Chapter 17
Computational Intelligence and Blockchain-Based Security for Wireless Sensor Networks

Renu Mishra
Department of CSE, Sharda School of Engineering and Technology, Sharda University, Greater Noida,India

Inderpreet Kaur
Galgotia College of Engineering and Technology, India

Vishnu Sharma
Galgotia College of Engineering and Technology, India

Ajeet Bharti
Galgotia College of Engineering and Technology, India

ABSTRACT

A wireless sensor network (WSN) provides the base architecture to all popular technologies like internet of things (IoT), unmanned arial vehicle (UAV), etc. Recently, a push came to make the information available to humans from the real-time environmental data collected through small sensing devices. WSN is self-organized wireless ad hoc networks to facilitate the interaction between the human and physical worlds. Rapid growth in sensing devices connected to the internet with intelligence and capabilities also opens the door because more devices connected devices means more chances of security vulnerabilities. Blockchain (BC) technology is introduced to address authentication and other security-related challanges by eliminating the role of central authority. This chapter starts with unique characteristics and security challenges in WSN and further identified different ways to apply blockchain with its potential benefits. The chapter presented the integration of blockchain in CI-enabled WSN with respect to focused sectors.

DOI: 10.4018/978-1-6684-5250-9.ch017

INTRODUCTION

These days, we are aware of the vastly useful areas that wireless sensor networks (WSNs) have captured, including the fields of natural engineering, surveillance and security, modern observation, the agricultural sector, seismic location, and the development industry. A huge number of sensors to observe the properties of an area like temperature, air quality, and pressure.The sensor is having very limited capabilities and forward the collected information to a base computer (Selmic et al., 2016)..Recently more and more new applications are being popular in the commercial sectors that are getting benefits from basic WSN. Overall prosperity depends on how it is integrated with the Internet and other advanced wireless technologies. Security threats are a significant issue in WSNs. The cause is that SNs have limited resources and are vulnerable to attack. (Verma et al., 2022). There are typically two types of attacks carried out in WSNs. Internal attacks occur when SNs act selfishly to protect their energy and storage, as opposed to external attacks, in which the attackers seize control of the SNs to carry out malicious activities. Therefore, it is essential to locate and eliminate the malicious nodes from the network(Awan et al., 2022). Still WSN, which is composed of multiple sensor always has the risk of being data tampering and can be secured with smart solutions using Intelligence computing. Presentely smart sensors are coming with high computational capacities to handle various tasks with fullflaged operating system and also web protocol stack.Such a constraintless WSN makes the decentralized operation of the data collection and management processes very efficientely with the help of Computational intelligence (Akyildiz et al., 2002).The capsule of Blockchain and CI has been gaining significant attention among sensor based business solutions to be successfully deployed and tested in real-time scenario like intelligent monitoring of temperature, criminal activity in borders and surveillance on traffic monitoring, vehicular behavioron roads, water level and pressure, and remote monitoring of patients.Sinse WSN is more vulnarable so conventional security mechanisms cannot be fully applied in WSN where sensor nodes are connected to a common link in an attack prone environment.Every node should be able to identify the other node's identity and credentials. These identities and credentials must be mutually authenticated and also shielded to avoid future questions. The identification also leads to the privacy issue, so a good security solution must cover confidentiality, availability, and integrity of information carried in packets during routing because the information may be forwarded and misused by malicious node (Tyagi et al., 2020).Blockchain (BC) technology can be introduced as part of WSN with the goal of eliminating a central server to address such security and privacy concerns. You can use blockchain technology to design an Intelligent security solution for recent networking paradigms like Content-based Networking and internet-of-Things(Martin F.R. 2018).

The chapter presented the complete view that how Computational intelligence based security solutions get benefits from BlockchainTechnology and vice verca.Second section gives the preliminiary knowledge and Fundamentals of CI and Blockchain Technology with wide coverage of the types of Computational Intelligence Techniques.Third section highlights the limitation of BT and AI.Next forth section demonstrated that both Technologies can come together as complimentary for mutual benefits. Future research directions are covered in fifth section.At last the chapter gave the conclusion that convergence of blockchain and AI may bring the new value in WSN landscape globally.