Reliable Internet of Things

Subjects: Computer Science, Interdisciplinary Applications

Contributor: Mohammad Zubair Khan

The Internet of Things (IoT) is a vital component of many future industries. By intelligent integration of sensors, wireless communications, computing techniques, and data analytics, IoT can increase productivity and efficiency of industries. Reliability of data transmission is key to realize several applications offered by IoT.

Keywords: IoT ; resource allocation ; latency ; security ; metrics

1. Introduction

The Internet of Things (IoT) is one of the important technologies of this era that can add automation and smartness in several sectors such as transportation, health care, industries, agriculture, energy, and infotainment. It works by deploying sensors on different devices used in these sectors, hence allowing the measurement of important real-time data. These data are transmitted to the remote servers where it can be analyzed, and intelligent actions can be taken based on it [1][2][3][4][5][6][7][8][9][10][11][12][13][14][15].

IoT enables many important applications, including intelligent traffic management, safety-aware autonomous driving, saving electricity usage using smart grids, remote patient monitoring, machine health monitoring, smart industrial automation, and smart home security solutions [4][5]. In the era of Industry 4.0 and 6G communications, IoT applications will revolutionize how different industries operate.

There are several use cases of IoT in these industries. It can facilitate smart usage of electricity and communication flow between devices and the grid. Related to smart transportation, IoT can provide safety to drivers and passengers. Similarly, health care has several potential benefits offered by IoT regarding patient health monitoring and early diagnosis. IoT can also ensure health monitoring of machines used in various industries, thus improving the lifetime and working of the equipment.

The three major components of IoT will be sensing, communications, and data analytics. In the sensing part, various sensors such as temperature, current, humidity, heart rate, etc., will be deployed to get regular data measurements. In the communications part, technologies such as 6G will disseminate data from sensors to the cloud servers. Finally, data analytic algorithms will be extensively used to improve the working of IoT applications.

The successful working of IoT applications relies on reliable data transmission between sensors and servers. Reliability refers to robust communication with a high packet delivery ratio, low latency, and defense against network attacks. Each IoT application may have different Quality of Service (QoS) requirements. To realize a reliable and robust IoT network, meeting the QoS requirements is needed [16][17][18][19][20][21][22][23][24][25].

Efficient data transmission is a key challenge to ensure reliable IoT applications. This means that data are transmitted at a high data rate such that latency is within the QoS requirement. This is possible when resources such as spectrum utilization, medium access, transmit power, computation task offloading to fog nodes, etc., is optimized. Moreover, privacy and secrecy of communication, along with maintaining data integrity, are required.

2. Reliable Data Transmission in IoT Network

Figure 1 presented three major components of reliable IoT data dissemination. These include resource allocation, latency management, and security.

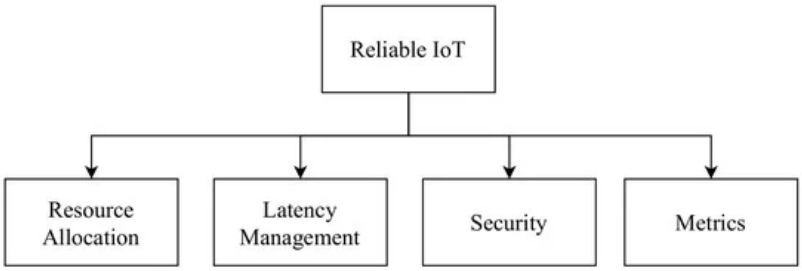

Figure 1. Key components of Reliable Data Transmission in IoT.

Efficient resource allocation is important for reliably sharing data between IoT nodes and servers. As the spectrum resource is limited due to large data generated by IoT nodes, it is important to propose intelligent spectrum utilization techniques. Techniques such as cognitive spectrum management could be used for sharing of spectrum bands by several IoT nodes. Transmit power is also an important resource that needs to be allocated carefully. To save energy of IoT nodes so that they can stay active for longer periods without charging, adaptive transmit power techniques are required.

Fog computing is a vital part of future IoT networks. Fog nodes located near the IoT devices provide storage and computational capacity to the IoT network. IoT networks can place popular and most useful content in the cache storage of these fog nodes. Hence, cache storage allocation is an important challenge. Moreover, IoT nodes may not perform all tasks locally and, therefore, will offload many tasks to these fog nodes. In this regard, optimal task offloading algorithms are needed to ensure that the computational capacity resource of fog nodes is used efficiently.

Latency management is another crucial unit of reliable data transmission in IoT. IoT applications may not work well if data are not shared within the desired latency. Many new applications such as autonomous driving and industrial automation have stringent latency requirements, and hence, latency management is needed. In this regard, smart retransmissions can add diversity and enhance the probability of quick packet reception at the receiver. Moreover, optimal medium access techniques need to be developed to allow IoT nodes quick and fair channel access.

Accurate data traffic prediction can support latency management techniques as knowledge of upcoming traffic at an IoT server, and fog node equips it to handle it better. Hence, Artificial Intelligence (AI) based techniques that forecast the frequency and size of data can be very useful. Besides, other network technologies can support IoT networks to transmit their data quickly. In this regard, Unmanned Aerial Vehicle (UAV) and vehicular network has the potential to act as a relay for data traffic generated by IoT nodes [26][27][28][29][30][31][32][33][34][35].

Security is an essential component of reliable data transmission in IoT. Several attacks may be generated in an IoT network that can compromise the privacy and confidentiality of data transmitted. Moreover, malicious nodes can insert fake and wrong data in the network that can affect the decision-making of IoT applications. To tackle this issue, advanced cryptographic techniques are needed that can ensure the security of transmitted data while keeping the required overhead to a minimum. As an increase in the security overhead can result in higher data latency, tradeoff between security robustness and latency needs to be evaluated.

Blockchain is an upcoming technology that can provide robust security to IoT devices. Hence, blockchain-based solutions need to be developed in the context of IoT applications. Other security techniques such as physical layer security can also improve the reliability of IoT networks. These techniques can work in collaboration with cryptographic techniques to provide a robust solution. Lastly, data integrity attacks and anomaly detection schemes are also required to ensure that correct data are received based on which decisions can be made.

3. Review of Recent Work in Literature on Reliable Data Transmission in IoT

3.1. Resource Allocation

Resource allocation is an important area of research for IoT applications. Since IoT devices are constrained in energy, computation, and transmission, intelligent and novel resource allocation techniques are needed. As shown in **Figure 2**, resources such as spectrum, the transmission power of IoT nodes, cache storage of IoT enabled fog nodes, computational capacity of IoT nodes and fog nodes, and data rate needs to be carefully allocated. We present a review of recent work related to efficient resource allocation for IoT networks in **Table 1**. In [36], the authors consider a Wireless Powered Communication Network (WPCN) based wireless power transfer scenario. The communication between Access Point (AP) and mobile users is the focus of the paper. The work provides an optimal algorithm to allocated resources,

including channel selection, transmission time, and transmit power. The joint optimization problem becomes non-convex and is solved using an iterative algorithm. Simulation results show improved sum-rate and reduced convergence time of the proposed algorithm.

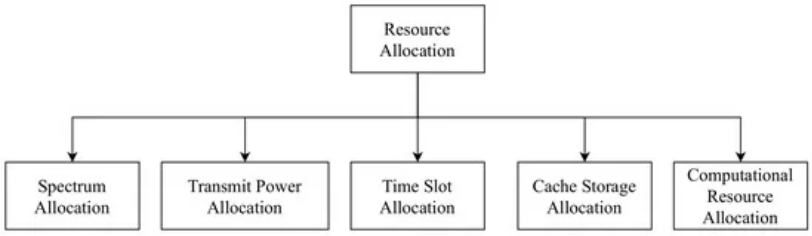

Figure 2. Different categories of recent work in Resource Allocation in IoT.

Table 1. Resource allocation in IoT: Recent literature review (S = Spectrum Allocation, P = Transmit Power Allocation, T = Time Slot Allocation, C = Cache Storage Allocation, M = Computational Resource Allocation).

Scenario	S	P	T	C	M	Key Idea	Results
Wireless power transfer [36]	✗	✓	✓	✗	✗	**AP and mobile user communication Optimal channel selection Optimal time resource allocation Optimal power resource allocation Iterative algorithm for non-convex optimization**	**Improved sum-rate Reduced convergence time**
Edge IoT [37]	✗	✗	✗	✗	✓	**IoT tasks offloaded to edge servers Q-learning to allocate resources Utility maximized and fairness Online Q-learning scheme Large state and action space Reduce computation overhead Reduce convergence time**	**Maximized application utility Improved fairness**
Smart factory [38]	✓	✗	✗	✗	✗	**IoT enabled machines Periodic data sharing with the server Spectrum allocation in variable interference Graph-Based Algorithm (GBA) used Maximum weight matching in bipartite graphs**	**Increased transmitting users Reduced transmission delay**
Content-centric computing IoT [39]	✗	✗	✗	✓	✗	**Improve Quality of Experience (QoE) Factor such as Mean Opinion Score (MOS) Cache resource allocation to improve QoE Shortest Path Tree (SPT) algorithm Deep-Q learning algorithm**	**Increased QoE Reduced network cost**
Energy self-reliant IoT network [40]	✗	✓	✓	✗	✗	**Relay node harvests renewable energy Relay node transmits data Relays provide RF power to IoT nodes Solved time and power resource allocation Lyapunov optimization for max throughput**	**Increased data rate Increased throughput**
UAV network supporting IoT [41]	✓	✓	✗	✗	✗	**IoT devices grouped into equal-sized clusters Matching theory-based algorithm Match UAV sub-channels to IoT nodes Interference is minimized Alternate optimization used Optimized placement of UAV nodes Optimized transmit power of IoT nodes**	**Reliable power selection Reduced power of IoT nodes**

In [37], the authors consider an edge IoT scenario where IoT devices offload their tasks to nearby edge nodes. The authors use machine learning algorithms for efficient task offloading. A Q-learning-based algorithm is developed to allocate computational resources. The goal of the protocol is to maximize the utility of applications and achieve fairness. Moreover, an online Q-learning scheme to handle large state and action space is proposed, which reduces computation overhead and convergence time. The performance evaluation shows maximized IoT application utility and improved resource allocation fairness.

The authors in [38] consider a smart factory scenario where IoT-enabled machines periodically share data with the server. These data can include different parameters of the machines. The work proposes a spectrum allocation technique in the case when bands are impacted by interference differently. A Graph-Based Allocation (GBA) algorithm is used for resource allocation. The spectrum allocation problem is formulated as a bipartite graph ad successive maximum weight matching is usedThe results show an increased number of users that transmit data. In addition, data transmission delay is considerably reduced.

The work in [39] considers a content-centric IoT scenario where devices offload their data to cache storage of fog nodes. The goal of the two proposed techniques is to improve user satisfaction in terms of Quality of Experience (QoE) by using efficient cache resource allocation. Factors such as the Mean Opinion Score (MOS) are considered while computing the QoE. The first technique uses Shortest Path Tree (SPT) algorithm, whereas the second technique uses the Deep Q-learning algorithmThe results show an increase in QoE and reduced network cost.

In [40], an energy self-reliant IoT network is considered. Relay nodes are chosen in the network that harvests energy using renewable sources. The relay node serves two purposes, enabling data transmission by forwarding signals from the source to the destination and powering multiple IoT nodes using RF signals. The authors solve the time and resource allocation problem using Lyapunov optimizationThe results show an increased achievable data rate and throughput.

The work in [41] considers a UAV network that supports IoT devices in terms of providing computation resources. IoT devices are grouped into equal-sized clusters. A matching theory-based algorithm is proposed that matches UAV sub-channels to IoT nodes such that interference is minimized. The work uses alternate optimization for optimal placement of UAVs and transmit power selection of IoT nodesThe results show improved reliability to achieve optimal transmit power. Moreover, IoT nodes use lower transmit power values when using the proposed algorithm.

3.2. Latency Management

Latency is a vital QoS indicator for IoT applications. Most applications are sensitive to latency and need a lower latency value within a threshold to ensure reliable communication. As shown in **Figure 3**, techniques such as smart retransmissions, resource allocation, multiple access and physical layer techniques, traffic prediction, and cooperation from other networks is used for improving the latency of IoT. This subsection provides an overview of work done in latency management in IoT as shown in **Table 2**.

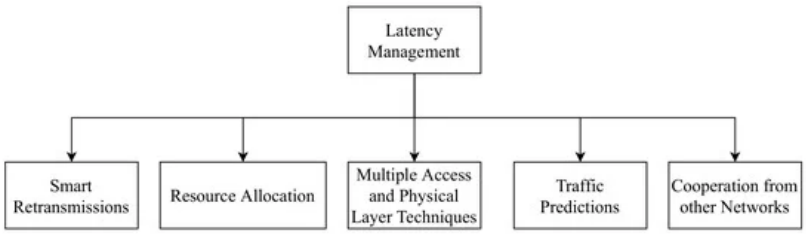

Figure 3. Different categories of recent work in Latency management in IoT.

Table 2. Latency management in IoT: Recent literature review (R = Smart Retransmissions, A = Resource Allocation, M = Multiple Access and Physical Layer Techniques, P = Traffic Prediction, O = Cooperation from other networks such as UAVs).

Scenario	R	A	M	P	O	Key Idea	Results
NB-IoT [42]	✓	✗	✓	✗	✗	**Retransmissions impact on energy and latency Optimal control & data channel duration selection Optimal selection of coverage class per user**	**Reduced energy consumption Reduced latency**
multiple RATs to connect with MEC [43]	✗	✓	✗	✗	✗	**Optimal task offloading decisions Amount of task locally computed Amount of task computed at MEC server Task splitting between MEC servers Optimal transmit power selection Optimal RAT selection for task offloading Alternate Convex Search (ACS) algorithm**	**Reduced energy consumption Reduced latency**

Scenario	R	A	M	P	O	Key Idea	Results
Cloud with several VNFs [44]	✗	✓	✗	✓	✗	**VNFs are mapped to different applications VNFs allocation to reduce latency Regression for predicting application demand Optimal allocation of VNFs as per demand Initial offline training followed by online training**	**Reduced latency Improved prediction accuracy**
Terrestrial networks, satellite IoT and MEC [45]	✗	✓	✗	✗	✗	**Data from IoT to satellites and gateways Satellites have energy constraints Data offloaded to gateways for processing Optimal IoT association with a satellite & a gateway Lagrange multiplier and DRL used**	**Reduced latency Reduced energy cost**
UAV assisted MEC based IoT [46]	✗	✓	✓	✗	✓	**UAV facilitates storage and computation UAV improves network coverage using relaying Problem divided into three subproblems First, IoT node and UAV association Second, communication resource scheduling Third, the UAV placement**	**Reduced latency**
Semi-blind downlink NOMA based IoT [47]	✓	✗	✗	✗	✗	**Improve SIC technique Interference AICA used**	**Improved signal to noise ratio Reduced latency**

The authors in [42] considered a narrowband IoT (NB-IoT) scenario where an increased number of retransmissions in the standard improves the packet delivery ratio but increases the energy consumption and latency. The proposed technique computes optimal durations of the control channel and data channel. Moreover, the authors also find out the optimal coverage class for each user where coverage class defines the number of retransmissions allowed. Simulation results highlight reduced energy consumption and reduced latency achieved by the proposed protocol.

The work in [43] considers a scenario where IoT devices use multiple Radio Access Technologies (RATs) to transmit data to the Mobile Edge Computing (MEC) server. The proposed protocol computes optimal task offloading decisions, including the number of tasks locally computed at IoT device, amount of task computed at MEC server, and task splitting between different MEC servers. Besides, optimal transmit power and RAT selection for task offloading are also proposed. The developed optimization problem is solved using the Alternate Convex Search (ACS) algorithm. The results highlight reduced energy consumption as well as reduced latency when the proposed protocol is used.

In [44], the authors consider a cloud scenario with several Virtual Network Functions (VNFs). VNFs are mapped to different applications such as delay-sensitive, mission-critical, and latency tolerant. The goal of the proposed technique is the efficient allocation of VNFs to reduce latency. The authors use a regression algorithm to predict the demand of each application type and make allocations accordingly. The proposed algorithm works initially on offline training. This is followed by online training afterward.

The work in [45] considers a terrestrial network scenario composed of IoT-enabled satellites and a MEC server. IoT nodes collect data and send it to satellites or satellite gateways for further processing. As satellites have energy constraints, they offload the IoT data to the gateways for further processing. The proposed work finds an optimal association between a satellite and a gateway using Lagrange multiplier and Deep Reinforcement Learning (DRL) techniquesThe results highlight reduced latency of IoT data at a reduced energy cost.

In [46], a UAV-assisted MEC-based IoT network scenario is considered. UAV facilitates computing in terms of storage and computation service. UAV can also improve network coverage by providing relaying services to overcome poor channel conditions. The problem is divided into three sub-problems. The first one deals with IoT nodes and UAV association, the second one handles scheduling of communication resources, and the last one manages UAV placement. The proposed algorithm shows low latency as compared to other related techniques.

The work in [47] considers a semi-blind Non-Orthogonal Multiple Access (NOMA) based IoT scenario. The proposed technique uses an interference Alignment Independent Component Analysis (AICA) as compared to the traditional Successive Interference Cancellation (SIC) techniqueThe results highlight improved signal-to-noise ratio and reduced latency.

3.3. Security

Security is an important requirement for reliable data transmission in IoT. Techniques that provide defense against malicious users and their attacks are required to ensure reliability in IoT. As shown in **Figure 4**, security techniques include cryptography techniques, blockchain-based techniques and data integrity detection techniques. In **Table 3**, we provide the recent work related to security in IoT.

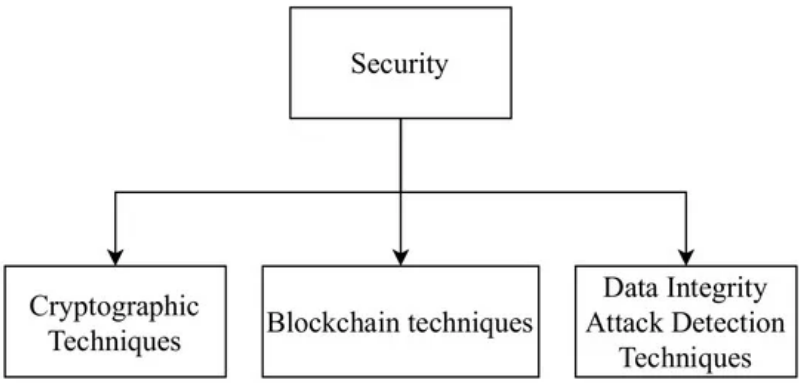

Figure 4. Different categories of recent work in Security in IoT.

Table 3. Security in IoT: Recent literature review (C = Cryptographic Technique, B = Blockchain, D = Data Integrity Attack Detection).

Scenario	C	B	D	Key Idea	Results
Anomaly detection at edge gateways [48]	✗	✗	✓	**Classify traffic as anomalous and normal based Fuzzy C-means clustering & fuzzy interpolation Access to malicious IoT nodes restricted**	**Improved accuracy Reduced false positive rate**
Transport layer security for IoT applications [49]	✓	✗	✗	**Reduce latency and achieve forward secrecy Identity-based cryptographic technique Identity-based encryption for client-server data**	**Reduced latency Reduced traffic overhead**
Secure 5G Internet of drones [50]	✗	✓	✗	**Blockchain for secure transmission Private blocks & Transactions are recorded Novel consensus algorithm is developed**	**Robustness against attacks Lower communication overhead Lower computation time**
IoT insider attacks [51]	✗	✗	✓	**Malicious attack detection from IoT insiders AI and distance based attacks classification**	**Improved accuracy Reduced computation time**
AES for constrained IoT devices [52]	✓	✗	✗	**Reduce complexity of the standard AES algo. Use a reduced number of rounds for algorithm Mathematical proof of proposed protocol**	**Reduced encryption time**
Data Integrity attacks in IoV [53]	✗	✗	✓	**Isolation forest algorithm used Find anomalies in traffic density information Detected anomalies verified Verification from the neighborhood area**	**Improved anomaly detection accuracy Reduced false positives**

The work in [48] proposes an anomaly detection technique for IoT devices. The proposed security algorithm is implemented at edge gateways and classifies traffic as abnormal and normal. The classification is done using fuzzy C-means clustering and fuzzy interpolation. Once the anomaly is detected, access to the malicious IoT nodes is restrictedThe results signify the performance of the proposed protocol in terms of improved accuracy of anomaly detection and reduced false-positive rate.

In [49], the authors proposed a transport layer security protocol for IoT applications. The goal is to reduce the latency and achieve forward secrecy. In this regard, an identity-based cryptographic technique is proposed. The key idea is that the client uses identity-based encryption to transmit data to the server when it receives no response from the serverThe results show reduced latency and reduced traffic overhead.

The work in [50] proposes a secure communication technique for 5G Internet of drones. Blockchain technology is used to ensure secure data transmission. Private blocks are created, and transactions are recorded in them. Moreover, a novel consensus algorithm is also developed. The result shows that the proposed protocol provides robustness against attacks, lower communication overhead, and lower computation time.

In [51], the authors propose a security protocol to detect malicious attacks which are from inside the IoT network. Artificial Intelligence (AI) based distance measurement techniques are used to identify and classify malicious attacksThe results show improved accuracy of detection and reduced computation time.

The authors in [52] provide Advanced Encryption Standard (AES) based security algorithm for constrained IoT devices. The proposed protocol reduces the complexity of the standard AES algorithm by using a reduced number of rounds. The mathematical proof of the proposed protocol is also providedThe results indicate reduced encryption time of the proposed protocol.

In [53], the authors present a technique to detect data integrity attacks in the Internet of Vehicles (IoVs). In this regard, the isolation forest algorithm finds anomalies in the traffic density information shared by vehicles. After detecting anomalies, verification messages are sent to neighborhood vehicles of potential malicious vehicles to verify if the data transmitted is malicious or correct. Simulation results show that improved accuracy of anomaly detection and reduced false positives.

References

1. Bhuiyan, M.N.; Rahman, D.M.M.; Billah, M.M.; 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, 10474–10498.
2. L-Turjman, F.A.; Deebak, B.D. Seamless Authentication: For IoT-Big Data Technologies in Smart Industrial Applica-tion Systems. IEEE Trans. Ind. Inform. 2021, 17, 2919–2927.
3. Bharadwaj, H.K.; Agarwal, A.; Chamola, V.; Lakkaniga, N.; Hassija, V.; Guizani, M.; Sikdar, B. A Review on the Role of Machine Learning in Enabling IoT Based Healthcare Applications. IEEE Access 2021, 9, 38859–38890.
4. Khan, S.; Alvi, A.N.; Javed, M.A.; Al-Otaibi, Y.D.; Bashir, A.K. An efficient medium access control protocol for RF energy harvesting based IoT devices. Comput. Commun. 2021, 171, 28–38.
5. Rahim, M.; Javed, M.A.; Alvi, A.N.; Imran, M. An efficient caching policy for content retrieval in autonomous con-nected vehicles. Transp. Res. Part Policy Pract. 2020, 140, 142–152.
6. Khan, S.; Alvi, A.N.; Khan, M.Z.; Javed, M.A.; Alhazmi, O.H.; Bouk, S.H. A novel superframe structure and optimal time slot allocation algorithm for IEEE 802.15.4–based Internet of things. Int. J. Distrib. Sens. Netw. 2020, 16, 1550147720984645.
7. Saad, W.; Bennis, M.; Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. IEEE Netw. 2020, 34, 134–142.
8. Tataria, H.; Shafi, M.; Molisch, A.F.; Dohler, M.; Sjöland, H.; Tufvesson, F. 6G Wireless Systems: Vision, Re-quirements, Challenges, Insights, and Opportunities. Proc. IEEE 2021, 109, 1166–1199.
9. Malik, U.M.; Javed, M.A.; Zeadally, S.; Islam, S.U. Energy efficient fog computing for 6G enabled massive IoT: Recent trends and future opportunities. IEEE Internet Things J. 2021.
10. Imran, K.; Anjum, N.; Mahfooz, S.; Zubair, M.; Yang, Z.; Malik, A.H.; Ali, Q.E.; Aman, M. Cluster-based group mobility support for smart IoT. Comput. Mater. Contin. 2021, 68, 2329–2347.

11. Shahid, H.; Ashraf, H.; Javed, H.; Humayun, M.; Jhanjhi, N.; AlZain, M.A. Energy optimised security against wormhole at-tack in iot-based wireless sensor networks. Comput. Mater. Contin. 2021, 68, 1967–1981.
12. Butt, T.M.; Riaz, R.; Chakraborty, C.; Rizvi, S.S.; Paul, A. Cogent and energy efficient authentication protocol for wsn in iot. Comput. Mater. Contin. 2021, 68, 1877–1898.
13. Kanwal, S.; Iqbal, Z.; Irtaza, A.; Ali, R.; Siddique, K. A genetic based leader election algorithm for iot cloud data processing. Comput. Mater. Contin. 2021, 68, 2469–2486.
14. Mittal, M.; Iwendi, C.; Khan, S.; Rehman Javed, A. Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg-Marquardt neural network and gated recurrent unit for intrusion detection system. Trans. Emerging Tel. Tech. 2021, 32, e3997.
15. Mittal, M.; Saraswat, L.K.; Iwendi, C.; Anajemba, J.H. A Neuro-Fuzzy Approach for Intrusion Detection in En-ergy Efficient Sensor Routing. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–5.
16. Cheng, Y.; Xu, Y.; Zhong, H.; Liu, Y. Leveraging Semisupervised Hierarchical Stacking Temporal Convolutional Network for Anomaly Detection in IoT Communication. IEEE Internet Things J. 2021, 8, 144–155.
17. Wang, J.; Hao, S.; Wen, R.; Zhang, B.; Zhang, L.; Hu, H.; Lu, R. IoT-Praetor: Undesired Behaviors Detection for IoT Devices. IEEE Internet Things J. 2021, 8, 927–940.
18. Sadawi, A.A.; Hassan, M.S.; Ndiaye, M. A Survey on the Integration of Blockchain With IoT to Enhance Perfor-mance and Eliminate Challenges. IEEE Access 2021, 9, 54478–54497.
19. He, Y.; Wang, Y.; Qiu, C.; Lin, Q.; Li, J.; Ming, Z. Blockchain-Based Edge Computing Resource Allocation in IoT: A Deep Reinforcement Learning Approach. IEEE Internet Things J. 2021, 8, 2226–2237.
20. Sun, S.; Du, R.; Chen, S.; Li, W. Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain. IEEE Access 2021, 9, 36868–36878.
21. Huong, T.T.; Bac, T.P.; Long, D.M.; Binh, N.T.; Luong, T.D.; Phuc, T.K. LocKedge: Low-Complexity Cyberattack Detection in IoT Edge Computing. IEEE Access 2021, 9, 29696–29710.
22. Khan, M.N.; Rao, A.; Camtepe, S. Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey. IEEE Internet Things J. 2021, 8, 4132–4156.
23. Zuo, J.; Lu, Y.; Gao, H.; Peng, T.; Guo, Z.; An, T.; Litt, E. Security-critical components recognition algorithm for complex heter-ogeneous information systems. Comput. Mater. Contin. 2021, 68, 2579–2595.
24. Rathee, G.; Iqbal, R.; Khelifi, A. Decision making in internet of vehicles using pervasive trusted computing scheme. Comput. Mater. Contin. 2021, 68, 2755–2769.
25. Guo, J.; Liu, Y.; Li, S.; Li, Z.; Kherbachi, S. Game-oriented security strategy against hotspot attacks for internet of ve-hicles. Comput. Mater. Contin. 2021, 68, 2145–2157.
26. Baek, H.; Lim, J. Design of future UAV-relay tactical data link for reliable UAV control and situational awareness. IEEE Commun. Mag. 2018, 56, 144–150.
27. Zhang, C.; Zhang, W.; Wang, W.; Yang, L.; Zhang, W. Research challenges and opportunities of UAV millime-ter-wave communications. IEEE Wirel. Commun. 2019, 26, 58–62.
28. Shang, B.; Marojevic, V.; Yi, Y.; Abdalla, A.S.; Liu, L. Spectrum sharing for UAV communications: Spatial spectrum sensing and open issues. IEEE Veh. Technol. Mag. 2020, 15, 104–112.
29. Bekkouche, O.; Samdanis, K.; Bagaa, M.; Taleb, T. A service-based architecture for enabling UAV enhanced network services. IEEE Netw. 2020, 34, 328–335.
30. Hellaoui, H.; Bekkouche, O.; Bagaa, M.; Taleb, T. Aerial control system for spectrum efficiency in UAV-to-cellular communications. IEEE Commun. Mag. 2018, 56, 108–113.
31. Wang, L.; Che, Y.L.; Long, J.; Duan, L.; Wu, K. Multiple access mmwave design for UAV-aided 5G communications. IEEE Wirel. Commun. 2019, 26, 64–71.
32. Wu, Q.; Liu, L.; Zhang, R. Fundamental trade-offs in communication and trajectory design for UAV-enabled wireless network. IEEE Wirel. Commun. 2019, 26, 36–44.
33. Challita, U.; Ferdowsi, A.; Chen, M.; Saad, W. Machine learning for wireless connectivity and security of cellu-lar-connected UAVs. IEEE Wirel. Commun. 2019, 26, 28–35.
34. Verdone, R.; Mignardi, S. Joint aerial-terrestrial resource management in UAV-aided mobile radio networks. IEEE Netw. 2018, 32, 70–75.

35. Qi, F.; Zhu, X.; Mang, G.; Kadoch, M.; Li, W. UAV network and IoT in the sky for future smart cities. IEEE Netw. 2019, 33, 96–101.
36. Asiedu, D.K.P.; Mahama, S.; Song, C.; Kim, D.; Lee, K.-J. Beamforming and Resource Allocation for Multiuser Full-Duplex Wireless-Powered Communications in IoT Networks. IEEE Internet Things J. 2020, 7, 11355–11370.
37. AlQerm, I.; Pan, J. Enhanced Online Q-Learning Scheme for Resource Allocation with Maximum Utility and Fairness in Edge-IoT Networks. IEEE Trans. Netw. Sci. Eng. 2020, 7, 3074–3086.
38. Librino, F.; Santi, P. Resource Allocation and Sharing in URLLC for IoT Applications Using Shareability Graphs. IEEE Internet Things J. 2020, 7, 10511–10526.
39. He, X.; Wang, K.; Huang, H.; Miyazaki, T.; Wang, Y.; Guo, S. Green Resource Allocation Based on Deep Reinforcement Learning in Content-Centric IoT. IEEE Trans. Emerg. Top. Comput. 2020, 8, 781–796.
40. Chen, X.; Liu, Y.; Cai, L.X.; Chen, Z.; Zhang, D. Resource Allocation for Wireless Cooperative IoT Network With En-ergy Harvesting. IEEE Trans. Wirel. Commun. 2020, 19, 4879–4893.
41. Liu, Y.; Liu, K.; Han, J.; Zhu, L.; Xiao, Z.; Xia, X.G. Resource Allocation and 3-D Placement for UAV-Enabled Ener-gy-Efficient IoT Communications. IEEE Internet Things J. 2021, 8, 1322–1333.
42. Azari, A.; Stefanović, Č.; Popovski, P.; Cavdar, C. On the Latency-Energy Performance of NB-IoT Systems in Providing Wide-Area IoT Connectivity. IEEE Trans. Green Commun. Netw. 2020, 4, 57–68.
43. Qin, M.; Cheng, N.; Jing, Z.; Yang, T.; Xu, W.; Yang, Q.; Rao, R.R. Service-Oriented Energy-Latency Tradeoff for IoT Task Partial Offloading in MEC-Enhanced Multi-RAT Networks. IEEE Internet Things J. 2021, 8, 1896–1907.
44. Kafle, V.P.; Muktadir, A.H.A. Intelligent and Agile Control of Edge Resources for Latency-Sensitive IoT Services. IEEE Access 2020, 8, 207991–208002.
45. Cui, G.; Li, X.; Xu, L.; Wang, W. Latency and Energy Optimization for MEC Enhanced SAT-IoT Networks. IEEE Access 2020, 8, 55915–55926.
46. Zhang, L.; Ansari, N. Latency-Aware IoT Service Provisioning in UAV-Aided Mobile-Edge Computing Networks. IEEE Internet Things J. 2020, 7, 10573–10580.
47. Wan, X.; Zhu, X.; Jiang, Y.; Liu, Y.; Zhao, J. An Interference Alignment and ICA-Based Semiblind Dual-User Down-link NOMA System for High-Reliability Low-Latency IoT. IEEE Internet Things J. 2020, 7, 10837–10851.
48. Hafeez, I.; Antikainen, M.; Ding, A.Y.; Tarkoma, S. IoT-KEEPER: Detecting Malicious IoT Network Activity Using Online Traffic Analysis at the Edge. IEEE Trans. Netw. Serv. Manag. 2020, 17, 45–59.
49. Li, P.; Su, J.; Wang, X. iTLS: Lightweight Transport-Layer Security Protocol for IoT With Minimal Latency and Perfect Forward Secrecy. IEEE Internet Things J. 2020, 7, 6828–6841.
50. Bera, B.; Saha, S.; Das, A.K.; Kumar, N.; Lorenz, P.; Alazab, M. Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment. IEEE Trans. Veh. Technol. 2020, 69, 9097–9111.
51. Khan, A.Y.; Latif, R.; Latif, S.; Tahir, S.; Batool, G.; Saba, T. Malicious Insider Attack Detection in IoTs Using Data Ana-lytics. IEEE Access 2020, 8, 11743–11753.
52. Mamvong, J.N.; Goteng, G.L.; Zhou, B.; Gao, Y. Efficient Security Algorithm for Power-Constrained IoT Devices. IEEE Internet Things J. 2021, 8, 5498–5509.
53. MJaved, A.; Khan, M.Z.; Zafar, U.; Siddiqui, M.F.; Badar, R.; Lee, B.M.; Ahmad, F. ODPV: An Efficient Protocol to Mitigate Data In-tegrity Attacks in Intelligent Transport Systems. IEEE Access 2020, 8, 114733–114740.