ISSN PRINT 2319 1775 Online 2320 7876

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

Examining Network-Level Routing in IoT Systems for Smart Cities and Deploying Blockchain-Based Security Measures

V. Ganesh

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

Abstract

This study presents a comprehensive analysis of network-level performance and the practical implementation of a smart city Internet of Things (IoT) system using an Infrastructure as a Service (IaaS) cloud computing architecture. The performance of the smart city IoT network topology is evaluated through simulation using the NS3 simulator, focusing on crucial performance-affecting parameters. The improved performance smart city topology is then put into practice within the IaaS architecture. The envisioned smart city IoT system is designed to monitor key parameters such as video surveillance employing thermal cameras (for detecting individuals with COVID-19-like symptoms), transportation, water quality, solar radiation, noise pollution, air quality (including O3, NO2, CO, and particulate matter), parking availability, significant landmarks, electronic suggestions, and public relations information. This monitoring is achieved over a wide area network with low power requirements, covering an area of 61.88 km x 61.88 km.Primary attention is given to addressing challenges related to IoT network-level routing, quality of service (QoS), and implementation-level security. A network topology analysis is conducted at the simulation level to enhance routing and QoS. To enhance security, a decentralized approach based on blockchain technology is adopted, aiming to bolster the overall performance of the IoT system. **Keywords:** IoT technology ,Smart applications ,Network simulation , Blockchain technology

Introduction

ISSN PRINT 2319 1775 Online 2320 7876

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

To Smart City IoT System Network Level Routing Analysis and Blockchain Security-Based Implementation In the rapidly evolving landscape of urban development, the concept of smart cities has emerged as a transformative paradigm[1]. Central to this concept is the integration of the Internet of Things (IoT) technology, which empowers cities with the capability to intelligently monitor and manage various aspects of urban life, from transportation and energy consumption to public safety and environmental quality [2]. As smart city initiatives continue to gain momentum, the need for robust and efficient network infrastructure becomes paramount. This necessitates a thorough analysis of network-level routing strategies to ensure seamless communication and data flow within the IoT ecosystem.One of the critical challenges faced by smart city IoT systems is the dynamic and diverse nature of the devices and sensors interconnected within the network [3]. Efficient routing mechanisms are indispensable to ensure timely and reliable delivery of data between these devices, facilitating real-time decision-making and response [4]. Therefore, this study delves into the intricate realm of network-level routing analysis, aiming to optimize data transmission pathways within the smart city IoT network. Furthermore, the proliferation of IoT devices and the data they generate raises significant concerns about security and privacy [5]. The distributed and interconnected nature of IoT systems amplifies vulnerability to cyber threats, necessitating innovative approaches to safeguard sensitive information. In this context, blockchain technology has emerged as a promising solution [6], offering decentralized and immutable data storage, authentication, and encryption [7]. This study recognizes the imperative of ensuring the security of smart city IoT systems and explores the implementation of blockchain-based security measures.

The primary objectives of this research are two fold:

1. **Network Level Routing Analysis:** This aspect of the study involves a comprehensive examination of network-level routing strategies within a smart city IoT ecosystem. By leveraging simulation tools and techniques, we seek to identify and optimize key performance parameters that influence data transmission efficiency, latency, and reliability [8]. The insights gained from this analysis will inform the design of an optimized routing framework tailored to the unique requirements of a smart city environment.
2. **Blockchain Security-Based Implementation:** The study recognizes the significance of fortifying smart city IoT systems against security breaches and unauthorized access. To this end, the research explores the integration of blockchain technology as a security-enhancing mechanism. By establishing a decentralized and tamper-proof data infrastructure [9], we aim to enhance data integrity, authentication, and confidentiality across the smart city IoT network. In summary, this research embarks on a journey to unlock the full potential of smart city IoT systems through a dual-focused approach. By

ISSN PRINT 2319 1775 Online 2320 7876

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

dissecting network-level routing intricacies and harnessing blockchain's security capabilities [10], the study endeavors to contribute to the realization of resilient, efficient, and secure smart city ecosystems that empower urban communities to thrive in the digital age [11].

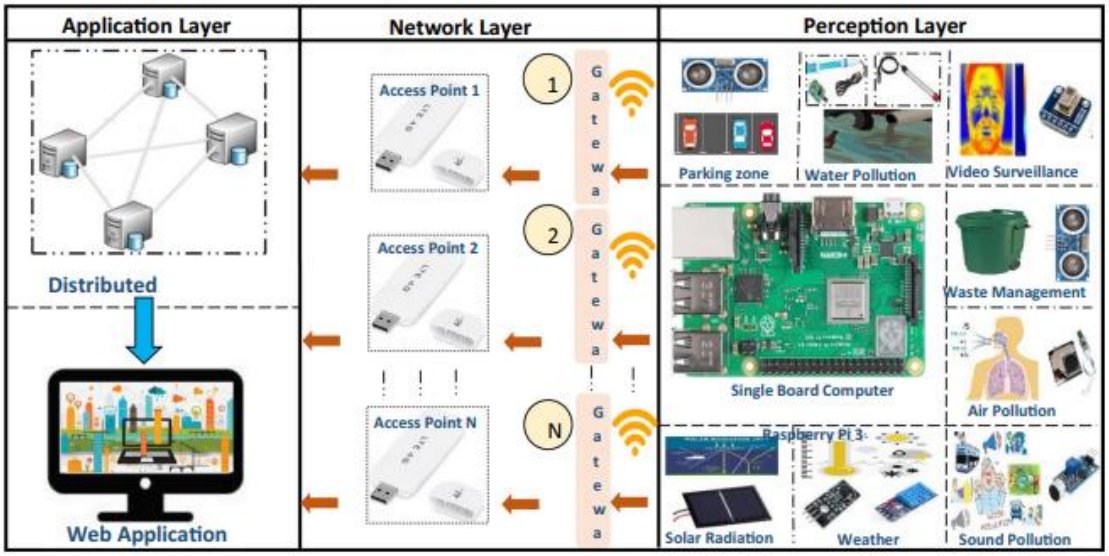


Fig. 6 Model structure of smart city IoT

Methodology

Conduct an extensive review of existing literature on smart city IoT systems, network-level routing strategies, and blockchain technology for security enhancement.Identify key challenges, trends, and best practices in network routing optimization and blockchain-based security implementation within smart city contexts [12].Gather relevant data regarding the smart city's IoT infrastructure, including device types, communication protocols, traffic patterns, and environmental parameters.Utilize simulation tools such as NS3 to create a virtual model of the smart city IoT network, incorporating realistic spatial layouts and device distribution [13].Generate synthetic data streams to emulate various IoT applications and interactions within the simulated environment.Implement different routing algorithms commonly used in IoT networks, such as AODV, DSR, and RPL.Measure and analyze performance metrics, including packet delivery ratio, end-to-end delay, throughput, and energy consumption [14].Optimize routing parameters and algorithms based on simulation results to enhance data transmission efficiency and reliability.Identify critical security requirements for the smart city IoT system, such as data integrity, authentication, and access control [15].Design a blockchain-based architecture tailored to the smart city IoT context, considering factors like consensus mechanisms and data encryption.Integrate blockchain nodes within the simulated network and establish secure

ISSN PRINT 2319 1775 Online 2320 7876

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

communication channels between IoT devices and the blockchain network.Develop a prototype of the smart city IoT network with the optimized routing framework and integrated blockchain security measures. Deploy the prototype in a controlled physical or virtual environment to validate the effectiveness of the proposed solutions. Conduct comprehensive testing scenarios to assess the system's performance under various conditions, including network congestion, device mobility, and security threats. Compare the performance of the optimized routing algorithms against baseline routing methods, highlighting improvements in terms of data delivery, latency, and energy efficiency.Evaluate the impact of blockchain-based security on data integrity, authentication, and protection against cyber attacks.Quantify the trade-offs between enhanced security measures and potential resource overhead. Interpret the results of the routing analysis and blockchain security implementation, addressing how each solution contributes to the overall effectiveness of the smart city IoT system. Discuss the implications of the findings on network performance, security posture, and scalability for real-world smart city deployments. Summarize the key insights gained from the study, emphasizing the significance of optimized network routing and blockchain security for smart city IoT systems. Highlight any limitations encountered during the research and propose potential avenues for further exploration, such as hybrid routing approaches or advanced blockchain integration techniques. By following this comprehensive methodology, the study aims to provide a holistic understanding of network-level routing optimization and blockchain-based security in the context of smart city IoT systems. The combination of theoretical analysis, simulation-based experiments, and practical implementation will contribute to advancing the knowledge and capabilities in creating resilient and secure urban IoT environments.

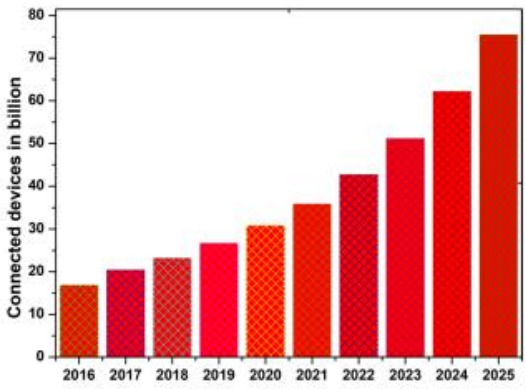


Fig. 1 IoT devices usage growth in billion (Source: Statista)

Fig. 2 Smart city parameters

ISSN PRINT 2319 1775 Online 2320 7876

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

Table 1 Network and implementation level IoT challenges

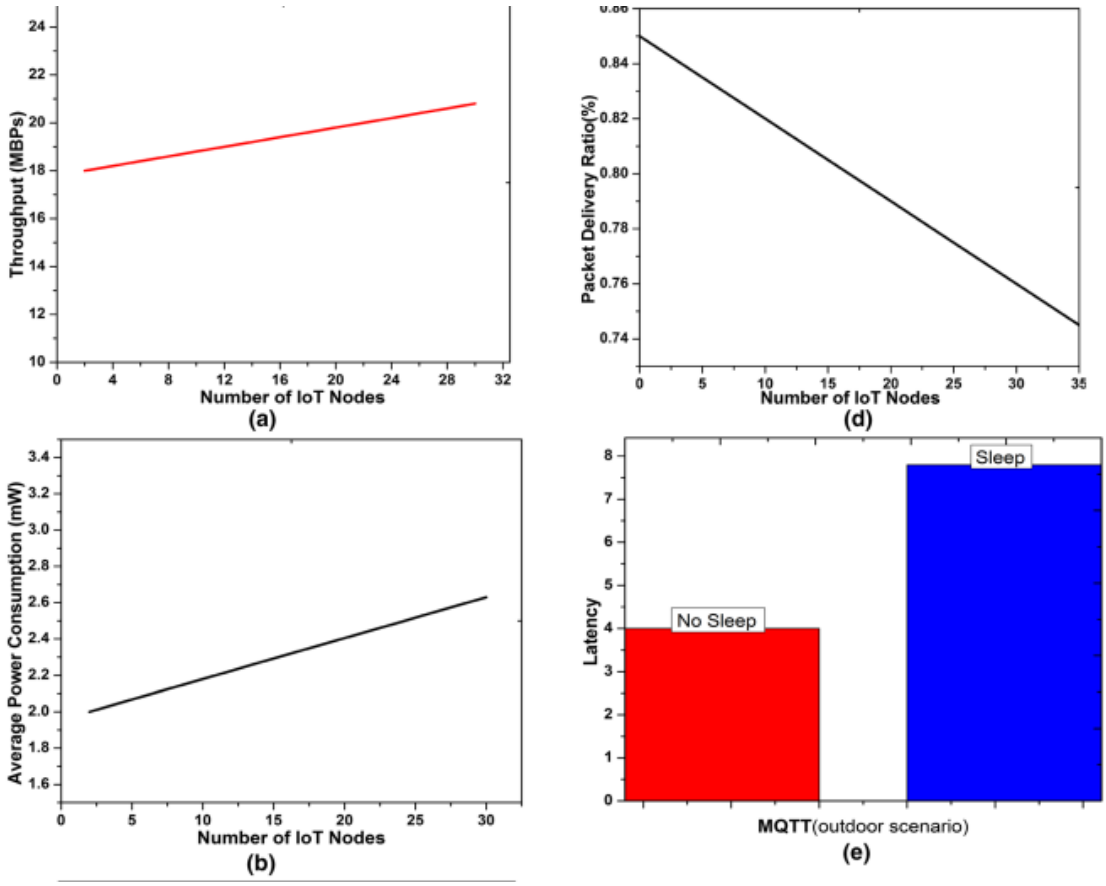
Level	Challenges	Solution
Sensor	Node capturing, false data injection, eavesdropping and interference, malicious code injection, side-channel attacks, booting attacks, sleep deprivation attacks	Encryption, digital signature
Network	Routing, patch loss, congestion control, reliability, scalability, and quality of service (QoS)	Network level simulation analysis
Implementation	Sensing of physical parameter accurately, Privacy, security, storage, data analysis and visualization	Blockchain, ICN, SDN

Table 2 Comprehensive study of smart city IoT related work

Refs.	Topic discussed related to smart city	Strength	Simulation used (tool)	Routing topology	Protocols
[31]	Smart energy management system	Context life cycle for IoT-based smart cities	Yes (FIWARE)	–	MQTT
[32]	Traffic Classification	Network security and quality of service	No	Random	COAP
[33]	Generic IoT Networks	Hierarchical IoT network (HIoTN)	No	–	Authentication Protocol (UAKMP)
[34]	IoT with Blockchain	IoT interface with blockchain	No	–	MQTT
[35]	Key oriented verification style for IoT devices using blockchain	Blockchain with authentication	Yes (ns-3)	–	MQTT
[36]	Bloom filters, to make compact names from node reports; data	DIstributed NAming Service (DINAS)	Yes (contiki/cooja)	–	MAC, IPv6, RPL

ISSN PRINT 2319 1775 Online 2320 7876

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



Conclusion

This paper introduces a smart city IoT system designed to monitor critical variables such as thermal camera-based video surveillance, air and water quality, noise pollution, weather conditions, solar radiation, waste management, parking availability, electronic suggestions, and prominent landmarks. The initial phase involves conducting virtual simulations using NS-3 to assess the feasibility of the smart city IoT network configuration. Subsequently, the IoT system is put into practical operation, ensuring both high-quality service delivery and robust security measures. This innovative approach strengthens the overall system's protection against threats, improves its ability to handle increased demands, and optimizes resource utilization, leading to a more reliable and efficient smart city ecosystem.

Refernces

ISSN PRINT 2319 1775 Online 2320 7876

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

1. Rahman MA, Rashid MM, Hossain MS, Hassanain E, Alhamid MF, Guizani M (2018) Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. IEEE Access 7:18611–18621

2. Santos PM, Rodrigues JGP, Cruz SB, Lourenc T ¸ d'Orey OPM, Luis Y, Rocha C, Sousa S, Cris´ostomo S, Queir´os C, Sargento S, Aguiar A, Barros J (2018) PortoLivingLab: an IoT-based sensing platform for smart cities. IEEE Internet of Things Journal 5(2):523–532

3. Kumar K, Saraswat S, Jindal SK et al (2021) Experimental validation of an iot based device selective power cut mechanism using power line carrier communication for smart management of electricity. J Electr Eng Technol 16:67–77

4. Xu B, Da Xu L, Cai H, Xie C, Hu J, Bu F (2014) Ubiquitous Data accessing method in IoT-based information system for emergency medical services. IEEE Tran Ind Inf 10(2)

5. Hebal S, Harous S, Mechta D (2021) Energy routing challenges and protocols in energy internet: a survey. J Electr Eng Technol 16:3197–3212

6. André da Costaa C, Pasluostab CF, Eskoferb B, Bandeira da Silvaa D, Righia RR (2018) Internet of health things: toward intelligent vital signs monitoring in hospital wards. Artif Intel Med, 89

7. Aslam MM, Irshad MN, AZEEM, H. (2020) Cost efective and energy efcient intelligent smart home system based on IoT. Afyon Kocatepe Üniversitesi Uluslararası Mühendislik Teknolojileri ve Uygulamalı Bilimler Dergisi 3(1):10–20

8. Y.-B. Lin, and H.-C. Tseng (2018) FishTalk: An IoT-based Mini Aquarium System. IEEE Access 7

9. Gao G, Xiao K, Chen M (2019) An intelligent IoT-based control and traceability system to forecast and maintain water quality in freshwater fsh farms. Comput Electron Agric, 166

10. Tzounis A. Katsoulas N, Bartzanas T, Kittas C (2017) Internet of Things in agriculture, recent advances and future challenges. Biosyst Eng 164(31)

11. Zhang W, Guo W, Liu X. Liu Y, Zhou J,. Li B, Lu Q, Yang S (2017) LSTM-based analysis of industrial IoT equipment. IEEE Access 13(9)

ISSN PRINT 2319 1775 Online 2320 7876

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

12. Gronau N,. Ullrich A,. Teichmann M (2017) Development of the Industrial IoT competences in the areas of organization. Process, and interaction based on the learning factory concept. Proc Manuf 9

13. Boyes H, Hallaq B, Cunningham J, Watson T (2018) The industrial internet of things (IIoT): an analysis framework,". Comput Ind 101:1–12

14. Hafdh B, Al Osman H, Arteaga-Falconi J, Dong H, EL Saddik A (2017) SITE: the simple internet of things enabler for smart homes. IEEE Access 5:2034–2049

15. Mehta R, Sahni J, Khanna K (2018) Internet of things: vision, applications and challenges. Procedia Computer Science 132:1263–1269