Review

iMedPub Journals
http://www.imedpub.com/

American Journal of Computer Science and Information Technology

2019
Vol.7 No.1:31

DOI: 10.21767/2349-3917.100031

A Review on Security Attacks and Solution in Wireless Sensor Networks

Muhammad Asim Khan[1*], Mansoor Khan[2]

[1]Department of Information technology, Telecommunication, Hazara University, Garden Campus, Mansehra, Pakistan

[2]Department of Computer Science, University of Haripur, Pakistan

[*]**Corresponding author:** Muhammad Asim Khan, Department of Information technology, Telecommunication, Hazara University, Garden Campus, Mansehra, Pakistan, E-mail: muhammadasimkhan56@gmail.com

Received Date: November 21, 2018**; Accepted Date:** January 11, 2019; **Published Date:** February 08, 2019

Citation: Khan AS, Khan M (2018) A Review on Security Attacks and Solution in Wireless Sensor Networks. Am J Compt Sci Inform Technol Vol.7 No. 1: 31

Abstract

Wireless Sensor Network (WSN) utilizes small sensors with constrained properties to broadcast, collect, and sense the data in numerous applications. As WSN is an interest gaining technology. Security challenges become the main issue, especially in task like mission critical application. In this article, we identify the security attacks in WSN and identify the major solution for these attacks. These attacks are of three major categories; service integrity and network availability, privacy and confidentiality, and the integrity of data and major solution for these attacks. In addition, we also explain the methods and techniques used in these categories for the defense purposes and summarize the open research issues in these areas.

Keyword:

Wireless sensor network; Security; Privacy; Confidentiality; Availability; Integrity

Introduction

Advanced technologies have made possibilities to evolve tiny sensor nodes with compact hardware at very low prices. It is suitable to form a wireless sensor network (WSN), which is self-organized and self-healing network consist of dense or small number of sensor nodes, to remote and even hostile areas to perform certain monitoring tasks. For example, reconnaissance of battle field, surveillance of coast and border, rescue and search, outer space and deep ocean exploration, monitors level of pollution, traffic integral structural of buildings. Some other applications are, sensing of climate, office control, and sensing home environments like light, temperature and moisture [1]. In WSN the collected data is not directly transmit to the user, indeed, sensed data is initially aggregated and then transmit [2]. A WSN consist of sink, base station or gateway, which connect all the nodes with each other to form a network and should be connected to end user. At the sensor node data is compressed and then transmitted to sink or base station, due to which end user can see the results of an activity [3,4]. Sometimes data packets are sent to the user terminal via multiple intermediate nodes. This type of transmission is known as multi-hop transmission.

The wireless sensor node having limited resources, however, the objective is to achieve goals with minimum energy consumption, usage of minimum memory and less computation cost. Moreover, these nodes are self-healing and self-organize into network to co-operate for sensing/aggregation of particular information or execution of specific activity. Since, these sensor nodes are usually working in harsh and unattended environment without any protection, and wireless media is used for communication by sensor nodes. Thus they are unprotected to a vast range of attacks. WSN applications should be secured in specific number of all critical applications; the data exchanged among WSN nodes need superior level of security. In some of military applications, number of sensor nodes co-operate with each other for target tracking [5]. Hence, the exchange of information among these nodes is related to the target position. The operation of this application can disturb by attackers injecting false message. In application like medical, the collected information of patient by sensor nodes kept protected and confidential [6]. Secure network communication may also important for the privacy of location, which is major factor in military application, animal monitoring and homeland security applications [7]. Hence, a secure network communication method shall be applied for the protection of inter-network communication from security attacks, such as modifying text, eavesdropping and injecting messages [8].

The rest of the article is organized as follows. The next section explain the security requirements in WSN, section 3 classify the security threats, section 4, 5, 6 explain the attacks and solution for service integrity, network availability, privacy, confidentiality, and integrity of data in WSN, section 7 simply summarize this article, section 8 explain the research issues and section 9 conclude this article.

Security Requirements in WSN

In this section we give a review of the basic requirements that WSNs, typically have to achieve.

Availability

In timely manner, the services served by the WSN should be always available. Attacks of resource depletion are the major classes of attacks attempt to fail this property.

Integrity

It is the guarantee that data can only modified and exchange by the WSN nodes only.

Confidentiality

Secrete data exchanged and stored in WSN must not be reveal to unauthorized users. In some scenario, even the existence of communication between nodes must be kept hidden. To measure the confidentiality threats in WSN normally cryptographic tools are used. In changing topology of WSN, where nodes can leave or join the network, WSN must be addressed by the backward and forward secrecy. Forward secrecy refer to stop access any future communication with nodes that leave the network, and backward secrecy refer that before joining the network nodes are not in the position to receive or send any message.

Authorization

It refers that only authorized sensor nodes and entities must be able to access the network.

Non-repudiation

WSN must be able to separate and find compromised sensor nodes, it should be impossible for message sender to conquer challenge the message authorship.

Classes of security threats

Generally, attacks on WSN can be classified on the basis of attacker status, purpose of the attackers, and on the behavior of the attacker.

Status: These classifications of attacks are based on either the attacker is insider or outsider. Insider attackers are authorized sensor behaving in a vicious way while outsider attackers are not belonging to WSN but aim to disrupt the service provided by the network.

Purpose: This category only depends on the purpose of the attacker. Attacks on service integrity and network availability, try to disrupt the network services. Physical attack, denial of service (DoS), and routing attacks belonging to this category.

Behavior: The third classification differentiates active and passive attacks. The formers, physically access to some part of the WSN. While, latter just consist of eavesdropping exchanged data, analyzing and monitoring the network behavior.

Attacks against confidentiality and privacy are the attacks which aim to get insight on secret data. In such situation, the goal of attackers is to exchange data in network, information and functioning of the network topology, and information of contextual. Finally, attacks against the integrity of data try to change the transmitted data. Vicious nodes may inject wrong messages, replicate entire nodes or old packets, etc. [9].

Attacks and Solution for Service Integrity and Network Availability in WSN

Attacks against service integrity and network availability are habitually called denial of service (DoS) attacks, a foe attempts to subvert, destroy or disrupt the network services. DoS attacks target one of the WSN layer. Even, these attacks affect the physical, the network, the data link, and the transport layers. In this section we will summarize common DoS attacks on above mention layers.

Attacks and solution on physical layer

Generally, outsiders carried out active attacks, all based on a common access by accessing physically single or multiple sensor nodes tampering with hardware. More nearly, the purpose of the attacker is might be to alter the behavior of the sensor nodes, to interchange them with enemy sensor which is controlled by the attacker, or steal cryptographic or confidential information [10].

Tamper-resistant nodes are the best defense option against physical nodes tampering. However, one of the feasible and cheaper options is tamper-resistant hardware. As alternative solution are the software's, which were distinctly designed for the detection of tampering attacks, and primarily detect cryptographic data before the execution of protocol termination. Tampering with present node hardware had been investigated in [11]. The authors tell that, without the interference of the normal sensor operation generally has negligible impact. For serious attack, which results in the full control of the node, deceased the node for specific time from the network. Therefore, better defensive strategy is that, monitored node should be inactivity for long period.

The latest analysis of researchers show that the best countermeasure for sensor tampering is authentication of node using the hash function, this technique is preferable due to the establishment of session key, strong authentication of sensor node and maintain the efficiency of WSN [12].

A noise signal is generated by the attackers in jamming attack for disrupting original signal entirely or partially. A device which generate noise is so called jammer, which having the ability to interfere with the frequency of sensor in WSN. This activity is capable only if the SNR (signal-to-noise) is minimum than one. Depending on the power of transmission, the jammer can disturb the whole WSN or some area of network. A jamming attack may disrupt the network easily, if neglected in the initial design, despite of higher level security schemes. Jamming attacks classified as [13,14]:

Spot jamming it is the simplest technique. The attackers transmit all power verses the frequency signal. Usually, it is effective but this attack may be failed by changing the frequency.

Sweep jamming it's rapidly shift multiple frequencies to target a frequency in a quick succession. This activity is not continuous; the effect of sweep jamming is limited. Though, it could be forced many retransmission in WSN due to the loss of packets.

Barrage is jamming its target multiple frequencies at a time. The range of attacked increase and the output power decreased proportionally.

Deceptive jamming it's involved in replaying or fabricating valid signals incessantly on the channel. It is try to destroy the service of the network using the available bandwidth. This type of jamming can be applied to set of frequency or single frequency.

The radios having single-frequency are used by the first generation wireless sensors; therefor nodes were unsafe to the narrow band noise, either malicious or unintentional. For the reduction of noise vulnerability direct sequence spread spectrum (DSSS) is used by recent motes. Generally, particular countermeasures might be used against different jamming attacks. Power transmission regulation, antenna polarization, DSSS, directional transmission, ultra wide band technologies (UWB), frequency hopping spread spectrum (FHSS) and hybrid DSSS/FHSS are few examples [15,16]. Present security schemes which addresses attacks of jamming in WSN can be categorized as follow:

The aim of detection technologies is to detect jamming attacks instantly. It is observed by packet delivery ratio or carrier sensing time, signal strength to detect jammer presence individually. The detection is improved by presenting the concept of consistent checking, to classify the radio link whether its utility is poor, ratio of packet delivery is used, and then consistent checking is achieve to determine whether link quality is effected by the jamming attack [17].

Proactive countermeasures made the WSN immune against the jamming attacks instead of respond reactively to such attacks. DEEJAM is an example; this protocol had been presented for the defense using IEEE 802.15.4 against the secret jammers [18]. To contrast enemies which use the same hardware with same properties as the deployed sensor nodes, it uses the four defensive strategies altogether:

Frame masking this strategy is used for the defense only when the jammers steal the preamble bits and start Frame (SFD) Delimiter Sequence.

Channel hopping defend against jammers that try to capture activity of radio by radio signal strength indicator (RSSI) which is periodically sampled.

Packet fragmentation breaks every packet into small fragments which are separately transmitted with different SFDs on different channels. If transmission frequency rapidly changes, attacker cannot jam the right frequency at a time.

Redundant encoding handles jammer that blindly attacks a single channel by short pulses. It allows the recovery of packet even if a single fragment is corrupted, in this case bandwidth and energy usage are increased.

Reactive countermeasures empower reaction at the time of jamming attack. JAM algorithm is the perfect example [19], which increases the efficiency of the network by enabling the mapping and detection of jammed areas. In activity, sensor near the boundary of jammed area notify neighbors, these neighbors nodes start mapping the area that is presently jammed by exchanging of mapped messages. When the jammer stops attack or simply moves, the jammed nodes notify neighbor that it is recovered.

Mobile agent based techniques dominance Mobile Agents (Mas) that is autonomous process that could be moved from host-to-host and behaves on the behalf of users in the direction of completed assign task. JAD protocol is an example [20].

The jamming can analyze by three ways: techniques of detection, the localization technique, and the defensive algorithms. When the detection techniques are enhanced it increases the lifetime of the sensor node. Correct enemy position is specifying by the enhancement of localization techniques. The two recent algorithms FM-AM and ICMT proposed for the defense of jamming and considered the better countermeasure for jamming. The FM-AM is the hybrid algorithm while the ICMT is the advanced version of O-QPSK [14].

In radio interface attacks a steady or irregularly interference are produced by the attacker. The symmetry key algorithm is the solution of the attacks.

Attacks and solutions on data link layer

Several attacks in WSN can be attached with data link layer. All these attacks having two major objectives: (I) exhausting the power resources of nodes, in WSN most of the energy is consumed due to the communication and (II) degrading service timeliness.

Collision attacks are very similar to the jamming attacks in the physical layer. Attacker hacked/identify the WSN frequency by using his own frequency, and then attacker transmits a small signal as one byte to corrupt the entire message. The only proof of this attack is the false message reception which is detected by Cyclic Redundancy Code checking (CRC) on the data link layer. In this case, false message is automatically discard by this layer, which causes bandwidth and energy wastage. Forward Error Correcting (FEC) code is the possible solution for this attack which can recover lost data [21].

The selection of optimum channel resource allocation algorithm, the attractive sensing protocol for the monitoring of channel, and increase the amount of channels are an alternative solution for this type of problem. All these factors are integrated in SN protocol, which also consider the software and hardware design of sensor node [22].

The attackers direct/control and measure the efficiency of protocol and forced the sensor to spend extra energy as result

exhaustion occurs. The better solution for this type of attack is to reject extra network requests. A reliable protocol More the Safe, Less the Unsafe (MSLU), which is used to detect unauthenticated packets. If the probability report at the base station of the packet is high then the packet considered as authentic otherwise it is injected. The MSLU is one of the recent protocols which is the best solution for exhaustion [23,24].

Unfairness attacks, the enemy transmit excessive number of packets when medium is ideal, to prevent the sensor nodes from transmitting packets. So as a result, real-time applications are possibly fail and service quality should be degraded. Though, this attack is normally considered very weak type of DoS, because by using small packets this attack can be limited, in such case that channel is only seized for limited time.

In WSNs, sleep mode is used by sensor nodes to maintain energy/power and increase the lifetime. Attacks against this activity of nodes are called denial-of-sleep or sleep deprivation torture studied in. There are three methods to reduce the effect of sleep deprivation. The first and significant method is strong authentication of data-link-layer to defend denial-of-sleep attacks. The TinyOS and TinySEC are the existing authentication algorithms for the implementation, based on IEEE 802.15.4. The second option is protection of anti-reply, CARP protocol is one of the famous algorithm [25]. The last is broadcasting attack protection which allows capturing denial-of-sleep attack. The Zero Knowledge Protocol (ZKP) is the latest protocol for the solution of denial-of-sleep attacks, in this protocol the authentication of the node to send the synchronization message [23].

Attacks and solution on network layer

At this layer, number of attacks may be disrupting the availability of network. We will explain them with their corresponding countermeasures. However, the security at routing layer mostly depends upon authentication. Due to the limited resources, authentication in WSN could not depend on public-key cryptography. Based on hash functions and symmetric keys. Subramanian and Zhang [26] proposed a message authentication technique which achieves the goals of immediate authentication, non-repudiation, and scalability.

Against the network layer direct attack can try to alter, spoof, or false reply to routing information. The enemy may change data flow toward him by destroying original information. An effective solution against the spoof and altering data is message authentication code (MAC). Timestamps or counters could be used to defend reply attacks [27]. Generally, the authors proposed is [28] two different algorithms that alleviate the effects of misbehavior routing, the path rater and watchdog. Watchdog identify nodes which having misbehavior attitude and path rater avoid effected nodes from routing.

Hello message is used for the discovery of the neighbor nodes and create automatically a network. Many protocols are used for Hello flooding. However, the enemy having higher transmitter power transmits multiple hello packets which can damage/corrupt node and make the other nodes believe that the damage sensor is in their neighborhood. Though, data message routed to the dead node will be even sent into nonexistence [29], causing both energy wasting and data loss. Simply, the solution to this attack is checking acknowledgment of every transmission link. A signal strength method is proposed in [30] to prevent and detect these attacks.

Sink/Black hole attacks works by initiating the sensor nodes to route traffic along a number of negotiated sensors that can then access or drop all the routed messages. This type of attack can be discovered by monitoring transmission and to listening by neighbors and the best solution for these attacks are probably advanced algorithms such as REWARD [31]. This attack can be dangerous when the attackers know the exact position of the sink node; attackers detect and attack on sink node which is called sink whole attack. The Mint Route protocol is used in WSN against these attacks [32].

The powerful and fast connection between two distant compromised nodes in Wormhole attack established to ruin routing information. The enemy can handle data between the two nodes locations, and convince the other nodes to know that this path is the quickest to the whole network. A packet leashes protocol is best solution for countering and detecting Wormhole attacks [33].

When an effected sensor does not follow the network routing protocol, but behave like filter, dropping certain messages and forwarding other, then the WSN faced the problem of selective forwarding attack [34]. The special case of selective forwarding attack is black hole attack where all the routed packets are loss/dropped. The best solution for the tackling/detecting selective forwarding attacks is multipath routing using redundant methods, these algorithms increase the probability by sending same data packets along multipath to reach the destination [35].

Sybil attacks occur when the malicious node attempting multipath identities. Sybil attacks are first introduced in peer-to-peer network but Wanger and Karlof introduced that Sybil attacks can be present in WSN as a threat. Distributed, routing storage algorithm, and fault tolerant algorithms can be affected by Sybil attacks [36]. The major countermeasures for Sybil attacks are (i) testing radio resources, that willing, all the nodes transmit signal in different channel at the same time, (ii) key validation for pre-distribution of key randomly, (iii) verification of nodes position.

Attacks and solution on transport layer

Transport layer protocols are classified into two types of algorithms; algorithms provide reliability and protocols that provide congestion control. Reliability is more relevant, which guarantee that the lost packets are detected and retransmitted until reach to their destination. The two major types of attacks in transport layer are desynchronization and flooding [37].

Desynchronization attack, the enemy transmit duplicate messages containing false sequence number or flags to interrupt the existing connection between two end-sensors. These attacks prevent end nodes transmission and drain the energy of the sensor by constantly sending retransmission requests. The effective and typical solution to this attack is the authentication.

Flooding attacks drain the resources memory of the sensor nodes, by unicasting multiple connection establishment messages to the victim. The client puzzles algorithm is suitable solution for flooding in WSN [38].

Attacks and solution for privacy and confidentiality in WSN

As the WSN become common, the more privacy and confidentiality represent two major concerns.

Table 1: The Summary of Attacks and Solution in WSN

WSN Layers	Attackers Target	Class of Attacks	Solution/Defense	References
Physical Layer	Integrity, secrecy, privacy, and availability	Tampering, jamming, Eavesdropping	Tampering detection software, tamper-proofing, sensor node monitoring, hash function, detection strategies, reactive, mobile-agent-based, defensive protocols, spread spectrum, priority message, duty cycle, region mapping, cryptographic techniques.	[10] [11] [12] [45] [46]
Data Link Layer	Integrity and availability	Sleep deprivation, exhaustion, collision, unfairness, information about routing, black hole, hello flooding, sinkhole, wormhole	Authentication of link-layer, auto-reply, protection of broadcast attacks, nodes authentication, limitation of rate, packet authentication, codes for forward error correction, attractive sensing protocols, monitor transmission, multiple channels, data aggregation, codes for error correction, MAC, authentication, REWARD, Path rater, watchdog, bidirectional checking, signal strength, secure routing and redundancy.	[11] [21] [22] [23] [24] [26] [35] [36]
Transport Layer	Integrity and availability	Selective forwarding, Sybil, Desynchronization, and flooding.	Redundancy, probing, IDs, authentication, multihop acknowledgment, multipath routing, radio source testing, validation of key for predistribution, position verification, cryptography, and puzzles.	[11] [35] [36] [38]
Network Layer	Integrity, secrecy and privacy	Analysis of traffic and injection, alteration and duplication of packets	Randomization of communication, authentication of data	[40] [41] [42] [43]

For example (**Table1**), in applications like military confidentiality is necessary and the privacy is essential for sensing data and give the priority over confidentiality. In much application, like commercial and health monitoring applications confidentiality and privacy both are essential. Eavesdropping and traffic analysis are two major classes of these attacks.

If end-to-end communication is not secure, and anyone access/trapped the communication data by eavesdropping on the radio frequency band of the network. This type of enemy is considered as passive attacker which can steal sensitive and private information. The general method to handle this attack is cryptography [39]. The symmetric-key cryptography is preferable than public-key cryptography in WSN due to limited power of computational. The SPIN algorithm is best countermeasure for eavesdropping [27].

Encryption of single node data is not sufficient to guarantee secrecy/privacy in wide sense. An enemy can analyze data traffic overhead to get important/essential information about the topology of the network and the sensed data. Just influence analysis of traffic, the enemy identify nodes with major roles, or run designed of targeted attacks to maximize harm. The countermeasure is proposed by Deng et al versus traffic analysis attack for the security of base station [40]. Wadaa et al also proposed a protocol for the randomization of communication during set-up phase of network, for the protection of WSN infrastructure [41].

Attacks and solution for integrity of data in WSN

When the attackers corrupt record/data the data integrity is violated, and sink node is unable to recover the original sensor nodes sensed data. The data erasure is the simplest attack which compromise the sensed data, that is, erases any specific information before reaching the sink node. In general there are three classes of attacks against the integrity in WSN, alteration, packet- injection, and node replication.

To modify gathered data by the network, the enemy having three main classifications: false data is injected completely, packets are replicated which are previously captured, or alter the intercepted messages. The insider attacker can easily run these attacks and difficult for outsider because the outsider must have to break the authentication of the WSN. Generally, symmetric cryptographic protocols are applicable in WSN instead of Asymmetric protocols. Generally TESLA, µTESLA, and BECAN like protocols are best countermeasure against these attacks [42], [43].

In Node replication attacker captures a sensor node without being detected, he can easily use that node to inject fake data and authentication. Even if nodes used in WSNs are not normally tamper-proof, the limited number of nodes are used by the adversary for control in many application. The centralized solution for this attack is that nodes periodically transmit a list of their neighbor nodes, including location and IDs of nodes [42]. Another protocol having emergent properties is proposed for

this attack aiming to limit the communication which causes the minimum power consumption [44].

Summary

In this article we discussed the major security attacks and their corresponding solutions in WSNs, classified these threats with respect to their relative target. Depending on the different service provided, defensive mechanisms need to protect the security of WSNs like, (I) availability of network and service integrity, (II) privacy and confidentiality of data and (III) integrity of data. Dealing with service and network reliability, we additionally differentiate the attacks based on the different layers, which intelligently modify the nature of threats and their corresponding solution/defense. Security techniques must be implemented on each layer of WSN.

Research Issues

Research challenges may depend on the application of WSN. However, In WSN few issues should need further/extended research that saturates the WSN. These researches comprise to make privacy and security well-suited with scalability, fighting against DoS attacks, enhancing the efficiency of bandwidth, dealing with the mobility of nodes and also make the WSN worldwide standardization.

Conclusion

WSN are introduced for some specific applications. These applications are not too much limited, including target tracking in military, surveillance of different systems, monitoring of environments, and monitoring different industrial machines. As the WSN is wireless and self-organized and self-healed therefore having different features. The major two features are the asset and weakness of WSN. The encouraging factors, which WSN is very flexible, easy to deploy and comparatively very cheap, which describe their popularity and great momentum both for military and civil applications. The negative factors including that WSN are very susceptible to the attacks against integrity of service, availability, privacy and Security. Certainly, depending on radio communication which enables the eavesdropping, DoS attacks and interception, while a self-organized and self-healing topology without integrated control disposed to the attacks against the authentication, such as replication, suppression, and impersonation of the nodes etc.

Elsewhere the above common advantages and disadvantages, there is excessive multiplicity in WSN. In spitefulness of the above multiplicity, aggregation and encryption of data seem very useful existent with symmetric key cryptography to moderate the vulnerability and scalability in WSN.

References

1. Chan H, Perrig A (2003) Security and privacy in sensor networks. Computer 36:10.
2. Elson J, Estrin D (2004) Sensor networks: a bridge to the physical world Wireless sensor networks. Lect Notes Comput Sc 3:20.
3. Vadlamani S, Medal H, Eksioglu B (2014) Security in Wireless Networks. A Tutorial. NATO Science for Peace and Security Series —D: Information and Communication Security, Vol. 37, IOS Press, pp. 272–288.
4. Arms SW, Townsend CP, Churchill DL, Galbreath JH, Mundell SW (2005) Power management for energy harvesting wireless sensors. Smart Structures and Materials. International Society for Optics and Photonics.
5. Steed A Richard M (2008) Using tracked mobile sensors to make maps of environmental effects. Pers Ubiquit Comput 12: 331-342.
6. Sakarindr, Pitipatana, and Nirwan Ansari. Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks. IEEE Wirel Commun 14: 5.
7. Abuzneid AS, Sobh T, Faezipour M (2015) An enhanced communication protocol for location privacy in WSN. Int J Distributed Sensor Networks 11:4.
8. Cheikhrouhoua O, Koubâa A, Dini G, Alzaid H Abid M (2012) LNT: A logical neighbor tree secure group communication scheme for wireless sensor networks. Ad Hoc Networks 10: 7
9. Pietro RD, Guarinoa S, Verde NV, Ferrer JD (2014) Security in wireless Ad-Hoc networks–a survey. Comput Commun 51: 15.
10. Sert SA, Onur E, Yazici A (2015) Security attacks and countermeasures in Surveillance Wireless Sensor Networks. 2015 9th International Conference on Application of Information and Communication Technologies (AICT), Russia.
11. Sen J (2012) Security in wireless sensor networks. Wireless Sensor Networks: Current Status and Future Trends.
12. Mensah HN, Henry, Boateng KO, Gadze JD (2015) Comparative analysis of energy usage of hash functions in secured Wireless Sensor Networks. Int J Comput Appl T 109:11
13. Mpitziopoulos A, Gavalas D, Konstantopoulos C, Pantziou G (2009) A survey on jamming attacks and countermeasures in WSNs. IEEE Commun Surveys Tutorials Vol 11: 4.
14. Kishk AM, Messiha MW , Fishawy NA, Alkafs AA, Madian AH (2015) Proposed Jamming Removal Technique for Wireless Sensor Network. Int J Scientific Res Net Security Commun 3: 2.
15. Oppermann, Stoica L, Rabbachin A, Shelby Z, Haapola J (2004) UWB wireless sensor networks: UWEN-a practical example. IEEE Commun Mag 42: 12.
16. Balanis CA (2016) Antenna theory: analysis and design. 4th Edition, John Wiley & Sons,
17. Xu W, Trappe W, Zhang Y, Wood T, WINLAB (2005) The feasibility of launching and detecting jamming attacks in wireless networks. Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, USA.
18. Wood AD, Stankovic JA, Zhou G (2007) DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks. 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, USA.
19. Dener M (2014) Security analysis in wireless sensor networks. Int J Distrib Sens N 10: 10
20. Mpitziopoulos A, Gavalas D, Konstantopoulos C, Pantziou G (2009) JAID: An algorithm for data fusion and jamming avoidance on distributed sensor networks. Pervasive Mob Comput 5: 2.
21. Mišic VB, Fung J, Mišic J (2005) MAC Layer Attacks in 802.15. 4 Sensor Networks. Security in Sensor Networks. IEEE International

Conference on Mobile Adhoc and Sensor Systems Conference, USA.

22. Ma, Naji (2005) Design of Multi-Channel Wireless Sensor Networks Based On Compressive Sensing Theory and Spectrum Sensing Theory. Int J Smart Home 9: 9
23. Arif S (2016) Security Issues in Mobile Wireless Networks. Network Security Attacks and Countermeasures : 49.
24. Kamarei M, Barati AHN, Patooghy A, Fazeli M (2015) The More the Safe, the Less the Unsafe: An efficient method to unauthenticated packets detection in WSNs. 2015 7th Conference on Information and Knowledge Technology (IKT), Iran.
25. Zhang, Wensheng, Nalin Subramanian, and Guiling Wang (2008) Lightweight and compromise-resilient message authentication in sensor networks, IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, USA.
26. Prrig A, Szewczyk R, Tygar JD, Wen V, Culler DE (2002) SPINS: security protocols for sensor networks. Wirel Netw 8: 521-534
27. Zin SM, Anuar NB, Kiah MLM, Ahmedy I (2015) Survey of secure multipath routing protocols for WSNs. J Netw Comput Appl 55: 123-153.
28. Karlof C, Wagner D (2003) Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks 1: 293-315.
29. Singh VP, Jain S, Singhai J (2010) Hello flood attack and its countermeasures in wireless sensor networks. IJCSI Int J Comp Sci 7: 23-24.
30. Karakehayov Z (2005) Using REWARD to detect team black-hole attacks in wireless sensor networks. Workshop on Real-World Wireless Sensor Networks REALWSN.
31. Krontiris L, Dimitriou T, Giannetsos T, Mpasoukos M (2007) Intrusion detection of sinkhole attacks in wireless sensor networks. International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Net Distrib Robotics 150-161.
32. Hu YC, Perrig A, Johnson DB (2003) Packet leashes: a defense against wormhole attacks in wireless networks. INFOCOM 2003. IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428), USA.
33. Alrajeh NA, Khan S, Shams B (2013) Intrusion detection systems in wireless sensor networks: a review. Int J Distributed Sens Net 9: 5
34. Garg N, Garg S (2015) A Characteristics Study of Routing Protocols in Wireless Sensor Network. Int J Curr Eng Technol 5: 2165-2168.
35. Yadav S, Yadav RS (2016) A review on energy efficient protocols in wireless sensor networks. Wirel Netw 22: 335-350.
36. Mansouri D, Mokddad L, Othman JB, Ioualalen M (2015) Preventing Denial of Service attacks in Wireless Sensor Networks. 2015 IEEE International Conference on Communications, UK.
37. Mulla MRI, Patil R (2016) Review of Attacks on Wireless Sensor Network and their Classification and Security. Imperial J Interdisciplinary Res 2: 7.
38. Dai HN, Wang Q, li D (2013) On eavesdropping attacks in wireless sensor networks with directional antennas. Int J Distrib Sens N 9: 8.
39. Wadaa A, Olariu S, Wilson L, Eltoweissy M, Jones K (2004) On providing anonymity in wireless sensor networks. Proceedings. Tenth International Conference on Parallel and Distributed Systems, 2004. ICPADS 2004, USA.
40. Eschenauer L, Gligor VD (2002) A key-management scheme for distributed sensor networks, Proceedings of the 9th ACM conference on Computer and communications security, USA.
41. Lu R, Lin X, Zhu H, Liang X, Shen X (2011) BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. IEEE T Parall Distr 23: 32-43.
42. Pathan ASK (2010) Security of self-organizing networks: MANET, WSN, WMN, VANET (1st edn) Auerbach Publications, USA.
43. Badawya A, Elfouly T, Khattab T, Mohamed A, Guizanib M (2016) Unleashing the secure potential of the wireless physical layer: Secret key generation methods. Phys Commun-Amst 19: 1-10.
44. Rezvani M, Ignjatovic A, Bertino E, Jha S (2014) Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks. IEEE T Depend Secure 12: 98-110.
45. Yong W, Attebury G, Ramamurthy B (2006) A survey of security issues in wireless sensor networks. IEEE Commun Ser Tutorials, 8: 2-23.
46. Gardašević G, Veletić M, Maletić N, Vasiljević D, Radusinović I, et al. (2017) The IoT Architectural Framework, Design Issues and Application Domains, Wireless Pers Commun 92: 127-148.