A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective

M. A. Burhanuddin[1], Ali Abdul-Jabbar Mohammed[1], Ronizam Ismail[2], Mustafa Emad Hameed[3], Ali Noori Kareem[4] and Halizah Basiron[1]
[1]*Faculty of Information and Communications Technology, UTeM, Melaka, Malaysia.*
[2]*Kolej Universiti Islam Melaka, Kuala Sg Baru, Melaka, Malysia*
[3]*Faculty of Electronics and Computer Engineering, UTeM, Melaka, Malaysia.*
[4]*Department of Computer Engineering Techniques, AlYarmouk University College, Diyala, Iraq.*
burhanuddin@utem.edu.my

***Abstract*— The Internet of Things is becoming a very promising paradigm with the extensive market adoption of the development of associated technologies, such as; cloud computing, near-field communications, wireless mobile networks, etc. This will expose the future direction of communication around the world. Wireless Sensor Networks together with the existing communication technologies are enabling the continuous integration of controlling and processing the functionality of the Internet of Things applications. Since Wireless Sensor Networks are typically deployed for gathering sensitive information from unattended or hostile environments, they are exposed for security attacks, which are strongly affecting the user privacy and the network performance. There are various security mechanisms and solutions for Wireless Sensor Networks that have been proposed in the previous works. Therefore, it is mandatory to give attention for its applicability and feasibility features in terms of related security challenges based on the Internet of Things perspectives. The purpose of this paper is to explore and show the influence of Wireless Sensor Networks security challenges within the perspective of the Internet of Things and its applications. Consequently, an exploration of the major and minor security requirements in the Wireless Sensor Networks has been made in this paper, accompanied by a classification of the available attacks and threats against these requirements. Finally, a discussion on the Internet of Things security issues and challenges in Wireless Sensor Networks is provided.**

***Index Terms*— Internet Of Things; Security Attacks And Threats; Security Challenges; Security Requirements; Wireless Sensor Networks.**

I. INTRODUCTION

The Internet of Things (IoT) paradigm has the attractive to be the most emerging and promising area of technological advance in the future, that it will change our insights of communication. There are several technologies that lay the foundation of this modern prototype, such as Wireless Sensor Networks (WSNs), cloud services, Middleware, Radio Frequency Identification (RFID), etc. [1]. Accordingly, these technologies become a vital factor in many IoT application domains including Smart Cities, automotive, Connected Industry, environmental and healthcare monitoring, Nano-scale applications, and many other fields [2]. The WSN's can obtain the near-field communications amongst numerous low-power and multi-functioning objects or nodes, which are structured based on ad-hoc manners. Since the deployment cost is a vital aspect of IoT applications, WSN's are usually composed of low-cost sensor devices that have restricted communication and computation resource capabilities with strict resource constraints [3]. Moreover, the task of WSN's protocols is to configure the network and collect the data and information packets from several sensor nodes of certain environment. Altogether, the security challenges with adopting IoT technologies must be strictly considered to avoid transforming this promising technology into prevalent surveillance issue [4].

The most key issue of utilizing the WSN's into IoT applications is that addressing the heterogeneity of security and privacy concerns in its requirements and properties. This is due to the diversity range of the methods and protocols in WSN's and the traditional telecommunication networks, which are more critical for this type of applications. Thus, proper evaluation mechanisms are required. As most WSN's deployments in IoT are utilized for gathering sensitive data and information from unattended or hostile environments [5]. Therefore, it is required a certain level of protection regarding unauthorized access to these sensitive data and information, because it is not possible to sacrifice the security and privacy of user data. The common WSNs uses are depended on routing and radio transmission nature of these networks which make it exposed to a variety security attacks. With the restricted computational capabilities of sensor nodes, there are many difficulties to utilize public-key cryptography to enhance WSN's security [6]. Consequently, the commonness of proposed solutions to secure routing and data gathering protocols are basically adopting symmetric-key cryptography, which is poses additional security challenges.

With the purpose of understanding the relationship of security issues and challenges in WSN's with the perspective of IoT and its applications, it is compulsory to study the influence of IoT vision in the different security requirements that should be investigated in the WSN's as described in (Section 2). Furthermore, it is important to identify and describe the possible Attacks and Threats on the major security requirements and its influences on the WSN's values as categorized in (Section 3). Then, providing an extensive discussion of securing the major WSN's requirements by covering the main security issues and challenges in this area which is in (Section 4). Compared to the specific security problems of the WSN's which is well researched in the previous works, the complete integration into IoT applications still has the challenges to solve many security investigation difficulties.

II. IOT SECURITY REQUIREMENTS IN WSN'S

Security is a significant aspect of IoT applications, due to the challenging task of protecting the sensitive information transmitted specially within WSN's, and this is because the unique properties of the hostile environments around WSN's [7]. Particularly, security is a mandatory aspect in a complex and dynamic systems just as the IoT services and applications [8]. The WSN's which comply under Ad-hoc manner are providing quite a lot of interesting advantages such as mobility and advanced scalability to large scale of deployments [9]. Thus, it can be truly considered as a future key of IoT deployments, such as industrial monitoring, environmental and healthcare monitoring. Nevertheless, there are several challenges should be solved which are more numerous (e.g. unreliability of communication, deployment and immense scale, and operation unattended) [10]. The security requirements of IoT can encompass together the traditional networks with requirements appropriate the unique constraints of WSN's. Therefore, the security requirements that should be investigated in the WSN's [14, 15, 16] can be classified to major and minor requirements [14] as follows:

A. The Major Requirements:

The major requirements are considered as the standard security requirements, which are as the following:

1. Data Confidentiality: the ability of ensuring that the secrecy of transmitting sensitive sensed data is never revealed to eavesdroppers e.g., passive attackers, so that this data remain confidential. The collected and transmitted sensing data should not be exposed to unauthorized parties. This is by using data encryption with a secret key in the data gathering process, which is only understood by the desired recipients and receivers [11].
2. Source Authentication: the ability of ensuring the reliability of the collected and transmitted sensing data through the WSN's by verifying its source and data origin. Therefore, the communication turns out to be genuine since the malicious node cannot pretense in place of a trusted node. Consequently, Source Authentication is very important for decisions making and exchanging the control information of the WSN's [12].
3. Data Integrity: ensuring and confirming that the collected and transmitted data within the WSN's have never been tampered, altered, or corrupted by adversaries, malicious intermediate nodes, or even by accident due to the harsh communication environment of WSN's.
4. Availability: it ensures that the desired WSN's is available for the communication services and each node can use the network resources even with the attendance of denial-of-service attacks. Since the WSN's is collecting and transmitting the sensing data in charge of the communication services duty, the availability of WSN's is very essential for the survivability of IoT services and applications.

B. The Minor Requirements:

1. Data Freshness: The insurance of freshness in each transmitted message protects the data communication structures against replayed attacks. This is by ensuring that the old messages will not be replayed again, so the transmitted data will be recent [14], and it can be achieved by adding a time-related counter into the transmission packet.
2. Self-Organization: According to the organization nature of WSN's, it doesn't have a fixed infrastructure which make each sensor node independent and flexible to be self-organized for different situations.
3. Time Synchronization: It is required in the most WSN's applications, for example; to achieve power efficient mechanism, the sensors radio could be turned off periodically.
4. Secure Localization: WSN's efficiency is often rely on its capability of accurately and automatically locating all the network sensors. Nevertheless, attackers have the ability of reporting false signal strengths or replaying signals to unsecured location data.

III. ANALYSIS OF POSSIBLE ATTACK AND THREATS

The network attack is an effort of gaining unauthorized access for getting sensitive information or compromising the confidentiality, authentication, integrity, or availability of the network. Accordingly, the WSN's can be exposed to numerous types of attacks, which are in this paper mainly classified to three categories in proportion to the major security requirements in [14, 15] as showed in the Table 1.

Table 1
Analysis of possible attacks and threats

Security Requirements	Possible Attacks		Description
Confidentiality and Authentication	Node replication attack		Replicate or copy a legitimate node identifier and add node copies into the existing WSN [15], this will lead to the ability of communicating the entire network from the replicated node [16].
	Attacks on privacy	Eavesdropping and passive monitoring attack	When the WSNs communications have not been protected with an effective cryptographic mechanism, the adversary can listen to the communication data and easily realize its contents [17].
		Traffic analysis attack	The attacker can detect some nodes with special roles or activities which may provide important information about WSNs communications [17].
		Camouflage attack	Adding malicious intermediate nodes to the WSNs by the attacker [11]. Later, these nodes can be used to masquerade as a regular node for advertising false routing information and attracting the communication packets into further forwarding in the intended WSNs.
Service Integrity	stealthy attacks		Adversaries can use stealthy attacks against the WSN's service integrity. The adversaries goal by using stealthy attacks is to force the WSN's for accepting false data values.

Availability	Denial of Service (DoS) attacks	Physical Layer	Jamming attack	Interfere with the authorized radio frequencies of the WSN's nodes [15, 18].
			Tampering attack	Physically accessing the WSN's nodes and extracting its data such as the cryptographic keys and other sensitive information [18].
		The data Link Layer	Collisions attack	The collision arises when the transmission of different nodes is running concurrently with the same frequency range.
			Exhaustion attack	Repeat collisions attack to consume all energy resources of the WSN's nodes until these nodes become dead to perform the resource exhaustion. [19]
			Unfairness attack	Perform unfairness through irregularly using the mentioned link layer attacks against the WSN's.
		Network and Routing Layer	Spoofed, Altered, or Replayed Routing Information attack	Disrupt the WSN's traffic by spoofing, altering, or replaying the routing information whilst exchanged among the sensor nodes.
			Selective Forwarding attack	Use the selective forwarding attack by creating malicious nodes or compromising the network nodes. The attack can be adopted by using these nodes to selectively forward specific packets and drop others. [19]
			Black Hole Attack	A specific form of the selective forwarding attack wherein the malicious or compromised nodes drop all the packets that received.
			Sinkhole attack	Prepare a compromised node to be looks more attractive to its neighboring nodes by providing false routing information.
			Sybil attack	One node submits several identities to the WSN's. Essentially, this attack is easily affecting algorithms and protocols such as distributed storage, and fault-tolerant schemes.
			Wormholes attack	A link among two portions of the WSN's which is characterized by the low latency and provides the ability for attacker to replay the network messages. [19]
			Hello flood attacks	The adversaries may use the Hello Flood attacks via high-powered transmitter node for deceiving many nodes to believe that they are neighbors and within its range.
			Acknowledgment spoofing attack	Spoof the overheard acknowledgment messages between the attacking node and its neighbors to spread false information such as wrong node status among the WSNs.
		Transport Layer	Flooding attack	Frequently creating new connection requests or otherwise ignoring the legitimate requests while either connection resources are become exhausted or run to the maximum limit. [19]
			Desynchronization attack	This is may be achieved as example by frequently spoofing messages in the direction to end host until it requests to retransmit the missed frames.

IV. Discussion on IOT Security Issues and Challenges in WSN's

The IoT architecture is complex in nature and assumed to deal with billions of sensors and objects, which are interacting with each other and with other entities, such as human beings or virtual entities [8]. It is essential to secure and protect all these interactions with preservation of the highest system performance and limiting total incidents which are affecting the entire IoT. There are multiple attack vectors available to adversaries because of the key features of IoT, such as; global connectivity and accessibility (anyone can access in anyhow and anytime) [20]. Various heterogeneous objects that are presented in different contexts and communicating each other fulfil the complexity of the IoT and then further complicate the deployment of security mechanisms. However, the security services and solutions becomes a significant challenge and still in its initial stages. The current research of WSN's security mainly provides solutions for subjective problems without considering the impact of IoT principles and features as the studied in this paper.

A. Confidentiality Challenges

In IoT security, the most challenging task is to keep communication data and information confidential. There are several standard encryption functions which can be used to achieve data secrecy among the communicating parties, such as shared secret key and common encryption algorithms, e.g., the AES block cipher, Blowfish, and Triple DES [21]. However, adopting the data encryption alone as a security mechanism is not enough for protecting the data and information privacy. The attacker can execute a traffic analysis towards the eavesdropped cipher data, so a sensitive information about this data can be released easily. Moreover, node compromise is complicating the confidentiality challenges when a malicious node is compromised as one endpoint of the communication so a sensitive data and information is possible to be released. Furthermore, when utilizing a group shared key, the malicious node can successfully compromise the radio frequency range of other sensor nodes and then eavesdrop and decrypt the sensitive data and information within the communication.

B. Source Authentication Challenges

The adversaries in the ordinary sensor networks do not just make alteration to the communication packets; as well, their attacks can be including additional injected false packets [14]. Since WSN's is used in a shared wireless communication medium and applied in unattended environments, it is quite challenging task to ensure data authentication. Source authentication can be attained by symmetric and asymmetric mechanisms, where the sending and receiving nodes share secret keys to verify the resource identity [13], which is necessary to empower sensor nodes to distinguish between maliciously injected and spoofed packets or the original packets from the legitimate source. Practically, the data authentication is required in the most of applications, as

example of the military and safety-critical applications, the adversaries have obvious motivations to attack the sensor nodes by maliciously injected data reports or false routing information. Correspondingly, the civilian applications which is expected as comparatively non-adversarial environment, it is still exposed to risk without data authentication. Even if data authentication avoids the WSN's from maliciously injecting or spoofing packets by attackers, it is not solving the node compromise problem since the compromised node can authenticate itself into the network by getting the secret keys from the legitimate nodes. Nevertheless, intrusion detection techniques can be used to discover the compromised nodes around the network and rescind their cryptographic secret keys.

C. Data Integrity Challenges

Once the WSN's has a valid confidentiality measures, the adversaries are perhaps unable to thieve the communication data. However, there is possibility of WSN's to be compromised by alterations. This is when a false data injected by a malicious node presented in the network or even when a damage or loss of data caused by unsteady conditions of the wireless channel [14]. For instance, some malicious nodes may inject a false data or change the data inside the communication packets. At that time, these modified packets will be sent to the receiver (e.g., the base station of the WSN's). Nevertheless, the loss or damage of the sensed data may happen without the frivolity of a malicious node for the reason of the harsh communication environment. Accordingly, the data integrity is very important to ensure that any transmitted data within the WSN's has not been transformed or destroyed in transit.

D. Availability Challenges

The WSN's can be attacked with jam communications through an extravagant communications or computations, that may attack the sensor nodes or any part of the WSN's and as a result affecting the survivability of network. Nevertheless, the failure of the base station availability ought to ultimately threaten the whole operation of WSN's. Practically, as example of the monitoring application in manufacturing process, the impact of losing availability can cause a disappointment to sense the potential accidents and subsequently the financial loss. The availability of WSN's can be achieved through the modicum presence of the benign node failures or compromised nodes [13]. The adjustment of standard encryption algorithms to appropriate WSN's security requirements leads to extra costs. There are many approaches proposed in the literature, some of them adopt code modifying and reused as much possible codes. Other approaches used additional communications for attaining same goal. Also, more approaches impose strict limitations to data access, or even suggested inadequate schemes (e.g., central point scheme) just to shorten the algorithm. Therefore, the availability requirement is principal for preserving the operational services of WSN's and likewise in maintaining the whole network throughout its lifetime.

V. Conclusion

This paper has assembled the four fundamental security requirements of the WSN's and endeavored to give an illustration of each to give the field researchers a foundation stage of the WSN's opportunities in IoT applications. In general, there is still much work to be carried out in this field, particularly in figuring out how to consolidate the majority security challenges of the future IoT service into an omnipresent, all-powerful service went for conveying communication whenever, anyplace, for anyone, and for everything.

Acknowledgment

The authors would like to thank UTeM Zamalah scheme, Universiti Teknikal Malaysia Melaka (UTeM) for providing financial support and facilities in this study. Also, gratefully we would like to acknowledge and thank Kolej Universiti Islam Melaka (KUIM) to support this research.

References

[1] L. In and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, ScienceDirect, vol. 58, no. 4, pp. 431-440, 2015.

[2] G. Gordana, M. Veletić, N. Maletić, D. Vasiljević, I. Radusinović, S. Tomović and M. Radonjić, "The IoT Architectural Framework, Design Issues and Application Domains," Wireless Personal Communications, Springer Science and Business Media, pp. 1-22, 2016.

[3] K. Nacer, M. R. Abid, D. Benhaddou and M. Gerndt, "Wireless Sensors Networks for Internet of Things," Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), EEE Ninth International Conference on, pp. 1-6, 2014.

[4] I. Gudymenko, K. Borcea-Pfitzmann and K. Tietze, "Privacy implications of the Internet of Things," In Constructing Ambient Intelligence, Springer Berlin Heidelberg., vol. 277, pp. 280-286, 2012.

[5] A. Sahabul and D. Debashis, "Analysis of security threats in wireless sensor network," International Journal of Wireless & Mobile Networks, arXiv preprint arXiv, vol. 6, no. 2, pp. 35-46, 2014.

[6] M. Prabhudutta, P. Sangram, S. Nityananda and S. S. Satapathy, "SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY." 13 ().," Journal of Theoretical & Applied Information Technology, vol. 13 , pp. 14-27, 2010.

[7] C. Delphine, R. Andreas, M. Parag and S. Ralf, "Wireless sensor networks and the internet of things: selected challenges," Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze, pp. 31-34, 2009.

[8] R. Rodrigo, Z. Jianying and L. Javier, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, ScienceDirect, Elsevier B.V., vol. 57, no. 10, pp. 1-14, 2013.

[9] P. Tiwari, V. P. Saxena, R. G. Mishra and D. Bhavsar, "Wireless Sensor Networks: Introduction, Advantages, Applications and Research Challenges," HCTL Open International Journal of Technology Innovations and Research (IJTIR), vol. 14, pp. 1-11, April 2015.

[10] R. Singh, J. Singh and R. Singh, "SECURITY CHALLENGES IN WIRELESS SENSOR NETWORKS," IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), vol. 6, no. 3, 2016.

[11] S. Jaydip, "A Survey on Wireless Sensor Network Security," International Journal of Communication Networks and Information Security, vol. 1, no. 2, pp. 55-78, 2009.

[12] W. Yong, A. Garhan and R. Byrav, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 1-22, 2006.

[13] S. Elaine and P. Adrian, "Designing secure sensor networks," IEEE Wireless Communications, vol. 11, no. 6, pp. 38-43, 2004.

[14] D. Padmavathi and M. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," International Journal of Computer Science and Information Security, vol. 4, no. 2, pp. 1-9, 2009.

[15] a. Bryan, A. Perrig and V. GligorP, "Distributed detection of node replication attacks in sensor networks," IEEE Symposium on Security and Privacy (S&P'05), pp. 49-63, 2005.

[16] H. a. A. P. Chan, "Security and privacy in sensor networks," IEEE Computer Magazine, vol. 36, no. 10, pp. 103-105, 2003.

[17] J. P. Walters, L. Zhengqiang, S. Weisong and C. Vipin, "Wireless sensor network security: A survey," Security in distributed, grid, mobile, and pervasive computing, pp. 367-404, 2007.

[18] A. Mukherjee, A. F. S. Ali, H. Jing and S. A. Lee, "Principles of physical layer security in multiuser wireless networks: A survey,"

IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1550-1573, 2014.

[19] A. S. Sastry, S. Shazia and S. Vagdevi, "Security threats in wireless sensor networks in each layer," International Journal of Advanced Networking and Applications, vol. 4, no. 4, p. 1657, 2013.

[20] G. Han, S. S. C. Lei and H. Jiankun, "Security and privacy in Internet of things: methods, architectures, and solutions," Security and Communication Networks, vol. 9, no. 15, pp. 2641-2642, 2016.

[21] J. Thakur and K. Nagesh, "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis," International journal of emerging technology and advanced engineering, vol. 1, no. 2, pp. 6-12, 2011.