Opinion
Volume 11:4, 2022

International Journal of Sensor Networks and Data Communications

ISSN: 2090-4886 Open Access

Privacy and Trust Issues also in WSN Systems

Guangjie Han*

Department of Information & Communication Systems, Hohai University, Changzhou, P.R China

Introduction

Wireless Sensor Networks (WSNs) are now a focus of research and are proving to be a very useful technology for a wide range of applications, including those related to the environment, the military, health, the home, and the workplace. Mobile Wireless Sensor Networks (MWSN) and static wireless sensor networks are two different types of WSN (SWSN). The MWSN is a specialised wireless network made up of a sizable number of mobile sensors, but the instability of its topology causes a number of performance problems when data is routed via it. Due to some limitations imposed by the sensor nodes, SWSNs made up of static nodes and static topology also face some of the same security issues as MWSNs. The main difficulties that WSNs face, particularly while routing, are security, privacy, resource and computation limitations, and dependability issues. These issues are addressed by WSN routing protocols [1].

Description

WSN routing systems must guarantee network confidentiality, integrity, privacy preservation, and dependability in order to address these issues. As a result, effective and energy-conscious countermeasures must be created to stop network intrusion. We discuss various WSN configurations, issues, fixes, and a point-to-point multi-hop-based secure solution for efficient routing in WSNs in this chapter. WSNs are cutting-edge technology with numerous potential uses, including battlefield surveillance, emergency response, healthcare monitoring, and accident detection, such as the identification of elderly people who have fallen. WSNs, however, are frequently put into use in hostile or unmanaged areas. A sensor network is the perfect platform for attackers to carry out any kind of wicked deeds due to its wireless nature and resource limitations [2].

The spread of networked sensors, actuators, and heterogeneous devices has been made easier by the quick advancements in hardware, software, and communication technologies. One illustration is single board computers, which gather and exchange a lot of data to provide a new class of advanced services that are accessible to everyone, anywhere, at any time. The term "Internet of Things" is frequently used to describe this environment (IoT). Both the number of deployments for Sensor Networks (SN) and the Internet of Things (IoT) increased dramatically in recent years. Investments and research initiatives coming from business, academia, and government are helping to fuel this on-going and exponential expansion, while strong technology adoption rates among consumers and technologists across disciplines are also driving these technologies' penetration [3-5].

***Address for Correspondence:** Guangjie Han, Department of Information & Communication Systems, Hohai University, Changzhou, P.R China; E-mail: hanguangjie232@gmail.com*

Received: 02 April, 2022, Manuscript No. sndc-22-68692; **Editor Assigned:** 04 April, 2022, PreQC No. P-68692 **Reviewed:** 16 April, 2022, QC No. Q-68692; **Revised:** 21 April, 2022, Manuscript No. R-68692; **Published:** 28 April, 2022, DOI: 10.37421/2090-4886.2022.11.157

Conclusion

To ensure that we receive correct data for humidity or moisture, we must have confidence in the sensors. It is not sufficient to establish confidence simply by observing the physical presence of sensors in the environment being viewed; we also need to be certain that the data originate from actual sensors. Previous articles, which did not take into account building mutual trust between the sensors, base station, and monitoring application, did not cover the design and execution of a monitoring system. The introduction of the temporal dimension of trust in a humidity and moisture sensor monitoring environment, as well as the extended trust that offers assurance in the trustworthiness of data for further analysis, are the key contributions of this work. After the designated time, neither the data nor their creation is altered. The remainder of the essay is structured as follows. The studies in the monitoring of industrial and agricultural environments, as well as models of trust in the IoT context, are presented in the following part. A trustworthy wireless sensor network model for monitoring humidity and moisture is described in Section.

The new agricultural practises known as smart farming, precision agriculture, or smart agriculture allow for the intensive production of agricultural goods. To assure product quality, these agricultural practises demand the use of contemporary communication and information technology. Soil moisture sensors are used in autonomous plant growing systems to improve the time and energy effectiveness of irrigation systems and cut water usage. The IL-69 soil moisture sensor has been employed in the automation of a sprinkler system. Sensor data can be shown in real time on an LCD screen and on a website. WSNs are susceptible to a range of attacks. These assaults can be broadly divided into passive and active categories. The operation of the network is not hampered by passive attacks. In this instance, the attacker observes without altering the data that is exchanged within the network. Since the procedure is unaffected, passive attacks are exceedingly challenging to detect. While during active attacks, data is changed, disrupting regular network operations. The majority of this chapter's attention is given to active attacks. It should be emphasised that assaults on WSNs are not just limited to denial of service attacks; they also include node takeovers, attacks on routing protocols, and attacks on the physical security of a node.

References

1. Haseeb, Khalid. "An energy efficient and secure IoT-based WSN framework: An application to smart agriculture." *Sensors* 20 (2020): 2081.
2. Shafiq, Maryam. "Robust cluster-based routing protocol for IoT-assisted smart devices in WSN." *Comp Mater Continua* 67 (2021): 3505-3521.
3. Lavanya, S. "A Tuned classification approach for efficient heterogeneous fault diagnosis in IoT-enabled WSN applications." *Measurement* 183 (2021): 109771.
4. Seyhan, Kübra. "Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security." *J Infor Security Appl* 58 (2021): 102788.
5. Yu, Keping. "Blockchain-enhanced data sharing with traceable and direct revocation in IIoT." *IEEE Trans Indu Infor* 17 (2021): 7669-7678.

How to cite this article: Han, Guangjie. "Privacy and Trust Issues also in WSN Systems." *J Sens Netw Data Commun* 11 (2022): 157.