Journal of Information Assurance and Security
ISSN 1554-1010 Volume 6 (2011) pp. 331-345

A Comparison of Transport and Application Layers Attacks on Wireless Sensor Networks

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] Department of Information Technology, Anzali International Branch, The University of Guilan, Rasht, 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 transport and application layers attacks and most of traditional networks security techniques are unusable on WSNs [1, 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, including an overview of WSNs, security in WSNs, the threat model on WSNs, a wide variety of WSNs' transport and application layers 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 transport and application layers attacks on WSNs are introduced. Also, this paper discusses known approaches of detection and defensive mechanisms against the transport and application layers attacks; this would enable it security managers to manage the transport and application layers attacks of WSNs more effectively.**

Key words: wireless sensor network (WSN), security, transport, application, attacks, detection, defensive mechanism.

I. 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 and 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 networks. 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 transport and application layers 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 transport and application layers attacks and comparison them to each other, include classification of WSN's transport and application layers 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 transport and application layers 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 transport and application layers attacks on WSNs; in section 6 is considered WSNs' transport and application layers attacks,

their goals, effects, possible detection and defensive mechanisms, and extracts their different features, then classifies the transport and application layers attacks based on extracted features and compares them to each other; and finally, in section 7, we present our conclusion.

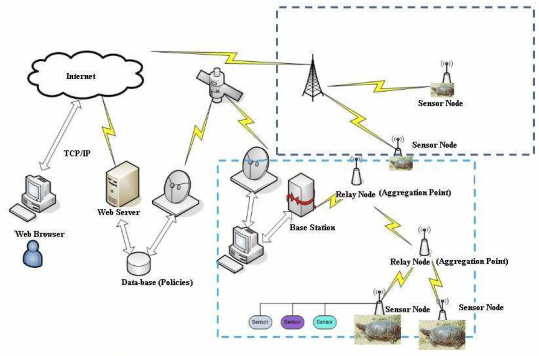


Figure 1. WSN's architecture

II. 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)

A. Definition and suppositions of WSNs

A WSN is a heterogeneous system consists of hundred 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].

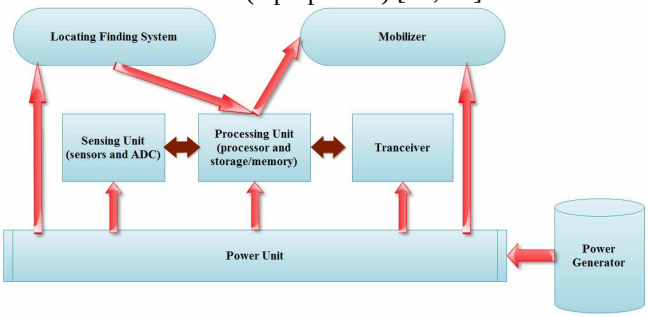


Figure 2. WSN's node architecture

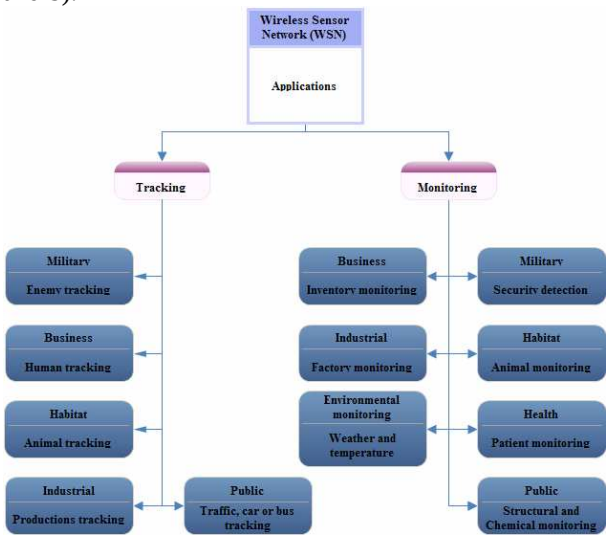
B. WSNs characteristics and weakness

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],
- Immunity and high density;
- 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,
- Autonomously, infrastructure-less [8],
- Open/hostile-environment nature [8, 10],

C. WSN's applications

In general, there are two kind 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

D. 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;

III. Security in WSNs

Now, intrusion techniques in WSNs are growing; 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. Necessities of security in WSNs are:

- Correctness of network functionality;
- Unusable typical networks protocols [2, 19];
- Limited resources [22, 24];
- Untrusted nodes [19, 20];
- Requiring trusted center for key management [19],
    - Authenticating nodes to each other [25];
    - Preventing from existing attacks and selfishness [24];
    - Extending collaboration;

A. 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];

B. Security issues

This section states most important discussions on WSNs; it is including:

- Key establishment,
- Secrecy,
- Authentication,
- Privacy,
- Robustness to DoS attacks,
- Secure routing, node capture [13, 19];

C. 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.

D. 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, 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' transport and application layers 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.

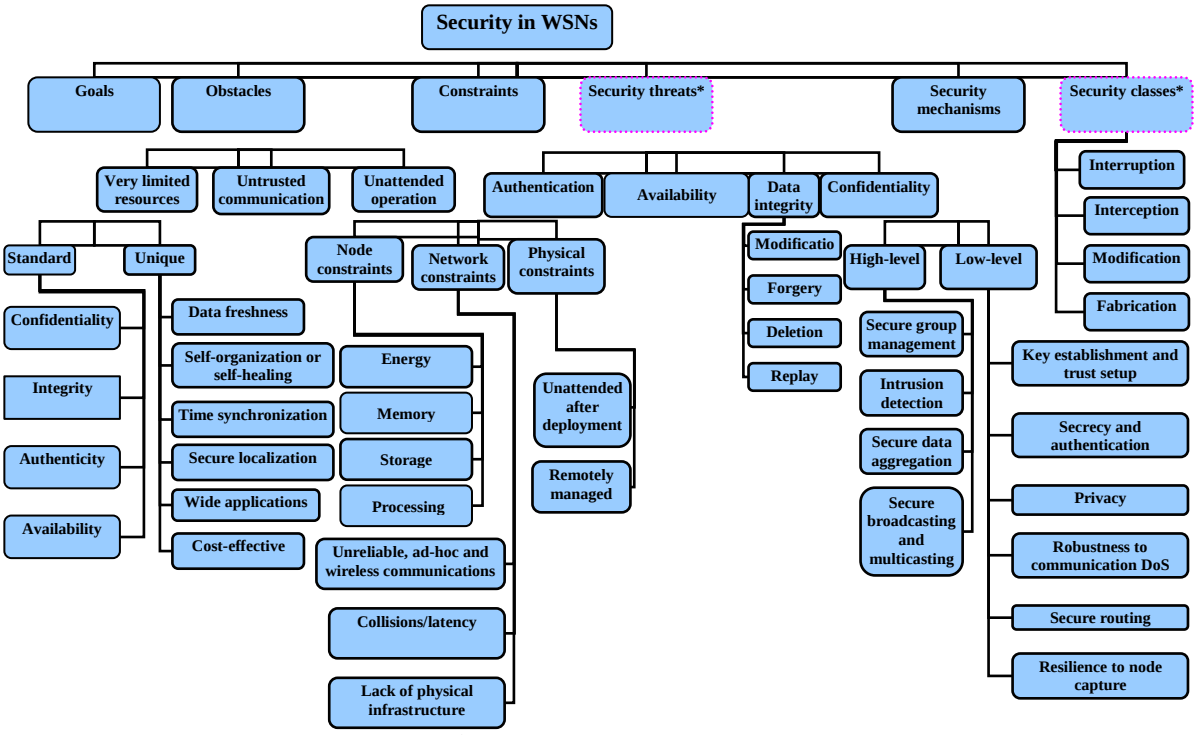


Figure 4. Security in WSNs

IV. 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).

A. Attacks based on damage/access level

In this subsection is presented the classifications of WSNs' transport and application layers attacks based on their damage level or attacker's access level, including:

1) Active attacker

These kinds of attacker do 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;

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;

B. Attacks based on attacker location

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

1) External attacker (outsider)

Some of 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;

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;

C. 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:

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;

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;

D. Attacks based on function (operation)

Transport and application layers attacks in WSNs classify into three types, based on their main functionality; this subsection presented them, include:

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;

2) Availability

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

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

3) Stealthy

These kinds of attacks are operating stealthy on the communication channel; such as:

- Eavesdropping [2, 8, 20];
- False data injection into the WSN;

Most important effects of these attacks are including:

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

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

Table 1. Threat model of WSNs

As shown in table1, damage level of transport and application layers 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),

[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;

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).

V. Definitions, strategies and effects of transport and application layers attacks on WSNs

WSNs are designed 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 transport and application layers attacks, such as DoS attacks, selective forwarding (message selective forwarding), de-synchronization, clock skewing and other attacks to transport and application layers protocols [2, 19]. Attackers can gain access to sensor nodes, flood the WSN and enforce re-synchronizing the nodes, or propagate or broadcast false transport and application layers information into the WSNs, or launch DoS attacks against transport and application layers. Now, in table2 is presented the definitions of transport and application layers attacks on WSNs, and then it classified and compared them to each others based on their strategies and effects.

Attacks/criteria	Definition	Techniques	Effects
Node capture	• Direct physical access, capture and replace/subvert the sensor nodes; • 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[5]; • Non-invasive attacks[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;	• Damage and modify physically ⇨ stop/alter nodes' services [3]; • 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;
Flooding attack[7] or packet replication attack	• Flooding on application layer: exhausting the resources of sensors [21]; • Flooding on routing layer: a node generates and propagates numerous route requests[8];	• Simple broadcast flooding; • Simple target flooding; • False identity broadcast flooding; • False identity target flooding; • Enforcing additional processing to nodes[9]; • Compromised routing information;	• Resource exhaustion; • Reducing WSN's availability; • Blowing up the traffic statistics of the WSN or a certain node and lead to considerable damage costs;
HELLO flood	• Bombing/flooding whole network with routing protocol's HELLO packets [9] (with more energy [4, 7]), that announcing false neighbor status using powerful radio transmitter [10];	• Luring sensors; • Broadcast high power HELLO message to legitimate nodes [4]; • Forged/false advertising high quality route to sink [10];	• Disrupt topology construction; • Network and routing confusion/destruction; • Exhausting nodes' energy; • Decrease efficiency and cooperation[10]; • Increase the WSN latency;
Selective forwarding	• In application layer (message selective forwarding): the attacker	• In application layer: understanding the semantics of	• Drop/alter certain messages;

[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] Applications of flooding: constructing routing tree, clock synchronization and information query;
[8] Similar to rushing attack, a node generates numerous route requests; or flooding the WSN by broadcast or retransmit or replicate packets that previously received from other nodes to the entire network or to a particular set of nodes;
[9] by replication, or send successively requests to establish connection with a node until its death, or opening a large number of connections (stateful connections) with another node to exhaust its resources (similar to the TCP SYN attack);
[10] only a few normal nodes responding to the real base station; decrease/degradation the WSN efficiency; increase the WSN latency/delay;

	selectively sends the information of a particular sensor [3][11]; • In network layer (sensor selective forwarding): the attacker sends/discards the information from selected sensors [3]; • There are 2 modes of this attack: Simple mode attack [10][12] and complex mode attack [10][13];	the payload of the application layer packets[14]; but in routing layer: • Reducing the latency and deceiving the neighboring nodes; • Misuse of nodes' faithful (which forward all received messages); • Packet dropping or modification or suppression; • The attacker is on the route of packet transfer in a multi-hop network; otherwise, needs to position himself in the routing path using other attacks (the Sybil, sinkhole and routing table poisoning attack)[15];	• Influencing the WSN traffic; • Impossibility verifying malicious nodes;
De-synchronization Attacks	• Disrupting the established connections between two legitimate nodes by re-synchronizing their transmission [1][16];	• Sending repeatedly forged or false messages; • Re-synchronizing transmissions;	• Disrupt communication; • Go out the synchronization; • Resource exhaustion;
Data aggregation distortion	• Attack against data integrity; • Disrupting data aggregation, modifying collected data and distorting the final aggregation results computed by the base station [3];	• Using the routing layer knowledge; • Data modification[17]; • Launching blackhole or sinkhole attacks [3];	• Incorrect view of the monitored environment; • Totally disrupted data aggregation; • Trigger other cross-layer attacks;
Clock skewing	• Disseminating false timing information to desynchronize the sensors [3][18]; • Skewing affected sensors' clocks;	• Broadcasting or propagate wrong timing information [3]; • Skewing affected sensors' clocks;	• Being out of synchronization; • Being unstable [3][19]; • Communications disruption[20]; • Waste nodes' energy;
Denial of Service (DoS) attacks[21]	• A general attack includes several types other attacks in different layers of WSN, simultaneously [26]; • Reducing the WSN's availability [19, 26];	• Physical layer attacks techniques (Jamming, tampering); • Link layer attacks techniques (collision, exhaustion, unfairness); • Routing layer attacks techniques (neglect and greed, homing, misdirection, blackholes); • Transport layer attacks techniques (malicious flooding, de-synchronization); • Application layer attacks	• Effects of physical layer, link layer, routing layer, transport layer and application layer attacks;

[11] the adversary has to be on the path between the source and the destination, and is thus responsible for forwarding packet for the source;
[12] blackhole form that compromised node refuse to forward any packets;
[13] selective form that compromised node forwards/drops certain packets;
[14] The adversary is on the path between the source and the destination; the attack can be launched by forwarding some or partial messages selectively but not others; in this case, the attacker needs to understand the semantics of the payload of the application layer packets and select the packets to be forwarded based on the semantics;
[15] In network layer this attack can take place only when the attacker is on the route of packet transfer in a multi-hop network. If the attacker happens to be on the route, it can just discard the packets from some selected nodes at its will. Otherwise, before the attack can be launched, it needs to position himself in the routing path using other attacks such as the Sybil attack, sinkhole attack and routing table poisoning attack;
[16] 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;
[17] Maliciously modifying aggregated data and distorting the computed final aggregation results;
[18] Sending false beacon packets with wrong timing information; the targets of this attack are those sensors in need of synchronized operations;
[19] Oscillating between the two states, include true/false beacon packets ⇨ true/wrong timing information ⇨ true/false synchronization, periodically;
[20] Prevent from exchanging any useful information between normal nodes;
[21] an adversary tries to: subvert, disrupt or destroy the WSN's functionality; degrade or eliminate the network's capacity; jams the entire system communication; reducing the WSN availability, integrity and redundancy; prevents from a service fully; aims user domain buffer and kernel domain; it may occurs by the unintentional failure of nodes or malicious action; the simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled;

		techniques (clock skewing);	

Table 2. Transport and application layers attacks on WSNs (classification and comparison based on strategies and effects)

VI. Comparison transport and application layers attacks on WSNs

WSNs are vulnerable against to transport and application layers 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.

A. Transport and application layers attacks classification based on threat model of WSNs

In this section, we have been tried to compare the transport and application layers 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).

Attacks/features	**Security class**[22]	**Attack threat**[23]	**Threat model**[24]		
			Attacker location	**Attacking device**	**Attacks on WSN's protocols**
Node capture	Interruption, interception, modification, fabrication	Availability, integrity, confidentiality, authenticity	External	Both	Active
Flooding	Modification, fabrication	Availability, integrity, authenticity	Internal	Mote	Active
HELLO flood	Fabrication	Availability, authenticity	Internal	Mote	Active
Selective forwarding	Modification	Availability, integrity	Both	Both	Active
Desynchronization	Modification, fabrication	Availability, authenticity	External	Both	Active
Data aggregation distortion	Modification	Availability, integrity	Both	Both	Active
Clock skewing	Modification, fabrication	Availability, integrity, authenticity	External	Both	Active
Denial of Service (DoS) attacks	Interruption, interception, modification, fabrication	Availability, integrity, confidentiality, authenticity	Both	Both	Active

Table 3. WSN's transport and application layers attacks classification based on WSNs' threat model

[22] Security class: the nature of attacks; include interruption, interception, modification and fabrication;
[23] Attack threat: security service attacked; threaten/affected security dimension; include confidentiality, integrity, authenticity and availability;
[24] 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));

Following figure (figure5) shows the nature of WSN's transport and application layers attacks; it compares these attacks based on their nature by presents the percentage of WSNs' transport and application layers attacks which based on interruption, interception, modification or/and fabrication; as a result, the nature of most these attacks is modification (almost 87 percent of them).

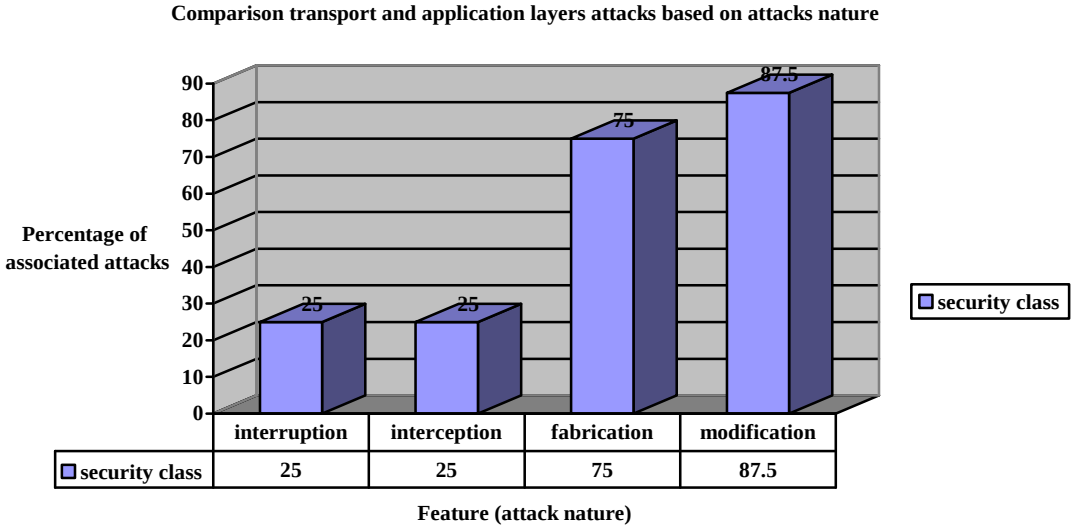


Figure 5. Comparison transport and application layers attacks based on their nature

Following diagram (figure6) shows a comparison of WSNs' transport and application layers attacks based on their security threats factors including confidentiality, integrity, authenticity and availability, in percentage; for example, it presents almost 25 percent of security threat of WSNs' transport and application layers attacks is confidentiality and the nature of 75 percent of them is fabrication (fabricating data or identity). As shown in figure6, aim of most WSNs' transport and application layers attacks is attacking availability.

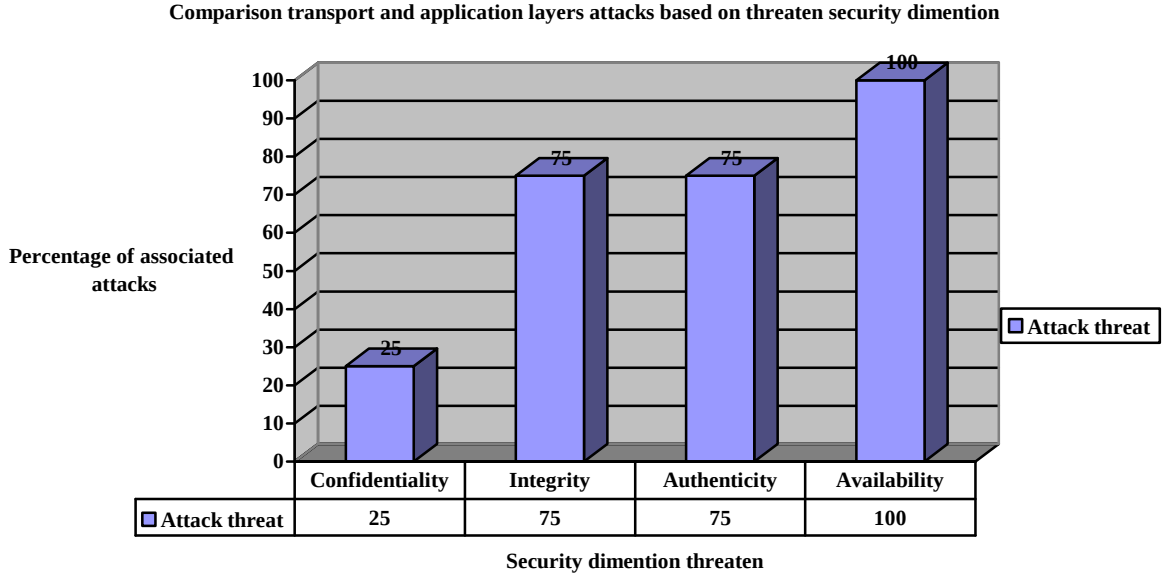


Figure 6. Comparison transport and application layers attacks based on affected security dimension

Following figure (figure7) shows a comparison transport and application layers attacks based on the threat model of WSNs; As shown figure7, the occurred percentage of WSNs' transport and application layers attacks, in attacker location, are 25 percent internal, 37.5 percent external and 37.5 percent from both; i.e. most of WSNs' transport and application layers attacks are occurring from out of WSNs' range and attackers can trigger them by mote-class or laptop-class devices. Also, it presents all of transport and application layers attacks on WSNs are active; i.e. almost 100 percent of WSNs' transport and application layers attacks are active. Besides, figure7 shows most attacks on transport and application layers layer of WSNs are external attacks.

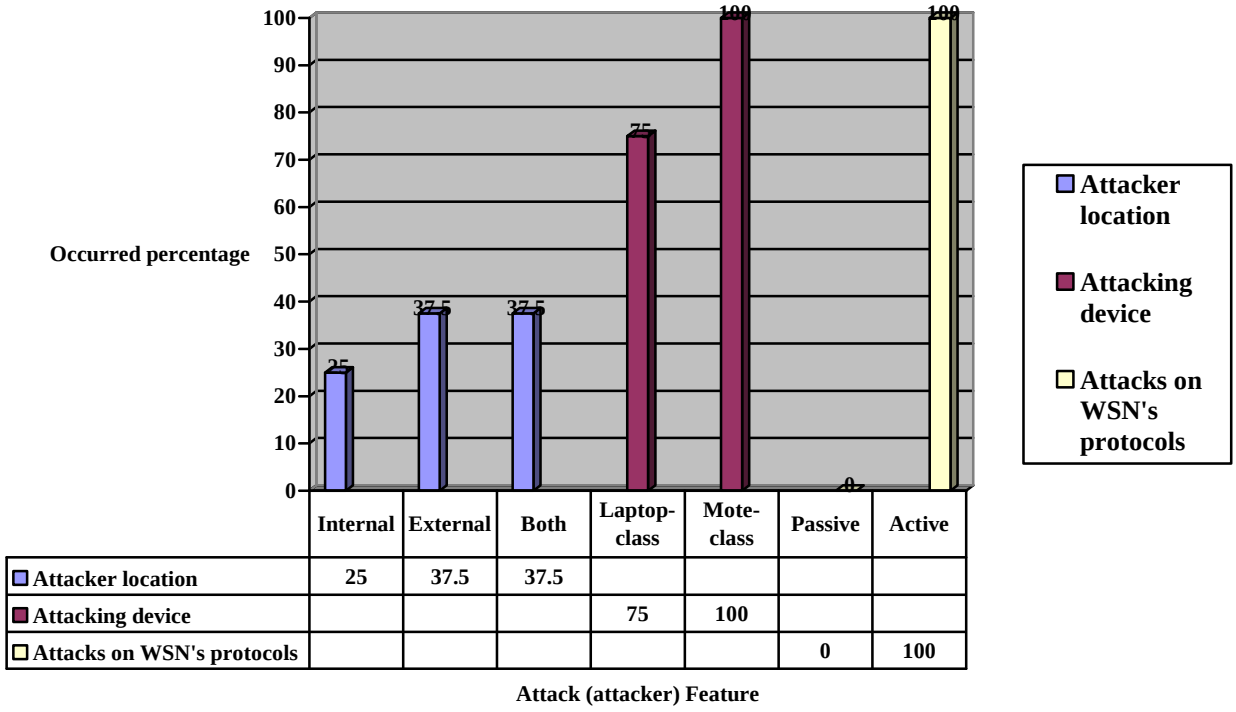


Figure 7. Comparison transport and application layers attacks based on the threat model

B. Transport and application layers attacks comparison based on their goals and results

In transport and application layers, attacker can disrupt the WSN's functionality by tampering with transport and application layers services such as modifying transport information and replicating data packets. As shown in table4, it categorizes the transport and application layers attacks of WSNs, based on their goals, effects and results. Also table4 compares WSNs' transport and application layers 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, contributors of all following transport and application layers 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 are including passive damage, partial degradation of the WSN functionality and total broken of the WSN's services or functionality.

Attacks/ features	**Purpose**[25]	**Technical capability**	**Vulnerability**[26]	**Network layer**	**Main target**[27]	**Final result**[28]
Node capture	Unfairness; to be authenticated; to be authorized	Time and high-tech equipments	Physical	Application;	physical	PTDB
Flooding [1]	Unfairness	Battery	Logical	Transport; application	lis	PTDB
HELLO flood [1]	Unfairness	Radio	Logical	Transport	lps	PTDB
Selective forwarding [1]	Unfairness	-	Logical	Application	lps	PTDB
De-synchronization [1]	Disrupt communication; unfairness	-	Logical	Transport; application	lis	PTDB

[25] Purpose: passive eavesdrop, disrupt communication, unfairness, to be authorized, to be authenticated;
[26] Vulnerabilities: physical (hardware), logical;
[27] Main target: physical (hardware), logical (lis: logical-internal services or lps: logical-provided services);
[28] 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);

Data aggregation distortion	Unfairness	-	Logical	application	lps	PTDB
Clock skewing	Disrupt communication; unfairness	-	Logical	Application	lis	PTDB
Denial of Service (DoS) attacks	All purpose	Radio; battery; time and high-tech equipments	Logical; physical	All layers	Physical; Logical (lis and lps)	Passive damage; PTDB

Table 4. Transport and application layers attacks comparison based on attacks' goals and their results

Following figure (figure8) shows that how much percentage of WSNs' transport and application layers attacks are happened by targeting the fairness, confidentiality, authentication, authorization and disrupt communication on WSNs' functionalities, services and resources; for example, almost 100 percent of these attacks are aiming the fairness of WSNs, and then they lead to unfairness.

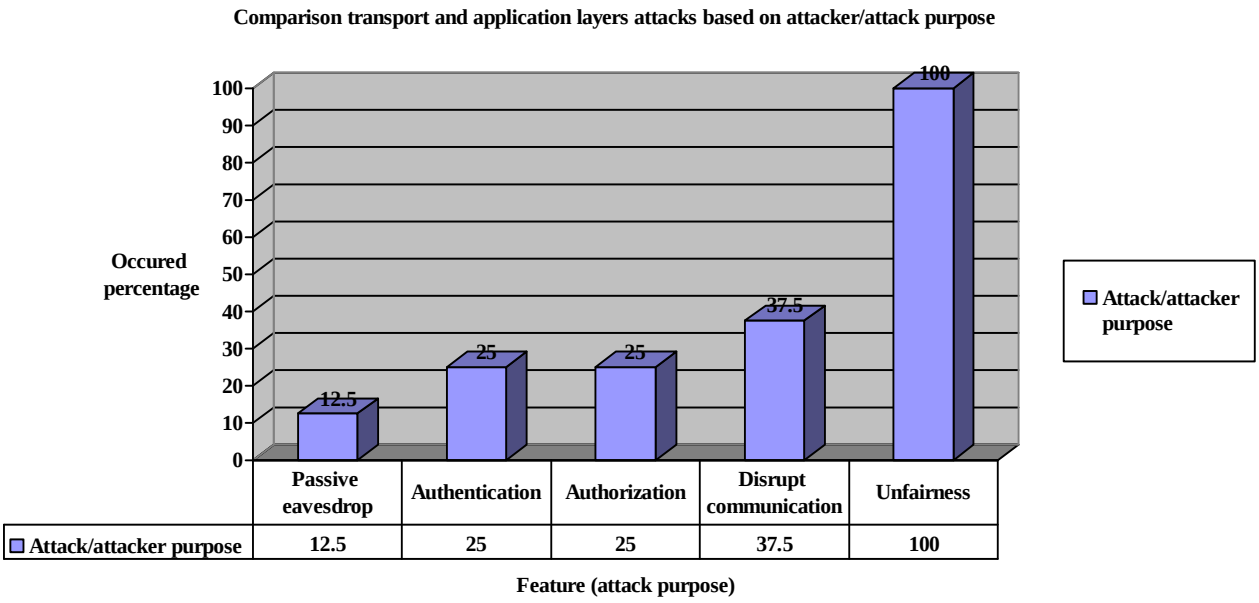


Figure 8. Comparison transport and application layers attacks based on attacks' purpose

Figure9 is presenting the percentage of every one of kinds of transport and application layers attacks vulnerabilities and their main target on WSNs, including: 25 percent of them are attacking the WSNs' hardware, 50 percent of them are aiming the WSNs' logical-internal services and 50 percent are targeting the logical-provided services by WSNs. Thus, most transport and application layers attacks on WSNs have logical vulnerabilities and only almost 25 percent of them have physical harm/effects.

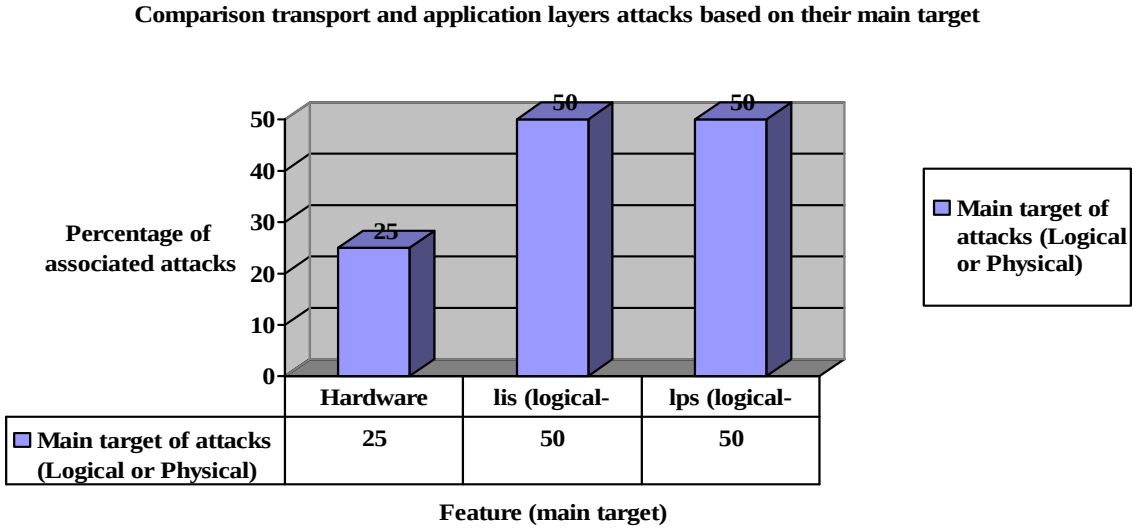


Figure 9. Comparison transport and application layers attacks based on their main target

C. Detection and defensive strategies of WSNs' transport and application layers attacks

In following table (table5), we present a classification and comparison of detection and defensive techniques on WSNs' transport and application layers attacks.

Attacks/criteria	**Detection methods**	**Defensive mechanisms**
Node capture	• 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);	• Optimizing and using crypto-processors or physically secure processors; • Applying standard precautions[29] ; • Hardware/software alerter; • Camouflaging/hiding sensors; • Developing and use of proper protocols[30]; • Access restriction [3]; • Encryption [3]; • Physical protection; • Data integrity protection; • Data confidentiality protection; • Malicious node detection techniques; • Local removing or exclude the captured node; • Using decomposition techniques;
Flooding attack or packet replication attack	• False routing information detection [3][31]; • Wormhole detection [3][32];	• Client puzzles [2]; • Limiting the number of node's connections [21]; • Routing access restriction[33]; • Key management; • Secure routing [5];
HELLO flood	• Misbehavior detection techniques;	• Suspicious node detection by signal strength [2]; • Restricting the number of nodes' neighbors; • Authentication, link layer encryption and global shared key mechanisms[34];
Selective forwarding	• False routing information detection [3]; • Malicious node detection techniques; • Wormhole detection [3];	• Regular network monitoring; • Using another route; • Dynamically pick packet's next hop from a set of candidates; • Combinational methods[35]; • Authentication, link layer encryption and global shared key techniques; • Routing access restriction [3]; • Key management; • Secure routing; • Data integrity protection [3]; • Data confidentiality protection [3];
De-synchronization Attacks	• Strong and un-forgeable authentication mechanisms;	• Strong authentication mechanisms[36]; • Time synchronization, cooperatively[37]; • Maintaining proper timing;
Data aggregation distortion	• Misbehavior detection techniques; • Malicious node detection techniques;	• Access control; • Data integrity protection [3]; • Data confidentiality protection [3];

[29] 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;
[30] such as Localized Encryption and Authentication protocol (LEAP); or using combinational methods such as block ciphers for encryption and MACs for authentication;
[31] using misbehavior detection methods such as watchdogs or IDS or reputation;
[32] use of techniques such as synchronized clocks, directional antennas and multi-dimensional scaling;
[33] multipath routing; using authentication techniques include: end to end and hop to hop authentication;
[34] Multi-path routing, identity verification (node authentication by base stations or create pair-wise shared key for message authentication), bidirectional link verification and authenticated broadcast;
[35] combine link layer multipath routing and probabilistic routing dynamically (random/probabilistic selection/choose of paths to destination dynamically);
[36] to control the identity and the integrity of packets; exchanging packets that are authenticated (including all control fields in the transport protocol header);
[37] Using different neighbors for time synchronization;

Clock skewing	• Strong and un-forgeable authentication mechanisms; • Misbehavior detection techniques;	• Strong authentication mechanisms; • Data integrity protection [3]; • Data confidentiality protection [3]; • Malicious node detection;
Denial of Service (DoS) attacks	• Detection methods of physical, link, routing, transport and application layers attacks;	• Defensive mechanisms of physical layer, link layer, routing layer, transport layer and application layer attacks;

Table 5. Transport and application layers attacks on WSNs (classification based on detection and defensive mechanisms)

VII. Conclusion

Security is a vital requirement and complex feature to deploy and extend WSNs in different application domains. The most security transport and application layers attacks are targeting network 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' transport and application layers attacks and classify them; our approach to classify and compare the WSN's transport and application layers attacks is based on different extracted features of WSN's transport and application layers, attacks' and attackers' properties, such as the threat model of WSNs, transport and application layers 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' transport and application layers attacks are occurring based on any one attacks' classifications features. Figure10 shows most affected features of WSNs' transport and application layers attacks. Our most important findings are including:

- Discussion typical WSNs' transport and application layers attacks along with their characteristics, in comprehensive;
- Classification and comprehensive comparison of WSNs' transport and application layers attacks to each other;
- Link layer encryption and authentication mechanisms can protect against outsiders, mote-class attackers and HELLO flood attack;
- Encryption is not enough and inefficient for inside attacks and laptop-class attackers;
- The transport and application layers attacks are often launching combinational (intra-layer or cross-layer);
- The different kinds of transport and application layers attacks may be used same strategies;
- The same type of defensive mechanisms can be used in multiple transport and application layers attacks, such as misbehavior detection;
- The accuracy of solutions against transport and application layers attacks depends on the characteristics of the WSN's application domain;
- As presented in table6, 87.5 percent of transport and application layers attacks' nature is modification; 25 percent of transport and application layers attacks threaten confidentiality, etc;
- As shown in figure10, the nature of 87.5 percent of WSNs' transport and application layers attacks is modification; 100 percent of them are targeting availability; most of these attacks are out of the WSNs' range (external: 37.5 percent) and lead to high-level damages (active attacks: 100 percent); 100 percent of attacks' purpose is unfairness; 50 percent of transport and application layers attacks' main target is WSNs' logical internal services and 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 transport and application layers 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.

Attack or attacker feature		**Criteria**	**Percent (percentage of occurred)**
Security class		Interruption	25
		Interception	25
		Modification	87.5
		Fabrication	75
Attack threat		Confidentiality	25
		Integrity	75
		Availability	100
		Authenticity	75
Threat model	Attacker location	Internal	25
		External	37.5
		Both	37.5
	Attacking device	Mote-class	100
		Laptop-class	75
	Attacks on WSN's protocols	Passive	0
		Active	100
Attacker purpose		Disrupt communication	37.5
		Authentication	25
		Authorization	25
		Passive eavesdrop	12.5
		Unfairness	100
Attack main target		Physical (hardware)	25
		Logical-internal services	50
		Logical-provided services	50

Table 6. Occurred percentage of each attacks' classification features

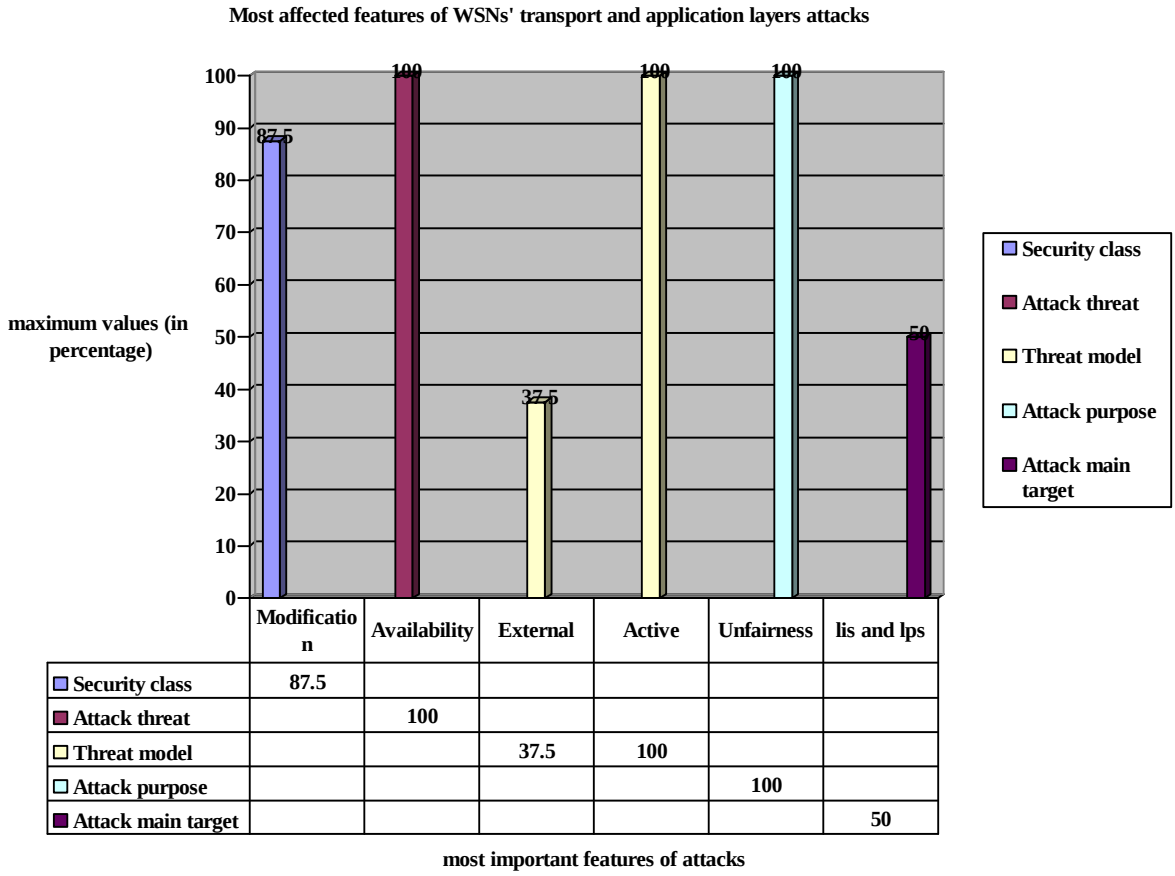


Figure 10. Most affected features (have maximum values) on WSNs' transport and application layers attacks

VIII. Future works

We also can research about following topics:

- Securing wireless communication links against DoS attacks;
- Resources limitations techniques;
- Using public key cryptography and digital signature in WSNs ;
- Countermeasures for (combinational) transport and application layers attacks;
- Designing proper transport and application layers protocols for WSNs;
- Optimizing existing WSNs' transport and application layers protocols;

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] I. Krontiris, T. Giannetsos and T. Dimitriou; Launching a Sinkhole Attack in Wireless Sensor Networks, the Intruder Side; Athens Information Technology, Peania; Athens, Greece.

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

[14] A. Saini and H. Kumar; Comparison Between Various Black Hole Detection Techniques in MANET; Panjab University, Chandigarh; National Conference on Computational Instrumentation (NCCI); Mar 2010.

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

[16] Y. Hu, A. Perrig and D. B. Johnson; Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols; ACM; Carnegie Mellon University; Rice University; San Diego, California, USA; Sep 2003.

[17] I. Ullah and S. U. Rehman; Analysis of Black Hole attack On MANETs Using Different MANET Routing Protocols; Master Thesis, Electrical Engineering, Thesis no: MEE-2010-2698; School of Computing Blekinge Institute of Technology, Sweden; Jun 2010.

[18] C. Tumrongwittayapak and R. Varakulsiripunth; Detecting Sinkhole Attacks in Wireless Sensor Networks; ICROS-SICE International Conference; 2009.

[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] B. Parno and A. Perrig; Distributed Detection of Node Replication Attacks in Sensor Networks; Carnegie Mellon University.

[24] J. R. Douceur; the Sybil Attack; Proc. 1st ACM Int'l. Wksp. Peer-to-Peer Systems; 2002.

[25] J. Newsome, E. Shi, D. Song and A. Perrig; the Sybil Attack in Sensor Networks: Analysis & Defenses; Center for Computer and Communications Security; 2004.

[26] 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.