ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

CHALLENGES IN IOT AND SENSOR NETWORKS

VEMULAKONDA SRINIVASA RAO Assistant Professor Department of Information Technology
NRI Institute of Technology (Autonomous) AGIRIPALLI Krishna Dt. A.P
GADIREDDY RAJASEKHAR REDDY Assistant Professor Department of C.S.E
V.K.R, V.N.B & A.G.K College of Engineering GUDIVADA Krishna Dt. A.P

Abstract
The exponential growth in mobile traffic seen in the last couple of years, mainly due to the vast amount of wireless devices, such as smart phones and the Internet of Things (IoT), has resulted in the wireless network industry producing and collecting an unprecedented amount of data (Bi et al., 2015). According to the International Data Corporation, by 2025 the number of devices connected to the Internet will be around 42 billion, and a total of 80 zettabytes of data will be generated in the same year. There is no doubt that we are ushering in a new era, since IoT and Artificial Intelligence (AI) are deepening their integration in society and the roll-out of 5G technology will spur new innovations across all industries. The innovation in the IoT ecosystem is bridging the gap between the real and digital world; we are creating a hyper-connected society where devices are no longer used only to exchange data but are becoming more and more intelligent and context aware. The advancements in sensing, data processing, and cloud and communication technology has enabled the systems to interact with the environment and optimize processes via learning through interactions. This will lead to the creation of smart spaces and self-aware interconnected "things" for health, mobility, digital society, food, energy, and environmental applications (Qiu et al., 2018). In future, the IoT development process will most likely evolve from vertical to polymorphic applications, supporting both personal and industry users (Chen et al., 2014). To provide a pervasive, unified, and seamless experience to the end users, there are many challenges that need to be addressed, including: technology standards, interoperable module components supporting heterogeneous applications and requirements at several layers, the designing of low-cost IoT terminals with low-active power, and solutions guaranteeing end-to-end privacy and security (Chen et al., 2014).

Key Words: application, communication, internet of things, sensor, solutions, technology

Introduction

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.

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

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. 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. 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. 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.

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. Particularly, security is a mandatory aspect in a complex and dynamic systems just as the IoT services and applications. 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. 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). 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 can be classified to major and minor requirements 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.
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.
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.

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

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 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.

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. 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). 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. 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 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. 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, 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

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

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.

References

1. 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.
2. 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.
3. 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.
4. 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.
5. H.A.P.Chan, "Security and privacy in sensor networks," IEEE Computer Magazine, vol. 36, no. 10, pp. 103-105, 2003.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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
14. S.Elaine and P. Adrian, "Designing secure sensor networks," IEEE Wireless Communications, vol. 11, no. 6, pp. 38-43, 2004.
15. 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.