A COMPARISON OF PHYSICAL ATTACKS ON WIRELESS SENSOR NETWORKS

Dr. Shahriar Mohammadi[1] and Hossein Jadidoleslamy[2]

[1] Information Technology Engineering Group, Department of Industrial Engineering, K.N. Tossi University of Technology, Tehran, Iran
Smohammadi40@yahoo.com
[2] Master of Science Student, Department of Information Technology, University of Guilan, Guilan, Iran
Tanha.hossein@gmail.com

ABSTRACT

Wireless sensor networks (WSNs) have many potential applications [1, 5] and unique challenges. They usually consist of hundreds or thousands small sensor nodes such as MICA2, which operate autonomously; conditions such as cost, invisible deployment and many application domains, lead to small size and limited resources sensors [2]. WSNs are susceptible to many types of physical attacks [1] and most of traditional networks security techniques are unusable on WSNs[2]; due to wireless and shared nature of communication channel, untrusted transmissions, deployment in open environments, unattended nature and limited resources [1]. So, 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' physical attacks and a comparison of them. This work enables us to identify the purpose and capabilities of the attackers; also, the goal, final result and effects of the physical attacks on WSNs are introduced. Also this paper discusses known approaches of security detection and defensive mechanisms against the physical attacks; this would enable it security managers to manage the physical attacks of WSNs more effectively.

KEYWORDS

Wireless Sensor Network (WSN), Security, Physical, Attacks, Detection, Defensive Mechanism

1. INTRODUCTION

Advances in wireless communications have enabled the development of low-cost and low-power wireless sensor networks (WSNs) [1]. WSNs have many potential applications [1, 5] 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" [3], which have more powerful resources than normal sensors. Aggregation points collect information from their nearby sensors, integrate them and then forward to the base stations to process gathered data, as shown in figure1. limitations such as cost, invisible deployment and variety application domains, lead to requiring small size and limited resources (like energy, storage and processing) sensors [2]. Also, WSNs are vulnerable to many types of attacks such as physical attacks; they are one of the most malicious and harmful attacks on WSNs. Due to unsafe and unprotected nature of communication channel [4, 9, 22], untrusted and broadcast transmission media, deployment in hostile environments [1, 5], automated nature and limited resources, the most of security techniques of traditional networks are impossible in WSNs; therefore, security is a vital and complex requirement for these

DOI : 10.5121/ijp2p.2011.2203

networks, especially against to the physical attacks. It is necessary to design an appropriate security mechanism for these networks [5, 6], 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 physical 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 obstacles and security requirements of WSNs,
- The threat model on WSNs,
- A wide variety of WSN's physical attacks and comparison them to each other, include classification of WSN's physical 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 is presented an overview of WSNs; while section 3 focused on security in WSNs and presents a diagram about it; section 4 considers the threat model in WSNs; section 5 includes definitions, strategies and effects of physical attacks on WSNs; in section6 is presented WSNs' physical attacks, their goals, effects, possible detection and defensive mechanisms, and extracts their different features, then classifies the physical attacks based on extracted features and compares them to each other; and finally, in section 7, we present our conclusion.

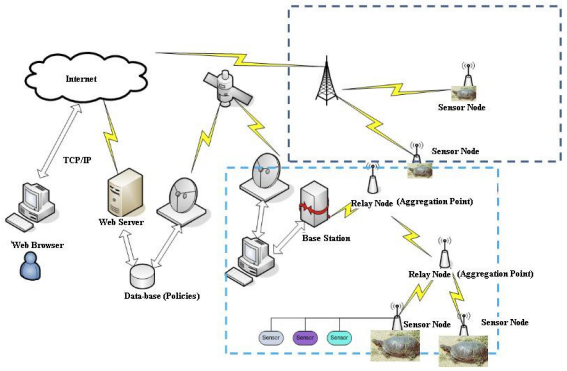


Figure 1. WSN's architecture

2. OVERVIEW OF WSNS

In this section, we present an outline of different dimensions of WSNs, such as definition, characteristics, applications, constraints and challenges; as presented in following subsections (subsection 2.1, 2.2, 2.3 and 2.4)

2.1. Definition and suppositions of WSNs

A WSN is a heterogeneous system consists of hundreds or thousands low-cost and low-power tiny sensors to monitoring and gathering information from deployment environment in real-time [6, 7, 8]. Common functions of WSNs are including broadcast and multicast, 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 following figure (figure2). The existing components on WSN's architecture are including 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 [6] and homogeneous WSN versus heterogeneous [6]. Some of common suppositions of these networks are:

- Insecure radio links [8, 9, 10],
- Packet injection and replay [8, 9],
- Non tamper resistant [10],
- Many normal sensor nodes (high-density) and low malicious nodes,
- Powerful attackers (laptop-class) [10, 20].

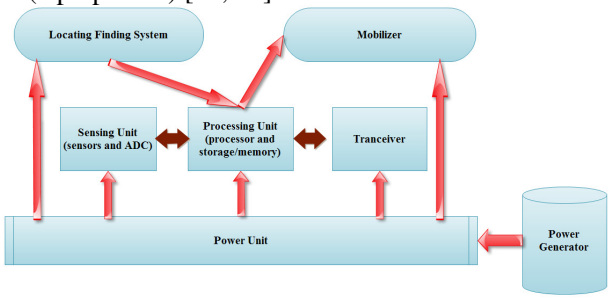


Figure 2. WSN's node architecture

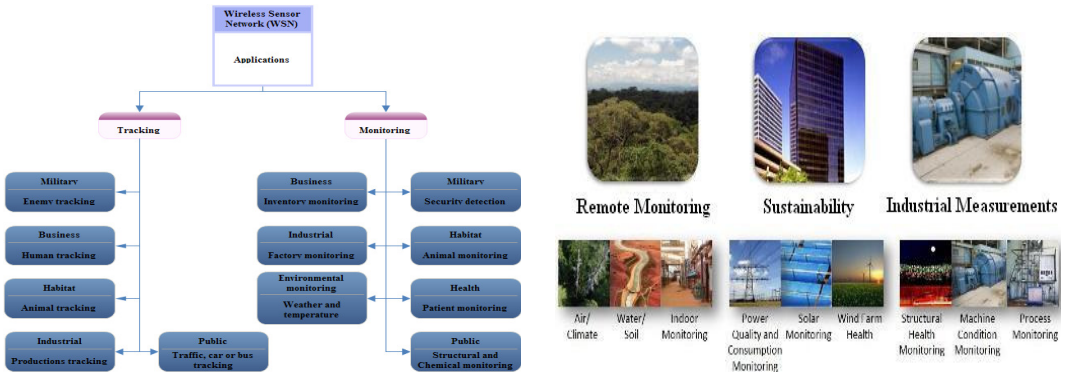
2.2. WSNs characteristics and weakness

Most important characteristics of WSNs are including:

- Constant or mobile sensors (mobility),
- Sensor limited resources [4, 18] (radio communication, energy and processing [4]),
- Low reliability, wireless communication [4] and immunity,
- Dynamic/unpredictable WSN's topology and self-organization [4, 21],
- Ad-hoc based networks [8, 19],
- Hop-by-hop communication (multi-hop routing) [11, 12, 21],
- Non-central management, **a**utonomously and infrastructure-less [8],
- Open/hostile-environment nature [8, 10] and high density;

2.3. WSN's applications

In general, there are two kinds of applications for WSNs including, monitoring and tracking [8]; therefore, some of most common applications of these networks are: military, medical, environmental monitoring [2, 6, 8], industrial, infrastructure protection [2, 8], disaster detection and recovery, agriculture, intelligent buildings, law enforcement, transportation and space discovery (as shown in figure3: a and b).



(a) (b)

Figure 3. WSN's applications

2.4. Vulnerabilities and challenges of WSNs

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

- Theft (reengineering, compromising and replicating),
- Limited capabilities [13, 14] (DoS attacks risks, constraint in using encryption),
- Random deployment (hard pre-configuration) [13, 22],
- Unattended nature [13, 19, 21, 22];

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

- Deployment on open/dynamic/hostile environments [19, 20, 22] (physical access, capture and node destruction);
- Insider attacks;
- Inapplicable/unusable traditional security techniques [2, 14, 22] (due to limited devices/resources, deploying in open environments and interaction with physical environment);
- Ad-hoc based deployment [19, 20] (dynamic structure and topology, self-organization);
- Resource scarcity/hungry [4, 17, 22] (low and expensive communication and computation/processing resources);
- Immense/large scale (high density, scalable security mechanism requirement);
- Unreliable communication [4, 22] (connectionless packet-based routing ⇨ unreliable transfer, channel broadcast nature ⇨ conflicts, multi-hop routing and network congestion and node processing ⇨ Latency);
- Unattended operation [9, 20] (Exposure of physical attacks, managed remotely, no central management point);
- Redesigning security architectures (distributed and self-organized);
- Increased attacks' risks and vulnerabilities [22], new attacks, increased tiny/embedded devices, multi-hopping routing (selfish) [21];
- Devices with limited capabilities [15, 16], pervasiveness (privacy worries), wireless (medium) [4, 13, 22] and mobility;

3. SECURITY IN WSNS

Now, intrusion techniques in WSNs are growth; 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 [2, 19];
- Limited resources [22];
- Untrusted nodes [19, 20];
- Requiring trusted center for key management [19],
    - Authenticating nodes to each other;
    - Preventing from existing attacks and selfishness;
    - Extending collaboration;

3.1. Why security in WSNs?

Security in WSNs is an important, critical issue, necessary and vital requirement, due to:

- WSNs are vulnerable against security attacks [22, 23] (broadcast and wireless nature of transmission medium);
- Nodes deploy on hostile environments [19, 20, 22] (unsafe physically);
- Unattended nature of WSNs [9, 20];

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, node capture [13, 19];

3.3. Security services

There are many security services on WSNs; but some of their common are including encryption and data link layer authentication [17, 19, 20, 24], multi-path routing [19, 21, 24, 25], identity verification, bidirectional link verification [19, 21, 25] and authenticated broadcasts.

3.4. Security protocols

This section presents most common security protocols of WSNs, containing:

- SNEP: Secure network encryption protocol (secure channels for confidentiality, integrity by using authentication, freshness);
- µTESLA [6, 19] (Micro timed, efficient, streaming, loss-tolerant authentication protocol, authentication by using asymmetric authenticated broadcast);
- SPIN (Sensor protocols for information via negotiation): The idea behind SPIN is to name the data using high-level descriptors or meta-data. Before transmission, metadata are exchanged among sensors via a data advertisement mechanism, which is the key feature of SPIN. Each node upon receiving new data, advertises it to its neighbors and interested neighbors, i.e. those who do not have the data, retrieve the data by sending a request message. There is no standard meta-data format and it is assumed to be application specific. There are three messages defined in SPIN to exchange data between nodes, include: ADV message to allow a sensor to advertise a particular meta-data, REQ message to request the specific data and DATA message that carry the actual data [11, 21];

- Broadcasts of end-to-end encrypted packets [24, 25] (authentication, integrity, confidentiality, replay);

As figure4 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' physical 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 table3.

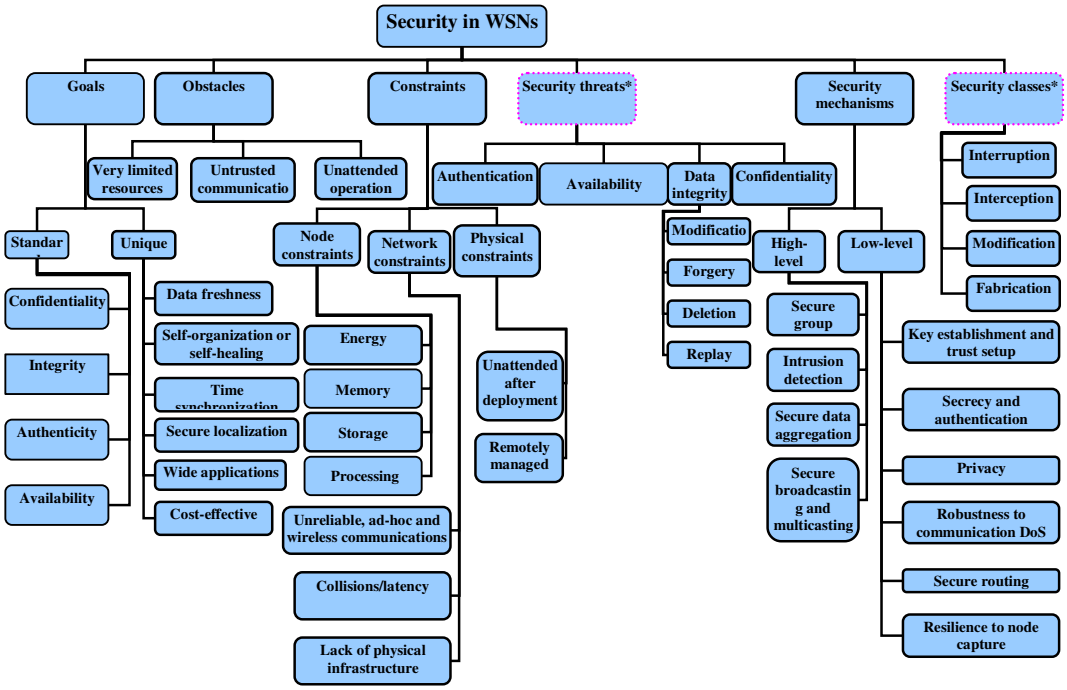


Figure 4. Security in WSNs

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); as presented in following subsections (subsection 4.1, 4.2, 4.3 and 4.4).

4.1. Attacks based on damage/access level

In this subsection is presented the classifications of WSNs' physical 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 [2, 8];
- Packet modification [19];
- Unauthorized access, monitor, eavesdrop and modify resources and data stream;
- Creating hole in security protocols [20];

- Overloading the WSN;

Some of most 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 following functions;

- Attacker is similar to a normal node and gathers information from the WSN;
- Monitoring and eavesdropping [2, 20] 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' physical 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 [2, 19] (from out of the WSN range);
- Device: Mote/Laptop class;
- Committed by illegally parties [2, 7];
- Initiating attacks without even being authenticated;

Some of common effects of these attacks are including:

- 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, 5, 7];
- Authorized node in the WSN is malicious/compromised;
- Executing malicious data or use of cryptography contents of the legitimate nodes [19, 20];
- 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) [7, 8];
- 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 [2];
- Passive eavesdrop [19] 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)

Physical 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 [4, 20];
- Packet replay, spoofing or modification;
- Injecting false data into the WSN [5, 6];
- 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 [2, 8, 20];
- 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;

Table 1. Threat model of WSNs

Attack category/ features	Types	Damage level[1]	Ease of identify[2]	Attacker presence[3]
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

As shown in table1, damage level of physical 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 PHYSICAL ATTACKS ON WSNS

WSNs are designed in layered form; this layered architecture makes these networks susceptible and lead to damage against many kinds of attacks. For each layer, there are some attacks and defensive mechanisms. Thus, WSNs are vulnerable against different physical attacks, such as DoS attacks, jamming, device tampering and other physical attacks [2, 19]. Attackers can gain fully access to sensor nodes, extract and reveal sensitive and sensed information, or launch DoS attacks against the WSN. Now, in table2 is presented the definitions of physical layer attacks on WSNs, and then it classified and compared them to each others based on their strategies and effects.

Table 2. Physical attacks on WSNs (classification and comparison based on strategies and effects)

Attacks/criteria	Attack definition	Attack techniques	Attack effects
Signal/radio jamming	• The adversary tries to transmit radio signals emitted by sensors to the	• Constant jamming (continuously propagate RTS signals) [14];	• Radio interference; • Resource exhaustion;

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

	receiving antenna at the same transmitter frequency band [14] or sub-band; • Radio interference [14];	• Deceptive jamming [14]; • Random jamming [14]; • Reactive jamming [14]; • Using interrupting signals;	
Device tampering attack or Node capture attack (physical layer) or node subversion attack (routing layer) or node cloning attack (application layer)	• Direct physical access, capture and replace/subvert the sensor nodes [15]; • The types of this attack classify based on control/access level to node[4] and based on require time to attack (short, medium , long attack);	• Invasive attacks [15][5]; • Non-invasive attacks [15][6]; • Eavesdropping on the wireless medium, collect information about the WSN and capture nodes based on the learned information; • Replacing or displace or insert sensor nodes [15];	• Damage and modify physically ⇨ stop/alter nodes' services; • The captured node destruction; • Take complete control over the captured node; • Take over/compromise the entire WSN and prevent from any communication; • The captured node displacement or cloning/replication; • Software vulnerabilities; • Launching a variety of insider attacks;
Path-Based DoS (PDoS)	• Typical combinational attacks include jamming attack; send a large number of packets to the base station by attacker [16];	• Sending a large number of packets to the base station [16]; • False-Endorsement-Based DoS [17, 18][7] ; • Jamming attack;	• Nodes' battery exhaustion [16]; • Network disruption; • Falsely excluding nodes from local report [17, 18]; • Reducing the WSN's availability;
Node outage	• Stopping the functionality of WSN's components, such as a sensor node or a cluster-leader;	• Physically[8] ; • Logical[9] ;	• Stop nodes' services; • Take over/compromise the partial/entire the WSN and prevent from some communication; • Impossibility reading gathered information; • Launching a variety of other attacks;
Eavesdropping	• Detecting the contents of communication by overhearing/stealthy attempt to data;	• Interception; • Abusing of wireless nature of WSNs' transmission medium; • Using powerful resources and strong devices, such as powerful receivers and well designed antennas;	• Launching other attacks (wormhole, blackhole); • Extracting sensitive WSN information; • Delete the privacy protection and reducing data confidentiality;
Denial of Service (DoS) attacks	• A general attack includes several types other attacks in different layers of WSN, simultaneously [23]; • Reducing the WSN's availability [19, 23];	• Physical layer attacks techniques; • Link layer attacks techniques; • Routing layer attacks techniques; • Transport layer attacks techniques; • Application layer attacks techniques;	• Effects of physical layer, link layer, routing layer, transport layer and application layer attacks;

[4] Full-access to read/write microcontroller, partial/entire reading information from flash/RAM memory, reading sensed information, tampering radio communication link;
[5] Physical capture of sensor node and access to the hardware level components like chips;
[6] Include: JTAG, exploiting the Bootstrap Loader (BSL), external flash or EEPROM (Eavesdropping on the conductor wires connecting the external memory chip with the micro controller ⇨ data access; Connect a second microcontroller to I/O pins of flash chip ⇨ possible overwrite microcontroller program by attacker ⇨ node destruction), side-channel attack, timing attacks, frequency-based attacks, attacks on the block cipher;
[7] send false acknowledgment to reporter node by attacker;
[8] capture and physically damage ⇨ stop functionality;
[9] using other attacks such as collision or exhaustion or unfairness ⇨ node's resources exhaustion ⇨ stop node's functionality;

6. COMPARISON PHYSICAL ATTACKS ON WSN

WSNs are vulnerable against physical 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.

6.1. Physical attacks classification based on threat model of WSNs

In this section, we have tried to compare the physical attacks of WSNs based on attacks' nature and effects, attackers' nature and capabilities, and WSN's threat model; as shown in following table (table3).

Table3 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 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).

Table 3. WSN's physical attacks classification based on WSNs' threat model

Attacks/features	Security class[10]	Attack threat[11]	Threat model[12]		
			Attacker location	Attacking device	Attacks on WSN's protocols
Signal/radio jamming	Modification	Availability, integrity	External	Both	Active
Device tampering	Interception, modification, fabrication	Availability, integrity, confidentiality, authenticity	External	Laptop	Active
Node capture	Interruption, interception, modification, fabrication	Availability, integrity, confidentiality, authenticity	External	Both	Active
Path-Based DoS (PDoS)	Modification, fabrication	Availability, authenticity	External	Both	Active
Node outage	Modification	Availability, integrity	External	Both	Active
Eavesdropping	Interception	Confidentiality	External	Both	Passive
Denial of Service (DoS) attacks	Interruption, interception, modification, fabrication	Availability, integrity, confidentiality, authenticity	Both	Both	Active

Following figure (figure5) shows the nature of WSN's physical attacks; it compares these attacks based on their nature by presents the percentage of WSNs' physical attacks which based

[10] Security class: the nature of attacks; include interruption, interception, modification and fabrication;
[11] Attack threat: security service attacked; threaten/affected security dimension; include confidentiality, integrity, authenticity and availability;
[12] 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));

on interruption, interception, modification or/and fabrication; as a result, the nature of the most of these attacks is modification (almost 86 percent of them).

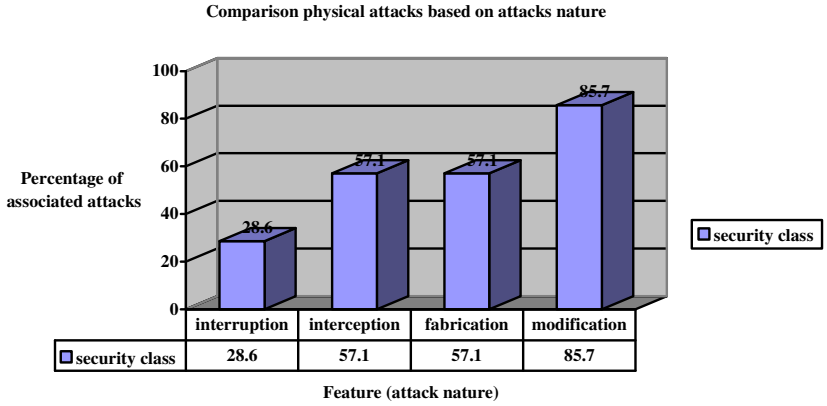


Figure 5. Comparison physical attacks based on their nature

Following diagram (figure6) shows a comparison of WSNs' physical attacks based on their security threats factors including confidentiality, integrity, authenticity and availability, in percentage; for example, it presents almost 57 percent of security threat of WSNs' physical attacks is confidentiality and the nature of 57.1 percent of them is fabrication (fabricating data or identity). As shown in figure6, the aim of the most WSNs' physical attacks is attacking availability (almost 86 percent).

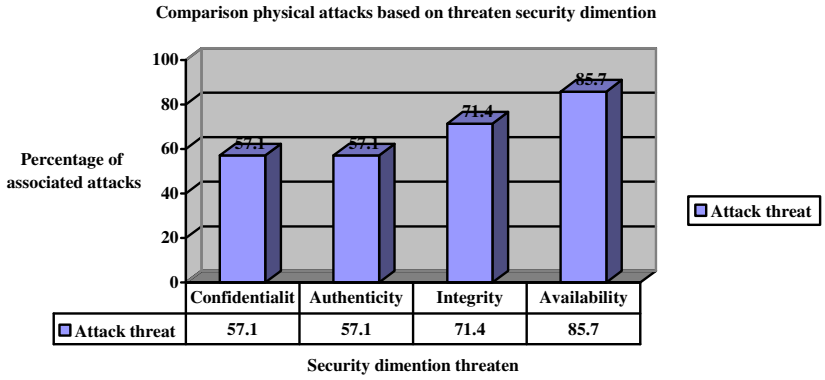


Figure 6. Comparison physical attacks based on affected security dimension

Following figure (figure7) shows a comparison physical attacks based on the threat model of WSNs; As shown figure7, the occurred percentage of WSNs' physical attacks, in attacker location, are 14.3 percent internal and 100 percent external; i.e. most of WSNs' physical 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 physical attacks on WSNs are active, except eavesdropping; i.e. almost 86 percent of WSNs' physical attacks are active. Besides, figure7 shows most attacks on physical layer of WSNs are external attacks.

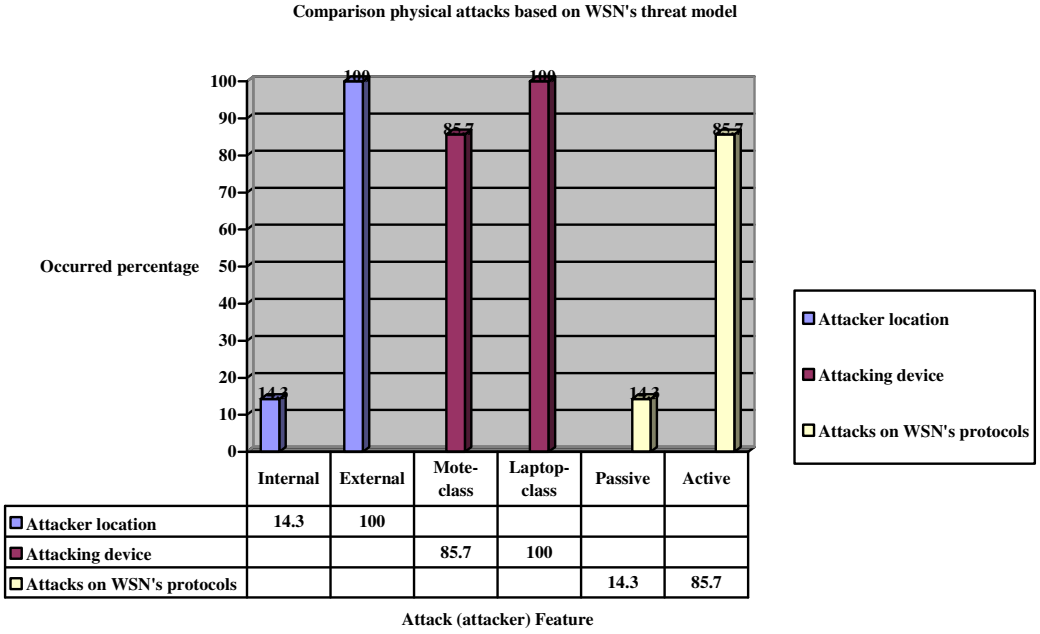


Figure 7. Comparison physical attacks based on the threat model

6.2. Physical attacks comparison based on their goals and results

In physical layer, attacker can disrupt the WSN's functionality by tampering with physical sensor nodes such as modifying and to destroy sensors, physically. As shown in table4, in this section, we categorize the physical attacks of WSNs, based on their goals, effects and results. Also table4 compares WSNs' physical 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 physical attacks (shown in table4) 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), logical (lis: logical-internal services or lps: logical-provided services) or their both. Final result of these attacks is including passive damage, partial degradation of the WSN functionality and total broken of the WSN's services or functionality.

Table 4. Physical attacks comparison based on attacks' goals and their results

Attacks/ features	Purpose[13]	Technical capability	Vulnerability[14]	Main target[15]	Final result[16]
Signal/ radio jamming [1]	Disrupt communication	Radio	Logical	lps	PTDB[17]
Device tampering [1]	Unfairness; to be authenticated; to	Time and high-tech equipments (include expertism information;	Physical	physical	PTDB

[13] Purpose: passive eavesdrop, disrupt communication, unfairness, to be authorized, to be authenticated [1];
[14] Vulnerabilities: physical (hardware), logical [1];
[15] Main target: physical (hardware), logical (lis: logical-internal services or lps: logical-provided services) [1];
[16] 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) [1];
[17] PTDB: Partial or Total, Degradation or Broken;

	be authorized	high-tech and expensive equipment to extract information)			
Node capture	Unfairness; to be authenticated; to be authorized	Time and high-tech equipments	Physical	physical	PTDB
Path-Based DoS (PDoS)	Unfairness	Battery	Logical	lis	PTDB
Node outage	Unfairness	-	Logical	lis; lps	PTDB
Eavesdropping	Passive eavesdrop of data	Powerful resources and devices	Logical	lps	Passive damage; partial degradation
Denial of Service (DoS) attacks	All purpose	Radio; battery; time and high-tech equipments	Logical; physical	Physical; Logical (lis and lps)	Passive damage; PTDB

Following figure (figure8) shows that how much percentage of WSNs' physical attacks are happened by targeting the fairness, confidentiality, authentication, authorization and disrupt communication on WSNs' functionalities, services and resources; for example, almost 71 percent of these attacks are aiming the fairness of WSNs, and then they lead to unfairness.

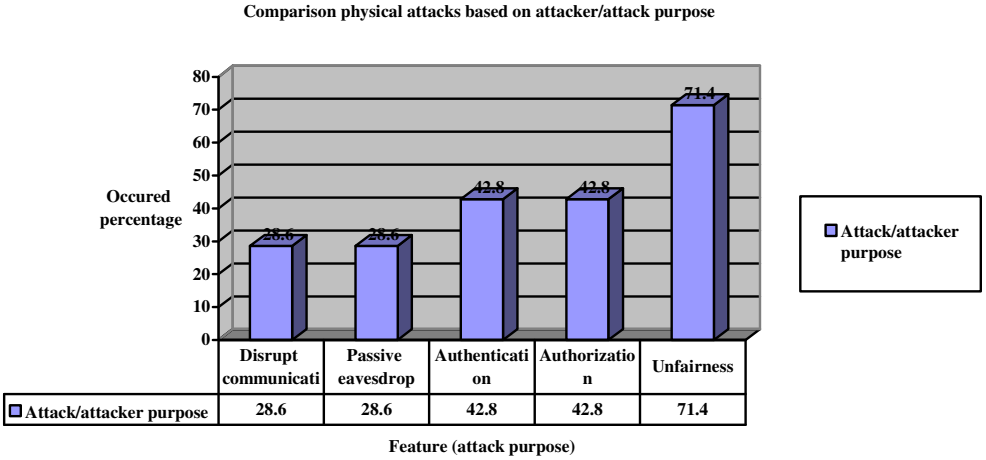


Figure 8. Comparison physical attacks based on attacks' purpose

Figure9 is presenting the percentage of every one of kinds of physical attacks vulnerabilities and their main target on WSNs, including: 42.8 percent of them are attacking the WSNs' hardware, 42.8 percent of them are aiming the WSNs' logical-internal services and 57.1 percent are targeting the logical-provided services by WSNs. Thus, most physical attacks on WSNs have logical vulnerabilities and only almost 42.8 percent of them have physical harm/effects.

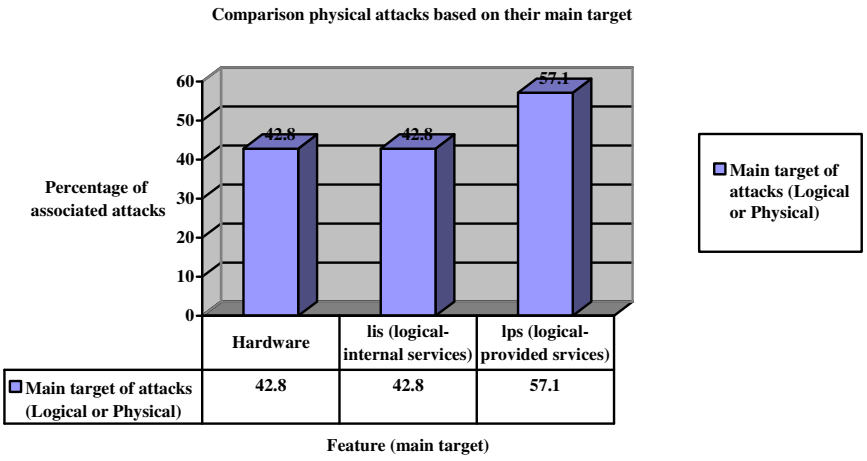


Figure 9. Comparison physical attacks based on their main target

6.3. Detection and defensive strategies of WSNs' physical attacks

In following table (table5) a classification and comparison of detection and defensive techniques on WSNs' physical attacks is presented.

Table 5. Physical attacks on WSNs (classification based on detection and defensive mechanisms)

Attacks/criteria	Detection methods	Defensive mechanisms
Signal/radio jamming	• Statistical information [14][18]; • Combinational methods (signal strength and PDR); • Channel utility degradation than a threshold; • Detecting background noise; • Misbehavior detection techniques;	• Access restriction[19]; • Encryption; • Error-correction; • Mode change[20] ; • Lower duty cycle; • Reporting attack to base station; • Buffering; • Mapping protocol;
Device tampering attack or Node capture attack (physical layer) or node subversion attack (routing layer) or node cloning attack (application layer)	• Node disconnection/absence from the network; • Regular monitoring and nodes'/neighbors' cooperation (such as watchdog or IDS); • Existence interference in functionality of node; • Node destruction (physically); • Using key management protocol (using algorithmic methods) [15]; • Misbehavior detection techniques;	• Optimizing and using crypto-processors or physically secure processors; • Applying standard precautions[21] ; • Hardware/software alerter; • Camouflaging/hiding sensors; • Developing and use of proper protocols[22]; • Access restriction; • Physical protection; • Data integrity protection[23] ; • Data confidentiality protection[24]; • Malicious node detection techniques[25]; • Local removing or exclude the captured

[18] such as signal strength, carrier sense time on the channel and packet Delivery Ratio (PDR);
[19] Include: sleeping/hibernating, directional adaptive antennas and variations of spread-spectrum communication such as frequency-hopping spread spectrum (FHSS);
[20] Channel surfing method by frequency hopping modulation; or change transmission power level;
[21] Designing standard precautions to protect microcontrollers from unauthorized access, such as disabled the JTAG interface, use a good password for the bootstrap loader, or use of tamper-resistant sensor packages;
[22] such as Localized Encryption and Authentication protocol (LEAP); or using combinational methods such as block ciphers for encryption and MACs for authentication;
[23] using authentication techniques such as end-to-end or hop-to-hop or multipath; enforcing misbehavior detection techniques to detect anomalies;
[24] using cryptography/encryption techniques and protection and changing of secret keys;
[25] Using key management protocol to detect the injection of malicious nodes; using algorithmic solutions/methods;

		node[26] ; • Using decomposition techniques;
Path-Based DoS (PDoS)	• Misbehavior detection techniques;	• Using Redundancy; • Anti-attack for FEDoS [17, 18]; • Ack verification; • Jamming's anti-attacks; • Gray-listing;
Node outage	• Node disconnection from the network; • Regular monitoring and nodes' cooperation; • Existence interference in common operation of node; • Node destruction (physically);	• Providing an alternative path; • Developing appropriate and robust protocols; • Defensive mechanisms against physical and node capture attacks[27];
Eavesdropping	• Eavesdropping is a passive behavior, thus it is rarely detectable; • Misbehavior detection techniques;	• Access control; • Reduction in sensed data details; • Distributed processing; • Access restriction; • Strong encryption techniques;
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. CONCLUSION

Security is a vital requirement and complex feature to deploy and extend WSNs in different application domains. The most security physical attacks are targeting WSN security dimensions such as integrity, confidentiality, authenticity and availability.

In this paper, we analyze different dimensions of WSN's security, present a wide variety of WSNs' physical attacks and classify them; our approach to classify and compare the WSN's physical attacks is based on different extracted features of WSN's physical layer, attacks' and attackers' properties, such as the threat model of WSNs, physical attacks' nature, goals and results, their strategies and effects and finally their associated detection and defensive techniques against these attacks to handle them, independently and comprehensively. Table6 presents how much percentage of WSNs' physical attacks are occurring based on any one attacks' classifications features. Figure10 shows most affected features of WSNs' physical attacks. Our most important findings are including:

- Discussion typical WSNs' physical attacks along with their characteristics, in comprehensive;
- Classification and comprehensive comparison of WSNs' physical attacks to each other;
- Link layer encryption and authentication mechanisms can protect against outsiders and mote-class attackers; but encryption is not enough and inefficient for inside attacks and laptop-class attackers;
- The physical attacks are often launching combinational (such as eavesdropping and then jamming);
- The different kinds of physical attacks may be used same strategies;
- The same type of defensive mechanisms can be used in multiple physical attacks, such as misbehavior detection;
- The accuracy of solutions against physical attacks depends on the characteristics of the WSN's application domain;

[26] Designing mechanisms to remove a sensor node that be absent from the WSN for a long time by that node's neighbors; or excluding the compromised node or absent node (for a long time) from the WSN;

[27] Using tamper-proofing/tamper-resistant sensor packages; using special alerting hardware/software to the user; camouflaging/hiding sensors;

- As presented in table6, 85.7 percent of physical attacks' nature is modification; 57.1 percent of physical attacks threaten confidentiality, etc;
- As shown in figure10, the nature of 85.7 percent of WSNs' physical attacks is modification; 85.7 percent of them are targeting availability; most of these attacks are out of the WSNs' range (external: 100 percent) and lead to high-level damages (active attacks: 85.7 percent); 71.4 percent of attacks' purpose is unfairness; 57.1 percent of physical 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 physical 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	28.6
		Interception	57.1
		Modification	85.7
		Fabrication	57.1
Attack threat		Confidentiality	57.1
		Integrity	71.4
		Availability	85.7
		Authenticity	57.1
Threat model	**Attacker location**	Internal	14.3
		External	100
	Attacking device	Mote-class	85.7
		Laptop-class	100
	Attacks on WSN's protocols	Passive	14.3
		Active	85.7
Attacker purpose		Disrupt communication	28.6
		Authentication	42.8
		Authorization	42.8
		Passive eavesdrop	28.6
		Unfairness	71.4
Attack main target		Physical (hardware)	42.8
		Logical-internal services	42.8
		Logical-provided services	57.1

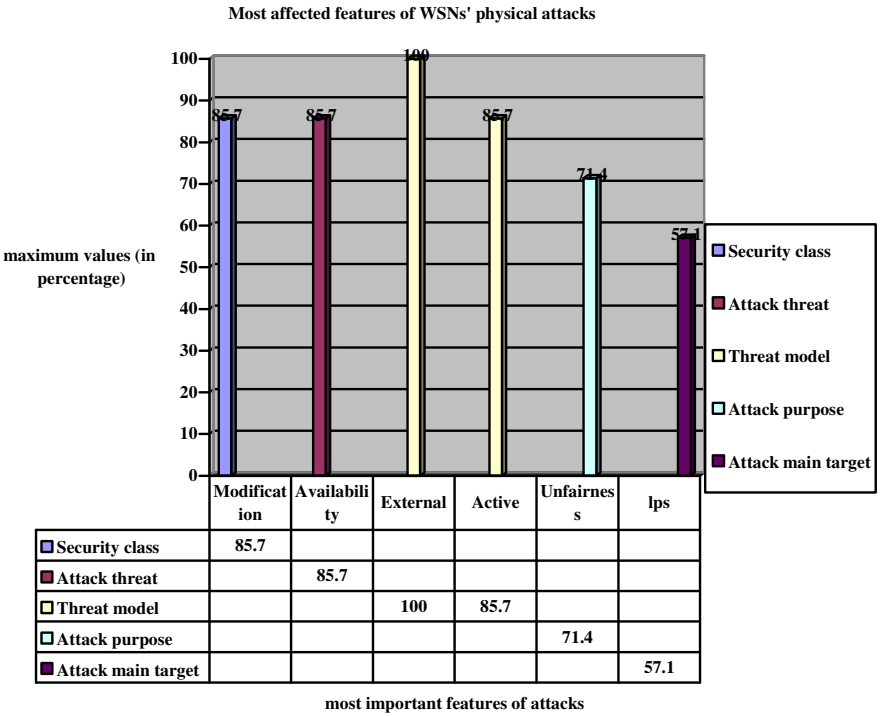


Figure 10. Most affected features (have maximum values) on WSNs' physical attacks

8. FUTURE WORKS

We also can research about following topics:

- Securing wireless communication links against eavesdropping 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 physical attacks;

REFERENCES

[1] W. Znaidi, M. Minier and J. P. Babau; An Ontology for Attacks in Wireless Sensor Networks; INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (INRIA); Oct 2008.

[2] 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.

[3] K. Xing, S. Sundhar, R. Srinivasan, M. Rivera, J. Li and X. Cheng; Attacks and Countermeasures in Sensor Networks: A Survey; Computer Science Department, George Washington University; Springer, Network Security; 2005.

[4] T. A. Zia; A Security Framework for Wireless Sensor Networks; Doctor of Philosophy Thesis; The School of Information Technologies, University of Sydney; Feb 2008.

[5] M. Saxena; Security in Wireless Sensor Networks: A Layer-based Classification; Department of Computer Science, Purdue University.

[6] Z. Li and G. Gong; A Survey on Security in Wireless Sensor Networks; Department of Electrical and Computer Engineering, University of Waterloo, Canada.

[7] 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.

[8] 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.

[9] 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 (IJCSIS), vol. 4, No. 1& 2; Department of Computer Science, Avinashilingam University for Women, Coimbatore, India; 2009.

[10] C. Karlof and D. Wagner; Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures; Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols; In First IEEE International Workshop on Sensor Network Protocols and Applications; University of California at Berkeley, Berkeley, USA; 2003.

[11] A. Perrig, R. Szewczyk, V. Wen, D. culler and D. Tygar; SPINS: Security Protocols for Sensor Networks; Wireless Networking ACM CCS; 2003.

[12] E. Shi and A. Perrig; Designing secure sensor networks; Wireless Communication Magazine; 2004.

[13] A. Perrig, J. Stankovic and D. Wagner; Security in Wireless Sensor Networks; In Communications of the ACM Vol. 47, No. 6, 2004.

[14] W. Xu, K. Ma, W. Trappe and Y. Zhang; Jamming Sensor Networks: Attack and Defense Strategies; IEEE Network; 2006.

[15] A. Becher, Z. Benenson and M. Dornseif; Tampering with Motes: Real-World Attacks on Wireless Sensor Networks; RWTH Aachen University; 2006.

[16] J. Deng, R. Han and S. Mishra; Defending against Path-based DoS Attacks in Wireless Sensor Networks; in SASN '05: Proc. 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks; 2005.

[17] C. Kraub, M. Schneider and C. Eckert; Defending against False Endorsement-based DoS Attacks in Wireless Sensor Networks; in WiSec: Proc. 1st ACM Conference on Wireless Network Security; 2008.

[18] C. Kraub, M. Schneider and C. Eckert; An Enhanced Scheme to Defend against False-Endorsement-Based DoS Attacks in WSNs; in IEEE International Conference on Wireless & Mobile Computing; Networking & Communication; 2008.

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

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

[21] R. H. Khokhar, M. A. Ngadi and S. Mandala; A Review of Current Routing Attacks in Mobile Ad Hoc Networks; Faculty of Computer Science and Information System, Department of Computer System & Communication, University Technology Malaysia (UTM); Malaysia.

[22] T. Kavitha and D. Sridharan; Security Vulnerabilities in Wireless Sensor Networks: A Survey; Journal of Information Assurance and Security; 2009.

[23] A. Wood and J. Stankovic; Denial of Service in Sensor Networks; IEEE Computer Mag.; 2002.

Authors Biographies

S. Mohammadi is a former senior lecturer at the University of Derby, UK. He also used to be a Network consultant in the UK for more than fifteen years. He is currently a lecturer in the University Of Khajeh, Nasir, Iran. His main research interests and lectures are in the fields of Networking, Data Security, Network Security, and e-commerce. He may be reached at Mohammadi@kntu.ac.ir or smohammadi40@yahoo.com.

H. Jadidoleslamy is a Master of Science student at the Guilan University in Iran. He received his Engineering Degree in Information Technology (IT) engineering from the University of Sistan and Balouchestan (USB), Iran, in September 2009. He will receive his Master of Science degree from the University of Guilan, Rasht, Iran, in March 2011. His research interests include Computer Networks (especially Wireless Sensor Network), Information Security, and E-Commerce. He may be reached at tanha.hossein@gmail.com.