IJCCN International Journal of Computer Communications and Networks,
VOLUME 4, ISSUE 1, FEBRUARY 2014, ISSN 2289-3369
WWW.IARTC.NET

A Comprehensive Comparison of Attacks in Wireless Sensor Networks

Hossein Jadidoleslamy

Information Technology Engineering Group, Department of Information Technology, Communications and Security, Malekashtar University of Technology (MUT), Tehran, Iran
Tanha.hossein@gmail.com

Abstract— Wireless Sensor Networks (WSNs) are vulnerable to different kinds of attacks and most of traditional networks security techniques are unusable on WSNs; due to untrusted transmissions, deployment in open and hostile environments, unattended nature and limited resources. So, security is a vital and complex requirement for these networks. This paper focuses on security of WSNs and its main purpose is discussing on WSNs' attacks in different layers, including of physical layer attacks, link layer attacks, routing layer attacks, transport layer attacks and application layer attacks. It classifies and compares different attacks based on their nature and goals; i.e. this paper is expressing purpose and capabilities of attackers and it is presenting goals and result of different attacks on WSNs.

Index Terms— Wireless Sensor Network (WSN), Security, Attacks, Physical, Data Link, Routing, Transport, Application, Comparison.

1 Introduction

Wireless Sensor Networks (WSNs) are usually including of many sensor nodes and a Sink; sensor nodes are monitoring different environments in cooperative or autonomously; then, they send the gathered data to the Sink and the Sink is doing final processes on gathered data. In summarized, a Wireless Sensor Network (WSN) is a wireless network with following major features [1, 2, 13]:

- Infrastructure-less;
- Data centric and no public address, often;
- Consisting of many tiny (small size, low-cost and low-power) sensor nodes;
- Nodes distribution with high density in operational environment;
- Insecure radio links;
- Different architectures: hierarchical/flat, centralized/distributed or homogenous/heterogeneous;
- Limited resources (radio range, bandwidth, energy, memory and processing capabilities);
- Main application domains: monitoring and tracking;

In continue, Figure1 is represented an outline of different aspects of WSNs.

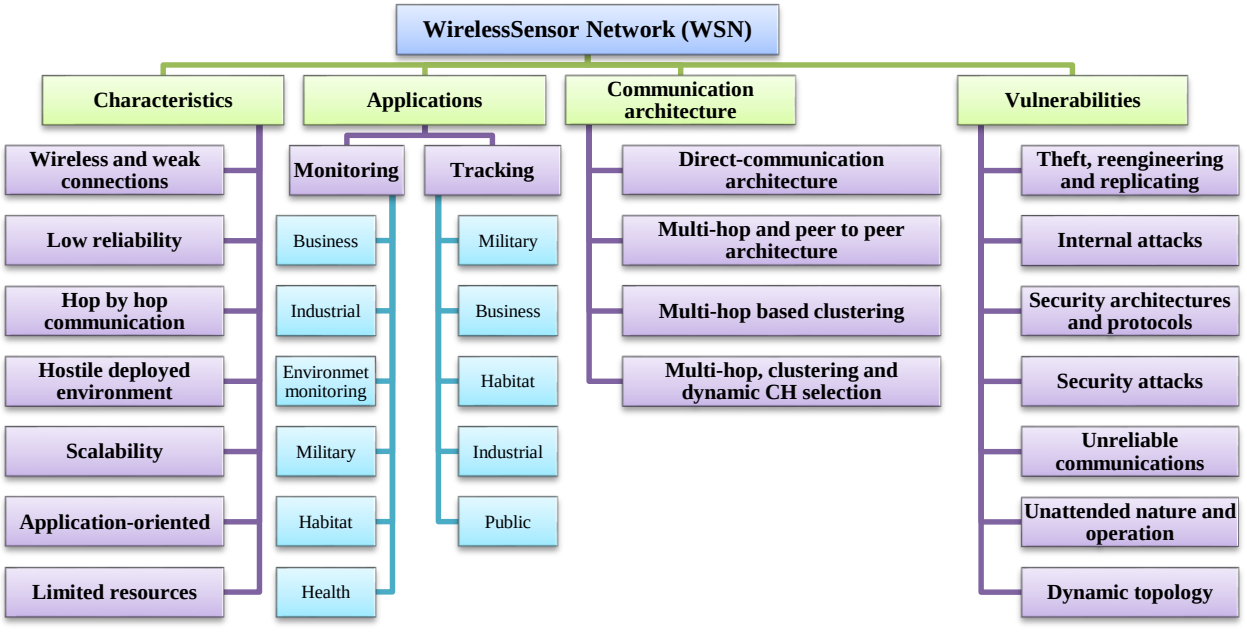
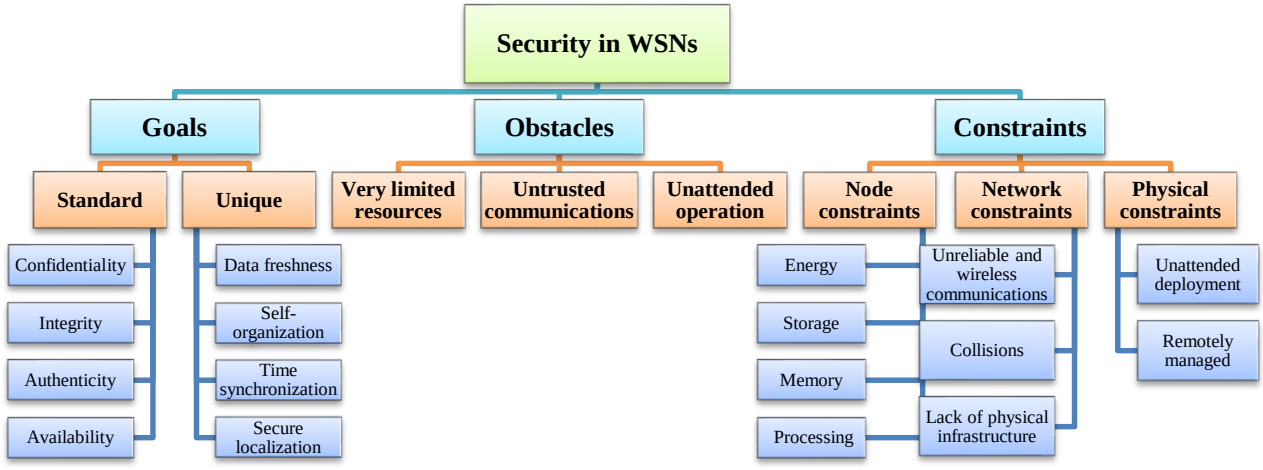
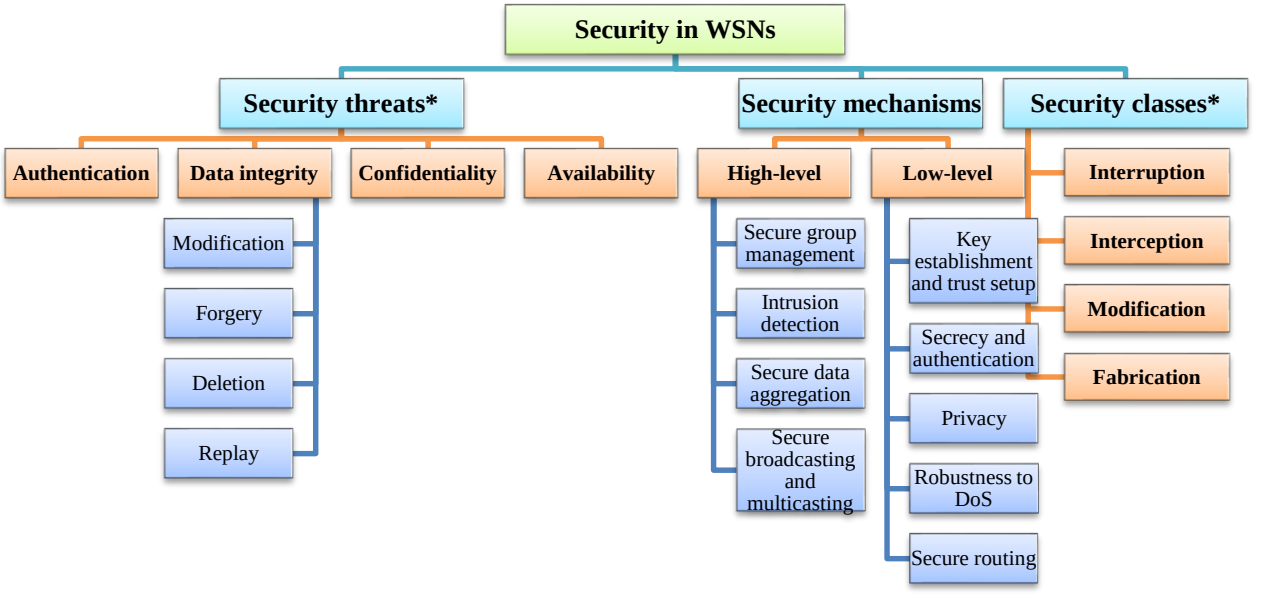


Fig. 1. WSNs' different aspects

WSNs are vulnerable to many types of attacks and due to free, unsafe and unprotected nature of communication channel, untrusted and broadcast transmission media, deployment in hostile environments and limited resources, security in WSNs is a vital and complex requirement. Besides, most of existent security mechanisms of traditional networks are impractical in WSNs [3, 4]. So, it is necessary to design appropriate security mechanisms for these networks. The security mechanisms should cover different security dimension of WSNs, including of confidentiality, integrity, availability and authenticity. Necessities of security in WSNs are: correctness of network functionality, unusable typical networks protocols, WSNs' limited resources, untrusted nodes and requiring trusted center for key management, preventing from existent attacks, selfishness and extending collaboration. Some of most important issues on WSNs' security are: key establishment, secrecy, authentication, privacy, robustness to DoS attacks and secure routing [5, 6, 13]. In other direction, there are many security services on WSNs, such as encryption and data link layer authentication, multi-path routing, identity verification, bidirectional link verification and authenticated broadcasts. Figure2 is showing most important dimensions of security in WSNs; however, this paper considers only star spangled blocks to classify and compare WSNs' attacks.



(a)



(b)

Fig. 2. (a) and (b): Security in WSNs

The threat model of WSNs classifies and compares WSNs' attacks or attackers based on their nature and goals [7, 8, 9]. Figure3 is showing the WSNs' threat model.

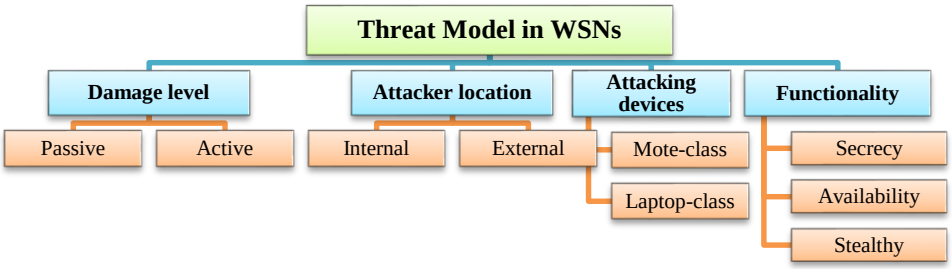


Fig. 3. Threat model in WSNs

TABLE 1. THREAT MODEL OF WSNS

Attack category	Types	Damage level	Ease of identify	Attacker presence
Based on damage level	Active	High	Easy	Explicit
	Passive	Low	Hard	Implicit
Based on attacker location	External	Low	Easy	Implicit
	Internal	High	Hard	Implicit
Based on attacking devices	Mote-class	Low	Hard	Implicit
	Laptop-class	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 attacks on WSNs can be high (serious effect on the WSN) or low (limited effect on the WSN); besides, the attackers verification can be easy or hard; also the attackers' presence can be explicit (serious damage) or implicit.

The main purpose of this paper is presenting an overview of different attacks on WSNs. It is considering a wide variety of WSN's attacks, extracting their different features, classifying and comparing them based on their result, nature, purpose and WSNs' threat model. So, this work introduces the result, nature, purpose and capabilities of WSNs' attacks and attackers. The rest of this paper is organized as: section 2 is presented an overview of physical attacks on WSNs; section 3 focused on link layer attacks on WSNs; section 4 considers routing attacks of WSNs; section 5 includes different dimensions of transport and application layers attacks on WSNs; and finally, section 6 states the conclusion and future works.

2 PHYSICAL ATTACKS ON WIRELESS SENSOR NETWORKS

2.1 Definitions and result of physical attacks

WSNs are vulnerable against different physical attacks. Attackers can gain fully access to sensor nodes, extract and reveal sensitive and sensed data, or launch DoS attacks. Table2 is presented the WSNs' physical layer attacks.

TABLE 2. PHYSICAL ATTACKS ON WSNS

Attack	Attack definition	Attack result
Jamming	Transmitting radio signals at the same frequency band (radio interference) [10, 11, 13, 14];	• Radio interference; • Resource exhaustion;
Device Tampering	Direct physical access and capture sensor nodes [12, 13];	• Damaging and modifying physically; stopping/changing nodes' services; • Taking full control on the captured node; • Taking over the entire WSN; • Software vulnerabilities; • Launching internal attacks;
Path-Based DoS	Sending many packets to the Sink by attacker [13, 15];	• Nodes' battery exhaustion; • Network disruption; • Falsely excluding nodes from local report; • Reducing the WSN's availability;
Node Outage	Stopping functionality of the WSN's components, such as a sensor node [13];	• Stop nodes' services; • Taking over the WSN and preventing from some communications; • Impossibility reading the gathered data; • Launching other attacks;

2.2 Physical attacks classification based on the threat model

This section tried to compare the physical attacks of WSNs based on the WSNs' threat model, as shown in Table3. Security class is the nature of attacks, including of interruption, interception, modification and fabrication. Attack threat shows which security dimension affected or threaten; it is including of confidentiality, integrity, authenticity and availability.

TABLE 3. WSN'S PHYSICAL ATTACKS CLASSIFICATION BASED ON THE WSNS' THREAT MODEL

Attack	Security class	Attack threat	Threat model		
			Attacker location	Attacking device	Attack nature
Jamming	Interruption, modification	Availability, integrity	External	Both	Active
Device Tampering	Interruption, modification, fabrication	Availability, integrity, confidentiality, authenticity	External	-----	Active
Path-Based DoS	Interruption	Availability	Internal	Laptop-class	Active
Node outage	Interruption	Availability	External	Both	Active

Figure4 shows the security class of WSN's physical attacks; it compares these attacks based on their nature by presents the percentage of WSNs' physical attacks which based on interruption, interception, modification and fabrication; as a result, nature of most physical attacks is interruption (almost 100 percent).

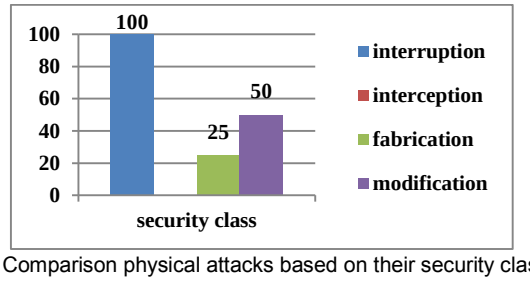


Fig. 4. Comparison physical attacks based on their security class

Figure5 shows a comparison of WSNs' physical attacks based on attack threat, in percentage; for example, it presents almost 25 percent of security threat of WSNs' physical attacks is confidentiality. As shown in Figure5, the aim of most WSNs' physical attacks is attacking to availability (almost 100 percent).

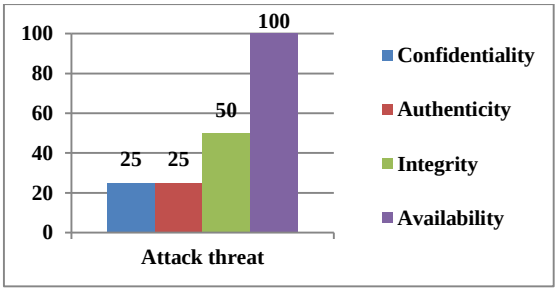


Fig. 5. Comparison physical attacks based on threaten security dimension

Figure6 is showing a comparison of physical attacks based on the threat model; as shown in Figure6, the occurred percentage of WSNs' physical attacks, in attacker location, are 25 percent internal and 75 percent external; i.e. most of WSNs' physical attacks are occurring from out of WSNs' range. Also, it presents all physical attacks on WSNs are active. Besides, most attacks on physical layer of WSNs are laptop-class attacks.

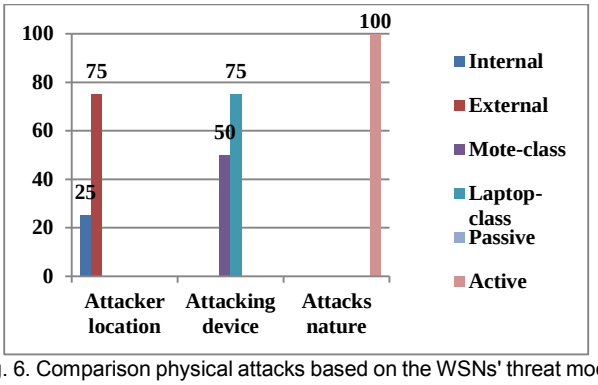


Fig. 6. Comparison physical attacks based on the WSNs' threat model

2.3 Physical attacks comparison based on their purpose

Table4 compares WSNs' physical attacks based on attacks' or attackers' purpose; it is including of passive eavesdrop, disrupt communication, unfairness, authorization and authentication.

TABLE 4. PHYSICAL ATTACKS COMPARISON BASED ON ATTACKS' PURPOSE

Attack	Purpose
Jamming	Disrupt communication, unfairness
Device Tampering	Unfairness; to be authenticated; to be authorized
Path-Based DoS	Unfairness
Node outage	Unfairness

Figure7 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 100 percent of these attacks are aiming the fairness of WSNs.

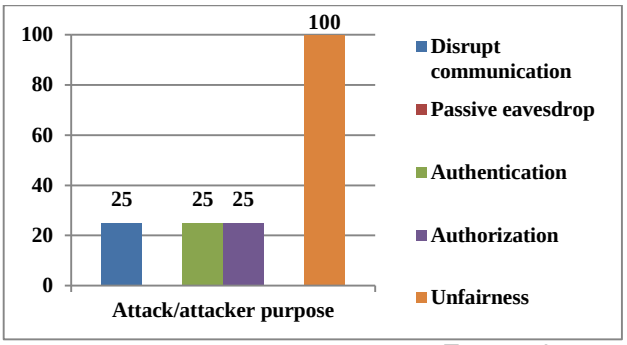


Fig. 7. Comparison physical attacks based on attacks' purpose

3 Link Layer Attacks on Wireless Sensor Networks

3.1 Definitions and result of link layer attacks

WSNs are vulnerable against to different link layer attacks. Attackers can gain access to transmission media, creating radio interference, preventing from legitimate sensor nodes to communicate or launching DoS attacks. Table5 is presented the link layer attacks on WSNs.

TABLE 5. LINK LAYER ATTACKS ON WSNS

Attack	Attack definition	Attack result
Collision	Message transmission by two nodes on a same frequency, simultaneously [8, 16];	• Interferences; • Data or control packets corruption; • Energy exhaustion;
Resource Exhaustion	Repeated collisions and continuous retransmission until the sensor node death [6, 8, 16];	• Resources exhaustion; • Compromising availability; • Message modification;
Traffic manipulation	Regular monitoring and computing some parameters based on affected MAC protocol ⇨ time adjustment ⇨ transmitting messages just at the moment when normal nodes do so [16];	• Excessive packet collisions; • Aggressively competition or contention for channel usage; • Decreasing signal quality and network availability; • Unfair bandwidth usage; • Degradation of the WSN performance; • Traffic distortion;
Unfairness	Partial DoS attack; it is using other attacks such as collision and resource exhaustion, continuously [8, 16];	• Decreasing utility and efficiency of services; • Nodes' hungry for channel access; • Limiting channel access and undermine communication channel capacity;

3.2 Link layer attacks classification based on the threat model

This section tried to compare the WSNs' link layer attacks based on the WSNs' threat model, as shown in Table6.

TABLE 6. WSN'S LINK LAYER ATTACKS CLASSIFICATION BASED ON THE WSNS' THREAT MODEL

Attack	Security class	Attack threat	Threat model		
			Attacker location	Attacking device	Attack nature
Collision	Modification	Integrity	Internal	Both	Active
Resource Exhaustion	Modification	Availability, integrity	External	Laptop-class	Active
Traffic manipulation	Interception, modification	Availability, integrity, confidentiality	External	Mote-class	Active
Unfairness	Interruption, modification	Availability, integrity	External	Laptop-class	Active

Figure8 shows the security class of WSN's link layer attacks; it compares these attacks based on their nature by presents the percentage of WSNs' link layer attacks which based on interruption, interception, modification and fabrication; as a result, nature of most link layer attacks is modification (almost 100 percent).

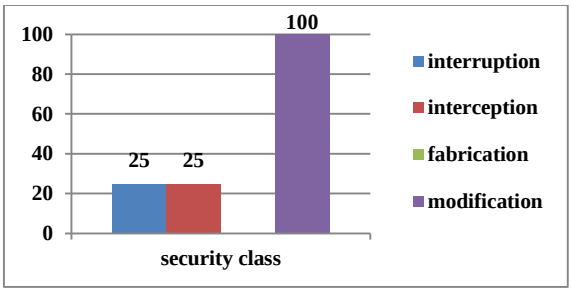


Fig. 8. Comparison link layer attacks based on their security class

Figure9 shows a comparison of WSNs' link layer attacks based on attack threat, in percentage; for example, it presents almost 25 percent of security threat of WSNs' link layer attacks is confidentiality. As shown in Figure9, aim of most WSNs' link layer attacks is attacking to integrity.

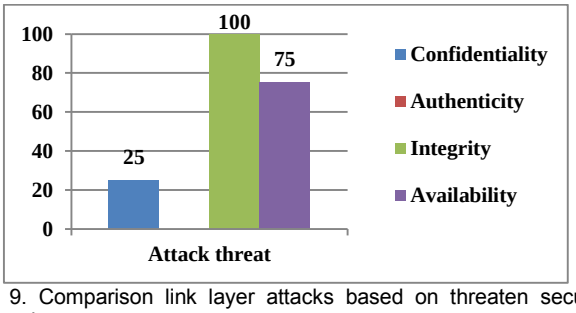


Fig. 9. Comparison link layer attacks based on threaten security dimension

Figure 10 is showing a comparison link layer attacks based on the threat model of WSNs; As shown in Figure10, the occurred percentage of WSNs' link layer attacks, in attacker location, are 25 percent internal and 75 percent external; i.e. most of WSNs' link layer attacks are occurring from out of WSNs' range. Also, it presents almost all link layer attacks on WSNs are active. Besides, most attacks on link layer of WSNs are laptop-class attacks.

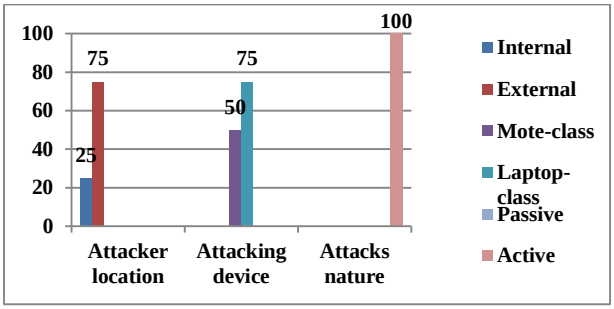


Fig. 10. Comparison link layer attacks based on the WSNs' threat model

3.3 Link layer attacks comparison based on their purpose

Table7 compares WSNs' link layer attacks based on attacks' or attackers' purpose.

TABLE 7. LINK LAYER ATTACKS COMPARISON BASED ON ATTACKS' PURPOSE

Attack	Purpose
Collision	Unfairness
Resource Exhaustion	Unfairness
Traffic manipulation	Unfairness
Unfairness	Disrupt communication, Unfairness

Figure11 is showing how much percentage of WSNs' link layer attacks are happened by targeting the fairness, confidentiality, authentication, authorization and disrupt communication on WSNs' functionalities, services and resources; for example, almost 100 percent of these attacks are aiming the fairness of WSNs.

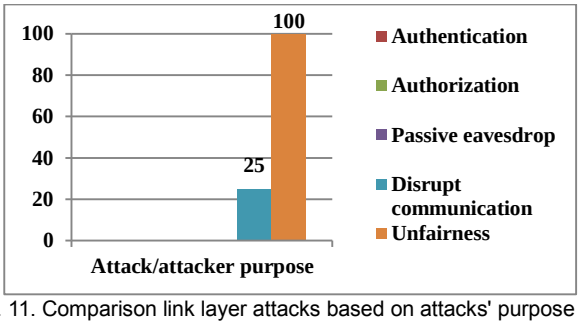


Fig. 11. Comparison link layer attacks based on attacks' purpose

4 ROUTING ATTACKS ON WIRELESS SENSOR NETWORKS

4.1 Definitions and result of routing attacks

WSNs are vulnerable against different routing attacks. Attackers can gain access to routing paths and redirect the traffic, propagating false routing information into the WSN or launching DoS attacks. Table8 is presented the routing attacks on WSNs.

TABLE 8. ROUTING ATTACKS ON WSNS

Attack	Attack definition	Attack result
Homing	Regular monitoring and analyzing the traffic, communication patterns and sensor nodes	• Verifying, locating and destroying vital resources; • Extracting the sensitive network information;

	activities ⇨ verifying and locating vital resources [17];	• Launching active attacks; • Threaten data confidentiality and privacy;
Neglect and greed	Dropping incoming packets, randomly (neglectful) and giving undue priority to its own messages (greedy);	• Consistently degrade or block traffic; • Packet drop; • Influencing or limiting the WSN traffic;
Rushing	Quick broadcasting the false advertisings of route request through the WSN [17, 19];	• Discarding correct requests; • Launching other attacks; • Partitioning the network; • Inability to discover any useful routes; • Strengthening the attackers' position;
Gratuitous detour	Making a route through attacker appear longer where a shorter route exists and would otherwise be used, by adding virtual nodes to the route;	• Resources exhaustion; • Routing loops; • Routing inconsistencies; • Network partition; • Misdirection;
Node malfunction	Inaccurate data generation;	• Integrity destruction; • Degradation the WSN efficiency; • Resources exhaustion;
HELLO flood	Flooding whole network with routing protocol's HELLO packets, that announcing false neighbor status by using of powerful radio transmitter [8, 17, 18];	• Disrupting topology construction; • Network and routing destruction; • Exhausting nodes' energy; • Decreasing efficiency; • Increasing WSN latency;
Flooding	Generating and propagating numerous route requests [17, 18];	• Resource exhaustion; • Reducing availability; • Blowing up the traffic statistics of the WSN or a certain node and enforcing additional processes;
Sinkhole	Attracting all possible traffic to a compromised node by placing a malicious node closer to the sink and enabling selective forwarding [17, 23];	• Triggering other attacks; • Information modification, fabrication and packet dropping; • Resource exhaustion;
Black-hole	A kind of DoS attack which attacker swallows all received data (dropping all incoming packets) [8, 17, 20, 21];	• Decreased the throughput of a subset of nodes; • Network partition; • High rate of packet loss; • Limiting or preventing of data transmission;
Wormholes	Tunneling and replicating messages from one location to another through alternative low-latency links, by colluding two active nodes (laptop-class) and establishing better communication channels (tunnel). Wormhole nodes operate fully invisible [17, 18, 22];	• Routing disruption; • False or forged routing information; • Confusion and WSN disruption; • Exploiting the routing race conditions; • Change network topology; • Prevention of path detection process; • Changing normal messages stream;
Spoofed, altered or replayed routing information	Making a path cycle between source and destination nodes; A type of DoS attack that injecting faked or false routing information into the WSN;	• Network partition; • Misdirection; • Resources exhaustion; • Reducing network lifetime; • Discard routing information; • Wrong routing tables;
Acknowledge spoofing	Spoofing link layer ACKs of overheard packets;	• False view of the WSN; • Launching selective forwarding attack; • Packet loss or corruption;
Sybil	A single node forges multiple identities [17, 18, 24];	• Breaking the data integrity and accessibility; • Geographical and multipath routing protocols disruption; • Reducing the effectiveness of fault tolerant schemes;
Eavesdropping	Regular overhearing, detecting and analyzing the transmitted data and sensor nodes activities ⇨ extracting and revealing the sensitive information (privacy violation) ⇨ harming to the WSN;	• Monitoring and access to the WSN's information; • WSN partial disruption; • Launching other attacks; • Extracting sensitive information; • Deleting the privacy protection and reducing data confidentiality;

Selective forwarding	Sending or dropping data of special nodes; there are 2 modes of this attack: Simple mode attack and complex mode attack [17, 18];	• Dropping or modifying certain messages; • Influencing the WSN traffic; • Impossibility verifying malicious nodes;
Misdirection	Misrouting traffic flows in one direction to a distant node; i.e. forwarding messages to a wrong path;	• Packets misdirection; • Wrong routing tables; • Resources exhaustion; • Network partition; • Reducing the WSN's availability;

4.2 Routing attacks classification based on the threat model

This section tried to compare the WSNs' routing attacks based on the WSN's threat model, as shown in Table9.

TABLE 9. WSN'S ROUTING ATTACKS CLASSIFICATION BASED ON THE WSNS' THREAT MODEL

Attack	Security class	Attack threat	Threat model		
			Attacker location	Attacking device	Attack nature
Homing	Interception	Confidentiality	Internal	Mote-class	Passive
Neglect and greed	Fabrication	Availability, authenticity	Internal	Mote-class	Active
Rushing	Modification, fabrication	Availability, integrity, authenticity	Internal	Mote-class	Active
Gratuitous detour	Interruption, fabrication	Availability, integrity, authenticity	Internal	Mote-class	Active
Node malfunction	Interruption, fabrication	Availability, authenticity	External	Laptop-class	Active
HELLO flood	Interruption, fabrication	Availability, authenticity	Internal	Mote-class	Active
Flooding	Interruption, modification, fabrication	Availability, integrity, authenticity	Both	Laptop-class	Active
Sinkhole	Modification, fabrication	Availability, integrity, authenticity	Internal	Mote-class	Active
Black-hole	Fabrication	Availability, authenticity	Internal	Mote-class	Active
Wormholes	Fabrication, interception	Confidentiality, authenticity	External	Laptop-class	Active
Spoofed, altered or replayed routing information	Fabrication, modification	Integrity, authenticity	Both	Both	Active
Acknowledge spoofing	Fabrication, modification	Integrity, authenticity	Internal	Mote-class	Active
Sybil	Modification, fabrication	Availability, authenticity, integrity	Internal	Mote-class	Active
Eavesdropping	Interception	Confidentiality	External	Both	Passive
Selective forwarding	Modification	Availability, integrity	Internal	Both	Active
Misdirection	Interruption, modification, fabrication	Availability, integrity, authenticity	Internal	Both	Active

Figure12 shows the security class of WSN's routing attacks; it compares these attacks based on their nature by presents the percentage of WSNs' routing attacks which based on interruption, interception, modification and fabrication; as a result, nature of most routing attacks is fabrication (almost 81 percent).

Fig. 12. Comparison routing attacks based on their security class

Figure13 is showing a comparison of WSNs' routing attacks based on attack threat, in percentage; for example, it presents almost 18 percent of security threat of WSNs'

routing attacks is confidentiality. As shown in Figure13, aim of most WSNs' routing attacks is attacking authenticity.

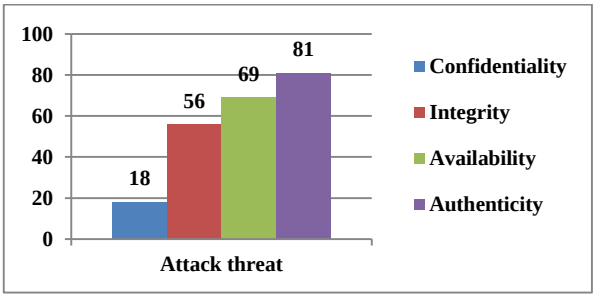


Fig. 13. Comparison routing attacks based on the threaten security dimension

Figure14 is showing a comparison routing attacks based on the threat model; As shown in Figure14, the occurred percentage of WSNs' routing attacks, in attacker location, are 81 percent internal and 31 percent external; i.e. most of WSNs' routing attacks are occurring from into the WSNs' range. Also, it presents most of routing attacks on WSNs are active; i.e. almost 88 percent of WSNs' routing attacks are active. Besides, Figure14 shows most attacks on routing layer of WSNs are mote-class attacks.

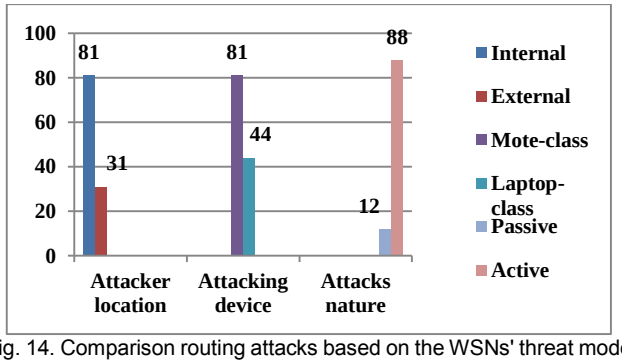


Fig. 14. Comparison routing attacks based on the WSNs' threat model

4.3 Routing attacks comparison based on their purpose

Table10 compares WSNs' routing attacks based on attacks' or attackers' purpose.

TABLE 10. ROUTING ATTACKS COMPARISON BASED ON ATTACKS' PURPOSE

Attack	Purpose
Homing	Passive eavesdrop of data
Neglect and greed	Unfairness
Rushing	Unfairness
Gratuitous detour	Unfairness
Node malfunction	Unfairness
HELLO flood	Unfairness; disrupt communication
Flooding	Unfairness; disrupt communication
Sinkhole	Unfairness
Black-hole	Unfairness
Wormholes	Unfairness; disrupt communication to be authenticated; to be authorized
Spoofed, altered or replayed routing information	Unfairness, disrupt communication
Acknowledge spoofing	Unfairness
Sybil	Unfairness; to be authenticated; to be authorized
Eavesdropping	Passive eavesdrop of data
Selective forwarding	Unfairness
Misdirection	Unfairness

Figure15 shows how much percentage of WSNs' routing attacks are happened by targeting the fairness, confidentiality, authentication, authorization and disrupt communication on WSNs' functionalities, services and resources; for example, almost 88 percent of these attacks are aiming the fairness of WSNs.

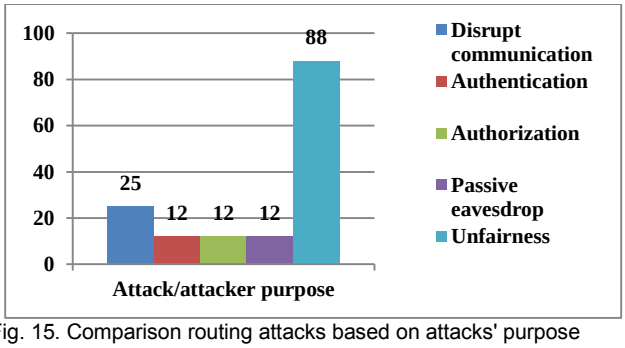


Fig. 15. Comparison routing attacks based on attacks' purpose

5 TRANSPORT AND APPLICATION LAYERS ATTACKS ON WIRELESS SENSOR NETWORKS

5.1 Definitions and result of transport and application layers attacks

WSNs are vulnerable against different transport and application layers attacks. Table11 is presented the transport and application layers attacks of WSNs.

TABLE 11. TRANSPORT AND APPLICATION LAYERS ATTACKS ON WSNS

Attack	Attack definition	Attack result

De-synchronization	Disrupting established connections between two legitimate nodes by re-synchronizing their transmission [25];	• Disrupt communication; • Going out the synchronization; • Resource exhaustion;
Data aggregation distortion	Attack against data integrity; it is disrupting data aggregation, modifying collected data and distorting the final aggregation results [25];	• Incorrect view of the monitored environment; • Totally disrupted data aggregation; • Triggering other cross-layer attacks;
Clock skewing	Disseminating false timing information to desynchronize the nodes [25];	• Being out of synchronization; • Being unstable; • Communications disruption; • Wasting nodes' energy;

5.2 Transport and application layers attacks classification based on the threat model

This section tried to compare the transport and application layers attacks of WSNs based on the WSN's threat model, as shown in Table12.

TABLE 12. WSN'S TRANSPORT AND APPLICATION LAYERS ATTACKS CLASSIFICATION BASED ON THE WSNS' THREAT MODEL

Attack	Security class	Attack threat	Threat model		
			Attacker location	Attacking device	Attack nature
De-synchronization	Interruption, 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

Figure16 is showing the security class 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 and fabrication; as a result, nature of most these attacks is modification (almost 100 percent).

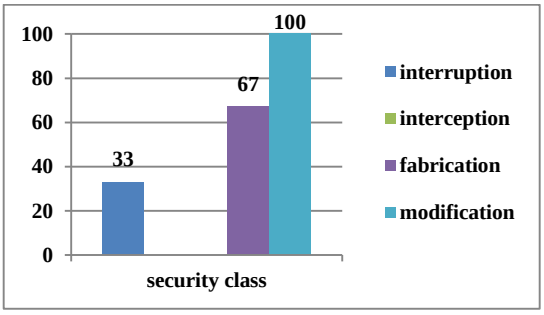


Fig. 16. Comparison transport and application layers attacks based on their security class

Figure17 shows a comparison of WSNs' transport and application layers attacks based on attack threat, in percentage; for example, it presents almost 0 percent of security threat of WSNs' transport and application layers attacks is confidentiality. As shown in Figure17, aim of most WSNs' transport and application layers attacks is attacking availability.

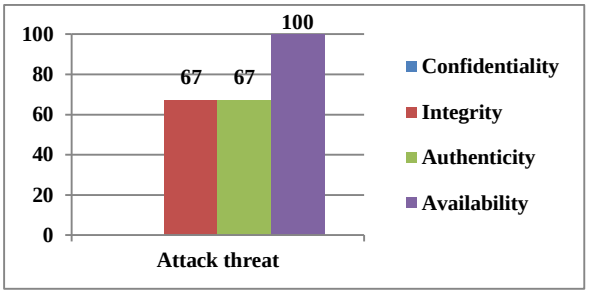


Fig. 17. Comparison transport and application layers attacks based on the threaten security dimension

Figure18 is showing a comparison of transport and application layers attacks based on the threat model; as shown in Figure18, the occurred percentage of WSNs' transport and application layers attacks, in attacker location, are 33 percent internal and 100 percent external; i.e. most of WSNs' transport and application layers attacks are occurring from out of WSNs' range. Also, it presents almost all transport and application layers attacks on WSNs are active.

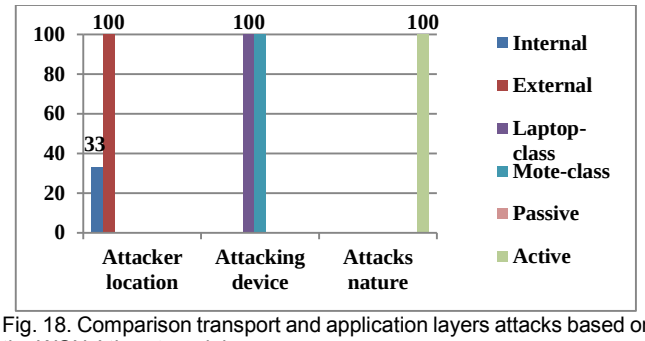


Fig. 18. Comparison transport and application layers attacks based on the WSNs' threat model

5.3 Transport and application layers attacks comparison based on their purpose

Table13 compares WSNs' transport and application layers attacks based on attacks' or attackers' purpose.

TABLE 13. TRANSPORT AND APPLICATION LAYERS ATTACKS COMPARISON BASED ON ATTACKS' PURPOSE

Attack	Purpose	Network layer
De-synchronization	Disrupt communication; unfairness	Transport; application
Data aggregation distortion	Unfairness	application
Clock skewing	Disrupt communication; unfairness	Application

Figure19 is showing how much percentage of WSNs' transport and application layers attacks are happened by targeting 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.

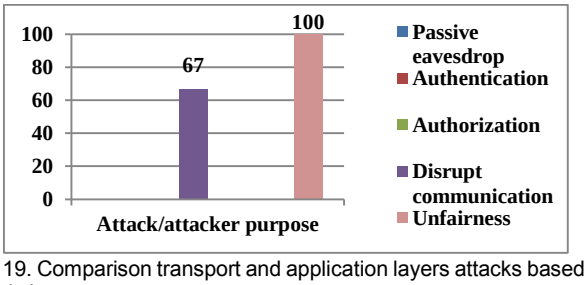


Fig. 19. Comparison transport and application layers attacks based on attacks' purpose

6 CONCLUSION AND FUTURE WORKS

Security is a vital and complex requirement to deploy and extend WSNs in different operational environments. This paper analyzes different dimensions of WSNs' security; it presents a wide variety of WSNs' attacks (including of physical, link layer, routing, transport and application layers attacks) and classify them; the used approach for classify and compare the WSNs' attacks is based on different extracted features of different WSNs' layer, attacks' and attackers' properties; such as the threat model of WSNs, attacks' nature, result and their goals, independently and comprehensively. Some of most important findings of this paper are as following:

- Encryption is not enough and inefficient for internal attacks and laptop-class attackers;
- Attacks are often launching combinational (intra-layer or cross-layer).
- As shown in Figure20, nature of about 100 percent of WSNs' physical attacks is interruption; almost 100 percent of them are targeting availability; most of these attacks are out of the WSNs' range (external: 75 percent) and lead to high-level damages (laptop-class attacks: 75 percent; active attacks: 100 percent); about 100 percent of physical attacks' purpose is unfairness.
- As shown in Figure21, nature of about 100 percent of WSNs' link layer attacks is modification; almost 100 percent of them are targeting integrity; most of these attacks are out of the WSNs' range (external: 75 percent) and lead to high-level damages (laptop-class attacks: 75 percent; active attacks: 100 percent); about 100 percent of link layer attacks' purpose is unfairness.
- As shown in Figure22, nature of about 81 percent of WSNs' routing attacks is fabrication; almost 81 percent of them are targeting authenticity; most of these attacks are from into the WSNs' range (internal: 81 percent) and lead to high-level damages (mote-class attacks: 81 percent; active attacks: 88 percent); about 88 percent of routing attacks' purpose is unfairness.
- As shown in Figure23, nature of about 100 percent of WSNs' transport and application layers attacks is modification; almost 100 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 (mote-class and laptop-class attacks: 100 percent; active attacks: 100 percent); about 100 percent of these attacks' purpose is unfairness.

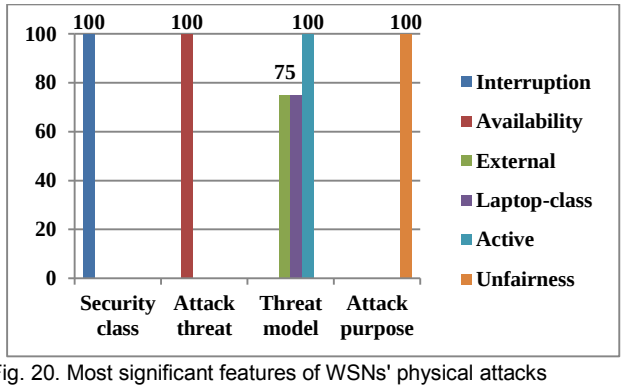


Fig. 20. Most significant features of WSNs' physical attacks

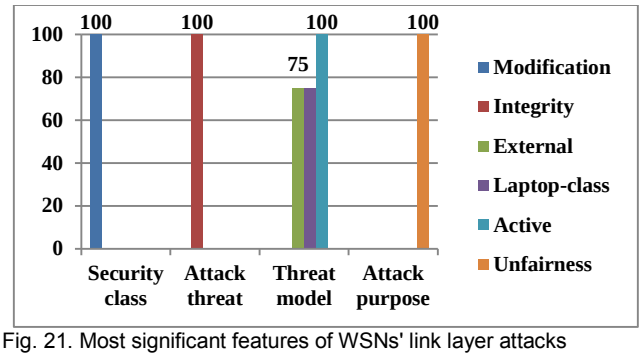


Fig. 21. Most significant features of WSNs' link layer attacks

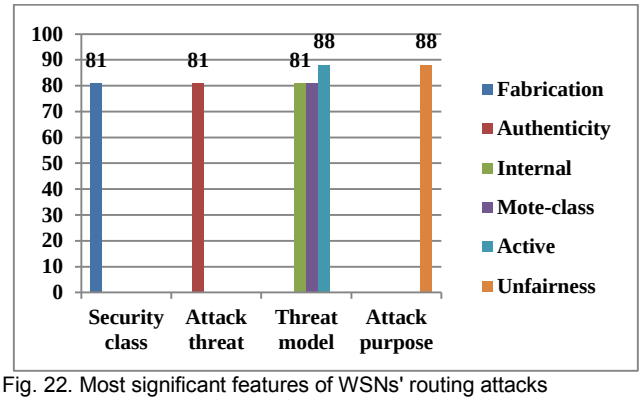


Fig. 22. Most significant features of WSNs' routing attacks

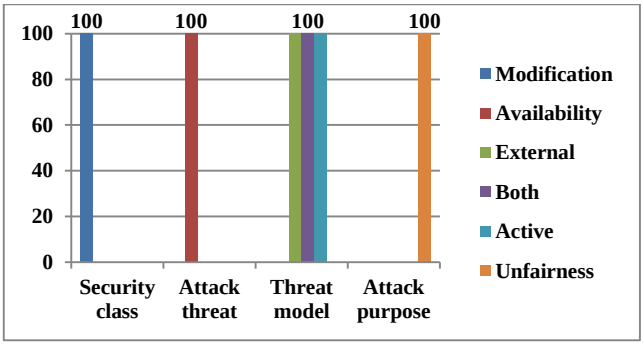


Fig. 23. Most significant features of WSNs' transport and application layers attacks

There are several additional issues should be further studied in future researches. Some of most challenging proposed topics of these issues as the next steps of this work are as following:

- Securing wireless communication links against eavesdropping, traffic analysis and DoS attacks;
- Designing secure MAC, routing and transport layers protocols or securing existent MAC, routing and transport layers protocols;
- Multipath routing in WSNs;
- Trust models in WSNs;
- Using public key cryptography and digital signature in WSNs;
- Countermeasures for physical, link, routing, transport and application layers attacks;

This work is hoping to introduce the purpose and capabilities of the attackers, precisely; also expressing the goal and result of the attacks on the WSNs' functionality, in comprehensive. It is hoping by reading this paper, readers can have a better view of different WSNs' attacks; so, it leads to design secure WSNs.

REFERENCES

[1] J. Yick, B. Mukherjee and D. Ghosal; Wireless Sensor Network Survey; Elsevier's Computer Networks Journal, 52, 2292-2330; 2008.

[2] I. Akyildiz, W. Su, Y. Sankarasubramania and E. Cayirci; A Survey On Sensor Networks; IEEE Communications Magazine, Vol. 40, No. 8, pp. 102–116; 2002.

[3] D.Thakral and N.Dureja; A Review on Security Issues in Wireless Sensor Networks; International Journal of Advanced Research in Computer Science and Software Engineering; Vol. 2, Issue 7; 2012.

[4] 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); 2008.

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

[6] K. Xing, S. Sundhar, R. Srinivasan, M. Rivera, J. Li and X. Cheng; Attacks and Countermeasures in Sensor Networks: A Survey; Springer, Network Security; 2005.

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

[8] 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; 2009.

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

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

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

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

[13] S.Mohammadi and H.Jadidoleslamy; A Comparison of Physical Attacks on Wireless Sensor Networks; International Journal of Peer to Peer Networks (IJP2P), Vol.2, No.2, pp. 24-42; 2011.

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

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

[16] S.Mohammadi, R.A.Ebrahimi and H.Jadidoleslamy; A Comparison of Link Layer Attacks on Wireless Sensor Networks; international Journal of Information Security (JIS), Vol. 2, No. 2, pp. 69-84; 2011.

[17] S.Mohammadi, R.A.Ebrahimi and H.Jadidoleslamy; A Comparison of Routing Attacks on Wireless Sensor Networks; International Journal of Information Assurance and Security (JIAS), Vol. 6, pp. 195-215; 2011.

[18] 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; 2003.

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

[20] A. Saini and H. Kumar; Comparison between Various Black Hole Detection Techniques in MANET; National Conference on Computational Instrumentation (NCCI); 2010.

[21] 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; 2010.

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

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

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

[25] S.Mohammadi and H.Jadidoleslamy; A Comparison of Transport and Application Layers Attacks on Wireless Sensor Networks; International Journal of Information Assurance and Security (JIAS), Vol.6, pp. 331-345; 2011.

AUTHOR BIOGRAPHY

H. Jadidoleslamy is a PhD student in Information Technology (IT)-Information Security at the Malekashtar University of Technology (MUT) in Tehran, Iran. He received his Bachelor Degree in Information Technology (IT) engineering from the University of Sistan and Balouchestan (USB), Zahedan, Iran, in September 2009. He also has been received his Master of Science degree from the University of Guilan, Rasht, Iran, in March 2011. His research interests are including Computer Networks (especially Wireless Sensor Network), Information Security (by focusing on Intrusion Detection System), and E-Commerce. He may be reached at tanha.hossein@gmail.com or jadidoleslamy@gmail.com.