdropping** | Passive eavesdrop of data | powerful resources and strong devices[15] | Logical | lps | Passive damage; partial degradation |
| **Impersonation** | All purpose | Time and high-tech equipments | Logical; physical | Physical; Logical (lis and lps) | Passive damage; PTDB |
| **Wormholes [1]** | Unfairness; to be authenticated; to be authorized | - | Logical | lps | Passive eavesdrop; PTDB |
| **De-synchronization** | Disrupt communication; unfairness | - | Logical | lis | PTDB |
| **Denial of Service (DoS) attacks** | All purpose | Radio; battery; time and high-tech equipments | Logical; physical | Physical; Logical (lis and lps) | Passive damage; PTDB |

[10]Purpose: passive eavesdrop, disrupt communication, unfairness, to be authorized, to be authenticated;
[11]Vulnerabilities: physical (hardware), logical;
[12]Main target: physical (hardware), logical (lis: logical-internal services or lps: logical-provided services);
[13]Final result: passive damage, partial degradation of the WSN duty/functionality, service broken/disruption for the entire WSN (partial or total/entire degradation/broken/disruption of the services/resources/functionality of the WSN);
[14]PTDB: Partial/Total Degradation/Broken;
[15]such as powerful receiver and well designed antenna;

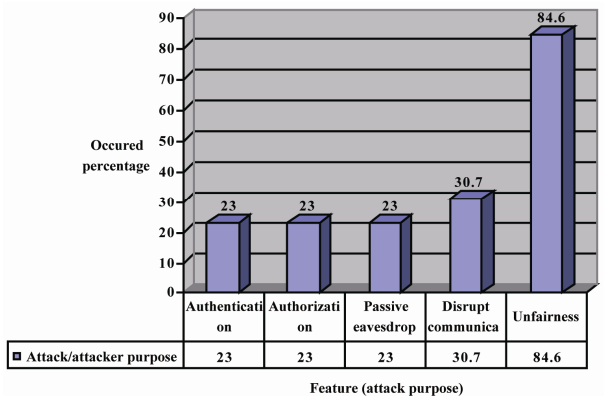



**Figure 8. Comparison link layer attacks based on attacks' purpose.**

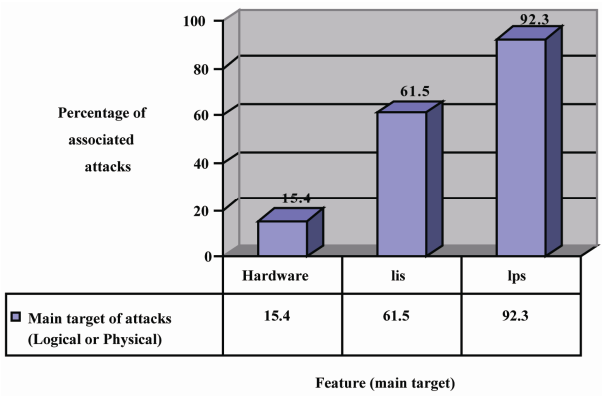



**Figure 9. Comparison link layer attacks based on their main target.**

**Table 5. Link layer attacks on WSNs (classification based on detection and defensive mechanisms).**

| Attack/criteria | Detection methods | Defensive mechanisms |
|---|---|---|
| **Node outage** | • Node disconnection from the network;<br>• Regular monitoring and nodes' cooperaion;<br>• Existence interference in common operation of node;<br>• Node destruction (physically); | • Providing an alternative path;<br>• Developing appropriate and robust protocols;<br>• Defensive mechanisms against physical and node capture attacks[16]; |
| **Link layer jamming** | • Misbehavior detection techniques[17];<br>• False identity detection techniques; | • Limiting the rate of MAC requests;<br>• Use of small frames;<br>• S-MAC defensive method [1][18], L-MAC defensive method [1][19] and B-MAC defensive method [1][20];<br>• Identity protection[21];<br>• Link layer encryption; |
| **Collision** | • Misbehavior detection techniques; | • All countermeasures of jamming attack;<br>• Error correction codes (such as CRC codes) [1];<br>• Time diversity; |
| **Resource Exhaustion** | • Misbehavior detection techniques; | • Limiting the MAC admission control rate [1];<br>• Random back-offs;<br>• Using Time-Division multiplexing;<br>• limiting the extraneous responses;<br>• Protection of WSN ID and other information; |
| **Traffic manipulation** | • Misbehavior detection techniques; | • Traffic analysis attack defenses;<br>• Collision attack defenses;<br>• Unfairness attack defenses;<br>• Misbehavior detection techniques;<br>• Identity protection;<br>• Link layer encryption;<br>• Limiting the rate of MAC requests;<br>• Use of small frames; |
| **Unfairness** | • Misbehavior detection techniques; | • Use of small frames [1,3,5]; |
| **Acknowledge spoofing** | • Misbehavior detection techniques; | • Using another route;<br>• Authentication, link layer encryption and global shared key techniques; |

[16]Using tamper-proofing/tamper-resistant sensor packages; using special alerting hardware/software to the user; camouflaging/hiding sensors;
[17]Include adjustment back-off values, watchdogs/IDS on every node, iterative probing mechanisms, game theory, misbehavior-resilient back-off algorithm, and rating nodes based on replication rate or node's cooperation in communication;
[18]Preventing clustering based analysis by narrowing the distance between the two clusters;
[19]Making the estimation of the clusters more difficult by changing the slot sizes (used for packet transmission) pseudo-randomly as a function of time;
[20]Shortening the preamble in order to make its detection harder;
[21]Using cryptography-based authentication or false identity detection techniques such as Radio resource test (Sybil attack), position verification (detecting immobile attackers), code attestation (differing executing code on malicious or compromised node rather than normal nodes ⇨ detecting attackers by validating executing code on nodes), sequence checking and identity association (associating node identity with used keys on communication by that node);

| | | |
|---|---|---|
| **Sinkhole** | • False routing information detection [4,13];<br>• Cooperating neighboring nodes to each other [13];<br>• Tree structure and verify by tree [13];<br>• Verify by Visual Geographical Map; | • Detection on MintRoute [3];<br>• Geographical routing protocols;<br>• Learning global map (if nodes are static and at known location);<br>• Scalability;<br>• Probabilistic next hop selection;<br>• leveraging global knowledge;<br>• Verifying and to trust information that advertised of neighbor nodes;<br>• Authentication, link layer encryption and global shared key techniques;<br>• Routing access restriction (R) [4];<br>• Wormhole detection (W) [4];<br>• Key management (K);<br>• Secure routing (S) [2]; |
| **Eavesdropping** | • Eavesdropping is a passive behavior, thus it is rarely detectable;<br>• Misbehavior detection techniques; | • Access control;<br>• Reduction in sensed data details;<br>• Distributed processing;<br>• Access restriction;<br>• Strong encryption techniques; |
| **Impersonation** | • False identity detection techniques (misbehavior detection techniques);<br>• False routing information detection;<br>• Collision detection techniques; | • Strong and proper authentication techniques;<br>• Using strong data encryption;<br>• Secure routing protocols;<br>• Central certificate authority;<br>• Pair-wise authentication;<br>• Network layer authentication;<br>• Adopt validation techniques;<br>• Identity protection;<br>• Link layer encryption;<br>• Limiting the rate of MAC requests;<br>• Use of small frames for each packet; |
| **Wormholes** | • False routing information detection;<br>• Wormhole detection [21];<br>• Combinational methods [21][22];<br>• Packet leashes techniques [14, 28]; | • Packet leach/leashes techniques [1,14,28][23];<br>• MAD protocol and OLSR protocol [1,14];<br>• Directional antennas [1,25];<br>• Multi-dimensional scaling algorithm (scalability) [1];<br>• Using local neighborhood information [1];<br>• DAWWSEN protocol [3][24];<br>• Designing proper routing protocols (clustering-based and geographical routing protocols);<br>• leveraging global knowledge;<br>• Verifying information that announce of neighbor nodes;<br>• Graphical Position System [25,28];<br>• Ultrasound [25];<br>• Global clock synchronization;<br>• Combinational methods (such as radio waves and ultraound);<br>• Authentication, link layer encryption and global shared key techniques;<br>• (R), (W), (K), (S) [2,4]; |
| **De-synchronization** | • Strong and un-forgeable authentication mechanisms; | • Strong authentication mechanisms;<br>• Time synchronization, cooperatively;<br>• Maintaining proper timing; |
| **Denial of Service (DoS) attacks** | • Detection methods of physical layer, link layer, routing layer, transport layer and application layer attacks; | • Defensive mechanisms of physical layer, link layer, routing layer, transport layer and application layer attacks; |

## 7. Conclusions

In this paper, we analyze different dimensions of WSN's security, present a wide variety of WSNs' link layer attacks and classify them; our approach to classify and compare the WSN's link layer attacks based on different extracted features of WSN's link layer, attacks' and attackers' properties, such as the threat model of WSNs, link layer attacks' nature, goals and results, their strategies and effects and finally their associated detection and

[22]Such as radio waves and ultrasound, measuring distance between nodes and comparing packet send and receive time with threshold;
[23]Geographical leashes and Temporal leashes ⇨ Physical monitoring of field devices and regular network monitoring by using source routing; monitoring system may use packet leach techniques;
[24]suspicious node detection by signal strength; a proactive routing protocol based on the hierarchical tree construction;

defensive techniques against these attacks to handle them, independently and comprehensively. **Table 6** presents how much percentage of WSNs' link layer attacks are occurring based on any one attacks' classifications features. **Figure 10** shows most affected features of WSNs' link layer attacks. Our most important findings are including:

- Discussion typical WSNs' link layer attacks along with their characteristics, in comprehensive;
- Classification and comprehensive comparison of WSNs' link layer attacks to each other;
- Link layer encryption and authentication mechanisms can protect against outsiders, mote-class attackers and link layer attacks such as link layer jamming, traffic manipulation and acknowledgement spoofing;
- Encryption is not enough and inefficient for inside attacks and laptop-class attackers; but clustering protocols can provide most secure solutions against inside attacks and compromised nodes;
- The link layer attacks are often launching combinational;
- The different kinds of link layer attacks may be used same strategies;
- The same type of defensive mechanisms can be used in multiple link layer attacks, such as misbehavior detection;
- The accuracy of solutions against link layer attacks depends on the characteristics of the WSN's application domain;
- As presented in table6, 84.6 percent of link layer attacks' nature is modification; 30.7 percent of link layer attacks threaten confidentiality, *etc*;
- As shown in **Figure 10**, the nature of 84.6 percent of WSNs' link layer attacks is modification; 76.9 percent of them are targeting integrity and availability; most of these attacks are out of the WSNs' range (external: 100 percent) and lead to high-level damages (active attacks: 92.3 percent); 84.6 percent of attacks' purpose is unfairness; 92.3 percent of link layer attacks' main target is WSNs' logical provided services;

This work makes us enable to identify the purpose and capabilities of the attackers; also the goal, final result and effects of the attacks on the WSNs' functionality. The next step of our work is considering other attacks on WSNs. We hope by reading this paper, readers can have a better view of link layer attacks and aware from some defensive techniques against them; as a result, they can take better and more extensive security mechanisms to design secure WSNs.

**Table 6. Occurred percentage of each attacks' classification features.**

| Attack or attacker feature | | Criteria | Percent (percentage of occurred) |
|---|---|---|---|
| **Security class** | | Interruption | 7.6 |
| | | Interception | 30.7 |
| | | Modification | 84.6 |
| | | Fabrication | 46.1 |
| **Attack threat** | | Confidentiality | 30.7 |
| | | Integrity | 76.9 |
| | | Availability | 76.9 |
| | | Authenticity | 38.4 |
| **Threat model** | **Attacker location** | Internal | 23 |
| | | External | 100 |
| | **Attacking device** | Mote-class | 100 |
| | | Laptop-class | 100 |
| | **Attacks on WSN's protocols** | Passive | 7.6 |
| | | Active | 92.3 |
| **Attacker purpose** | | Disrupt communication | 30.7 |
| | | Authentication | 23 |
| | | Authorization | 23 |
| | | Passive eavesdrop | 23 |
| | | Unfairness | 84.6 |
| **Attack main target** | | Physical (hardware) | 15.4 |
| | | Logical-internal services | 61.5 |
| | | Logical-provided services | 92.3 |

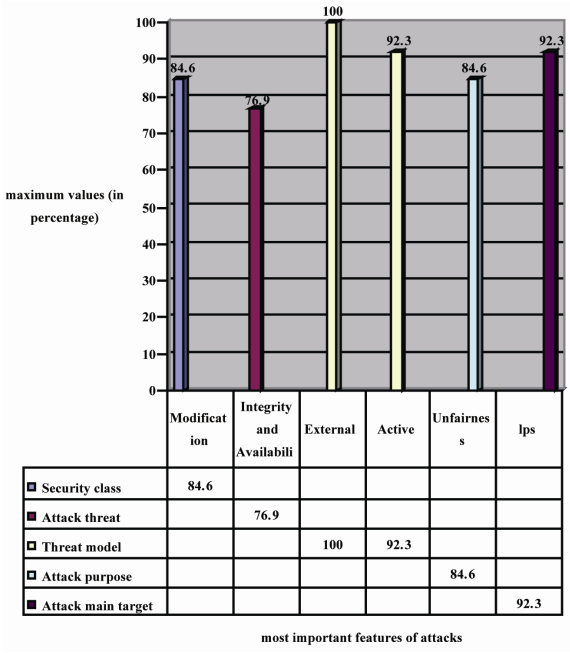



**Figure 10. most affected features (have maximum values) on wsns' link layer attacks.**

## 8. Future works

We also can research about following topics:

- Securing wireless communication links against eavesdropping, collision and DoS attacks;
- Resources limitations techniques;
- Using public key cryptography and digital signature in WSNs (of course with attention to WSN's constraints);
- Countermeasures for combinational link layer attacks;
- Designing proper link layer (MAC[25]) protocols for WSNs;
- Optimizing existing WSNs' MAC protocols;

## 9. References


[1] W. Znaidi, M. Minier and J. P. Babau, "An Ontology for Attacks in Wireless Sensor Networks," Institute National de Recherche en Informatique et en Automatique, October 2008.

[2] M. Saxena, "Security in Wireless Sensor Networks: A Layer-Based Classification," 2011. https://www.cerias.purdue.edu/apps/reports_and_papers/view/3106/

[3] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on Its Security Threats," *International Journal of Computers and Their Applications, Special Issue on "Mobile Ad-hoc Networks"*, Vol. 1, 2010, pp. 42-45.

[4] K. Xing, S. S. R. Srinivasan, M. Rivera, J. Li and X. Z. Cheng, "Attacks and Countermeasures in Sensor Networks: A Survey," *Network Security*, Springer, Berlin, 2010, pp. 251-272. doi:10.1007/978-0-387-73821-5_11

[5] T. A. Zia, "A Security Framework for Wireless Sensor Networks," PhD Thesis, University of Sydney, Sydney, February 2008.

[6] G. Padmavathi and 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, 2009, pp. 115-119.

[7] T. Kavitha and D. Sridharan, "Security Vulnerabilities in Wireless Sensor Networks: A Survey," *Journal of Information Assurance and Security*, Vol. 5, 2010, pp. 31-44.

[8] Z. Li and G. Gong, "A Survey on Security in Wireless Sensor Networks," 2011. http://www.cacr.math.uwaterloo.ca/techreports/2008/cacr2008-20.pdf

[9] A. Dimitrievski, V. Pejovska and D. Davcev, "Security Issues and Approaches in WSN," 2011 http://ict-act.org/ICT Innovations.../ictinnovations 2009_submission_21.pdf

[10] J. Yick, B. Mukherjee and D. Ghosal, "Wireless Sensor Network Survey," *Computer Networks*, Vol. 52, No. 12, 2008, pp. 2292-2330. doi:10.1016/j.comnet.2008.04.002

[11] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, Alaska, 11 May 2003, pp. 113-127.

[12] Y. Wang, G. Attebury and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Communication Surveys*, 2006.

[13] C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting Sinkhole Attacks in Wireless Sensor Networks," *ICROS-SICE International Joint Conference*, Fukuoka, 18-21 August 2009.

[14] R. H. Khokhar, M. A. Ngadi and S. Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks," *International Journal of Computer Science and Security*, Vol. 2, No. 3, 2008, pp. 18-29.

[15] Y. Zhou, Y. Fang and Y. Zhang, "Security Wireless Sensor Networks: A Survey," *IEEE Communication Surveys*, 2008.

[16] A. Perrig, R. Szewczyk, V. Wen, D. Culler and D. Tygar, "SPINS: Security Protocols for Sensor Networks," *Proceedings of 7th Annual International Conference on Mobile Computing and Networks*, Rome, July 2001.

[17] I. Krontiris, T. Giannetsos and T. Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks, the Intruder Side," *IEEE International Conference on Wireless & Mobile Computing, Networking & Communication*, Dalian, 12-14 October 2008, pp. 526-531.

[18] A. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks," *Communications of the ACM*, Vol. 47, No. 6, 2004, pp. .

[19] A. Saini and H. Kumar, "Comparison between Various Black Hole Detection Techniques in MANET," *National Conference on Computational Instrumentation*, Chandigarh, 19-20 March 2010, pp. 157-161.

[20] I. Ullah and S. U. Rehman, "Analysis of Black Hole attack On MANETs Using Different MANET Routing Protocols," Master Thesis, Blekinge Institute of Technology, Sweden, 2010.

[21] R. Maheshwari, J. Gao and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," *IEEE INFOCOM*, Alaska, 2007.

[22] Y-C. Hu, A. Perrig and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," *Proceedings of the 2nd ACM Workshop on Wireless Security ACM*, New York, 2003.

[23] J. R. Douceur, "The Sybil Attack," Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS), Cambridge, 7-8 March 2002.

[24] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," 3*rd International Symposium on Information Processing in Sensor Networks*, Berkeley, 26-27 April 2004.

[25] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," 3*rd International Symposium on Information Processing in Sensor Networks*,

Berkeley, 26-27 April 2004.

[26] B. Parno, A. Perrig and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," *Proceedings of the* 2005 *IEEE Symposium on Security and Privacy*, 8-11 May, 2005, Oakland, pp. 49-63.

[27] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer Magazine; Vol. 35, No. 10, 2002, pp. 54-62.

[28] Y. Hu, A. Perrig and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," *Proceedings of the* 22*nd Annual Joint Conference of the IEEE Computer and Communications Societies*, San Franciso, Vol. 3, 30 March-3 April 2003, pp. 1976-1986.