Please cite the Published Version

RESEARCH

Context-Aware Prediction with Secure and Lightweight Cognitive Decision Model in Smart Cities

Fatima Al-Quayed[1] · Mamoona Humayun[2] · Thanaa S. Alnusairi[1] · Inam Ullah[3] · Ali Kashif Bashir[4] · Tariq Hussain[5]

Abstract

Cognitive networks with the integration of smart and physical devices are rapidly utilized for the development of smart cities. They are explored by many real-time applications such as smart homes, healthcare, safety systems, and other unpredictable environments to gather data and process network requests. However, due to the external conditions and inherent uncertainty of wireless systems, most of the existing approaches cannot cope with routing disturbances and timely delivery performance. Further, due to limited resources, the demand for a secure communication system raises another potential research challenge to protect sensitive data and maintain the integrity of the urban environment. This paper presents a secured decision-making model using reinforcement learning with the combination of blockchain to enhance the degree of trust and data protection. The proposed model increases the network efficiency for resource utilization and the management of communication devices with the alliance of security. It provides a reliable and more adaptive paradigm by exploring learning techniques for dealing with the intrinsic uncertainty and imprecision of cognitive systems. Also, the incorporation of blockchain technology reduces the risk of a single point of failure, malicious vulnerabilities, and data leakage, ultimately fostering trust for urban sensor applications. It validates the incoming routing links and identifies any communication fault incurred due to malicious interference. The proposed model is rigorously tested and verified using simulations and its significance has been proven for network metrics in comparison to existing solutions.

Keywords Cognitive computing · Intelligent systems · Real-time applications · Security · Smart cities

Introduction

Internet of Things (IoT) and cognitive networks performed a significant role in shaping the way people interact with their surroundings and offering an efficient way for smart communication over different domains [1–3]. With the provision of wireless connectivity, IoT networks provide the convenience automation process to facilitate communication technologies for observing the ambiguous environment [4, 5]. Moreover, sensors enable intelligent and context-aware environmental analysis and report the collected data to cloud systems for central storage and timely processing [6–8]. Researchers are demanding to development of real-time dynamic approaches to handle efficient management of wireless devices with the

✉ Mamoona Humayun
  Mamoona.Humayun@roehampton.ac.uk

✉ Inam Ullah
  inam@gachon.ac.kr

  Fatima Al-Quayed
  ffalquayed@ju.edu.sa

  Thanaa S. Alnusairi
  thsnusairi@ju.edu.sa

  Ali Kashif Bashir
  Dr.alikashif.b@ieee.org

  Tariq Hussain
  uom.tariq@gmail.com

1   Department of Computer Science, College of Computer and Information Sciences, Jouf University, 72388 Sakakah, Al Jouf, Saudi Arabia

2   Department of Computing, School of Arts Humanities and Social Sciences, University of Roehampton, London SW15 5PJ, UK

3   Department of Computer Engineering, Gachon University, Seongnam 13120, Republic of Korea

4   Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, UK

5   School of Computer Science and Technology, Zhejiang Gongshang University, Hangzhou 310018, China

combination of future networks [9, 10]. The incorporation of future technologies and IoT in real-time applications enables innovative and immersive experiences, improved connectivity, and widespread use of smart devices for daily tasks [11, 12]. Moreover, Artificial Intelligence (AI)–based massive network connectivity is supported by many applications to provide decision-making systems in crucial environments [13–15]. While AI-enabled applications have some benefits for IoT electronics, they have some limitations as well in terms of computational cost for constrained devices and utilization of communication resources [16, 17]. Also, malicious devices may manipulate cognitive networks to produce unreliable decisions and compromise the authentication, security, and access control [18–20]. The main aim of our proposed model is to explore the significant research challenges for smart city IoT networks in terms of scalability and different network parameters. The routing performance is evaluated continuously using machine learning techniques, and a reward score by using dynamic threshold, congestion, and reliability factors. Moreover, next-hop is kept secured with the integration of secured techniques, and blockchain nodes attain the integrity of network with robust authentication and data verification. Also, the edges ensure the IoT environment is free of communication risks with high possibility of trusted communication. Our proposed model has made the following research contributions.

i.   Using intelligent criteria derived from reinforcement learning, routing connections have developed, providing long-run communication routes and strengthening the IoT system at a crucial time.
ii.   During inter-communication network services, the IoT devices are preserved by exploring contextual parameters, and alternative routes are generated with cognitive decision-making strategies.
iii.   Blockchain technology with the incorporation of trusted nodes guarantees the authorization of devices and provides privacy protection and efficient resource consumption.

This research work has the following subsections. The "Related Work" section covers related discussion. The proposed model is discussed in the "Context-Aware Predictive Cognitive Decision Model with Enhanced Security for Smart Cities" section. The "Secured Reinforcement Learning for IoT Networks in Smart City: A Simulation Evaluation" section discusses the experiment results. The research ended in the "Conclusion" section.

Related Work

Cognitive applications are significant in IoT networks because they are transformative in various appliances such as smart homes, surveillance, and healthcare systems [21, 22]. These systems are utilized to gather environmental data for remote monitoring and provide some cost-effective solutions with enhanced user experience. Significant advantages and opportunities are developed with the combination of future technologies, wireless devices, and edge computing [23–25]. In recent decades, they improved the facilities of industrial applications and the provision of crucial information to requested devices. However, smart networks are rapidly facing many research challenges to maintain sustainable solutions with effective processing for big data. In addition, attaining IoT security while carrying out cognitive operations in real-time applications provides a remarkable effect on bounded devices [26, 27]. In [28], the authors proposed an intelligent opportunistic routing protocol (IOP) for energy efficiency and network reliability by identifying the relay nodes using a machine learning technique. Applications for the proposed method could include e-healthcare services. Because it can connect multiple healthcare network devices in a better way and provide good reliability, the proposed method may help the network achieve reliability. In addition, by integrating IoT services, the proposed method helps the remote patient connect with healthcare services for a longer period while also saving energy. The proposed work has mainly focused on opportunistic routing without evaluating the significance of environmental and network factors. Moreover, it may perform optimally for large-scale network particularly under varying network conditions. Authors [29] investigated numerous network issues related to security for edge computing–based Unmanned Aerial Vehicle (UAV) delivery systems. Such problems arise due to malicious attacks, unauthorized access, and data breaches in the communication system. A novel security framework A2DSEC is proposed for the detection, authentication, and defense of network devices. The proposed framework ensured the security of user identity authentication, with effective and lightweight warning messages, thus providing a robust security system with a timely response. It provided a security framework for UAV delivery systems, however lacks the highlighting of the research issues in terms of network scalability. In addition, it may not be fully functional for adaptive edge computing environment and not efficiently manages the resource management.

In [30], the authors provide an energy-efficient distributed adaptive cooperative routing (EDACR) for wireless multimedia sensor networks (WMSN), taking into consideration the quality of service (QoS) and energy

conservation limitations. A smart system is developed by exploring reinforcement learning to execute QoS and energy-balanced routing with the support of both latency and reliability. The simulation results demonstrate that less energy is consumed while maintaining QoS as compared to the distributed adaptive cooperative routing protocol and the classic cooperative protocol. The proposed solution provided an energy-efficient network but failed to consider congestion and IoT data load on constraint devices. Authors [31] have proposed a new protocol called the Trust-Based Secure Intelligent Opportunistic Routing Protocol (TBSIOP). Three different WSN attributes are used by the proposed protocol to calculate a node's probability of being malicious. These characteristics are utilized in the computation of trust and are sincere in energy depletion (Ed), sincere in acknowledgments (ACKs), and sincere in forwarding data packets (Fs). The relay selection algorithm of the proposed protocol blocks malicious nodes from being selected as relay nodes based on the computed trust factor. The proposed work focused on trust-based secured communication for IoT-based opportunistic routing and increases stability. However, it does not address the mobility issues for high-density networks and fails to cope with dynamic topologies. The proposed framework [32] highlights and resolves the issues of data security with authorized access, particularly for IoT applications. It combines the concept of blockchain and provides a secured mechanism for data sharing using three smart contracts in terms of access control, authentication, and decision-making. As compared to existing methods, the experiments revealed the proposed framework outcomes with cost-effective solutions with network scalability. The proposed approach provided a blockchain-based access control and data sharing system for smart devices, however lacks to cope with research problems for energy efficiency and latency when it is applied for high-scaled IoT environments. To collect the user location data while guaranteeing local, the authors proposed a framework for local differential privacy (LDP) in the last-mile delivery system of UAVs for edge computing [33]. It begins by dividing the data collection area with the support of a Quad-tree region retrieval method and gets user location distribution. Afterward, by exploring the Quad-tree, the user location matrix is derived, and using the LDP perturbation scheme, the location data is perturbed. In the end, blockchain technology is utilized to perturb the aggregated data and access its utility of dataset across different regions. However, it has not explored the integration of lightweight data encryption methods for constraint devices. Moreover, it also effects the network latency for crucial applications particularly within edge computing. In edge computing to address the privacy issue in UAV delivery, authors [34] utilized differential privacy and diffusion models to develop and

implement the framework for securing face recognition and identity authentication. Through edge computing nodes, the UAVs collect the user's biometric data while delivering and using a diffusion model for the transmission of data securely and to attain user privacy. On the other side, nodes at edge computing perform face recognition and authentication methods to certify that data can be accepted only by authentic users. However, in depth evaluation of the proposed solution under real-time IoT environment with different parameters and network conditions is not considered. Furthermore, the integration of advanced security mechanisms is not considered to cope potential communication threats on edge devices.

Context-Aware Predictive Cognitive Decision Model with Enhanced Security for Smart Cities

This section includes a detailed description of our proposed model for cognitive decision-making in smart networks while maintaining trustworthiness communication. Figure 1 depicts the various layers in the proposed model for the growth and development of smart city IoT networks. It is comprised of three main stages. In the first stage, sensors and communication electronics are interconnected with wireless technologies to form the smart city IoT network. The deployment is random and devices are constrained in terms of resources. Network devices are self-organized and maintain the communication topology dynamically. Nodes have limited transmission power and are mobile. Local edges are more powerful than ordinary sensors and collaborate with both lower and higher layers. In the second stage, devices are required to make decisions at each level to forward the collected data. Devices are required to choose the route link to follow based on a specific condition. In the third stage, security measurement is taken at each node to validate it against threats and attain
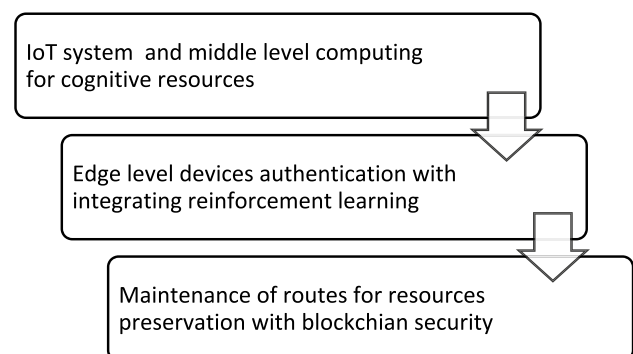

Fig. 1 Layers of the predictive and secured cognitive model for smart city IoT network

privacy for crucial data. Moreover, blockchain technology is adopted to ensure the integrity of data for smart city IoT networks. It is integrated into a proposed model for increasing network integrity with data transparency and security for IoT applications. Using decentralized computing, the blockchain guarantees the reliable and authorized access of data blocks through cryptographic hashes. Furthermore, the combination of symmetric keys and access control features of digital signatures decreases the risks of data tampering and breaches. In the development of the proposed model, our assumptions are as follows.

i. Communication between sensors occurs using Zigbee protocol with restricted constraints.
ii. The network is comprised of distributed deployment in the predefined communication area.
iii. Without any centralized control, devices are interconnected and transmit the data.
iv. Each device has a predefined distance and in case of long communication, multi-hop is adopted.
v. Sensor nodes can perform data aggregation to reduce network congestion.

The proposed model uses the concept of reinforcement learning to construct the routing chains for the transmission of network data in sensors-driven applications. Initially, each node acts as an agent and computes its reward using the energy threshold e_{thres}, congestion con, and reliability rel parameters as defined in Eq. 1. The computed weight values are stored in the routing table and updated based on external conditions.

$$R(n_i) = w_1.(1/e_{thres}) + w_2.(1/con) + w_3.rel \tag{1}$$

Energy threshold provides the triggering function as defined in Eq. 2, and alerts the system for the reselection of a new forwarder.

$$e_{thres} = e_{initial}*L \tag{2}$$

where L denoted the scaling factor of energy usage. Congestion con at node level n_i can be computed dynamically by utilizing the current load L_{cr} on the communication link, as shown in Eq. 3.

$$con(n_i) = {L_{cr}(i,j)}/{L_{mx}(i,j)} \tag{3}$$

where L_{mx} denotes the maximum load on the link. For optimal decision-making, the congestion level con_L is divided into low and high categories based on threshold T as given in Eq. 4.

$$con_L = \begin{cases} LOW, con(n_i) < T \\ HIGH, con(n_i) > T \end{cases} \tag{4}$$

The reliability of the IoT devices on the link provides a vital parameter based on traffic flow TF and packet lost ratio PLR, evaluating the robust decision while selecting the cost-effective channel and directly influencing the stability of the network, shown in Eq. 5.

$$Rel(i,j) = {1}/{(\frac{1}{TF} + \delta.PLR)} \tag{5}$$

Later, based on reinforcement learning, the proposed model computes the dynamic reward by incorporating the mechanism of updating weights in terms of learning rate and a reward function, as given in Eq. 6.

$$R_{n_i}(t\prime) = R_{n_i}(t).(1 - \alpha) + \alpha.R(n_i) \tag{6}$$

where
$R_{n_i}(t\prime)$ is the updated reward of the node n_i at time $t\prime$.
$R_{n_i}(t)$ denotes the exiting reward at time t.
α is the learning rate and its value must exist between 0 to 1.

This recursion process continues, with each updated reward new reward $R_{n_i}(t\prime)$ at time $t\prime$ is computed based on the previous reward weight $R_{n_i}(t)$; accordingly, the proposed model can learn and adopt the changes in networks. The flowchart of the proposed model in terms of efficient and intelligent data management for IoT applications using reinforcement learning is depicted in Fig. 2. After the formulation of the communication system, the initial weighted value for each node is determined and stored inside the local tables. Next, the source node identifies neighbors, and the reward value is computed using various metrics. Later, they are arranged inside the routing chains, and exploring the iterative process leads to the transfer of the proposed model in a recurrent learning state. Accordingly, the agents refine the routing decision based on the previous reward value and feedback. Table 1 describes the security measure of our proposed model against threats to cognitive networks. The distributed keys between devices comprised verification stages that enabled their decryption and authentication for authorized access control. The proposed model monitors the behavioral patterns and utilizes the unique identities of the devices for their verification. The malicious devices are marked with negative flags due to unexpected congestion or frequently invalid authentication attempts. The combination of blockchain undeniable ledger establishes the chain of data blocks. As a result, if any tampering occurs in the data block disrupts the generated hash of subsequent blocks, thus making it able to detect data tampering and accordingly, it attains data integrity. Moreover, the proposed model provides decentralized computing methods for IoT devices. In this case, if any device is faulty or compromised, then the distributed security methods isolate the faulty device

Fig. 2 Working flow of the proposed cognitive decision-making model using reinforcement learning
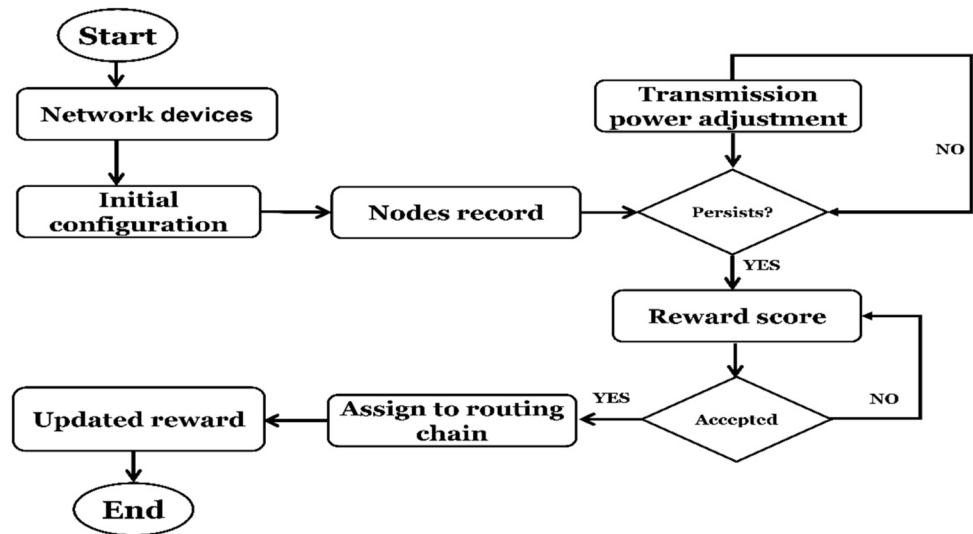

Table 1 Threats identification using security measurements

Proposed security measurement	Threat detection
Distribution of cryptographic keys and verification	Detects unauthorized devices using failed key verification
Detection of malicious device	By exploring abnormal behavior of the devices and failing to prove identity verification
Data integrity integrated blockchain	Using blockchain immutability detects tampered data and verification of data hashes
Resilience against key attacks	Regular updates of cryptographic methods and key renewal identify key attacks and potential vulnerabilities
Fault tolerance with decentralized control	Isolates the compromised nodes, and prevents cascading failures or attacks
Security practices and energy awareness	Maintaining energy efficiency while monitoring device performance to detect malicious behavior

affecting the rest of the network devices, and accordingly, it preserves the functionality of the system.

In the next phase, the proposed model explores blockchain technology with the combination of symmetric keys and protects the data in the form of interconnect blocks. The hash of each block is interconnected with the previous block which makes it difficult to decrypt the entire chain. In the proposed model, the local edges are required to generate and maintain the block of chains. Initially, the edge node distributes a symmetric key K_i for each device using the private key Pk and generates a digital signature dig_s to authenticate the keys. Let us consider $N_1, \ldots, N_k$ are set of neighbors, then individually signed symmetric keys SK_{signed} can be defined in Eq. 7.

$$SK_{signed} = dig_s(K_i, Pk) \tag{7}$$

In this way, the generated symmetric key is distributed securely and authenticated. Moreover, the integrated blockchain by edge nodes ensures the authenticity and integrity of the key management process by interconnecting keys at state $t + 1$ in a secured chain Sec_{Ch}, shown by Eq. 8.

$$Sec_{Ch}(t + 1) = H(Sec_{Ch}(t), SK_{signed}) \tag{8}$$

where $H(K_i)$ denotes the hash of the original private key Pk. Later, the set of data blocks D_i initiated the process of integrated data encryption E, combining $\propto_i$ a learning factor, as given in Eq. 9.

$$E = \sum_{i=1}^{k} \propto_i . (SK_{signed_i} \oplus D_i) \tag{9}$$

In Fig. 3, security is provided for the extracted route with the support of edges and integrated blockchain encryption. Devices are shared with signed symmetric keys from the edges and after verification, data blocks are encrypted in the chaining method. Each encrypted block connects with the previous block to make it harder for malicious devices to affect the integrity of crucial data. The proposed security system preserves data privacy and simultaneously authenticates devices over unreliable

Fig. 3 Security measurement of the proposed model using protected keys with integrated blockchain nodes
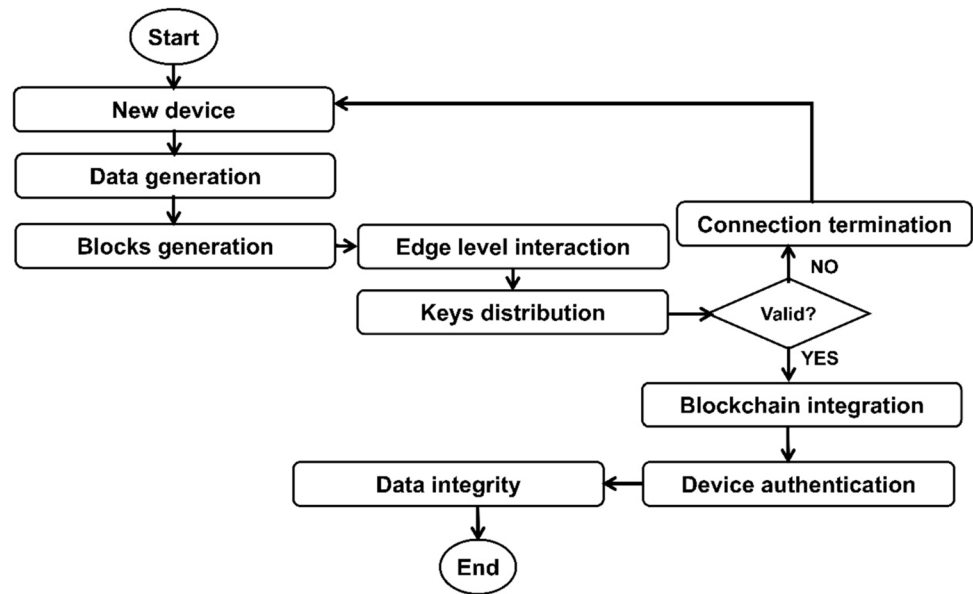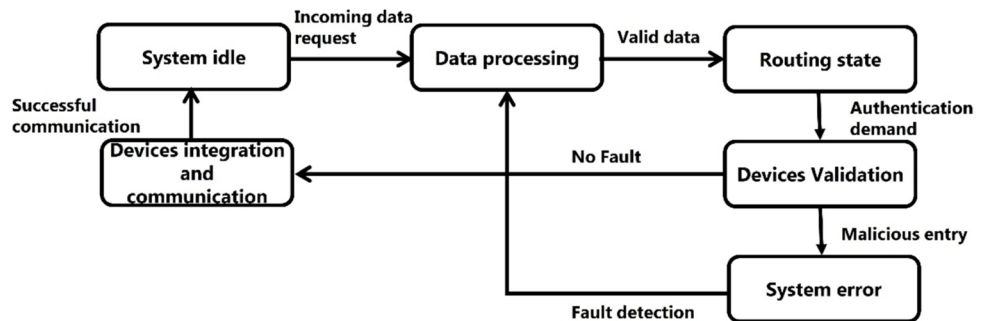

Fig. 4 States interaction of the proposed edged-based intelligent cognitive communication model

channels. The connection is terminated if any faulty request is generated by the source device. In Fig. 4, different states of the proposed model and their associated interaction are depicted. The security analysis of our proposed model for attaining fault tolerance and secured IoT communication is highlighted as follows.

Secured Reinforcement Learning for IoT Networks in Smart City: A Simulation Evaluation

In this section, we use simulations to explore reinforcement learning for testing the behavior of the proposed model by connecting varying sensors, gateways, and sink nodes to collect data in a smart city IoT network. Both the gateways and the nodes are mobile. The number of faulty nodes ranges from 10 to 20. The flood false packet generates bogus network traffic and increases the congestion, which is moderated by reinforcement learning–based decision-making. Moreover, these nodes are explored to detect

Table 2 Default parameters

Parameter	Value
Number of requests	10–50
Traffic type	CBR
Initial energy	2 j
Transmission power	5 m
Simulations	60
Nodes placement	Random
Simulation rounds	10,000 s
Simulation dimension	5000 m × 5000 m
Energy model	IEEE 802.15.4
Faulty devices	10–20
Device load	10–50 bytes

the privacy attacks on the communication model and evaluate its efficiency. We perform experiments using simulations across a network dimension of 5000 m × 5000 m. To capture the data from log files and extract the necessary

Fig. 5 Performance of packet
drop ratio with varying device
load and number of requests
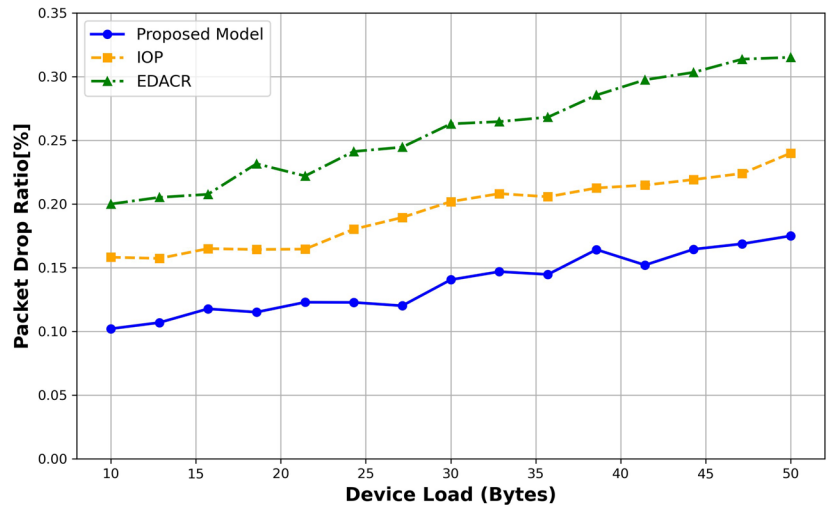
(a)
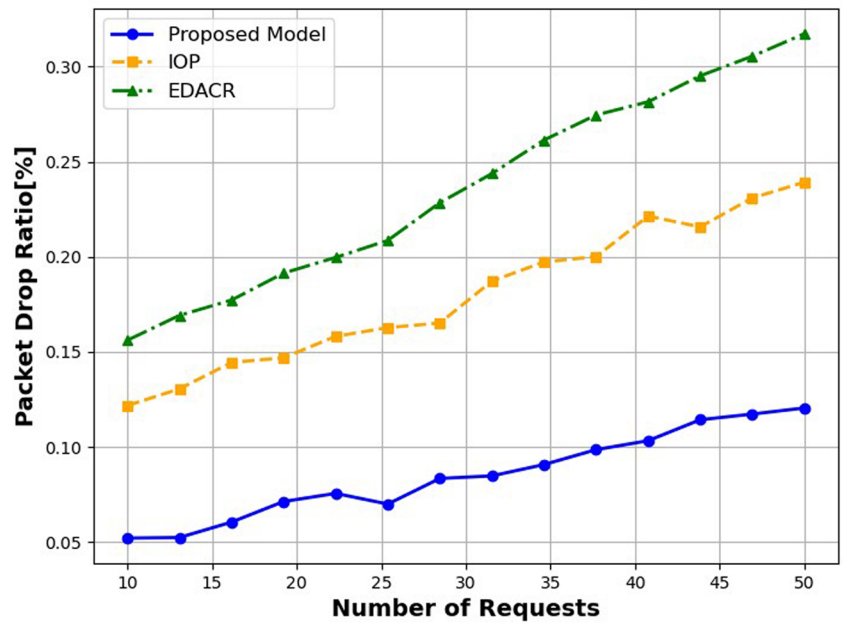
(b)

information for the results analysis, 60 simulations were conducted.

The purpose of the conducted simulations is to model real-world crucial operations such as traffic management and environmental monitoring. In these smart activities, security, efficient resource management, and timely response are critical. Table 2 defines the default parameters of the simulation. In terms of network throughput, packet drop ratio, node overhead, and energy consumption, the performance of the proposed model is evaluated as compared to existing solutions over varying device load (10–50 bytes) and number of requests (10–50).

Results Analysis

We compared the performance of the proposed model to the existing methods in terms of packet drop ratio in Fig. 5a and b. The proposed model significantly lowers the packet drop ratio by 27% and 38%. It is due to the integration of distributed decisions by exploring the optimization criteria and extracting the most reliable communication links for data routing. The weighted value explores link interference parameters in computation enabling the identification of the most reliable forwarding path and ensuring a high degree of data reception to the destination. Moreover, the security methods avoid malicious devices forwarding false route

request packets and reduce malicious traffic over the IoT system. As a result, with nominal link congestion and network traffic flowing, the proposed model lengthens the stability of links and ultimately improves the packet drop ratio in real-time data analytics. Figure 6a and b demonstrates the performance of energy consumption for the proposed model under varying device loads and number of requests. Comparing the proposed model to existing solutions, it was found to significantly improve energy consumption by 27% and 34%. It is the result of examining security techniques to build mutual trust and utilizing the secured communication process on the network edges. Also, the intermediate device uses a decision-making process using multi-facets to balance the routing data, and ignoring the same paths when sending the data. It decreases the power consumption for the constraint nodes and increases longevity for the

Fig. 6 Performance of energy consumption with varying device load and number of requests
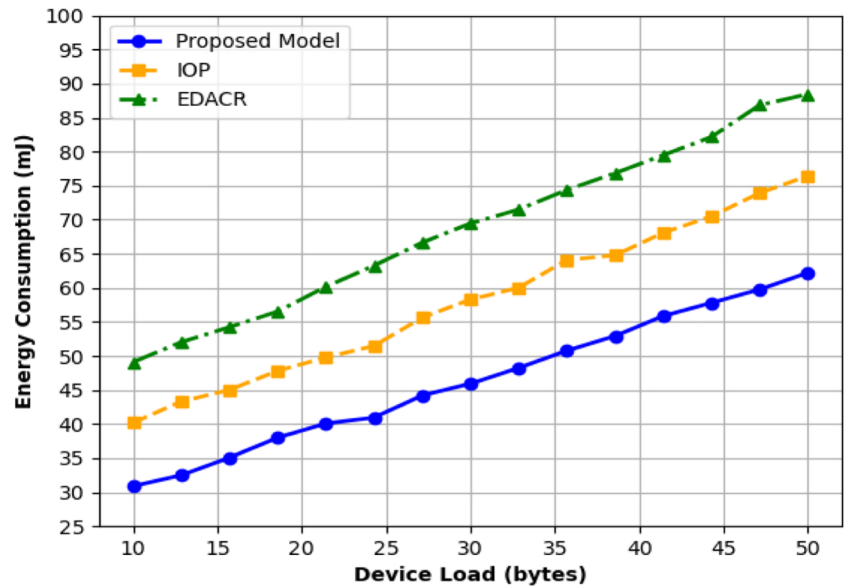

(a)
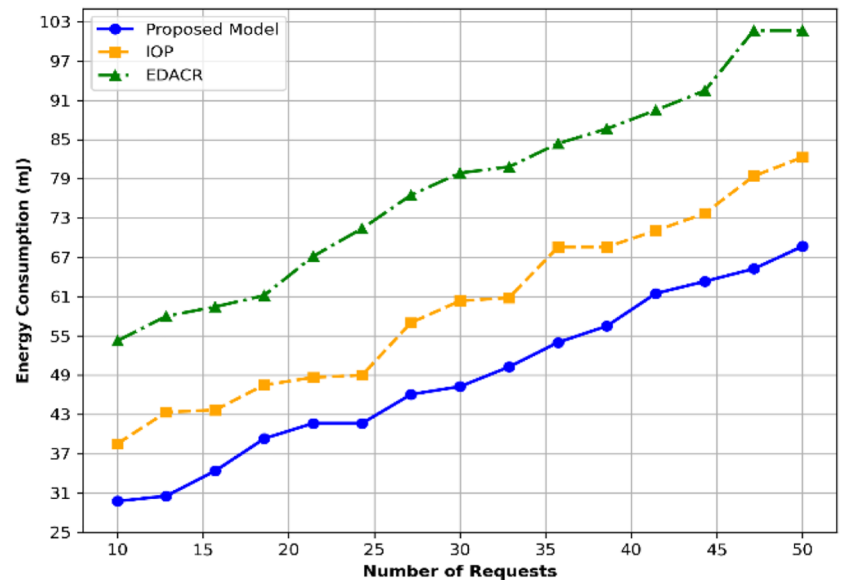
(b)

constraint-enabled routes. Furthermore, edged devices are stronger and validate the incoming data before transmitting it to end users. This strategy prevents energy outflows near processing servers and forms sustainable networks. Figure 7a and b shows the evaluation comparison of the proposed model with the existing solutions for communication overhead. When designing and implementing IoT networks, it is imperative to realize the significance of node overhead, particularly in constrained resources. According

to the performance results, the proposed model significantly reduces the node overhead against varying sensors and load by 28.6% and 35%, respectively. This is because the proposed model explores the iterative principle for the accomplishment of forwarding decisions and efficiently controls the energy and computing distribution across sensors. It re-evaluates the routing nodes whenever any interrupted intermediate links are identified due to high energy usage. Furthermore, the proposed model allows for more effective

Fig. 7 Performance of communication overhead with varying device load and number of requests
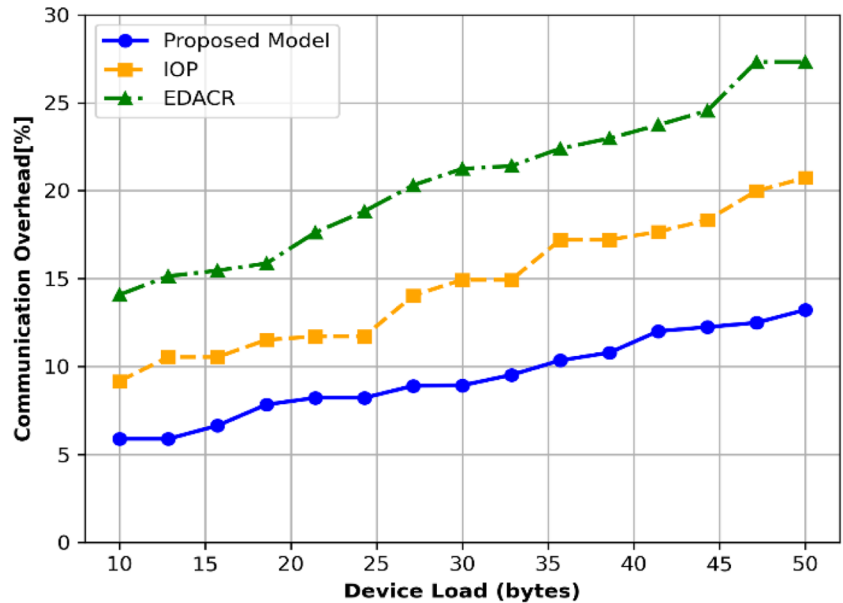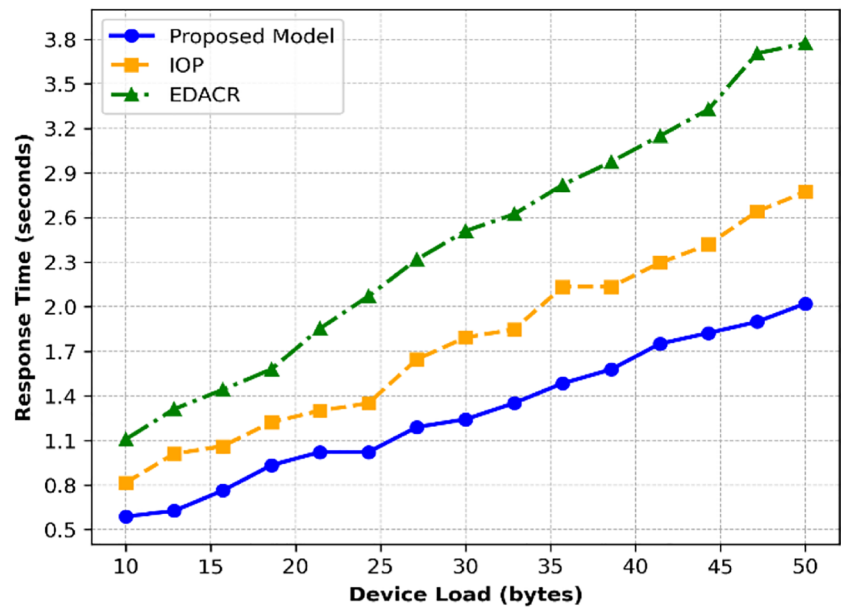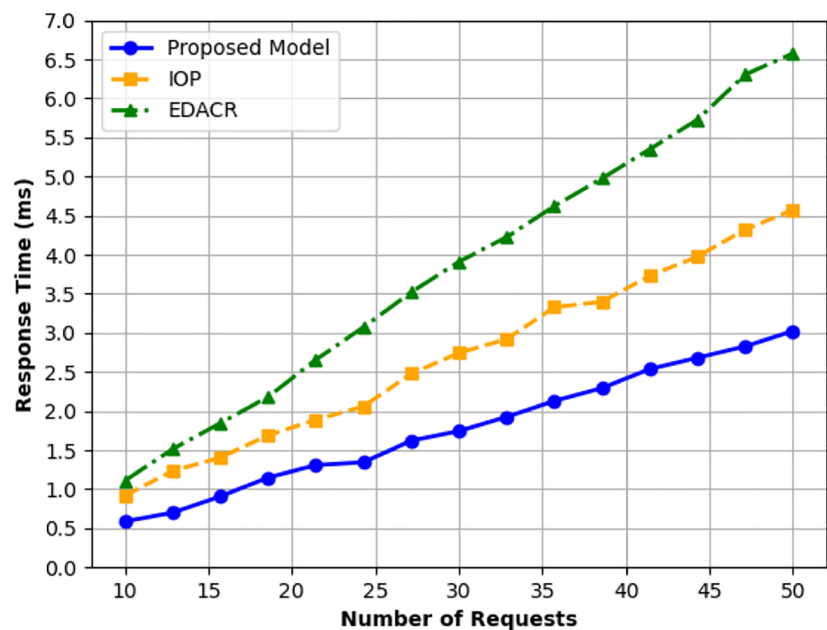

(a)
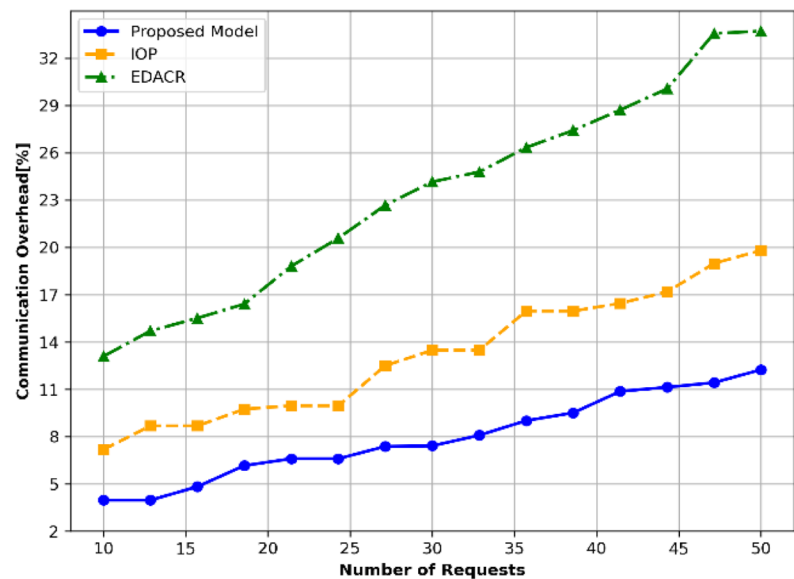
(b)

Fig. 8 Performance of response time with varying device load and number of requests

(a)

(b)

utilization of the network resources by incorporating link interference. In Fig. 8a and b, the performance evaluation of the proposed model is compared with existing solutions in terms of response time. The findings showed that, for varying device load and the number of requests, the proposed model improved response time by 23% and 29%, respectively. This is because the proposed model uses a weighted method to compute the initial weight for the formulation of routing solutions. Furthermore, intelligent computing

adopted to load the traffic and efficiently balance the congestion on the constraint devices. It improves the stability of the route and also transmits a high amount of data over the links for a crucial environment. Moreover, data from IoT applications is not sent for processing via wireless links that are frequently damaged or compromised, thus enhancing the performance of the system in terms of response time under crucial conditions.

Conclusion

Cognitive networks with IoT systems leverage many advanced techniques for the development of real-time dynamic applications. It ensures a timely communication system with efficient decision-making strategies for end users. With the integration of edges, many systems optimize the network behavior and increase the efficiency of constraint devices. However, the main research problem in IoT-driven cognitive networks is the growth of adaptive and learning algorithms to attain cost-effective resource allocation and improve energy efficiency for constrained environments. Moreover, ensuring real-time processing of IoT data with low overhead on network devices while preserving data privacy. This work presents a predictive model using reinforcement learning to maintain the routes among devices by exploiting contextual information of the environment. In addition, the involvement of network edges provides trusted data collectors with authentic and lightweight verification methods using cryptography. The combination of blockchain nodes in the routing chains not only achieves data privacy but also provides information integrity using the computation of hashes. It minimizes the risk of data compromise by implementing continuous monitoring and fault tolerance techniques, thus confirming trusted IoT environments. In future work, we intend to improve the performance of the proposed model with efficient load distribution on heterogeneous devices and consider the mobile SDN controller to deal with scalability. In addition, the advanced machine learning algorithms need to be seamlessly integrated with the proposed model to refine the decision-making system and make it sustainable for IoT network, particularly for limited resources.

Declarations

Conflict of Interest The authors declare no competing interests.

References

1. Sharma B, Obaidat MS. Comparative analysis of IoT based products, technology and integration of IoT with cloud computing. IET Networks. 2020;9(2):43–7.

2. Alsamhi SH, Afghah F, Sahal R, Hawbani A, Al-qaness MA, Lee B, Guizani M. Green internet of things using UAVs in B5G networks: a review of applications and strategies. Ad Hoc Netw. 2021;117:102505.

3. Deva Priya M, Rajkumar M, Karthik S, Christy Jeba Malar A, Kanmani R, Sandhya G, Anitha Rajakumari P. Emperor Penguin Optimization Algorithm and M-Tree-Based Multi-Constraint Multicast Ad Hoc On-Demand Distance Vector Routing Protocol for MANETs. In: 3rd EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing. Springer: 2022.

4. Perez AJ, Siddiqui F, Zeadally S, Lane D. A review of IoT systems to enable independence for the elderly and disabled individuals. Internet Things. 2023;21:100653.

5. Raihan A. An overview of the implications of artificial intelligence (AI) in sixth generation (6G) communication network. Res Briefs Inf Commun Technology Evol. 2023;9:120–46.

6. Bhuiyan MN, Rahman MM, Billah MM, Saha D. Internet of things (IoT): a review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. IEEE Internet Things J. 2021;8(13):10474–98.

7. Muzakkir Hussain M, Saad Alam M, Sufyan Beg M. Fog computing for smart grid transition: requirements, prospects, status quos, and challenges. in 2nd EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing: BDCC 2019. Springer; 2021.

8. Ali A, et al. A Resource-Aware Multi-Graph Neural Network for Urban Traffic Flow Prediction in Multi-Access Edge Computing Systems. IEEE Transactions on Consumer Electronics. 2024;70(4):7252–65.

9. Salahdine F, Han T, Zhang N. 5G, 6G, and Beyond: Recent advances and future challenges. Ann Telecommun. 2023;78:525–49.

10. Tan L, Xiao H, Yu K, Aloqaily M, Jararweh Y. A blockchain-empowered crowdsourcing system for 5G-enabled smart cities. Comput Standards Interfaces. 2021;76:103517.

11. Krishnamoorthy S, Dua A, Gupta S. Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. Journal of Ambient Intelligence and Humanized Computing. 2023;14(1)361–407.

12. Torres Vega M, Liaskos C, Abadal S, Papapetrou E, Jain A, Mouhouche B, Kalem G, Ergüt S, Mach M, Sabol T. Immersive interconnected virtual and augmented reality: a 5G and IoT perspective. J Netw Syst Manag. 2020;28:796–826.

13. Walia GK, Kumar M, Gill SS. AI-Empowered Fog/Edge Resource Management for IoT Applications: A Comprehensive Review, Research Challenges, and Future Perspectives. IEEE Communications Surveys & Tutorials. 2024;26(1):619–69. https://doi.org/10.1109/COMST.2023.3338015.

14. Zhang P, Chen N, Shen S, Yu S, Kumar N, Hsu C-H. AI-Enabled Space-Air-Ground Integrated Networks: Management and Optimization. IEEE Network. 2024;38(2):186–92.

15. Ullah I, Khan IU, Ouaissa M, Ouaissa M, El Hajjami S. Future communication systems using artificial intelligence, Internet of Things and data science. CRC Press; 2024.

16. Gill SS, Xu M, Ottaviani C, Patros P, Bahsoon R, Shaghaghi A, Golec M, Stankovski V, Wu H, Abraham A. AI for next generation computing: emerging trends and future directions. Internet Things. 2022;19:100514.

17. Hasan MK, Habib AA, Shukur Z, Ibrahim F, Islam S, Razzaque MA. Review on cyber-physical and cyber-security system in smart grid: standards, protocols, constraints, and recommendations. J Netw Comput Appl. 2023;209:103540.

18. Xenofontos C, Zografopoulos I, Konstantinou C, Jolfaei A, Khan MK, Choo K-KR. Consumer, commercial, and industrial iot (in) security: attack taxonomy and case studies. IEEE Internet Things J. 2021;9(1):199–221.

19. Newaz AI, Sikder AK, Rahman MA, Uluagac AS. A survey on security and privacy issues in modern healthcare systems: attacks and defenses. ACM Trans Comput Healthc. 2021;2(3):1–44.

20. Islam N, Haseeb K, Rehman A, Alam T, Jeon G. An adaptive and secure routes migration model for the sustainable cloud of things. Clust Comput. 2023;26(2):1631–42.

21. Chinnasamy P, Babu GC, Ayyasamy RK, Amutha S, Sinha K, Balaram A. Blockchain 6G-based wireless network security management with optimization using machine learning techniques. Sensors. 2024;24(18):6143.

22. Islam N, Haseeb K, Ali M, Jeon G. Secured protocol with collaborative IoT-enabled sustainable communication using artificial intelligence technique. Sustainability. 2022;14(14):8919.

23. Jamshed MA, Ali K, Abbasi QH, Imran MA, Ur-Rehman M. Challenges, applications, and future of wireless sensors in Internet of Things: a review. IEEE Sens J. 2022;22(6):5482–94.

24. Nurlan Z, Zhukabayeva T, Othman M, Adamova A, Zhakiyev N. Wireless sensor network as a mesh: vision and challenges. IEEE Access. 2021;10:46–67.

25. Carvalho G, Cabral B, Pereira V, Bernardino J. Edge computing: current trends, research challenges and future directions. Computing. 2021;103(5):993–1023.

26. Chinnasamy P, Vinothini C, Arun Kumar S, Allwyn Sundarraj A, Annlin Jeba S, Praveena V. Blockchain technology in smart-cities, in Blockchain technology: applications and challenges. Springer; 2021, p. 179–200.

27. Wahid A, Abideen SZU, Imtiaz N, Kamal MM, Alharbi A, Tolba A, Al-Khasawneh M, Ullah I. Enhancing security with hybrid active-passive RIS: a DRL approach against eavesdropping and jamming. IEEE Access, 2024.

28. Bangotra DK, Singh Y, Selwal A, Kumar N, Singh PK, Hong W-C. An intelligent opportunistic routing algorithm for wireless sensor networks and its application towards e-healthcare. Sensors. 2020;20(14):3887.

29. Yao A, Jiang F, Li X, Dong C, Xu J, Xu Y, Li G, Liu X. A novel security framework for edge computing based UAV delivery system. in 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE; 2021.

30. Wang D, Liu J, Yao D, Member I. An energy-efficient distributed adaptive cooperative routing based on reinforcement learning in wireless multimedia sensor networks. Comput Netw. 2020;178:107313.

31. Bangotra DK, Singh Y, Selwal A, Kumar N, Singh PK. A trust based secure intelligent opportunistic routing protocol for wireless sensor networks. Wireless Pers Commun. 2022;127(2):1045–66.

32. Chinnasamy P, Vinodhini B, Praveena V, Vinothini C, Sujitha BB. Blockchain based access control and data sharing systems for smart devices. in Journal of Physics: Conference Series. IOP Publishing; 2021.

33. Yao A, Pal S, Li X, Zhang Z, Dong C, Jiang F, Liu X. A privacy-preserving location data collection framework for intelligent systems in edge computing. Ad Hoc Netw. 2024;161:103532.

34. Yao A, Pal S, Dong C, Li X, Liu X. A framework for user biometric privacy protection in UAV delivery systems with edge computing. in 2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops). IEEE; 2024.