Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/MBE

MBE, 20 (11): 19174–19190.
DOI: 10.3934/mbe.2023847
Received: 13 August 2023
Revised: 21 September 2023
Accepted: 24 September 2023
Published: 13 October 2023

Research article

Multimedia IoT-surveillance optimization model using mobile-edge authentic computing

Faten S. Alamri[1] , Khalid Haseeb[2], Tanzila Saba[2], Jaime Lloret[3,]* and Jose M. Jimenez[3]

[1] Department of Mathematical Sciences, College of Science, Princess Nourah Bint Abdulrahman University, P.O.Box 84428, Riyadh, 11671, Saudi Arabia

[2] Artificial Intelligence & Data Analytics (AIDA) Lab CCIS, Prince Sultan University, Riyadh 12435, Saudi Arabia

[3] Instituto de Investigación para la Gestión Integrada de Zonas Costeras, Universitat Politenica de Valencia, 46730, Gandia, València, Spain

* **Correspondence:** Email: jlloret@dcom.upv.es.

Abstract: Smart technologies are advancing the development of cutting-edge systems by exploring the future network. The Internet of Things (IoT) and many multimedia sensors interact with each other for collecting and transmitting visual data. However, managing enormous amounts of data from numerous network devices is one of the main research challenges. In this context, various IoT systems have been investigated and have provided efficient data retrieval and processing solutions. For multimedia systems, however, controlling inefficient bandwidth utilization and ensuring timely transmission of vital information are key research concerns. Moreover, to transfer multimedia traffic while balancing communication costs for the IoT system, a sustainable solution with intelligence in real-life applications is demanded. Furthermore, trust must be formed for technological advancement to occur; such an approach provides the smart communication paradigm with the incorporation of edge computing. This study proposed a model for optimizing multimedia using a combination of edge computing intelligence and authentic strategies. Mobile edges analyze network states to discover the system's status and minimize communication disruptions. Moreover, direct and indirect authentication determines the reliability of data forwarders and network stability. The proposed authentication approach minimizes the possibility of data compromise and increases trust in multimedia surveillance systems. Using simulation testing, the proposed model outperformed other comparable work in terms of byte delivery, packet overhead, packet delay, and data loss metrics.

Keywords: Multimedia networks; emerging technologies; infrastructural development; future networks; edge computing

1. Introduction

Embedded systems and Internet of Things (IoT) technology are being used more frequently in the construction and growth of multimedia networks. They are found in various fields such as industry, hospitals, academia, and entertainment [1–3]. The discovery of the cellular spectrum, and wireless communication has brought the world several advanced capabilities for future networks [4, 5]. Due to rapid advances in sensor technology and the dynamic nature of wireless hardware, many multimedia surveillance systems are developed to sense and acquire data from the environment in the form of images, audio, and video [6, 7]. Such a network carries a huge multi-type data from the virtual networks and facilitates the process of data analysis to solve many real-life issues for smart cities and facilitate the heterogeneous network [8-10]. However, due to the data heterogeneity, researchers are trying to design intelligent solutions based on machine learning and decrease the complexity of smart applications [11–13]. On the other hand, IoT systems generate numerous events and incur overloads on the edges. Thus, to improve network concerns such as scalability and routing, quality of service must be incorporated into the development of crucial applications [14–16]. Using 6G technologies [17, 18], the interaction of smart objects need to improve for automatic data collection and analysis. Moreover, before sending data to the central station, edges should remove redundancies from surrounding nodes' data [19–21]. However, most solutions cannot balance the traffic flowing among the devices while carrying a high amount of data over distributed networks. In addition, due to the heavy load, many links fail during the routing process, resulting in higher retransmission costs [22–24]. Moreover, security is another primary goal for virtual networks to keep the privacy and authenticity of collected information. Adopting a secured communication system gives the surety for data availability for the embedded networks [25–27]. This research aims to provide a model for edge computing that incorporates sink intelligence. It increases the effectiveness of intelligent communication by balancing and controlling the communication load data links. In addition, edges play vital roles in facilitating the routing process by eliminating lengthy distances and reducing the number of retransmissions for multimedia applications. In addition, techniques for validating IoT network devices and securing peer-to-peer connections are examined. The following are the main contributions of this work.

i. Heterogeneous devices are linked together using optimization criteria to form a smart multimedia ecosystem with reliability and effective decisions.
ii. By distributing the data flow on the communication channels and multimedia sensors, the overheads in terms of computing cost are examined.
iii. The mobile-edged environment is established and maintained with a combination of private sessions. Such functionalities offer a more trustworthy system for authentic communication and reduce uncertainties.

The rest of the sections are organized in the following ways. Section 2 discusses the related work. In Section 3, the problem statement is defined. Section 4 provides a detailed discussion of the proposed work. Section 5 shows the simulation environment and experimental discussion. The conclusion is highlighted in Section 6.

2. Related work

To advance the development of intelligent and autonomous systems, the 6G wireless communication networks are expected to transform customer services and applications through IoT networks [28–30]. With the integration of future networks, wireless technologies play a prominent role in the development of multimedia systems; however, transmitting the collected data over virtual connections is a challenging task [31,32]. In recent years, the spread of technology has enabled people to communicate via multimedia in a variety of methods. The use of multimedia technology in various applications enables the storage, processing, and transmission of vital data in a variety of formats [33, 34]. Due to energy and computation constraints, security in terms of authentication and privacy is also a difficult challenge. It is the most crucial aspect of communication for authenticating multimedia sensors and private data [35,36]. To assure data transfer in the event of a defective route, an optimized multi-sink-based clustered WSN model [37] is proposed. This model also includes an extended ACO-based routing protocol (EARP) that is fault-tolerant and energy-efficient. In contrast to prior research, EARP addresses the constraints of forest fire detection applications such as fault tolerance, network lifetime, and response time. The proposed EARP and its relevant approaches are evaluated by an application-specific method based on network lifespan and reaction time in a general scenario. An energy-efficient 6G in-network computing paradigm incorporates network functionalities into a general computing platform instead of assigning computing duties to network devices [38].

The network node-integrated computing platform substitutes conventional network devices. Unlike traditional network devices, hypervisors and containers provide the network node with a uniform operating environment for application activities. Cloud servers or network nodes may process data. The network controller organizes processing activities on the node, transmitting application traffic. Our paradigm maximizes network node computing capabilities and reduces data center processing demand, network transmission overhead, and energy usage. The threshold-based cluster head (CH) selection stable election procedure (SEP) for heterogeneous networks [39] balances cluster members and the level of energy for the selected CH nodes. Sensor nodes are classified as standard, intermediate, or enhanced to balance the network load based on the initial energy supply. The experiment reveals that the proposed system outperforms SEP and DEEC protocols with an improved network lifetime and efficiency. A distributed two-stage offloading (DTSO) method [40] is proposed to offer a tradeoff solution. First, a combinatorial optimization problem is formed by incorporating channel interference and the queuing theory. The second stage involves converting the original issue into a nonlinear optimization problem, which is then solved using a sequential quadratic programming (SQP) method. To explicitly provide for an adjustable trade-off between delay and energy requirement across heterogeneous applications, the DTSO has introduced the elasticity parameter.

A new secured communication model with trust analysis and outlier detection based on fuzzy temporal clustering is proposed to track the communication nodes [41]. To help distinguish the malicious nodes from other nodes inside each cluster of the network, a fuzzy temporal rule and a distance-based outlier detection technique are also developed and included in the secured routing algorithm. The proposed safe routing algorithm utilizes trust and key management approaches to carry out effective node authentication and isolate malicious nodes from communication through outlier detection. An application is proposed [42] by exploring three different algorithms to increase a sensor network's performance in terms of sink node placement, route creation, and optimization using computational techniques. Opportunistic coding is also utilized at possible relays to decrease the rate of data retransmissions. As a result, the proposed solution combines the benefits of three algorithms for a prominent improvement in data transfer. Particle swarm optimization is used to first place the sink node, followed by minimal wiener spanning tree route construction from sensors and the sink of the specific cluster, which is further optimized by an artificial bee colony technique, and third, opportunistic packet amalgamation is used before transmitting to neighbors. Authors in [43] describe an edge-based, graph neural network-assisted video surveillance solution for a smart construction site. It makes use of the distributed computing model to achieve flexible resource allocation. To demonstrate the functionality of the mobile-edge network and improve the scheduling strategy used by the Deep-Q Network, a graph-assisted hierarchical reinforcement learning algorithm is developed. The proposed solution was tested in the commercial and residential buildings of a Fortune Global 500 real estate company, and it was found that the proposed algorithm is effective at preserving reliable accuracy with minor latency. In [44], authors introduced a hierarchical forest fire detection approach. The proposed framework hierarchically uses multimedia and scalar sensors to reduce visual data transfer. A lightweight deep learning model for network edge devices improves detection accuracy and reduces traffic between edge devices and the sink. Energy efficiency and detection accuracy are evaluated using various tests.

3. Problem statement

As a consequence of the work presented, it has been determined that edge computing and IoT networks have a positive effect on the design and maintenance of communication systems. These systems provide an intelligent network for multimedia applications and acquire observed data with the support of visual sensors to facilitate end users. However, due to various constraints on the multimedia environment, adaptive routing methods are necessary to achieve sustainable development for real-time and complex systems. Moreover, massive data from distributed devices also needs to be managed intelligently on intermediate devices. When analyzing future networks in the IoT era, security is also a significant concern.

4. Proposed emerging edge optimization multimedia model using an intelligent system

This section presents a thorough analysis of the system model and development components. We assumed that sensors are connected in the form of a weighted graph with edges. Each node has a GPS. Nodes store initial network properties of neighbors like distance, battery power and position. The neighboring tables are updated by exploring certain events. The system can use single-hop or multi-hop communication depending on location and transmission power. Edges are more resilient than sensors and can communicate with low and high-level tiers. Figure 1 depicts three fundamental stages of the proposed model. In the initial stage, multiple levels have been identified. Sensors exchanged their status and local data for the management of nearby neighbors. Later, adaptive routing methods are implemented by employing a distributed and weighted mechanism to select the optimal nodes at each stage according to greedy principles. To achieve efficient data routing decisions, the proposed model employs realistic factors in terms of energy, response time, and transmission distance. In the final phase, methods for achieving device authentication and protecting the confidentiality of incoming data are explored.

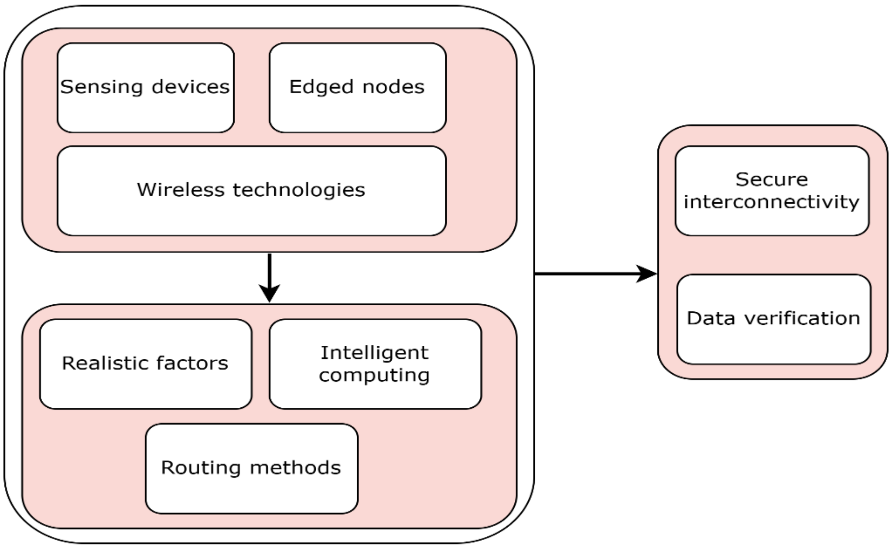


Figure 1. Designed components of the proposed model.

There are two primary algorithms in the proposed model. The first algorithm creates virtual routes for transferring the initial parameters and storing the entries in the routing tables. Afterwards, a distributed and intelligence strategy is developed to determine reliable and efficient adjacent nodes for the forwarding of multimedia traffic. It not only decreases the overheads on the constraint devices, but also offers cost-effective solutions to cope with massive amounts of communication mediums. In the second algorithm, mobile edges perform a vital role in identifying the malicious nodes from the communication system, accordingly decreasing the chances of network congestion by reducing data retransmission. Moreover, trust in the form of chaining the links provides reliable connections to ensure verification and privacy preservation. The network devices initially exchange local information with their neighbors so that they can update their communication parameters. The routing tables are dynamic and update when nodes either change their attributes or are unable to forward the network data. Moreover, edge devices are assumed more intelligent than multimedia sensors, allowing them to deal with uncertain scenarios and network anomalies. All the identities of the devices and communicated links are stored in the table which is located at the edge device. The edge devices are performing the role of gateways and decreasing the transmission distance from sensors to the sink. Unlike most of the existing work, our system utilizes the mobile edges that often flood their updated position with the nearest neighbors. The mobile edges M_EG are rotated with a constant velocity VT within a predetermined transmission range TR, as indicated in Eq 1.

$$VT(M\_EG) \leq TR \tag{1}$$

The identified neighbors further forwarded the updated location of mobile edge in their proximity by exploring routing tables. The proposed model employs greedy techniques at each phase and iterates this procedure until an end-to-end path is discovered. The selected route by the proposed model decreases the delay for data transmission and increases the maintainance of sensor data for multimedia networks. Let us consider that sensors $S_i = (S_1, S_2, \ldots., S_n)$ and channels $C_i = (C_1, C_2, \ldots., C_n)$ are integrated to formulate n pairs of routing paths R_i, as defined in Eq 2.

$$R_i = (R_1, R_2, \ldots., R_n) \tag{2}$$

Each pair is assigned a weighted value and all the values are summed up to find a more balanced and optimal cost. We assumed that X_i is the individual cost of each pair, as defined in Eq 3.

$$X_i= (X_1, X_2, \ldots., X_n) \tag{3}$$

The proposed model computes the cost based on depleted energy e, response time rt, and transmission distance td. Cost value provides a more efficient and long-term approach for multimedia traffic data routing. Before sending sensor data to data collectors, all parameters are reevaluated. The cost value is also recorded in the boundary table at network edges for ongoing network monitoring. The source node only establishes virtual connections V_{con} with its neighbor if its weighted cost X_i is less than the threshold $TRES$. This phase is repeated until the end-to-end route is obtained, as defined in Eq 4.

$$V_{con} = min\,(X_i) + \; mi\,n(X_{i+1}) + \cdots + \; min\,(X_n) \tag{4}$$

X_i value is based on the weighted computation such that each parameter in the evaluation offers a uniform contribution for node i to node j, as indicated in Eq 5.

$$X_i = \alpha.e_i + \beta.rt_{i,j} + \Upsilon.td_{i,j} \tag{5}$$

In Eq 5, the response time rt_i indicates the elapsed time between the paring nodes. Let us consider $rt_i, rt_{i+1}, \ldots, rt_n$ are response times that are recorded for n beacon messages, then average response time $avr(RT)$ can be computed as given in Eq 6.

$$avr(RT) = rt_i + rt_{i+1} + \cdots, + rt_n/n \tag{6}$$

In the next phase, edges are interconnected with each other to forward the data from the multimedia environment toward data centers. Each edge has a distinct identity and maintains the identities of the nearest edges. Data is therefore transmitted continuously from edge to edge until it reach data centers. To obtain the security system, device i combines its identity ID_i, secret key SK_i and nonce NC_i to generate randomness in communication and initiate the registration process. In consequence, Eq 7 provides a private value N_i. Moreover, the encrypted data block $E(D)$ is included with N_i, as shown in Eq 8.

$$N_i = (ID_i + SK_i) \,||\, NC_i \tag{7}$$

$$Z = N_i + E(D) \tag{8}$$

On the other hand, when node j receives the N_i, it applies Eq 9 and uses the same secret key SK_i in conjunction with the xor function to recover ID_i. If the identity matches the information stored at node j, registration is complete; otherwise, the connection is terminated.

$$ID_i = N_i + SK_i \tag{9}$$

Likewise, when the edge device ed receives the N_i from a nearby forwarder node, it verifies forwarder identity with its stored record; if successful, edge devices encrypt $E(D)$ with its private key and transfer it towards sink with inclusion of nonce NC_{ed}. Upon receiving the encrypted block, sink authenticate the received information using the public key of edge node and store the data in a cloud database. Table 1 shows the list of symbols and their notations.

Table 1. List of symbols.

Symbol	Notation	Symbol	Notation
M_EG	Mobile edges	td	Transmission distance
VT	Constant velocity	e	Energy
TR	Transmission radius	X_i	Weighted value
C_i	Channels	V_{con}	Virtual connection
S_i	Sensor nodes	rt_i	Response time
$TRES$	Threshold	N_i	Private value
R_i	Routes	$E(D)$	Encrypted data
NC_i	Nonce	SK_i	Secret key

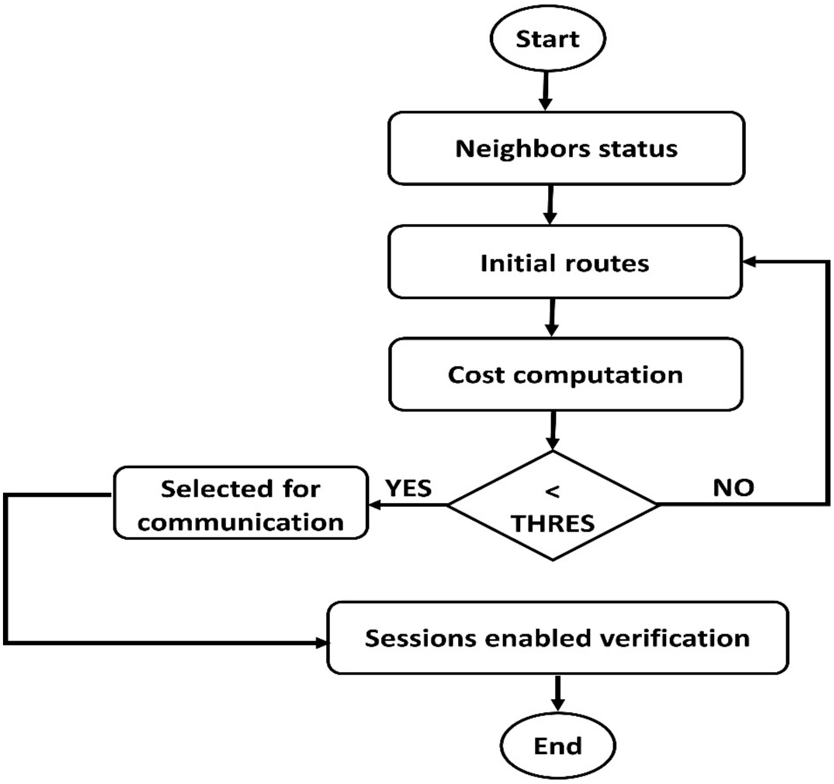


Figure 2. Greedy principles with intelligent edges for IoT multimedia system.

The flowcharts for routing methods in the IoT multimedia environment with uniform load distribution are depicted in Figure 2. After the collection of data, nodes collaboratively share their information for the construction of initial routes. The initial routes are refined at each stage using optimization techniques based on greedy principles until more reliable decisions are made for selecting the data forwarders. Each time, the evaluation set is replaced by exploring realistic network factors. Also, the node that is already a part of the routing chain is not permitted to participate in alternative routes. Figure 3 illustrates the functioning of the proposed security algorithm for obtaining authentication and privacy of IoT data. Before network data can be transmitted, each node must first be authenticated at the network edge using combination of identities and session keys. If a malicious node is identified, the communication channel is blocked and the neighbors are notified. In addition, routing packets on malicious channels are discarded and the routes reformulation procedure is reinitiated. In Figure 4, different states of the proposed model are highlighted. In the beginning, devices need to interact with each other to form the initial routing entries. Later, the cost computing function is utilized to extract the updated information and lead to optimized criteria for the selection of the data route. The optimization procedure depends on multiple quality-aware parameters that decrease the space and load complexity on constraint devices. This process is executed constantly for the development of a reliable IoT system. Moreover, the devices are required to authenticate with their associated identities, and accordingly, they are permitted to perform the transmission process of multimedia data. The pseudocode for proposed routing and security techniques is shown in Algorithm 1.

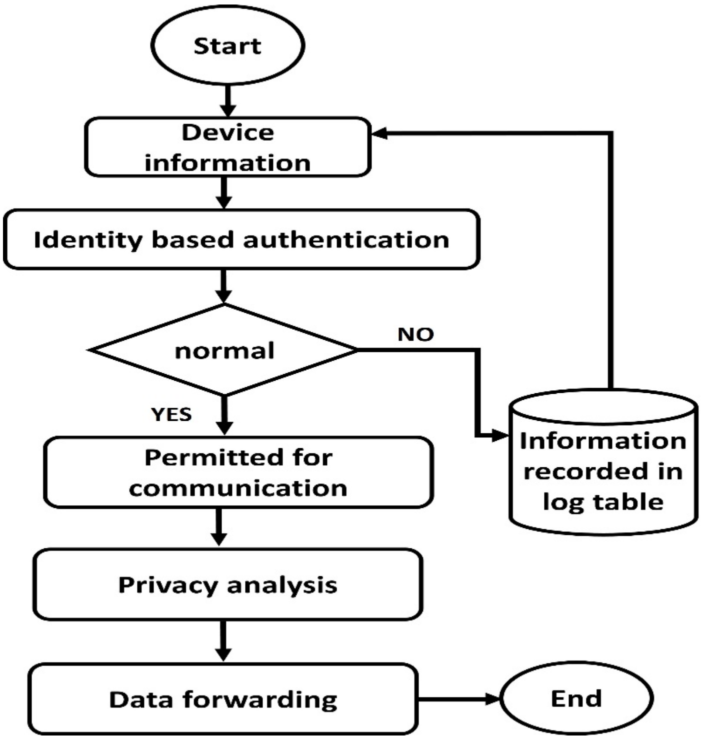

Start
Device information
Identity based authentication
normal
NO
YES
Information recorded in log table
Permitted for communication
Privacy analysis
Data forwarding
End

Figure 3. Authentic secured algorithm for malicious devices.

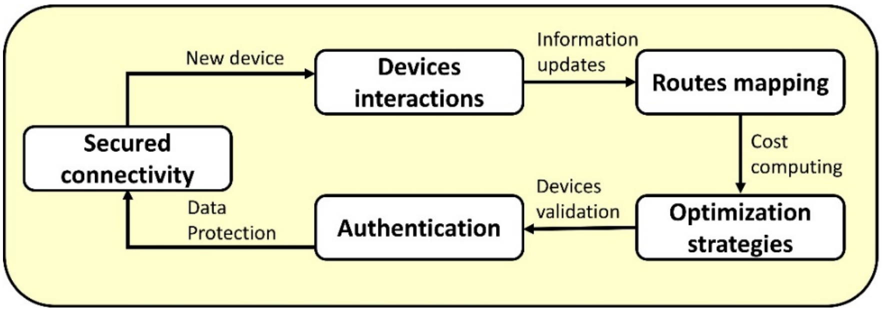
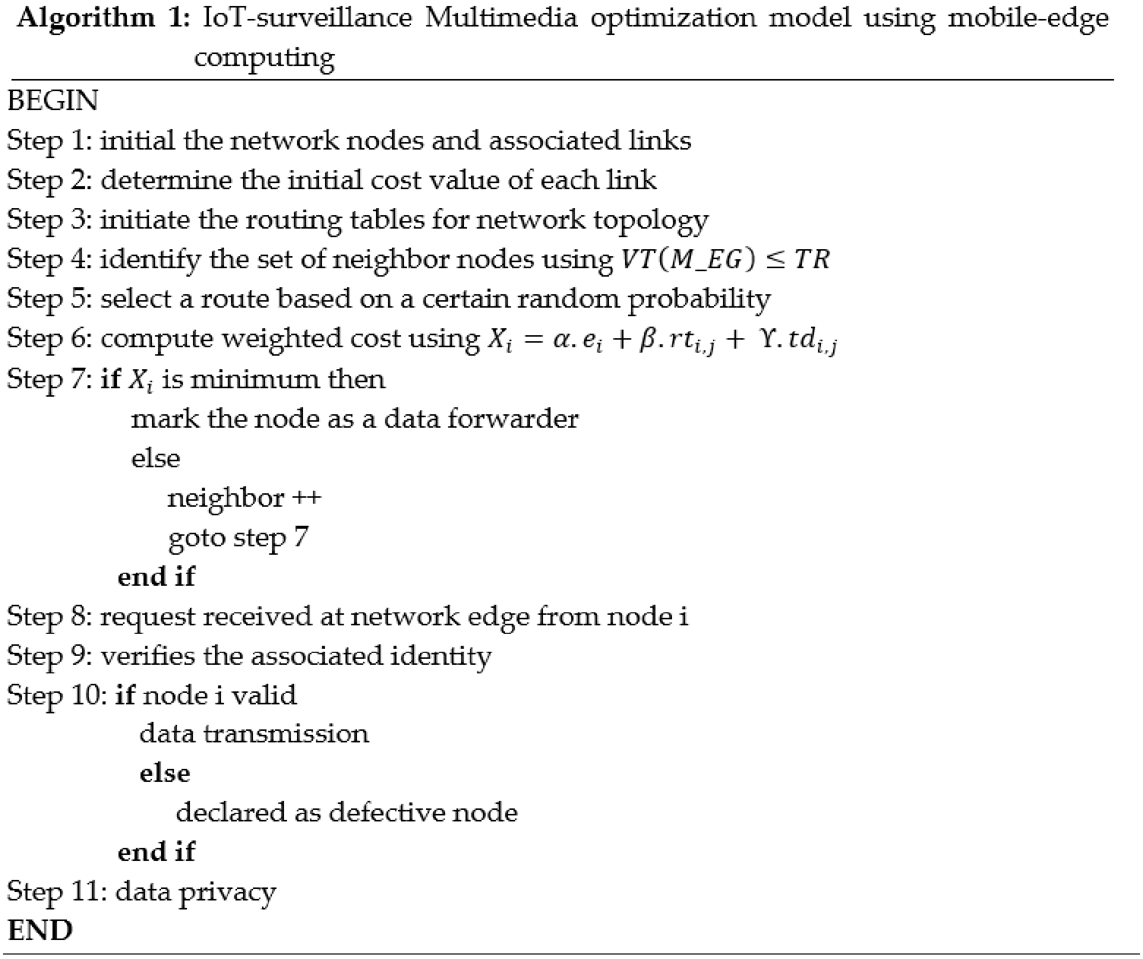


Figure 4. Authentic secured algorithm for malicious devices.



Algorithm 1: IoT-surveillance Multimedia optimization model using mobile-edge computing

```
BEGIN
Step 1: initial the network nodes and associated links
Step 2: determine the initial cost value of each link
Step 3: initiate the routing tables for network topology
Step 4: identify the set of neighbor nodes using $VT(M\_EG) \leq TR$
Step 5: select a route based on a certain random probability
Step 6: compute weighted cost using $X_i = \alpha.e_i + \beta.rt_{i,j} + \Upsilon.td_{i,j}$
Step 7: if $X_i$ is minimum then
            mark the node as a data forwarder
            else
               neighbor ++
               goto step 7
         end if
Step 8: request received at network edge from node i
Step 9: verifies the associated identity
Step 10: if node i valid
            data transmission
            else
               declared as defective node
         end if
Step 11: data privacy
END
```

Table 2. Simulation parameters.

Parameter	Value
Simulation area	500m x 500m
Sensors	15, 30, 45, 60, 75
Number of sink nodes	2
Initial energy	5 J
Transmission range	3m
Data traffic	CBR
Time slot	5min to 50min
Number of edges	2-10
Malicious nodes	3-12
Performance metrics	Number of data bytes, packet delays, packets overhead, retransmission ratio, loss rate

5. Analysis and results discussion

In this section, the performance analysis of the proposed model is analyzed as compared to other related work. We used sensors and edge nodes with NS-2.34 [45] to test several tests. The tests were conducted using a i7 and 256 GB of RAM. The nodes are randomly deployed in the field with 5J of initial energy. The transmission power of each node is fixed at 3m. The network field is in the range of 500m x 500m. The traffic type belongs to the constant bit rate (CBR). The edge nodes vary from 2 to 10 which have enough resources as compared to ordinary IoT sensors. Figure 5 shows the used topology in the experimental analysis. Sensors are grouped in a single layer for the formulation of the IoT network. The sinks are deployed randomly in the field to gather the sensed multimedia data. Edges are distributed across the boundary of the IoT layer that further communicates with network users. The performance is evaluated based on two scenarios, i.e. varying time slots and varying edges. We ran 40 samples of simulation to obtain performance results. Table 2 lists the simulation parameters.

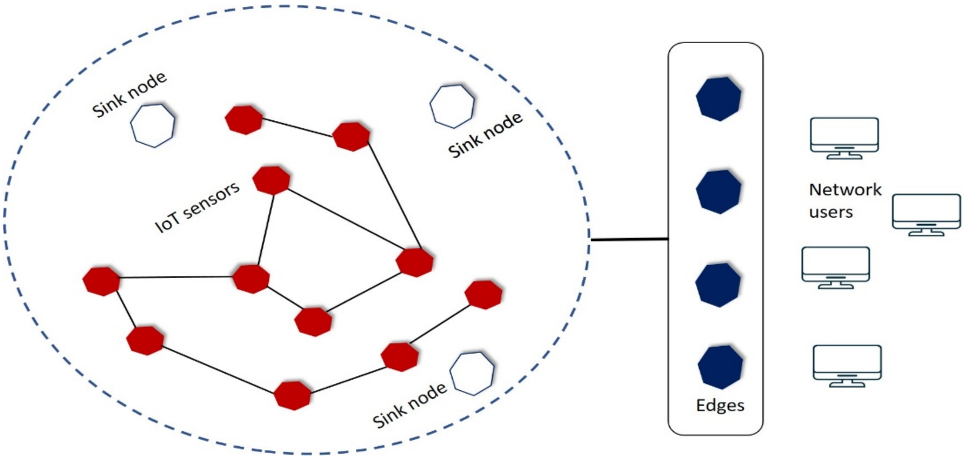
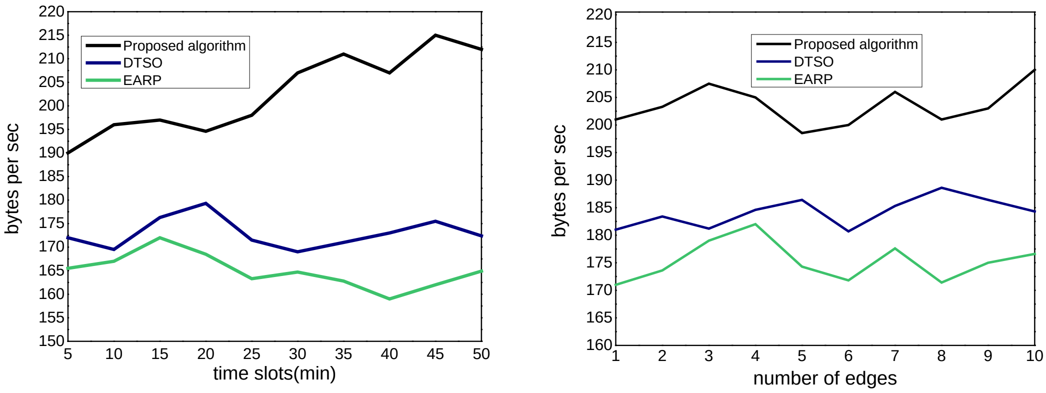


Figure 5. Designed topology for conducting experiments with sensors, sink nodes, edges, and network users.

5.1. *Analysis of data transmission*

According to Figures 6(a) and 6(b), the proposed model improved the delivery performance in terms of data bytes under varying time slots and edges. It is defined as transferring sensor data in its original form to a destination at a certain time. The experimental results demonstrate an improvement by an average of 12.4% and 16.3% for the proposed model in comparison to other work. It uses local and globally optimal solutions until end-to-end communication links are identified. Moreover, the updated parameters in collaborative criteria balance the consumption of network resources and ultimately efficiently utilize the communication bandwidth. Furthermore, edge nodes perform a key role in the proposed model, as they are intermediate devices nearest to the low-level tier and accordingly shorten the network routes. Such practice increases the delivery of IoT data with the least interruption. By utilizing the security solution, the data chunks are forwarded with trusted forwarders and reduce the chances for malicious packets to affect the actual nodes' communication. The proposed model and alternative solution are simulated in terms of nodes overhead against varying time and malicious nodes.



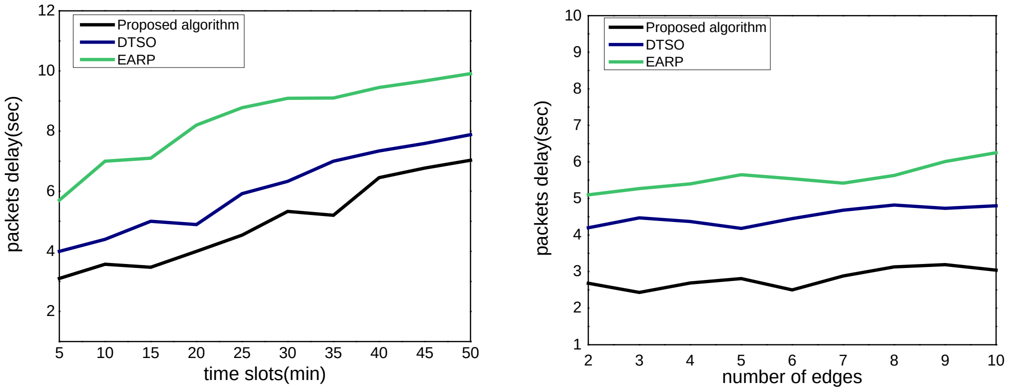
(a) Bytes delivery and time slots

(b) Bytes delivery and number of edges

Figure 6. Evaluation of transmission of data bytes with varying time slots and edges.

5.2. *Analysis of packet delay*

As depicted in Figures 7(a) and 7(b), the proposed model is compared with existing solutions for packet delay, which is defined as the length of time to travel across a network from a source to a destination. According to experimental results, the proposed model decreases the packet delay by an average of 7.9% and 10.6% in comparison to other approaches. This is because traffic is evaluated on the forwarding routes, and whenever it is higher than a certain limit, the proposed model initiates the collaborative criteria for the construction of an alternate route. Moreover, the sink node monitors the communication field with the support of edges, and it greatly reduces link damage even in the presence of malicious nodes. The security methods also offer the rapid detection of faulty nodes by exploring the nonce and unique identifications of nodes. Accordingly, the communication is not disturbed and the proposed model gives smooth transmission flowing over the IoT channels.



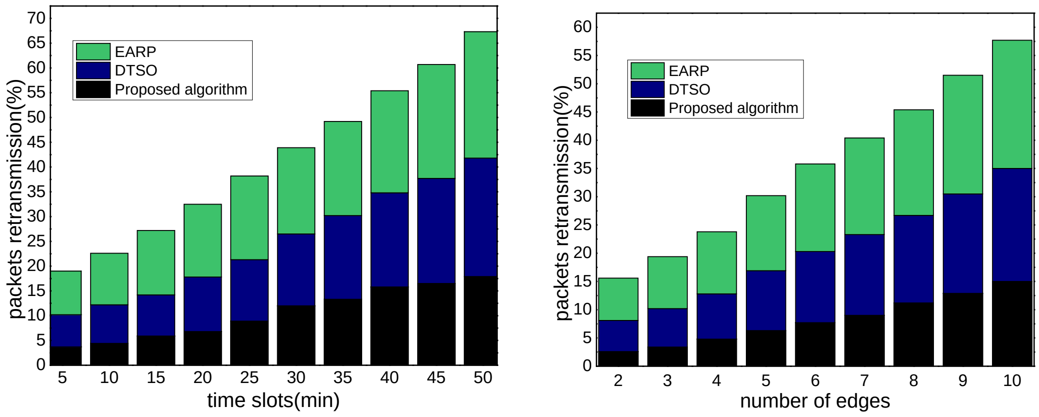
(a) Packets delay and time slots

(b) Packets delay and edges

Figure 7. Evaluation of the packets delay for varying time slots and edges.

5.3. *Analysis of retransmissions*

Figures 8(a) and 8(b) show the performance results of the proposed model with existing solutions under varying time slots and edges in terms of retransmissions. It can be defined the ratio of packets that are resent in the event of a link or data failure. It was observed that the proposed model improves the number of retransmissions by an average of 10.8% and 13.3% in comparison to the existing work. This is due to the collaborative decision of the low-level devices and maintaining their records based on the quality of service. In addition, route request is generated only when there is demand for data forwarding. The overloaded channels are identified intelligently and data is shared on the balanced routes in terms of traffic flow. For the overlooked damaged links, the proposed model decreases the number of retransmissions and frequently reduces the delay time among devices. Moreover, only the most recent information is maintained at the edges and longer routes are eliminated from the tables. This allows for rapid packet transmission from a source node toward edge nodes using an optimized selection of neighboring nodes.



(a) Retransmission and time slots

(b) Retransmission and edges

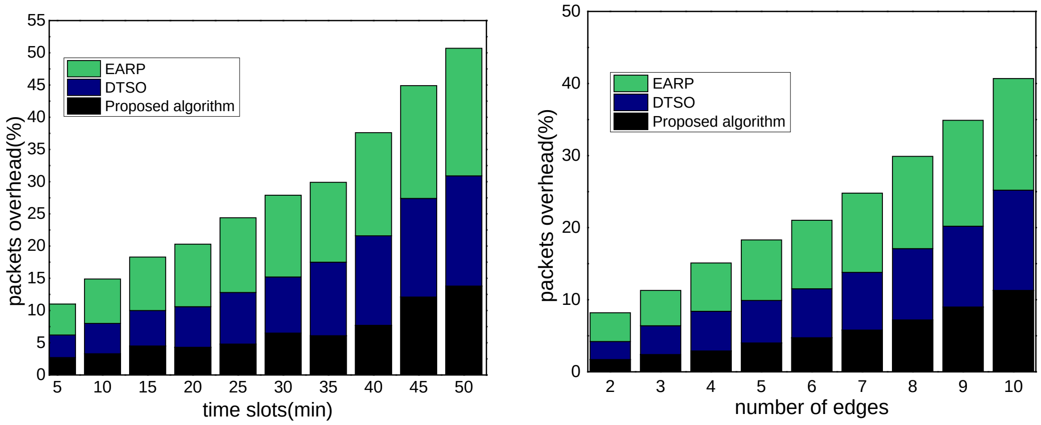
Figure 8. Evaluation of retransmission of packets for varying time slots and edges.

5.4. *Analysis of packets overhead*

The proposed model and alternative solution's performance are simulated in terms of packets overhead, as depicted in Figures 9(a) and 9(b). Packet overhead is defined as additional information sent along with the payload. According to experiments, the proposed model lowers overhead by 10.7% to 12.8% on average even if the number of malicious nodes increases. The neighbors' list is updated by exploring hop count and traffic flowing information, increases the efficient utilization of communication bandwidth. Based on the threshold method, the proposed model first checks whether a particular route is suitable for forwarding the IoT data or not. In case it is not an optimal decision, the proposed model investigates alternate routes for data transmission by balancing the load on the nodes. Moreover, the authentication methods of the proposed model decrease the probabilities for anomalies and, accordingly, it improves the communication cost for data aggregation at network edges.

5.5. *Analysis of loss rate*

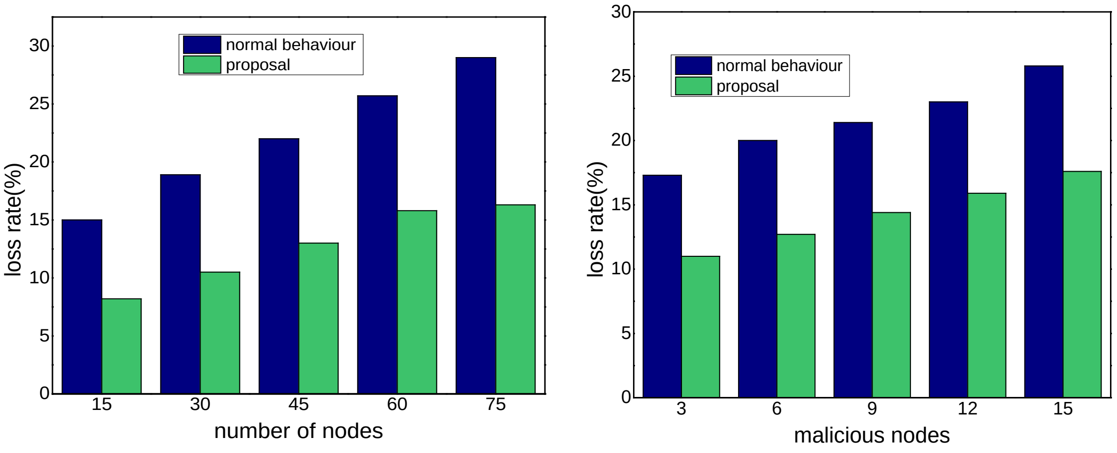
In Figures 10(a) and 10(b), simulation-based tests are shown to reveal the statistical result of the proposed model in terms of loss rate, which can be defined as the destruction of data packets sent over the communication link. The test was conducted to evaluate the normal and proposed behavior of the model in the presence of malicious nodes. The malicious nodes behave abnormally and false packets negatively affect response time for communication channels. Moreover, such nodes discard actual data from IoT sensors and increase compromise attacks. The experimental analysis is conducted under varying numbers of IoT nodes from 15 to 75. Under normal behavior, the simulation was tested without including malicious devices, while it was observed that the proposed model significantly improved the data loss rate by an average of 13.8% even in the existence of malicious nodes. This is due to the lightweight authentication and verification stage among ordinary sensors and edges. Moreover, data is fully protected with the support of encryption blocks, and without proper verification of nodes' identities, they are not allowed to cross the edge boundaries. All unknown data traffic is recorded in separate log files and, as a result, only communication links with malicious traffic below a certain threshold are marked as secure.



(a) Packets overhead and time slots

(b) Packets overhead and edges

Figure 9. Evaluation of packets overhead for varying time slots and edges.



(a) Loss rate and normal nodes

(b) Loss rate and malicious nodes

Figure 10. Evaluation of loss rate for varying normal and malicious nodes.

6. Conclusion

Tiny sensors, IoT and wireless technology make up smart networks, which collect and send massive amounts of data to cloud servers. The heterogeneous nodes collect multimedia data and enable network devices to access and further analyze the data. Homogeneous communication structures have been addressed in a variety of techniques with the support of edge computing, however, due to their resource limitations, embedded sensors-based systems face numerous research challenges. In addition, the integrity of information systems is also put at risk by unpredicted networks, which also presents various security problems. This research presents a multimedia surveillance system based on edge computing that manages IoT nodes with the help of mobile edges. Edges also control efficient data distribution by monitoring nearby neighbors and sharing reliable data within the network. In the proposed model, security methods are also used to achieve authentication and privacy. Before transmission of multimedia data, each device must first be authorized at the network edge using its identities and session keys. Experimental findings demonstrated the significant performance of the proposed work as compared to existing schemes, but it was noted that exploring any deep learning approach can further improve the intelligent criteria in routing the network data, and reduces the overheads on the constraint devices. In addition, in the future, we intend to increase the prediction capabilities of the proposed embedded system for detecting malicious activities using rules-based algorithms.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Funding

This research was funded by Princess Nourah bint Abdulrahman University and Researchers Supporting Project number (PNURSP2023R346), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Acknowledgement

This research was supported by Princess Nourah bint Abdulrahman University and Researchers Supporting Project number (PNURSP2023R346), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would also like to thank AIDA Lab CCIS Prince Sultan University, Riyadh KSA for support this publication.

Conflict of interest

The authors declare there is no conflict of interest.

References

1. Q. Tang, F. R. Yu, R. Xie, A. Boukerche, T. Huang, Y. Liu, Internet of intelligence: A survey on the enabling technologies, applications, and challenges, *IEEE Commun. Surveys Tutor.*, **24** (2022),

1394–1434. https://doi.org/10.1109/COMST.2017.2691349

2. I. Abunadi, A. Rehman, K. Haseeb, T. Alam, G. Jeon, A multi-parametric machine learning approach using authentication trees for the healthcare industry, *Expert Systems*, (2022), e13202. https://doi.org/10.1111/exsy.13202
3. I. Sarrigiannis, K. Ramantas, E. Kartsakli, P.-V. Mekikis, A. Antonopoulos, C. Verikoukis, Online VNF lifecycle management in an MEC-enabled 5G IoT architecture, *IEEE Int. Things J.*, **7** (2019), 4183–4194. https://doi.org/10.1109/JIOT.2019.2944695
4. S. H. Alsamhi, F. Afghah, R. Sahal, A. Hawbani, M. A. Al-qaness, B. Lee, et al., Green internet of things using UAVs in B5G networks: A review of applications and strategies, *Ad Hoc Networks*, **117** (2021), 102505. https://doi.org/10.1016/j.adhoc.2021.102505
5. L. Qiao, Y. Li, D. Chen, S. Serikawa, M. Guizani, Z. Lv, A survey on 5G/6G, AI, and Robotics, *Comput. Electr. Eng.*, **95** (2021), 107372. https://doi.org/10.1016/j.compeleceng.2021.107372
6. M. A. Matheen, S. Sundar, IoT multimedia sensors for energy efficiency and security: A review of QoS aware and methods in wireless multimedia sensor networks, *Int. J. Wireless Inform. Networks*, **29** (2022), 407–418. https://doi.org/10.1007/s10776-022-00567-6
7. M. K. Gupta, P. Chandra, Effects of similarity/distance metrics on k-means algorithm with respect to its applications in IoT and multimedia: A review, *Multi. Tools Appl.*, **81** (2022), 37007–37032. https://doi.org/10.1007/s11042-021-11255-7
8. L. A.Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider, IoT Privacy and security: Challenges and solutions, *Appl. Sci.*, **10** (2020), 4102. https://doi.org/10.3390/app10124102
9. J. Lloret, M. García, F. Boronat, IPTV: la televisión por Internet, Editorial Vértice, Málaga, España, (2008), 230.
10. A. Rego, A. Canovas, J. M. Jiménez, J. Lloret, An intelligent system for video surveillance in IoT environments, *IEEE Access*, **6** (2018), 31580–31598. https://doi.org/10.1109/ACCESS.2018.2842034
11. I. H. Sarker, Machine learning: Algorithms, real-world applications and research directions, *SN Computer Sci.*, **2** (2021), 160. https://doi.org/10.1007/s42979-021-00592-x
12. K. Haseeb, T. Saba, A. Rehman, I. Ahmed, J. Lloret, Efficient data uncertainty management for health industrial internet of things using machine learning, *Int. J. Commun. Syst.*, **34** (2021), e4948. https://doi.org/10.1002/dac.4948
13. J. Serra, L. Sanabria-Russo, D. Pubill, C. Verikoukis, Scalable and flexible IoT data analytics: When machine learning meets SDN and virtualization, in 2018 *IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2018, IEEE. https://doi.org/10.1109/CAMAD.2018.8514997
14. W. Chen, Intelligent manufacturing production line data monitoring system for industrial internet of things, *Computer Commun.*, **151** (2020), 31–41. https://doi.org/10.1016/j.comcom.2019.12.035
15. A. Rehman, T. Saba, K. Haseeb, R. Singh, G. Jeon, Smart health analysis system using regression analysis with iterative hashing for IoT communication networks, *Computers Electr. Eng.*, **104** (2022), 108456. https://doi.org/10.1016/j.compeleceng.2022.108456
16. L. Sanabria-Russo, J. Alonso-Zarate, C. Verikoukis. SDN-based pro-active flow installation mechanism for delay reduction in IoT, in 2018 *IEEE Global Communications Conference (GLOBECOM)*, 2018, IEEE. https://doi.org/10.1109/GLOCOM.2018.8647382
17. B. Zong, C. Fan, X. Wang, X. Duan, B. Wang, J. Wang, 6G technologies: Key drivers, core requirements, system architectures, and enabling technologies, *IEEE Vehicular Technol. Mag.*, **14**

(2019), 18–27. https://doi.org/10.1109/MVT.2019.2921398

18. L. Mucchi, S. Jayousi, S. Caputo, E. Paoletti, P. Zoppi, S. Geli, et al., How 6G technology can change the future wireless healthcare, in 2020 *2nd 6G wireless summit (6G SUMMIT)*, 2020, IEEE. https://doi.org/10.1109/6GSUMMIT49458.2020.9083916
19. S. A. Dehkordi, K. Farajzadeh, J. Rezazadeh, R. Farahbakhsh, K. Sandrasegaran, M. A. Dehkordi, A survey on data aggregation techniques in IoT sensor networks, *Wireless Networks*, **26** (2020), 1243–1263. https://doi.org/10.1007/s11276-019-02142-z
20. M. Alam, A. A. Aziz, S. Latif, A. Awang, Error-aware data clustering for in-network data reduction in wireless sensor networks, *Sensors*, **20** (2020), 1011. https://doi.org/10.3390/s20041011
21. X. Duan, N. Song, F. Mo, An edge intelligence-enhanced quantitative assessment model for implicit working gain under mobile internet of things, *Math. Biosci. Eng.*, **20** (2023), 7548–7564. https://doi.org/10.3934/mbe.2023326
22. L. P.Verma, V. K. Sharma, M. Kumar, A. Mahanti, An adaptive multi-path data transfer approach for MP-TCP, *Wireless Networks*, (2022), 1–28. https://doi.org/10.1007/s11276-022-02958-2
23. H.-S. Kim, J. Paek, D. E. Culler, S. Bahk, PC-RPL: Joint control of routing topology and transmission power in real low-power and lossy networks, *ACM Transact. Sensor Networks (TOSN)*, **16** (2020), 1–32. https://doi.org/10.1145/3372026
24. N. A. Zardari, R. Ngah, O. Hayat, A. H. Sodhro, Adaptive mobility-aware and reliable routing protocols for healthcare vehicular network, *Math. Biosci. Eng.*, **19** (2022), 7156–7177. https://doi.org/10.1007/s11036-022-02042-1
25. S. Ksibi, F. Jaidi, A. Bouhoula, A comprehensive study of security and cyber-security risk management within e-Health systems: Synthesis, analysis and a novel quantified approach, *Mobile Networks Appl.*, (2022), 1–21. https://doi.org/ 10.3934/mbe.2022338
26. J. Li, D. Greenwood, M. Kassem, Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases, *Autom. Construct.*, **102** (2019), 288–307. https://doi.org/10.1016/j.autcon.2019.02.005
27. G. Fortino, A. Guerrieri, P. Pace, C. Savaglio, G. Spezzano, Iot platforms and security: An analysis of the leading industrial/commercial solutions, *Sensors*, **22** (2022), 2196. https://doi.org/10.3390/s22062196
28. D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, et al., 6G Internet of Things: A comprehensive survey, *IEEE Int. Things J.*, **9** (2021), 359–383. https://doi.org/10.1109/JIOT.2021.3103320
29. M. Banafaa, I. Shayea, J. Din, M. H. Azmi, A. Alashbi, Y. I. Daradkeh, et al., 6G mobile communication technology: Requirements, targets, applications, challenges, advantages, and opportunities, *Alexandr. Eng. J.*, (2022). https://doi.org/10.1016/j.aej.2022.08.017
30. H. Lu, L. Wu, G. Fortino, S. Dustdar, Introduction to the special section on cognitive robotics on 5G/6G networks, 2021, in *ACM Transactions on Internet Technology (TOIT)* , **21**(2021), 1–3. https://doi.org/10.1145/3476466
31. W. Shi, W. Xu, X. You, C. Zhao, K. Wei, Intelligent reflection enabling technologies for integrated and green Internet-of-Everything beyond 5G: Communication, sensing, and security, *IEEE Wireless Commun.*, 2022. https://doi.org/10.1109/MWC.018.2100717
32. H. H. H.Mahmoud, A. A. Amer, T. Ismail, 6G: A comprehensive survey on technologies, applications, challenges, and research problems, *Transact. Emerg. Telecommun. Technol.*, **32** (2021), e4233. https://doi.org/10.1002/ett.4233

33. G. Rathee, A. Sharma, H. Saini, R. Kumar, R. Iqbal, A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology, *Multi. Tools Appl.*, **79** (2020), 9711–9733. https://doi.org/10.1007/s11042-019-07835-3
34. D. Singh, A. K. Maurya, R. K. Dewang, N. Keshari, A review on Internet of Multimedia Things (IoMT) routing protocols and quality of service, *Int. Multi. Things (IoMT)*, (2022), 1–29. https://doi.org/10.1016/B978-0-32-385845-8.00006-
35. A. A. Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, S. Kot, Internet of Things (IoT) security with blockchain technology: A state-of-the-art review, *IEEE Access*, (2022). https://doi.org/10.1109/ACCESS.2022.3223370
36. M. A. Jan, J. Cai, X.-C. Gao, F. Khan, S. Mastorakis, M. Usman, et al., Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions, *J. Network Computer Appl.*, **175** (2021), 102918. https://doi.org/10.1016/j.jnca.2020.102918
37. Moussa, N., D. Benhaddou, A. El Belrhiti El Alaoui, EARP: An Enhanced ACO-Based Routing Protocol for Wireless Sensor Networks with Multiple Mobile Sinks. *Int. J. Wireless Inform. Networks*, **29** (2022), 118–129. https://doi.org/10.1007/s10776-021-00545-4
38. N. Hu, Z. Tian, X. Du, M. Guizani, An energy-efficient in-network computing paradigm for 6G, *IEEE Transact. Green Commun. Network.*, **5** (2021), 1722–1733. https://doi.org/10.1109/TGCN.2021.3099804
39. A. Kumar, S. Sharma, N. Goyal, S. K. Gupta, S. Kumari, S. Kumar, Energy-efficient fog computing in Internet of Things based on routing protocol for low-power and lossy network with Contiki, *Int. J. Commun. Syst.*, **35** (2022), e5049. https://doi.org/10.1002/dac.5049
40. Z. Liao, J. Peng, J. Huang, J. Wang, J. Wang, P. K. Sharma, et al., Distributed probabilistic offloading in edge computing for 6G-enabled massive Internet of Things, *IEEE Int. Things J.*, **8** (2020), 5298–5308. https://doi.org/10.1109/JIOT.2020.3033298
41. K. Thangaramya, K. Kulothungan, S. I. Gandhi, M. Selvi, S. S. Kumar, K. Arputharaj, Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN, *Soft Comput.*, **24** (2020),16483–16497. https://doi.org/10.1007/s00500-020-04955-z
42. A. Singh, A. Nagaraju, Low latency and energy efficient routing-aware network coding-based data transmission in multi-hop and multi-sink WSN, *Ad Hoc Networks*, **107** (2020), 102182. https://doi.org/10.1016/j.adhoc.2020.102182
43. Z. Ming, J. Chen, L. Cui, S. Yang, Y. Pan, W. Xiao, et al., Edge-based video surveillance with graph-assisted reinforcement learning in smart construction, *IEEE Int. Things J.*, **9** (2021), 9249–9265. https://doi.org/10.1109/JIOT.2021.3090513
44. B. Kizilkaya, , E. Ever, H. Y. Yatbaz, A. Yazici, An effective forest fire detection framework using heterogeneous wireless multimedia sensor networks, *ACM Transact. Multi. Comput., Commun. Appl. (TOMM)*, **18** (2022), 1–21. https://doi.org/10.1145/3473037
45. O. Ibrihich, S.-d. Krit, J. Laassiri, S. El Hajji, Study and simulation of protocols of WSN using NS2, *Transact. Eng. Technol.*, 2015, Springer, 467–480. https://doi.org/10.1007/978-94-017-9804-4_32