electronics

MDPI

Article

Energy-Efficient Edge Optimization Embedded System Using Graph Theory with 2-Tiered Security

Tanzila Saba [1], Amjad Rehman [1], Khalid Haseeb [2], Saeed Ali Bahaj [3] and Gwanggil Jeon [1,4,*]

[1] Artificial Intelligence & Data Analytics Lab (AIDA) CCIS, Prince Sultan University, Riyadh 12435, Saudi Arabia
[2] Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Pakistan
[3] MIS Department, College of Business Administration, Prince Sattam bin Abdulaziz University, Alkharj 11942, Saudi Arabia
[4] Department of Embedded Systems Engineering, College of Information Technology, Incheon National University, Incheon 22012, Korea
* Correspondence: gjeon@inu.ac.kr

Abstract: The development of the Internet of Things (IoT) network has greatly benefited from the expansion of sensing technologies. These networks interconnect with wireless systems and collaborate with other devices using multi-hop communication. Besides data sensing, these devices also perform other operations such as compression, aggregation, and transmission. Recently, many solutions have been proposed to overcome the various research challenges of wireless sensor networks; however, energy efficiency with optimized intelligence is still a burning research problem that needs to be tackled. Thus, this paper presents an energy-efficient enabled edge optimization embedded system using graph theory for increasing performance in terms of network lifetime and scalability. First, minimum spanning trees are extracted using artificial intelligence techniques to improve the embedded system for response time and latency performance. Second, the extracted routes are provided with full protection against anonymous access in a two-tiered system. Third, the IoT systems collaborate with mobile sinks, and they need to be authenticated using lightweight techniques for the involvement in routing sensed information. Moreover, edge networks further provide the timely delivery of data to mobile sinks with less overhead on IoT devices. Finally, the proposed system is verified using simulations, revealing its significance to existing approaches.

Keywords: energy efficiency; artificial intelligence; Internet of Things; tiered security; edge processing; technological development

Citation: Saba, T.; Rehman, A.; Haseeb, K.; Bahaj, S.A.; Jeon, G. Energy-Efficient Edge Optimization Embedded System Using Graph Theory with 2-Tiered Security. *Electronics* **2022**, *11*, 2942. https://doi.org/10.3390/electronics11182942

Academic Editor: Shinichi Yamagiwa

Received: 14 August 2022
Accepted: 11 September 2022
Published: 16 September 2022

1. Introduction

Due to an emerging networking environment, the number of users and applications is growing exponentially. The traffic of data going through the base station also increases as the number of users increases. Device-to-device (D2D) communication is seen as one of the best ways to reduce the chance of cellular users losing service in 5G [1–3]. The cellular licensed band can be used for D2D communication in an underlay or an overlay mode [4,5]. Integrating sensors, embedded computing, and communication technologies are known as the Internet of Things (IoT). The IoT is designed to provide seamless services to everything, at any time, everywhere. After the internet and information and communication technology, IoT technologies play a critical role everywhere, especially in developing smart systems [6–8]. Accordingly, to researchers and the community, IoT will have a greater influence on society than the internet and information and communication technologies, which will benefit both sectors and society [9–11]. The usage of a prospective IoT system allows common system-level design challenges such as energy efficiency, robustness, scalability, interoperability, and security concerns to be addressed. A high degree of physical security is essential for

wireless communications in the IoT to complement conventional security measures used at high levels since IoT is anticipated to convey significant and private information [12,13].

On the other hand, edge computing is a standard evolving to meet the rising networking needs from end devices to intelligent objects [14,15]. For reduced latency, increased security, and privacy, edge computing enables the processing to be offloaded from cloud data centers to the network edge and edge nodes [16,17]. However, due to the complex relationships between edge devices, edge servers, and cloud data centers, energy efficiency in edge computing has received far less attention than it has in cloud data centers. Much research has investigated the development of the optimizing system with the support of artificial intelligence [18,19]. They increased energy efficiency with improved data delivery, but it is still a hot problem and needs more attention. The proposed solution should be able to impose the least overhead on low-powered devices and avoid unnecessary data transferring.

The proposed system provides the main contributions as follows:

i. It proposes an intelligent method for extracting minimal spanning trees using theory.
ii. The cost function is optimized using real-time parameters and, accordingly, end-to-end routes are identified.
iii. It provides security on two main entrance points: from the IoT system to edge devices and from edge devices to mobile sinks. Such tiers protect against network threats and increase the reliability of the nodes.
iv. The proposed system is tested and validated in its performance in terms of resource management and energy efficiency.

The rest of the paper is organized in the following subsections. Section 2 presents the related work. Section 3 highlights the problem statement. Section 4 explains the overview of the proposed system with all its components. In Section 5, the simulation environment is explained, and in Section 6, experimental results and discussions are provided. Finally, Section 7 ends this research work with future directions.

2. Literature Work

The IoT provides an internet-connected civilization where smart objects gather data and monitor environmental conditions. IoT deployment is hard and needs edge computing for the processing of real-time data and improved system performance [20–22]. Energy efficiency is one of the most demanding issues in IoT scenarios, as sensors, actuators, and smart devices are battery-powered devices with limited constraints. In [23] authors discuss utilizing an edge-IoT platform and a social computing framework to design a smart energy-efficient building system. The system was evaluated in a public venue, and the results illustrate edge computing's energy efficiency and framework benefits. The benefits include reduced IoT-edge-to-cloud data transfer, computation, and network costs. The authors of [24] studied the possibilities of merging blockchain with SDN. They presented a safe, energy-efficient blockchain-enabled SDN controller architecture for IoT networks utilizing a cluster topology and novel routing protocol. With the elimination of proof-of-work (POW) and the adoption of an effective authentication strategy with distributed trust, the design uses both public and private blockchains for peer-to-peer (P2P) communication between IoT devices and SDN controllers. In addition, the cluster-based routing protocol provided better throughput, lower latency, and lower energy consumption than EESCFD, SMSN, AODV, AOMDV, and DSDV. Network devices provide real-time data to gateways and remote servers for processing and display. Data transferred by these devices are subject to hostile attacks; thus, privacy and integrity must be maintained. In [25], the authors introduced LightIoT, a lightweight and secure connectivity method for healthcare infrastructure devices. LightIoT was initialized, paired, and authenticated. These steps assure data reliability by creating safe sessions among communication entities (wearable, gateways, and a remote server). Statistical findings showed that their technique was lightweight, robust, and resilient against various adversarial attacks and incurred substan-

tially lower computational and communication costs for transmitted data than previous approaches. The authors of [26] also presented a cooperative offloading approach based on the Lagrangian suboptimal convergent computation offloading algorithm (LSCCOA) for multiaccess MEC in a dispersed Internet of Things (IoT) network. A computational rivalry amongst SCDs for limited resources impeding job offloading for MEC is explored in a high-demand IoT network. The proposed suboptimal computational approach is applied to accomplish task offloading that is optimized at the cloud edge server without transferring it to the centralized network. In the form of a mixed-integer optimal solution, this led to a minimum weighted total of transmit power consumption and outputs. In addition, the resulting fast-convergent suboptimal method is used to solve the non-deterministic polynomial-time (NP) hard problem. To increase lifespan using a trustworthy approach, trust-based energy efficient data collecting with an unmanned aerial vehicle (TEEDC-UAV) scheme is proposed [27]. Firstly, an ant colony-based unmanned aerial vehicle (UAV) trajectory optimization technique is developed. This approach forms the most data anchors in the working field with the shortest route and improves network lifetime. To increase the trust for collected data, trust reasoning and evolution are presented and ensure the degree of privacy in sensor nodes. The issue of network throughput optimization for an IRS-assisted multihop MEC network is investigated in [28], where it is necessary to jointly optimize the IRS's phase shifts and the relays' resource allocation. However, it is challenging to address the studied problem by simply using known optimization techniques because of the coupling among the transmission lines of different hops generated by the utilization of the IRS and the complex multi-hop network topology. Fortunately, it has been demonstrated that the network throughput may be accurately approximated by the second smallest eigenvalue of the network Laplacian matrix by taking advantage of the underlying structure of the network topology and spectral graph theory. In [29], the authors have proposed a novel solution for optimizing security with IoT networks. The proposed approach implements the IoT security framework among devices using dominating sets and centrality measures. The findings show that the network's overall security improved, while there was a nominal effect on network traffic. In [30], the authors have presented a trust management system (TMS) for large-scale IoT systems called Trust2Vec. The proposed TMS can manage trust relationships in large-scale IoT systems and can counter large-scale trust attacks that are carried out by a large number of malicious devices. To navigate the trust relationship between devices and compute trust network embeddings, Trust2Vec uses a random-walk network exploration algorithm. This allows it to analyze the latent network structure of trust relationships even when there is no direct trust rating between two malicious devices. It also proposed a network embeddings community identification technique that recognizes and prevents communities of malicious nodes to detect large-scale attacks such as self-promotion and badmouthing.

3. Problem Statement

Researchers conclude that IoT systems are extensively used in several smart applications, including healthcare, smart homes, security surveillance, and the military. However, the limited resources explicitly reduce the performance results in terms of integrity and response interval. Furthermore, it is clear that a variety of solutions have been proposed to secure the IoT platform, but doing so results in more messages passing over the communication links, which negatively impacts the platform's sustainability. Additionally, the majority of the solutions do not make intelligent decisions, which usually results in retransmissions and incurs network congestion. Based on these constraints, our proposed system integrates edge computing with SDN controllers, which provide security using blockchain technology and intelligence utilizing graph theory.

4. Energy-Efficient Enabled Reliable Edge-SDN Protocol with Graph Theory

This section presents our proposed energy-efficient reliable edge network using graph theory. The proposed system learns from environmental and node behaviors. It not

only offers a fault-tolerant solution but, on the other hand, also prevents communication paradigms from external attacks. It consists of two layers. One layer is among IoT components and edge networks, and the second layer is among edge networks to mobile sinks. Moreover, the SDN controller supervises the overall communication with its intelligent decisions and improves the constraint utilization for the nodes. The phases of network creation, protocol communications, message flow, and security are all explained in this section. The SDN controller checks the network surroundings randomly, and, when it obtains unauthorized access, it sends alert messages to devices.

4.1. System Model

We model the network system with sensors N, edges, and sink nodes. Furthermore, SDN controllers are considered in the proposed system for efficient management of device constraints. Nodes belong to a particular group and each group is associated with the gateway. All the groups and nodes have unique identities. The received signal strength indicator (RSSI) determines the distance between nodes. The border nodes are considered edge nodes and have sufficient intelligence to make local decisions. All the edges are interconnected with each other to formulate a routing chain and provide the necessary information among network structures to the SDN controller. We assume the following network assumptions:

i. Nodes are randomly deployed in the targeted area.
ii. Nodes are static with mobile gateways.
iii. Gateways can perform data aggregation and maintain proximity tables.
iv. Tables are not static and frequently change the information when any event incurs.
v. Sensor nodes cannot direct communication with edge devices.
vi. If the residual energy of any node is below the threshold, its flag value is zero.

4.2. Discussion

In this section, we present the discussion of the proposed system. The various states of the proposed system and their interactions are depicted in Figure 1. Firstly, network nodes and devices need to register with the nearest gateway device, and later, the weighted condition is evaluated for the generation of subgraphs. Edge devices frequently transmit the network information to the SDN controller, which helps the system to cope with network monitoring. Once all is in control, the data are verified and nodes participate in the blockchain technology [31] to ensure security with integrity. Initially, each node begins to create its memory table with the received information of the neighbors. Then, each neighbor floods their local information with other nodes that reside in the same transmission range. Let us assume the initial routes are denoted by r_1, $r_1, r_1, \ldots,$ r_1. In the proposed system, whenever any node needs to transmit either its sense data or attributes, it follows any available route from the identified set, as defined below.

$$R_i = r1,\ r2,\ r3,\ \ldots.\ rn; \tag{1}$$

subject to

$$i\ \varepsilon\ N$$

In the proposed system, the nodes are organized in an undirected and weighted graph $G(N, E)$. The nodes have no circuit, and each edge has a single weighted value. The weighted value indicates the route cost. The combination of sub-routes made a cumulative cost $W(T)$, as given in Equation (2).

$$W(T) = \sum_i^k w\_i\ (u, v) \tag{2}$$

All the identified minimum spanning trees are considered as the groups. In the group's proximity, edge devices are located for data aggregation and transmission toward the SDN layer. Our system utilizes the concept of graph theory. It identifies minimum spanning

trees from Graph G. Each minimum spanning tree is referred to as a subset of Graph G. Moreover, the proposed system identifies primary and secondary minimum spanning trees as defined below.

$$S1,\ S2\ \varepsilon\ G(N,\ E) \tag{3}$$

In the proposed system, we explore the Krushkal algorithm for identifying subgraphs or minimum spanning trees [32]. The weighted cost is optimized rather than a single distance value and computed using dynamic attributes of the network. We consider energy e, link lost lnl, and latency_time l_t parameters for the evaluation of the minimum weighted cost of each link, as given in Equation (4).

$$min(w\_i) = 1/(e + lnl + l_t) \tag{4}$$

In Equation (4), e is computed based on the consumed power in sending and receiving the data packets, as given below.

$$K * (Pr + Pt)/N \tag{5}$$

where Pr is receiving power, Pt is transmission power, K denotes the number of data packets, and N is defined as nodes. In the local table, the entry of any node is maintained until its energy consumption is less than the preset threshold, as defined in Equation (6).

$$e(s\_i\ \varepsilon\ N,\ R) < threshold \tag{6}$$

Link interference determines the performance of the connected link among consecutive nodes. The link interference is the combination of the data lost DL and error computation EC, as given in Equation (7).

$$lnl = DL + EC \tag{7}$$

Whenever either data loss or the error ratio increases, the link performance obtained the least priority, and such a link is avoided from consideration in a communication system. To determine the latency time for a particular link, the proposed system utilizes the round-trip time (RTT) in flooding of some beacon messages, m. Thus, l_t can be determined, as given in Equation (8).

$$l_t\ =\ m\ *\ RTT \tag{8}$$

Moreover, in the proposed system, the outcome of all the metrics is forwarded to the SDN controller, and it creates a record of the individual route. The proposed system explores the intelligence of the SDN controller, which, whenever the value of the computed metrics decreases to a certain threshold, sends the reformulation of a route with the support of an edge device. The proposed system uses the Krushkal algorithm to construct a routing path with a minimum weighted cost:

i. Firstly, the source node selects the edge from its neighbor based on the minimum weighted cost $min(w\_i)$
ii. Moreover, it is continuously monitored so that the selected edge does not create a loop.
iii. Finally, the execution of the Krushkal algorithm stops if edges $m - 1$ are included in the route.

Figure 2 depicts the flowchart of the proposed system in terms of subgraph-based data transmission for IoT networks. The proposed system comprised two main components. First, each node in the network initialization process needs to be registered with the nearest gateways. Later, nodes are organized into undirected weighted graphs and based on the optimal condition, and the proposed system extracts various spanning trees. Among these spanning trees, the proposed system selects the minimum one for routing the IoT data with the support of gateways.

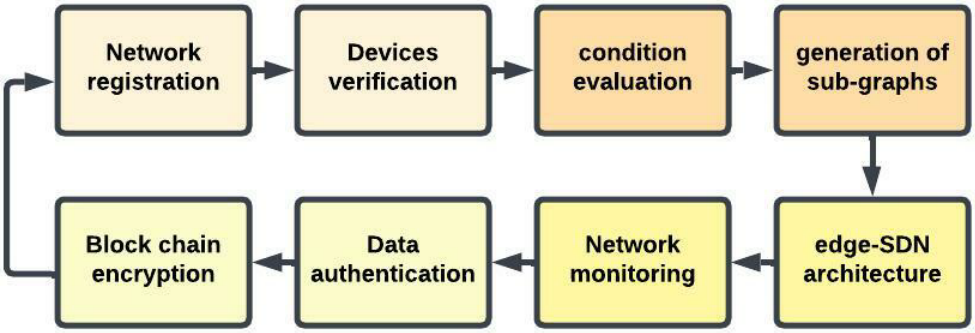


Figure 1. States of the proposed system with their interactions.

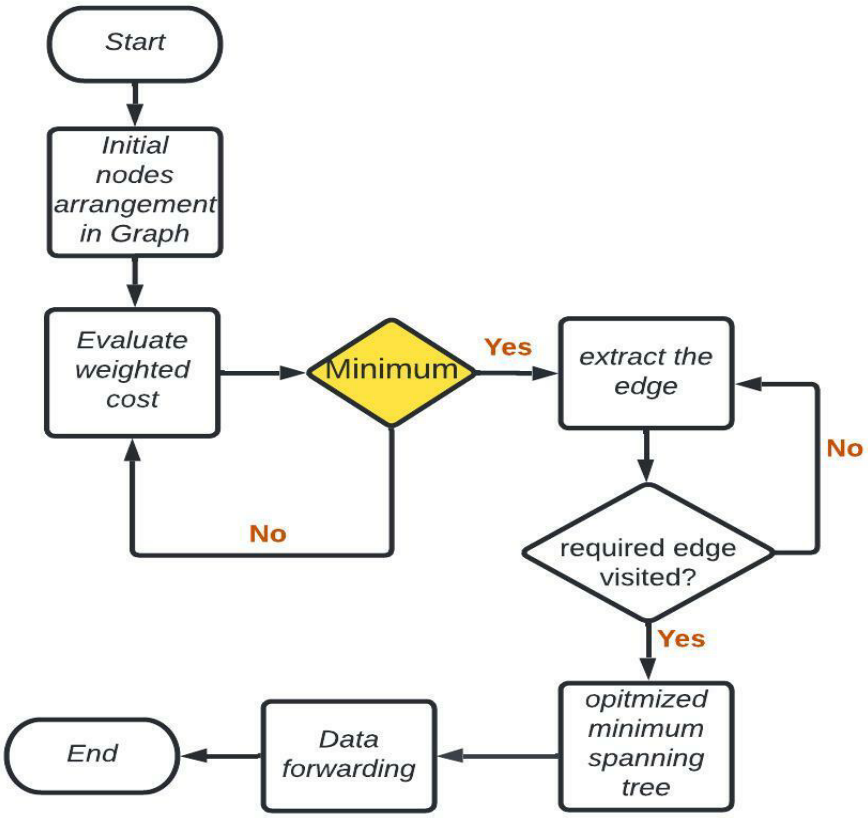


Figure 2. Flowchart of the proposed system for optimized subgraphs using graph theory.

4.3. IoT-Security with SDN Architecture

The proposed system provides the security for a two-tier architecture. In the first phase, nodes establish secure sessions with gateway nodes, and in the second phase gateway nodes communicate securely with SDN using the collaboration of edge devices. The main security measurements and computing costs are performed in the SDN controller. In the beginning, the sensor nodes are requested by edge nodes so their information can be registered in the SDN controller. The registration packet RQ is composed of node identity Nid, energy $Nenergy$, and time stamp TS fields, as given in Equation (9).

$$RQ = (Nid,\ Nenergy,\ TS) \tag{9}$$

Inside the table, the SDN controller also stores the neighbor identities. In the proposed system, the SDN controller acts as a key distribution center (KDC) and also has global knowledge of the entire network. Once the SDN controller receives the request of the nodes,

it verifies their identities using its table. If they are authentic, the SDN controller generates secret keys s_k for ni nodes that are digitally signed by its master key MK, as given below.

$$SDN \rightarrow ni: E\_MK(s\_k) \quad (10)$$

Upon receiving the keys, nodes verify them, and once the outcome is positive, the node registers itself in the blockchain. The blockchain is the combination of the hash values in the form of a chain, and this technology is executed until the entire route is fully secured against privacy and integrity attacks. The chain comprises various data blocks, and each block is separately encrypted with digital signs to ensure its authentication. Each device uses the principle of blockchain in a distributed manner and provides the system with the highest degree of reliability. The encryption of each block is performed with a one-time pad and data bits key by using the xor operation. The digital hashes offer the integrity of the devices. Any third-party or intermediate device is not permitted to access the IoT data until it has permission. The data-originating node can control its data and in which way it can be accessed by other devices. Figure 3 illustrates the working principle of the proposed system for ensuring security with the support of SDN controllers. On receiving the IoT data, the gateways further forward it to the edge layer for reducing the response time. Moreover, the data are also verified at edge devices, and, accordingly, the information regarding the data and the network is sent to the SDN controller. In this way, the SDN controller keeps the updated information about the network, and, if in any case, the performance is unsatisfactory, the SDN controller sends the warning message to the edge device to reformulate the routing process. After completing the routing phase and authentication processes, the proposed system explores blockchain technology, and nodes register themselves in the chain to ensure integrity with privacy.

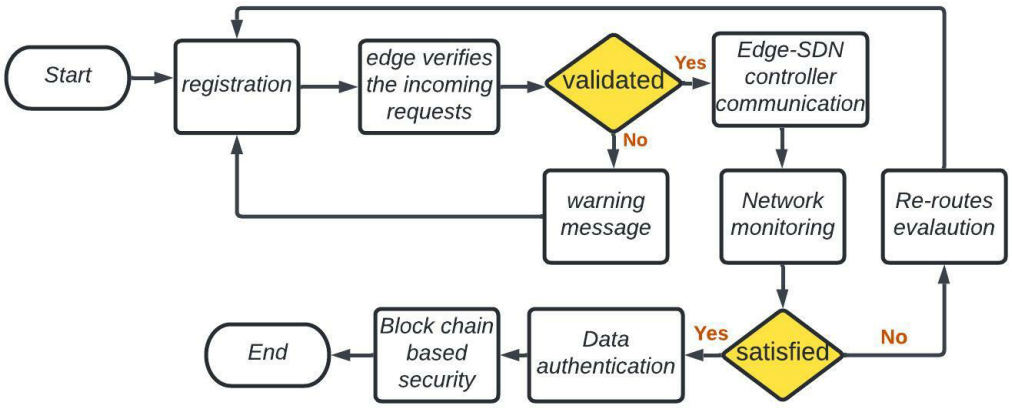


Figure 3. Flowchart of the proposed system for SDN-based security with blockchain.

5. Simulations

This section explains the proposed system's network design and evaluation results and other work. We simulated the network environment based on the varying size of data and the number of nodes. Nodes were deployed randomly with gateway and edge nodes. SDN controllers had no limitations in terms of constraints. We tested the experiments on a Core i7 laptop on Ubuntu operating with 32 GB RAM and 1 TB hard drive. The results were evaluated for throughput, packet drop ratio, propagation delay, and node overhead. The simulations were run with 75 to 375 nodes, and data sizes varied from 10 to 50 KB. The simulation was run for 5000 s. Nodes had a homogeneous structure in terms of resources. However, the initial energy of the nodes starts from 3j to 6j. We performed 15 simulations to evaluate the results. The transmission power of the nodes was fixed to 10 m. The network dimension was set to 5000 m $\times$ 5000 m. The number of gateways and edge devices was set to 10 and 5. Malicious nodes were also distributed in the simulated environment to evaluate the proposed system's link interruption and data accuracy performance. Table 1 shows the simulation parameters that were utilized in the experiments.

Table 1. Simulation parameters.

Parameters	Values
Simulation area	5000 m × 5000 m
Sensors	75–375
Data size	10–50 KB
Transmission power	10 m
Initial energy	3–6 j
Simulations	15
Edge devices	5
Gateway nodes	10
Size of control packet	512 bits

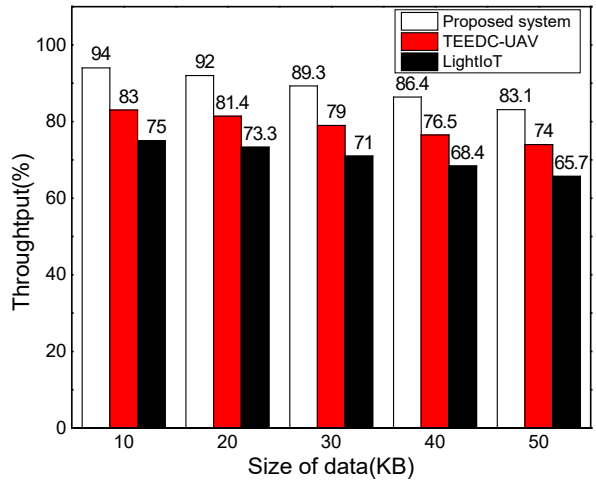
6. Results and Discussion

This section provides the experimental discussion in terms of various network metrics. The evaluation metrics are considered throughput, packet drop ratio, propagation delay, and node overhead. In terms of network throughput, the proposed system performed better than the previous work, as shown in Figure 4a,b. The proposed system significantly increased network throughput by an average of 19% and 22%, respectively, as shown by the experiment's findings. This is because the proposed system uses graph theory and extracts the spanning trees based on the minimum cost. Moreover, the routes were updated by exploring the link lost rate and latency parameters. It provided the timely delivery of actual data packets with efficient bandwidth utilization. The proposed security algorithm also increased the system's strength using private keys and eliminated the false packets from the actual data. Figure 5a,b compare the performance result of the proposed system with related solutions in terms of propagation delay. It was observed that as nodes and data sizes increased, the propagation delay also increases. However, the experimental results show that the proposed system improved the propagation delay by 19% and 31% on average. This was due to the artificial intelligence approach and computing of the cost function for determining optimal routes.

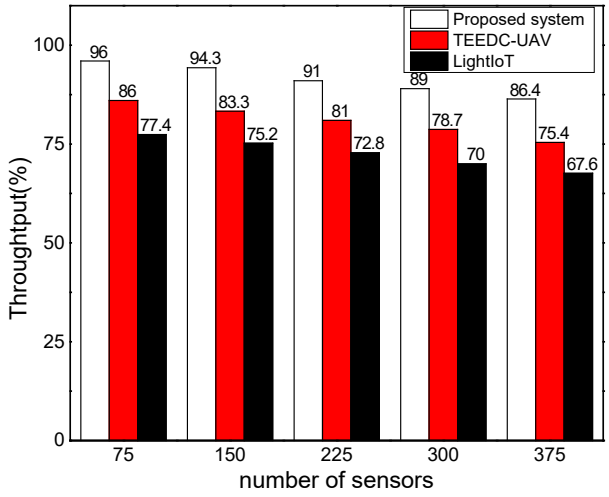
Furthermore, the subgraphs offered the shortest routes with link evaluation and led to a lower cost for the communication channels. Moreover, the proposed system minimized most harmful attacks from the IoT layer, and edge devices intelligently secured channels towards the SDN controller. Figure 6a,b illustrate how the SDS-GIoT protocol outperformed in contrast to other solutions in terms of the packet drop ratio. The performance results illustrate that when the number of nodes and data sizes grew, the packet loss fraction also rose. However, compared to other related work, the proposed system reduced packet loss rates by an average of 39% and 41%. This is because network resources are managed well, and the system is trained using graph theory principles. Moreover, the SDN controller continuously monitors the network flow and, whenever the performance is not satisfied, the SDN controller gives instructions to the edge device to reroute the data using various conditions. Furthermore, routing tables were updated, and those nodes were removed by the SDN controller, whose energy was less than the threshold. In comparison to the majority of the related work, the communication links were regularly monitored for latency and data loss. Whenever a harmful activity was carried out, the relevant warning messages were logged in the forwarding tables, and nodes were notified about the situation. The experimental findings of the proposed system are compared with other work in terms of nodes overhead, as illustrated in Figure 7a,b. It was observed that the node overhead increased as the number of nodes and data sizes increased. However, the proposed system balanced the energy load on the nodes and accordingly reduced the excessive overheads for the network. It was noticed that the proposed system improved the nodes' overhead by

an average of 28% and 37%, respectively. This is because of the use of intelligent computing, which increased the stability of the IoT network with the collaboration of edge computing.

Furthermore, the proposed system balanced network traffic load using SDN controller monitoring. The SDN controller had all the information about the network due to exploring the agents' capabilities. Accordingly, it efficiently decreased the additional overhead on the nodes and links for formulating routing paths. Moreover, SDN acts as a KDC and further minimized the overhead on the constraint nodes to ensure data security.



(**a**)



(**b**)

Figure 4. Performance results for varying data sizes and sensors for throughput. (**a**) Throughput with varying data size; (**b**) throughput with varying number of sensors.

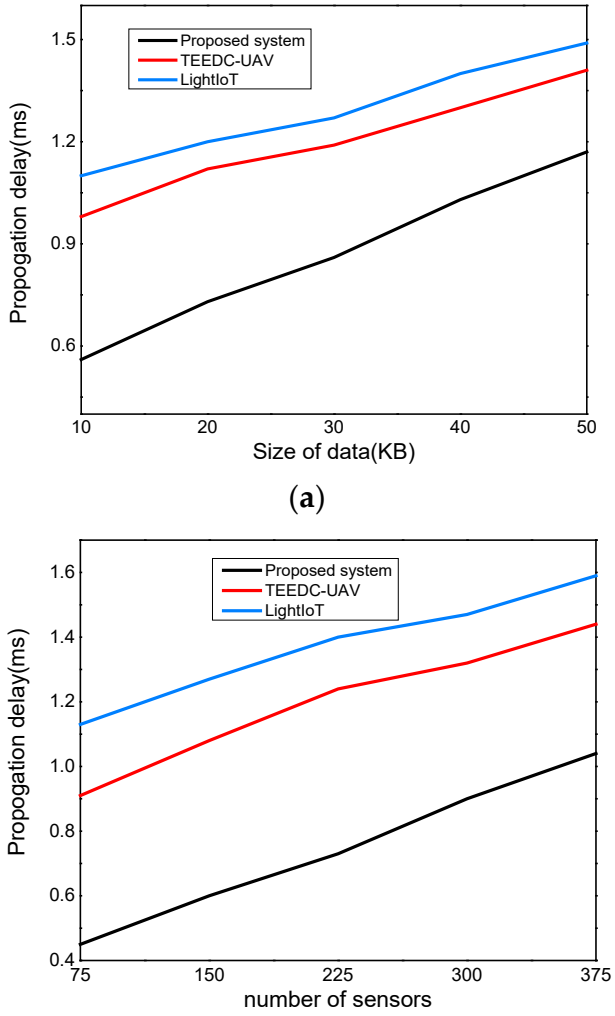


Figure 5. Performance results for varying data sizes and sensors for propagation delay. (**a**) propagation delay with varying data size (**b**) propagation delay with varying number of sensors.

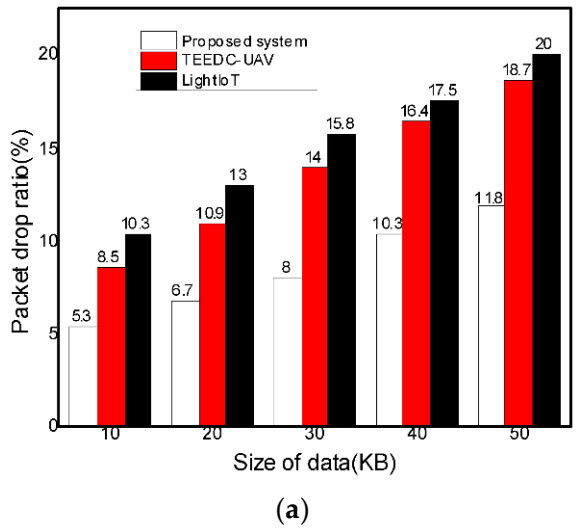
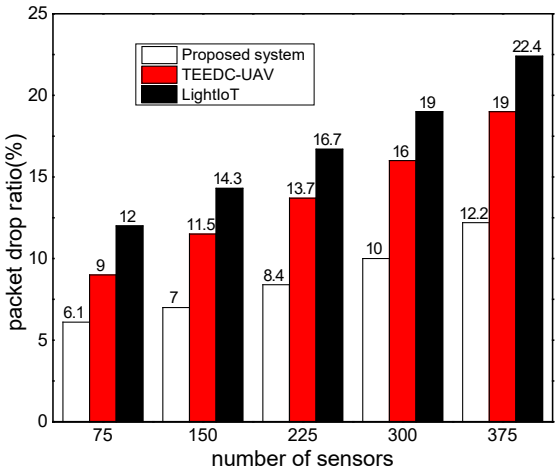
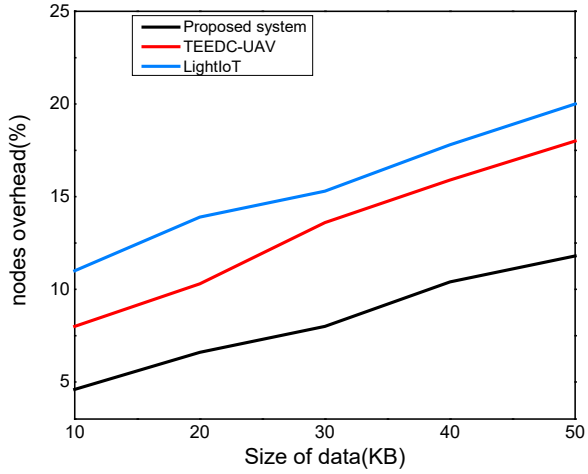


Figure 6. *Cont.*

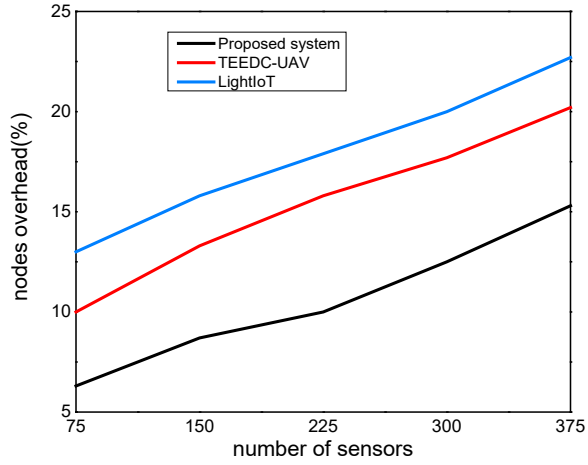


(**b**)

Figure 6. Performance results for varying data sizes and sensors for packet drop ratio. (**a**) Packet drop ratio with varying data size; (**b**) packet drop ratio with varying number of sensors.



(**a**)



(**b**)

Figure 7. Performance results for varying data sizes and sensors for nodes overhead. (**a**) Nodes overhead with varying data size; (**b**) nodes overhead with varying number of sensors.

7. Conclusions

The IoT provides significant growth in the development of smart things and applications. It combines with sensors, gateways, and many network services to provide an efficient communication system. However, most of the proposed solutions in the literature cannot optimize the link performance via balancing resource utilization and decreasing network overhead. Moreover, many solutions are not able to cope with privacy and authentication attacks. This work presents an energy-efficient edge optimization system using graph theory for increasing the network lifetime with lightweight overheads on constraint nodes. Furthermore, it provides security strategies using the intelligence of both edge devices and SDN controllers. The two-tiered security not only supports confidential communication but, on the other hand, also eliminates the security risks in the network registration phase. Using graph theory, the proposed system explores optimized subgraphs based on the link lost and latency factors. However, it was seen that the proposed system failed to identify the distributed attacks that denied the communication services. Moreover, it still has an additional cost in the formulation of reroutes. Thus, we aim to improve the proposed system using machine learning techniques and, explicitly, the overheads in terms of both route disruption and security.

Author Contributions: Conceptualization, T.S. and A.R.; methodology, A.R. and T.S.; software, K.H. and S.A.B.; validation, G.J., T.S.; formal analysis, S.A.B., A.R., and K.H.; investigation, G.J. and T.S.; resources, T.S. and G.J.; data curation, G.J.; writing—original draft preparation, T.S. and A.R.; writing—review and editing, K.H. and S.A.B.; visualization, G.J. and T.S.; supervision, T.S. and A.R.; project administration, T.S. and G.J.; funding acquisition, T.S. and G.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data is available in the manuscript.

Acknowledgments: This work was supported by the research SEED project "Low-power consumption optimizing algorithm using artificial intelligence for embedded IoT sensing system". Prince Sultan University, Riyadh Saudi Arabia, (SEED-CCIS-2022{110}) under "Artificial Intelligence & Data Analytics Research Lab. CCIS". The authors are thankful for the support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Noura, M.; Nordin, R. A survey on interference management for device-to-device (D2D) communication and its challenges in 5G networks. *J. Netw. Comput. Appl.* **2016**, *71*, 130–150. [CrossRef]
2. Li, J.; Lei, G.; Manogaran, G.; Mastorakis, G.; Mavromoustakis, C.X. D2D communication mode selection and resource optimization algorithm with optimal throughput in 5G network. *IEEE Access* **2019**, *7*, 25263–25273. [CrossRef]
3. Haseeb, K.; Rehman, A.; Saba, T.; Bahaj, S.A.; Lloret, J. Device-to-Device (D2D) Multi-Criteria Learning Algorithm Using Secured Sensors. *Sensors* **2022**, *22*, 2115. [CrossRef]
4. Pedhadiya, M.K.; Jha, R.K.; Bhatt, H.G. Device to device communication: A survey. *J. Netw. Comput. Appl.* **2019**, *129*, 71–89. [CrossRef]
5. Shamganth, K.; Sibley, M.J. A survey on relay selection in cooperative device-to-device (D2D) communication for 5G cellular networks. In Proceedings of the 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 1–2 August 2017; pp. 42–46.
6. Georgios, L.; Kerstin, S.; Theofylaktos, A. Internet of Things in the Context of Industry 4.0: An overview. 2019. Available online: http://dspace.vsp.cz/handle/ijek/103 (accessed on 13 September 2022).
7. Elansary, I.; Darwish, A.; Hassanien, A.E. The future scope of internet of things for monitoring and prediction of COVID-19 patients. In *Digital Transformation and Emerging Technologies for Fighting COVID-19 Pandemic: Innovative Approaches*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 235–247.
8. Tyagi, A.K.; Fernandez, T.F.; Mishra, S.; Kumari, S. Intelligent automation systems at the core of industry 4.0. In Proceedings of the International Conference on Intelligent Systems Design and Applications, online, 13–15 December 2021; pp. 1–18.

9. Swamy, S.N.; Kota, S.R. An empirical study on system level aspects of Internet of Things (IoT). *IEEE Access* **2020**, *8*, 188082–188134. [CrossRef]
10. Tabaa, M.; Monteiro, F.; Bensag, H.; Dandache, A. Green Industrial Internet of Things from a smart industry perspectives. *Energy Rep.* **2020**, *6*, 430–446. [CrossRef]
11. Rehman, A.; Saba, T.; Haseeb, K.; Larabi Marie-Sainte, S.; Lloret, J. Energy-Efficient IoT e-Health Using Artificial Intelligence Model with Homomorphic Secret Sharing. *Energies* **2021**, *14*, 6414. [CrossRef]
12. Wei, Z.; Masouros, C.; Liu, F.; Chatzinotas, S.; Ottersten, B. Energy-and cost-efficient physical layer security in the era of IoT: The role of interference. *IEEE Commun. Mag.* **2020**, *58*, 81–87. [CrossRef]
13. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet Things J.* **2019**, *6*, 8169–8181. [CrossRef]
14. Porambage, P.; Okwuibe, J.; Liyanage, M.; Ylianttila, M.; Taleb, T. Survey on multi-access edge computing for internet of things realization. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2961–2991. [CrossRef]
15. Chen, B.; Wan, J.; Celesti, A.; Li, D.; Abbas, H.; Zhang, Q. Edge computing in IoT-based manufacturing. *IEEE Commun. Mag.* **2018**, *56*, 103–109. [CrossRef]
16. Jiang, C.; Fan, T.; Gao, H.; Shi, W.; Liu, L.; Cérin, C.; Wan, J. Energy aware edge computing: A survey. *Comput. Commun.* **2020**, *151*, 556–580. [CrossRef]
17. Jiang, C.; Cheng, X.; Gao, H.; Zhou, X.; Wan, J. Toward computation offloading in edge computing: A survey. *IEEE Access* **2019**, *7*, 131543–131558. [CrossRef]
18. Di Vaio, A.; Palladino, R.; Hassan, R.; Escobar, O. Artificial intelligence and business models in the sustainable development goals perspective: A systematic literature review. *J. Bus. Res.* **2020**, *121*, 283–314. [CrossRef]
19. Ma, Y.; Wang, Z.; Yang, H.; Yang, L. Artificial intelligence applications in the development of autonomous vehicles: A survey. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 315–329. [CrossRef]
20. Rao, P.M.; Deebak, B. Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. *J. Ambient. Intell. Humaniz. Comput.* **2022**, 1–37. [CrossRef]
21. Fawzy, D.; Moussa, S.M.; Badr, N.L. The Internet of Things and Architectures of Big Data Analytics: Challenges of Intersection at Different Domains. *IEEE Access* **2022**, *10*, 4969–4992. [CrossRef]
22. 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.* **2022**, 1–12. [CrossRef]
23. Sittón-Candanedo, I.; Alonso, R.S.; García, Ó.; Muñoz, L.; Rodríguez-González, S. Edge computing, iot and social computing in smart energy scenarios. *Sensors* **2019**, *19*, 3353. [CrossRef]
24. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Zhang, Q.; Choo, K.-K.R. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Trans. Serv. Comput.* **2020**, *13*, 625–638. [CrossRef]
25. Jan, M.A.; Khan, F.; Mastorakis, S.; Adil, M.; Akbar, A.; Stergiou, N. LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 1202–1211. [CrossRef] [PubMed]
26. Anajemba, J.H.; Yue, T.; Iwendi, C.; Alenezi, M.; Mittal, M. Optimal cooperative offloading scheme for energy efficient multi-access edge computation. *IEEE Access* **2020**, *8*, 53931–53941. [CrossRef]
27. Jiang, B.; Huang, G.; Wang, T.; Gui, J.; Zhu, X. Trust based energy efficient data collection with unmanned aerial vehicle in edge network. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3942. [CrossRef]
28. Zhang, H.; He, X.; Wu, Q.; Dai, H. Spectral graph theory based resource allocation for IRS-assisted multi-hop edge computing. In Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 10–13 May 2021; pp. 1–6.
29. Godquin, T.; Barbier, M.; Gaber, C.; Grimault, J.-L.; Le Bars, J.-M. Placement optimization of IoT security solutions for edge computing based on graph theory. In Proceedings of the 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC), London, UK, 29–31 October 2019; pp. 1–7.
30. Dhelim, S.; Aung, N.; Kechadi, T.; Ning, H.; Chen, L.; Lakas, A. Trust2Vec: Large-Scale IoT Trust Management System Based on Signed Network Embeddings. Available online: https://arxiv.org/pdf/2204.06988.pdf (accessed on 1 August 2022).
31. Ali, O.; Jaradat, A.; Kulakli, A.; Abuhalimeh, A. A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access* **2021**, *9*, 12730–12749. [CrossRef]
32. Kleinberg, J.; Tardos, E. Algorithm Design. Available online: https://ict.iitk.ac.in/wp-content/uploads/CS345-Algorithms-II-Algorithm-Design-by-Jon-Kleinberg-Eva-Tardos.pdf (accessed on 1 August 2022).