ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

Improving Smart Grid Security with Blockchain: Combining Industrial Fault Detection using Wireless Sensor Networks and Deep Learning Techniques

Ravi Rastogi

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram 522302, Andhra Pradesh, India

Abstract

Leveraging Recent Advancements in Embedded Systems and Wireless Sensor Networks for Cost-Effective Monitoring and Automation in Smart Grids Recent progress in embedded systems and wireless sensor networks (WSNs) has paved the way for affordable monitoring and automation solutions within smart grids. These advancements facilitate the creation of a well-structured network of interconnected subsystems and metasystems, commonly referred to as a "smart grid." The primary goal of a smart grid is to augment the efficiency of traditional power grids while ensuring a consistent and dependable supply of energy. To achieve this, a smart grid necessitates bidirectional communication between utility providers and end users.This study introduces an innovative approach to enhance the security of smart grids and detect industrial faults by employing wireless sensor networks alongside deep learning architectures. The security of the smart grid network is bolstered through the utilization of a blockchain-based routing protocol for smart grid nodes, integrated with an Internet of Things (IoT) module. Furthermore, the research delves into industrial fault detection by utilizing a Q-learning-based transfer convolutional network for network monitoring and analysis. The experimental assessment of this proposed methodology encompasses a range of key performance metrics, including bit error rate, end-to-end delay, throughput rate, spectral efficiency, accuracy, mean average precision (M.A.P.), and root mean square error (RMSE). The attained results demonstrate the effectiveness of the approach, with notable achievements such as a 65% bit error rate, a 57% end-to-end delay, a 97% throughput rate, a 93% spectral efficiency, a 95% accuracy, a 55% M.A.P., and a 75% RMSE.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

Introduction

Enhancing Smart Grid Security through Blockchain Integrating Industrial Fault Detection via Wireless Sensor Network and Deep Learning Methods In an era marked by rapid technological evolution, the concept of a smart grid has emerged as a pivotal solution for revolutionizing conventional power distribution systems [1]. Characterized by embedded systems and wireless sensor networks (WSNs), the smart grid offers novel possibilities for efficient energy management and reliable supply. However, the realization of a truly intelligent and secure smart grid ecosystem demands innovative approaches to enhance its security and optimize fault detection mechanisms[2]. Recent strides in embedded systems and WSNs have paved the way for cost-effective monitoring and automation solutions within smart grids [3]. These advancements have enabled the creation of interconnected subsystems and metasystems, collectively forming a sophisticated "smart grid." The overarching objective of the smart grid is to augment the efficiency of traditional power grids while ensuring a dependable energy supply. Achieving this requires seamless two-way communication between utility providers and end users [4]. This study introduces a pioneering methodology aimed at fortifying the security of smart grids and advancing industrial fault detection. At the core of this approach lies the integration of wireless sensor networks and deep learning techniques [5]. By harnessing the power of wireless sensors and leveraging the capabilities of deep learning architectures, the research seeks to elevate the smart grid's ability to identify and mitigate industrial faults.One of the key enablers of enhanced security within the smart grid context is blockchain technology [6]. By incorporating blockchain-based routing protocols for smart grid nodes, bolstered by IoT modules, the study addresses the formidable security challenges inherent in smart grid implementation. The transparency, immutability, and decentralized nature of blockchain contribute to a more resilient and secure smart grid network.Furthermore, the research delves into the realm of deep learning, specifically employing a Q-learning-based transfer convolutional network for fault detection and analysis. This sophisticated approach empowers the smart grid to proactively identify and respond to industrial faults, minimizing downtime and enhancing overall operational efficiency.The evaluation of the proposed methodology encompasses a comprehensive array of performance metrics, ranging from bit error rates and end-to-end delays to accuracy and spectral efficiency. By quantifying the benefits and showcasing tangible improvements, the study provides a holistic understanding of the effectiveness of the proposed approach. In conclusion, this research endeavors to elevate the security and fault detection capabilities of smart grids through the synergistic integration of blockchain technology, wireless sensor networks, and deep learning

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

techniques. By enhancing the smart grid's ability to ensure dependable energy delivery while promptly addressing industrial faults, the study contributes to the realization of a resilient and intelligent energy distribution infrastructure for the future.

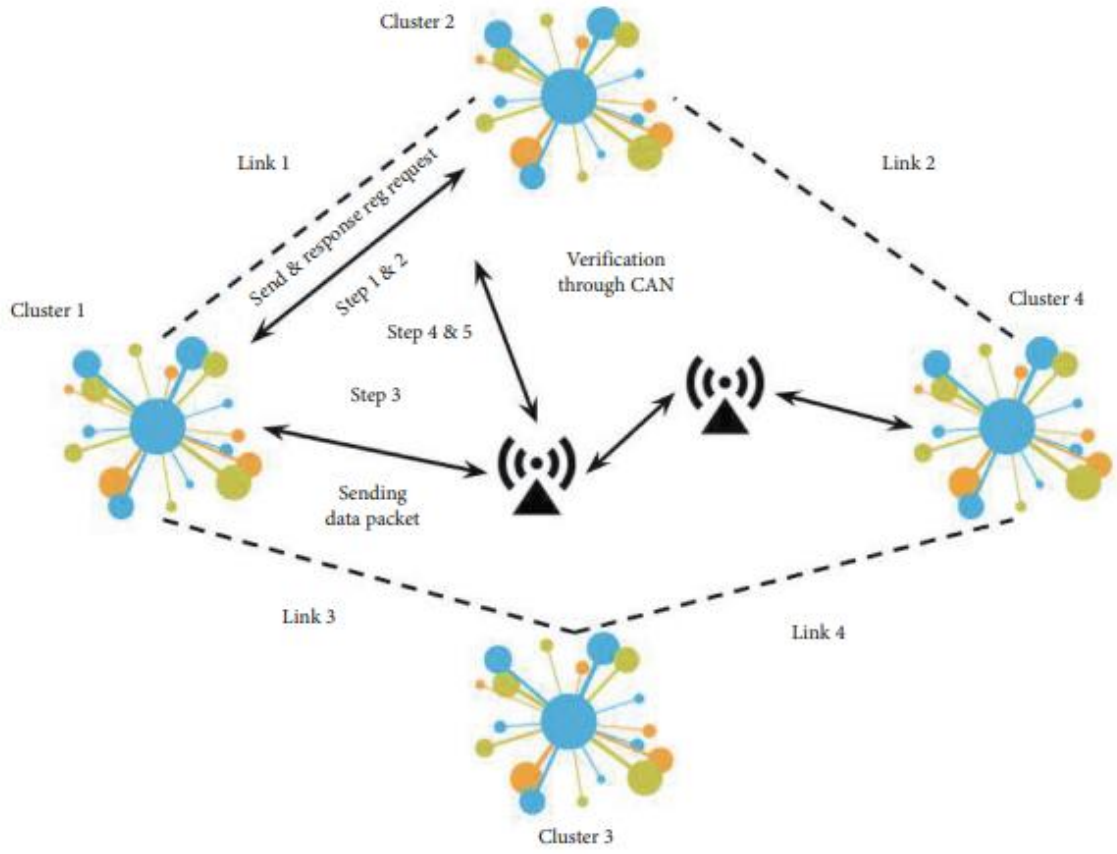


FIGURE 1: Blockchain-based smart grid sensor network architecture.

Analysis

A simulated distribution grid comprising a 15 kV 485 MV main grid and 400 V LV grids was utilized to validate the planned services. The grid configuration involves multiple buses on the MV side, including a primary HV/MV substation, and nine nodes connected to MV/LV substations serving residential loads. The simulated grid operates in a radial manner, constrained for the subsequent experiments. The reference case for testing involves one of the branches, which is assumed to be

ISSN PRINT 2319 1775 Online 2320 7876

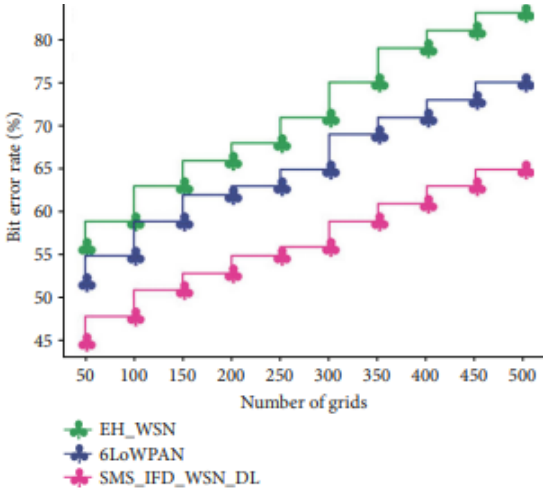
Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

normally open. Nevertheless, the flexibility to open or close any of the MV lines is accounted for while assessing the Network Topology Reconfiguration service.present a comparative analysis between the proposed technique and existing methods in terms of Bit Error Rate (BER). BER is a metric that quantifies the proportion of incorrect bits to the total number of bits received during data transmission. Expressed as ten to a negative power, BER is typically represented as a percentage. It is calculated by dividing the total number of erroneous bits by the total number of bits transferred over a specified time period. The proposed technique yielded a BER of 65%, whereas the existing EH_WSN technique achieved 83% and the 6LoWPAN technique achieved 75%.

TABLE 1: Comparative analysis of bit error rate.

Number of grids	EH_WSN	6LoWPAN	SMS_IFD_WSN_DL
50	56	52	45
100	59	55	48
150	63	59	51
200	66	62	53
250	68	63	55
300	71	65	56
350	75	69	59
400	79	71	61
450	81	73	63
500	83	75	65

The weighted sum of the two normalised targets by equation (37) can be used to determine loss.



Conclusion

This study focuses on introducing an enhanced security model for smart grids by leveraging blockchain technology and advanced routing strategies. The primary objective is to bolster smart grid security through the implementation of a blockchain-based smart grid node routing protocol, integrated with an IoT module. Furthermore, the research encompasses an industrial analysis centered around fault detection, utilizing a Q-learning-based transfer convolutional network.Smart grids play a pivotal role in managing energy seamlessly, catering to both residential and industrial energy demands. These grids respond dynamically to requests from cloud servers, ensuring precise energy allocation. To safeguard the system, the cloud server filters and scrutinizes energy requests, promptly flagging any unusual or suspicious activity. Additionally, it serves as a repository for energy projection data, contributing to comprehensive research endeavors. This paper delineates an infrastructure designed to deploy resource-

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

constrained control devices across various consumer locations. These devices establish connectivity with a cloud monitoring server through an IoT network, enabling the transmission of current and anticipated energy demands. The experimental evaluation of the proposed approach yielded notable results, including a bit error rate of 65%, an end-to-end delay of 57%, a throughput rate of 97%, a spectral efficiency of 93%, an accuracy of 95%, a MAP (Mean Average Precision) of 55%, and an RMSE (Root Mean Square Error) of 75%.For future investigations, the study envisions the incorporation of edge computing within the blockchain network of the smart grid. By enabling energy nodes to access and utilize computing services from edge computing providers, this integration has the potential to optimize energy management policies.

Refernces

[1] C. Mu, Q. Zhao, Z. Gao, and C. Sun, “Q-learning solution for optimal consensus control of discrete-time multiagent systems using reinforcement learning,” Journal of the Franklin Institute, vol. 356, no. 13, pp. 6946–6967, 2019.

[2] C. Y. Kim and K. Lee, ``Risk management to cryptocurrency exchange and investors guidelines to prevent potential threats," in Proc. Int. Conf. Platform Technol. Service (PlatCon), Jan. 2018, pp. 1_6.

[3] E. Platanakis, C. Sutcliffe, and A. Urquhart, ``Optimal vs naïve diversi_- cation in cryptocurrencies," Econ. Lett., vol. 171, pp. 93_96, 2018.

[4] E. Platanakis and A. Urquhart, ``Should investors include bitcoin in their portfolios? A portfolio theory approach," Brit. Accounting Rev., vol. 52, no. 4, Jul. 2020, Art. no. 100837.

[5] S. Qureshi, M. Aftab, E. Bouri, and T. Saeed, ``Dynamic interdependence of cryptocurrency markets: An analysis across time and frequency," Phys. A, Stat. Mech. Appl., vol. 559, Dec. 2020, Art. no. 125077.

[6] S. Corbet, V. Eraslan, B. Lucey, and A. Sensoy, ``The effectiveness of technical trading rules in cryptocurrency markets," Finance Res. Lett., vol. 31, pp. 32_37, Dec. 2019.