electronics

MDPI

Article

Smart Random Walk Distributed Secured Edge Algorithm Using Multi-Regression for Green Network

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

[1] Artificial Intelligence & Data Analytics Lab (AIDA), CCIS Prince Sultan University, Riyadh 11586, Saudi Arabia
[2] Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan
[3] Faculty of Applied Mathematics, Silesian University of Technology, 44-100 Gliwice, Poland
[4] MIS Department, College of Business Administration, Prince Sattam bin Abdulaziz University, Alkharj 11942, Saudi Arabia
* Correspondence: robertas.damasevicius@polsl.pl

Abstract: Smart communication has significantly advanced with the integration of the Internet of Things (IoT). Many devices and online services are utilized in the network system to cope with data gathering and forwarding. Recently, many traffic-aware solutions have explored autonomous systems to attain the intelligent routing and flowing of internet traffic with the support of artificial intelligence. However, the inefficient usage of nodes' batteries and long-range communication degrades the connectivity time for the deployed sensors with the end devices. Moreover, trustworthy route identification is another significant research challenge for formulating a smart system. Therefore, this paper presents a smart Random walk Distributed Secured Edge algorithm (RDSE), using a multi-regression model for IoT networks, which aims to enhance the stability of the chosen IoT network with the support of an optimal system. In addition, by using secured computing, the proposed architecture increases the trustworthiness of smart devices with the least node complexity. The proposed algorithm differs from other works in terms of the following factors. Firstly, it uses the random walk to form the initial routes with certain probabilities, and later, by exploring a multi-variant function, it attains long-lasting communication with a high degree of network stability. This helps to improve the optimization criteria for the nodes' communication, and efficiently utilizes energy with the combination of mobile edges. Secondly, the trusted factors successfully identify the normal nodes even when the system is compromised. Therefore, the proposed algorithm reduces data risks and offers a more reliable and private system. In addition, the simulations-based testing reveals the significant performance of the proposed algorithm in comparison to the existing work.

Keywords: smart development; edge computing; internet of things; multi-sensors; optimal system; green computing

Citation: Saba, T.; Haseeb, K.; Rehman, A.; Damaševičius, R.; Bahaj, S.A. Smart Random Walk Distributed Secured Edge Algorithm Using Multi-Regression for Green Network. *Electronics* **2022**, *11*, 4141. https://doi.org/10.3390/electronics11244141

Academic Editors: Juan M. Corchado, Byung-Gyu Kim, Carlos A. Iglesias, In Lee, Fuji Ren and Rashid Mehmood

Received: 6 November 2022
Accepted: 8 December 2022
Published: 12 December 2022

1. Introduction

Intelligence Edge Computing (IEC) enables 5G and other networks. Moreover, future 5G services and wireless communication networks are supported by IEC. IEC also allows driverless cars, augmented and virtual reality, big data analytics, and customer-oriented services [1,2]. Due to next-generation technologies, the IoT is performing a significant role in agriculture, healthcare, education, and energy sustainability [3–5]. Despite considerable advancement, 5G/6G technology has issues including traffic growth, confidentiality, cybersecurity, digitalization, and latencies [6,7]. Machine to Machine (M2M) communication is a potential technology for future generation communication systems. This communication paradigm enables ubiquitous communications with complete automated processes in which a large number of intelligent devices linked via networks communicate without direct human interaction [8–10]. M2M communication has a wide range of real-world applications, including e-healthcare, networks, intelligent transportation systems, environmental monitoring, smart cities, and industrial automation. In recent years, the significant

expansion of sensing technology has resulted in sensor applications for healthcare, handicapped patients care, suspicious activity detection, and surveillance [11–13]. Mobile sensors also produce a lot of useful data and deep learning has evolved as a way to extract features automatically. Smart cities need technology that can be effectively deployed to ensure a friendly and secure environment with sustainable qualities [14,15]. The IoT-based Wireless Sensor Networks (WSNs) can serve a variety of demands, including providing real-time plans for the emergency management of communication systems [16–18].

Fog computing produces large volumes of data, therefore aiding the development of more applications and services. Robotics, neuromorphic computing, computer graphics, Natural Language Processing (NLP), decision-making, and voice recognition have all benefited from advances in machine learning. Several studies have proposed using machine learning to solve fog computing issues [19–21]. Recent advancements in fog computing systems and fog services, such as resource management, privacy protection, lowering latency, energy consumption, and traffic modeling, have been made possible by the application of machine learning [22–24]. However, constraint networks with limited capabilities require a lightweight algorithm to reduce overhead in light of the intelligent communication paradigm [25–27].

The main contributions of the proposed algorithm are:

1. A smart multisensory interaction system to deal with delay tolerance and energy requirements with minimal network complexity.
2. Performing an initial random walk on the vertices and edges of graphs to identify random routes based on certain probabilities to formulate the network topology.
3. An optimized goal function to investigate a multi-regression model, and network devices computing optimal routes by adopting the learning process. In addition, lossy channels are determined to increase the data delivery performance.
4. A trusted paradigm coping with the identification of malicious activities and increasing the reliability of traffic flow. Moreover, to lower the network threats, it also manages effective communication between edges and sink nodes.

The sections of this research study are as follows. A discussion and review of the literature are presented in Section 2. The problem statement is presented in Section 3 and the proposed algorithm is designed and explained in Section 4. Finally, the experimental findings are presented in Section 5, and the conclusion is provided in Section 6.

2. Related Work

IoT and big data analytics infrastructures are rising faster than ever. Edge computing is data processing near IoT data collectors. Such technologies offer many smart services for the remote network with the help of intermediate wireless devices [28–30]. The authors of [30] reviewed the ideas, features, security, and applications of IoT-enabled edge computing in a data-driven future. They also explained how to create a scalable, dependable, and secure distributed edge computing system with risk-reduction approaches. Finally, they highlighted the issues in edge computing prospects. In [31], the authors integrated neural networks and fuzzy systems into a secure healthcare monitoring system to make it a smart healthcare model that selects priority based on sensor node health metrics. Their proposed model was comprised of a trusted environment that collects authorized physiological data from a patient's body and sends it via GSM module to an Azure IoT Hub, where raw data is converted into a linguistic representation using a logic-based algorithm trained in a Fuzzy-Based Inference System (FBIS) to determine the patient's status. They claimed that the system enables precise, real-time patient monitoring. However, the current IoT designs depend heavily on upstream communication channels, are centrally located and complex, and have inadequate secure communications. As a result, problems with data reliability arise. These problems include data loss, corruption injection, communications network overload, and excessive central node computing power.

In [32], a blockchain-based approach introduced the edge computing layer and a unique algorithm to improve the data quality and misleading information detection. In

the IoT, the authors of [33] proposed using edge computing to gather reliable data. The sensor nodes are assessed across several aspects to achieve precisely defined trust levels in this approach. Furthermore, the ideal mobility route is developed with high trust by translating a node's trust value into a force for mobile data collection. Additionally, to visit the sensors with measured trust levels and gather reliable data, a mobile edge data collector is deployed. The extended experiment confirmed that the efficiency of IoT systems based on reliable data-collecting models is significantly improved in terms of system security and energy saving. The fundamental shortcoming of present clustering is that packet loss is not included in their communication model, which produces unreliable communication and reduces medical node energy.

The authors of [34] proposed a Clustering Model for Medical Applications (CMMA) to choose cluster heads for IoMT-based applications. The proposed CMMA model has superior sustainability and energy consumption than comparable techniques. Thus, it minimizes the energy use of edge-computing-based IoMT systems and evenly distributes cluster heads throughout the network to improve its lifespan. A new architecture that blends a trust assessment method and service template with cloud and edge computing balancing dynamics is presented in [35]. In this architecture, the edge network and platform are intended to decrease resource consumption and provide trust assessment mechanism flexibility. To increase IoT-Cloud service efficiency, the cloud stores the service parameter template, and the edge platform stores the service parser template. The edge network may help the edge platform develop service parsing templates based on trust assessment and satisfy particular service needs. Experiments show that the edge-based design improves IoT-Cloud security and efficiency. Employing fog computing, the authors of [36] reduced e-healthcare latency. The IoT multimedia data transmission characteristics must be decreased because there is a significant need for healthcare multimedia analytics. Fog computing processes, stores, and analyses IoT and end-user data locally to reduce latency. In this study, a new Intelligent Multimedia Data Segregation (IMDS) approach employing machine learning (k-fold random forest) is suggested in fog computing to separate multimedia data and determine overall latency (transmission, computation, and network). The simulation-based results obtained a 92% classification accuracy, a 95% decrease in latency, and enhanced e-healthcare performance.

The authors of [37] proposed a repeated game model to strengthen the clustered WSNs-based IoT security and Data Trustworthiness (DT) against selective forwarding (SF) attacks. Furthermore, the model can maintain network stability, reduce power consumption from packet retransmission, and identify the HardWare (HW) failure of Cluster Members (CMs). The TDMA protocol is used by the model to speed up detection and prevent collisions between delivered packets at the Cluster Head (CH). Its purpose is to differentiate malicious CM from facing HW failure and keeps packets transmitting, whether isotropically or nonisotropically, from the CMs to the CH to maximize the DT. The authors in [38] presented the smart meters' significance and highlighted their security issues. They showed the involved features of smart meters in various applications. Moreover, the weaknesses of the smart meters are also identified. Eleven trust models were used to secure smart meters to attain security and privacy for collected data. In [39], the authors successfully presented an ensemble model for a highly accurate blast-induced PPV estimation in fragmenting rocks. An established machine learning algorithm was applied and offered an intelligent approach. As it is an inherently regression problem, they used 42 repressors in their forecasting model. Moreover, to attain the highest level of accuracy for the developed model, the authors successfully optimized the Decision Tree (DT) results and overcame its constraints.

To maximize the transmission of trustworthy data over clustered-WSNs (CWSNs), the authors proposed a trust model based on a non-zero-sum game strategy [40]. Two distinct attack-defense scenarios were built for the proposed model. The trust model was then utilized in the first scenario to defend against a Denial-of-Service (DoS) assault in which the attacker could completely or partially discard the delivered acknowledgments from a

CM to the CH. In the second case, the attacker could regularly infect the CMs. The model's goal is to protect CWSNs from ON-OFF attacks.

3. Problem Statement

Based on the research presented, it can be stated that smart and remote devices are often used for network monitoring forwarding the IoT data toward cloud systems. Such technologies are being aggressively studied for data collection from critical areas with the integration of machine learning methods [41]. Edge computing increases the efficiency of green technology, data sensing, and transmission of network information with manageable latency. Moreover, various solutions are being implemented to ensure data security for IoT systems, but at the cost of additional energy and memory resources [42,43]. In addition, the majority of solutions did not take into account cloud computing for overhead reduction and effective data processing, which prevents IoT devices from checking and forwarding essential data in a timely manner. Also, the protection of transferred data across unreliable networks with the integration of many intermediate devices has also been identified as one of the most challenging aspects, especially if devices are mobile.

This study thus presents a smart random walk distributed secured edge algorithm using the multi-regression model for green computing technologies, employing machine learning methods for the identification of intelligent routes towards the sink with the support of edge computing and increasing the efficacy of reliability by imposing nominal complexity on the constraint devices.

4. Distributed Random Walk Cooperative Edge Routing for Green Network

In this section, we present an explanation of the proposed algorithm. It contains a proposal overview, initial components, and a discussion of developed schemes.

4.1. Proposal Overview

The proposed algorithm is composed of two main schemes. One is a smart interaction with edge computing and the other is a trustworthy route establishment. The communication area is initially divided between sensors and IoT devices, and each device shares some necessary information for future interactions and decision-making. The network structure is organized in undirected Graph G that is comprised of Vertices V and Edges E. Furthermore, each edge has a weight and is initially assigned; later it can be altered with each learning iteration. We suppose network edges NE are rotatable and only nodes that are closer to the network borders are permitted to send aggregated data. We classify such nodes as heterogeneous because they require additional resources due to their extra functions.

4.2. Proposed RDSE Algorithm

In the RDSE algorithm, each component works independently and passes its outcomes to the next level for sustainable communication. The security phase is another main part of the proposed algorithm, which handles the network attacks for data concealing and reduces risks. In the RDSE algorithm, nodes are arranged in the form of boundaries and each boundary has exactly one gateway node for forwarding the surrounding data. The nodes whose radius R falls between a certain distance threshold D_{td} are allowed to communicate directly $direct_{com}$, otherwise multihop communication MH_{com} is adopted as stated in Equation (1).

$$\begin{cases} if\ R(i,\ j) \leq\ D_{td} \\ direct_{com} = True \\ false,\ otherwise \end{cases} \tag{1}$$

The data is transmitted from various boundaries until it is reached the nearest edge device. Once the edge device receives it, further collaboration is established to attain smooth communication with the sink node. Edge devices periodically announce their latest position with sensors and sink nodes. In the beginning, the RDSE algorithm utilizes the random walk and initiates the routing process by arbitrary nodes. Moreover, each node maintains the

record of its initial formulated route. Whenever any node needs to send its data, it explores the routing table and identifies its set of neighbors $S_i = s_1, s_2, \ldots, s_k$. Later, it selects an arbitrary node among S_i with a probability P_i and updates the information in its routing table by integrating the ID of the selected node. We assume the Random walk RW over the communication link is comprised of the sequence of vertices V_i as given in Equation (2)

$$RW = \sum_{i=0}^{n} V_i \tag{2}$$

After some rounds, nodes have created parallel random routes R_i to accomplish data transmission toward sink nodes. Subsequently, the RDSE algorithm offers intelligent decisions over the computed random paths based on machine learning, and a reliable path is obtained for Node-to-Node (N2N) communication. In the RDSE, two routing lists are formed, one for the visited nodes and a second for awaiting nodes. The information for the newly selected forwarder node is also stored in the edge records as given in Table 1. It is comprised of the node identity, node position, and computed weighted. The table is updated whenever either node changes its position or its weighted value is recomputed.

Table 1. Format of the edge records.

1 Byte	1 Byte	2 Bytes
Node identity	Node position	Computed weight

Each node in the RDSE algorithm obtains the attributes of neighboring nodes from the available list of search space and computes the weighted value W_i based on a multiple linear regression model, as given in Equation (3).

$$W_i = XB + \gamma, \tag{3}$$

where X denotes composite metrics and γ is the residual variable, as stated in Equations (4) and (5).

$$X = X_i, X_2, \ldots, X_n, \tag{4}$$

$$\gamma = \gamma_i, \gamma_2, \ldots, \gamma_n, \tag{5}$$

Based on Equation (6), X evaluates the multiple parameters to derive the independent decision for each node

$$X = DN + DC + LM \tag{6}$$

where DN is the distance to neighbors, DC is the distance to the centroid, and LM is the link measurement in terms of packet reception with error rate. The RDSE method determines the lossy connection by evaluating the packet loss rate over the communication channels, and if the threshold of data loss is higher than the threshold, the RDSE algorithm gives a low priority to that particular link and prohibits it from participating in data transmission. Figure 1 shows the flowchart of the RDSE algorithm for a machine learning-based smart edge routing. After the formulation of the network infrastructure, graphs are constructed, and neighboring information is collected in the form of tables. The random walk is performed to identify the set of random routes and to later generate more optimal decisions by exploring the multiple linear regression model. The RDSE algorithm attains reliable transmission on the channel based on the independent variables and leads to an improved network lifetime for green technologies. The data is forwarded to the sink node using edge devices and afterward, the data is routed to the cloud system with the assurance of consistency.

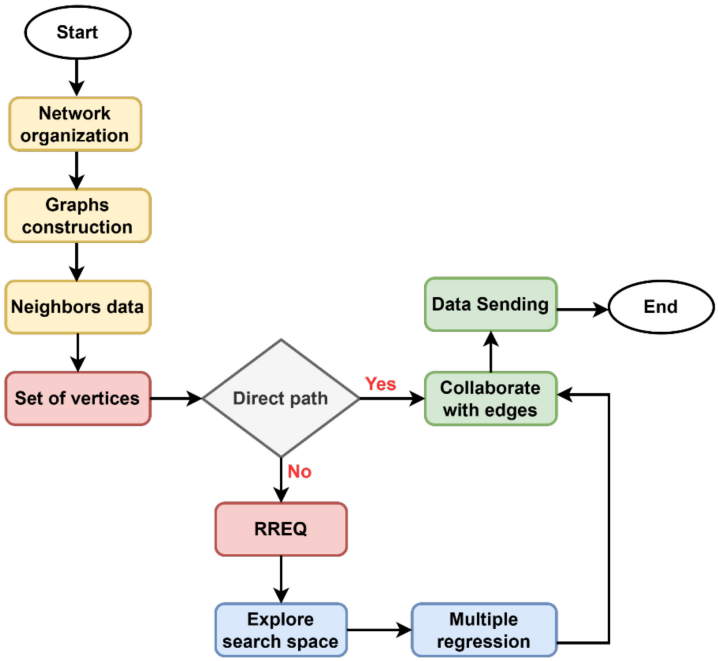

Figure 1. Smart random walk routing with the multi-regression model.

The source node constructs a routing list following the weighted value computation, and initially, the list simply contains the identification of the source node. Later, the source node includes the highest-weighted node in the routing list and sends the Route REQuest RREQ to it. Upon receiving the RREQ, the selected node sends back the ACK; accordingly, a one-to-one association is constructed for data routing. Then, multiple routes based on hopping are developed to ensure timely data delivery with the load distribution balanced on the communication links. In the other stage, the RDSE algorithm provides data privacy support with symmetric cryptography integration. Each node generates its symmetric key k_i and shares it with its neighbors. In addition, the sink node keeps track of the key distribution process and delivers the message for key regeneration after a particular session has ended. To achieve security and trusted communication, the RDSE algorithm uses a One-Time Pad (OTP) with the support of hashes. It is based on blocks and each block is operated with a distinct nonce. The generated key k_i for the security phase is entirely random and is only effective for the particular message m_i. Due to Xor operations, the proposed security solutions also have nominal overheads on IoT devices. The encryption process in this phase includes multiple Xor operations to generate cipher texts. In the RDSE algorithm, the cooperation of data forwarders, edges, and sink nodes results in the security of the sensor network. We assumed the data forwarder is represented by df, the edges are denoted by ed, and the sink node is denoted by sk. Each device has its own unique identity id_s for the sensor, id_e for the edge, and id_{sk} for the sink node. The communication is obtained in the form of encrypted blocks and each data block m_i is connected with its associated blocks. This behavior persists until the data is securely received at the sink node, as specified below.

$$H(df) = m_i \oplus id_s \tag{7}$$

$$H(ed) = H(df) \oplus id_e \tag{8}$$

$$H(sk) = H(ed) \oplus id_{sk} \tag{9}$$

Upon receiving the outcome of encrypted blocks as defined in Equations (7)–(9), the data center executes the decrypt function D to check and obtain the original sensor data specified in Equation (10).

$$D = (H(sk) \oplus id_{sk}) \oplus id_e) \ \oplus id_s \tag{10}$$

Figure 2 depicts the components of the proposed security algorithm by exploring symmetric keys with multiple Xor operations. In the beginning, sensor data are associated with symmetric keys. After the distribution of symmetric keys among devices, the incoming request is verified based on the identities. Once devices are verified, the OTP is explored to attain a secure session among devices, and for each session, there will be a separate OTP. The OTP is purely random to make it harder for the malicious device to detect incoming data and compromise its integrity. The proposed algorithm provides the encryption phase for each level, i.e., data forwarder to the edge device, and from the edge device to the sink node. Table 2 shows the notations that are used in the proposed protocol.

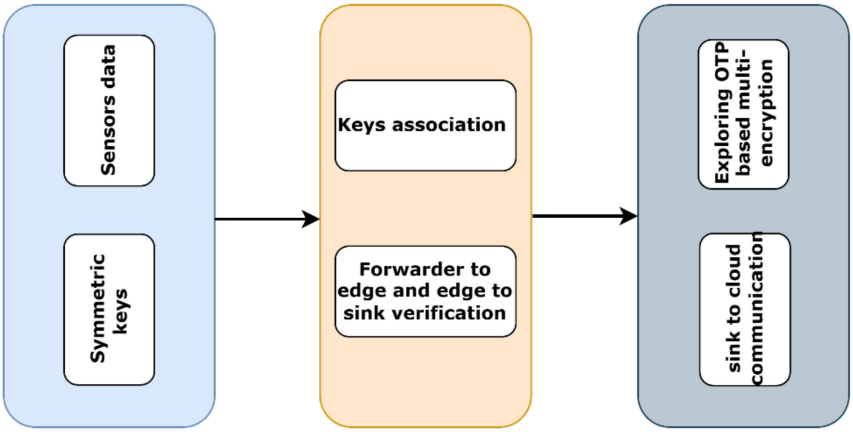

Figure 2. Proposed secured edge algorithm with the support of OTP.

Table 2. Notations of the proposed protocol.

Notations	Description
D_{td}	threshold
R_i	random routes
V_i	vertices
W_i	weighted value
X	composite metrics
γ	residual variable
RW	random walk
R	radius
P_i	probability
k_i	symmetric key
sk	sink node
ed	edges
df	data forwarder
id_e	edge identity
id_s	sensor identity
m_i	message
D	decryption
$\oplus$	Xor

5. Simulation Environment

This section describes the experiments that were conducted in a simulation environment. We compared the proposed algorithm with existing work from network throughput, data latency, node overhead, and the number of rounds. With the aid of sensors and IoT devices, we created a scenario with the support of NS-3. The sensors' data is gathered periodically and transmitted toward the sink node with the support of edges. The edges offer intelligent services for IoT networks and cloud systems. Table 3 is a list of the simulation parameters for the conduction of various experiments. The simulation experiments took place in a 500 m^2 area. In terms of communication resources, the sensors are battery-powered and homogenous. We considered 10 edge devices while the sensor nodes varied from 30 to 150 and remained static after deployment. Initially, the nodes' energy was set to 5J. The transmission power of all nodes was set to 5 m. Simulations were executed for 5000 sec with 30 samples of simulations collected to analyze the performance of the proposed algorithm and existing work. The packet sizes also varied in the range of 8 bytes to 40 bytes. The experiments were conducted in two simulation environments, i.e., varying nodes and varying data packets. We assumed the number of malicious nodes as 20. The malicious nodes behaved abnormally and compromised the performance in terms of flooding network threats.

Table 3. Simulation parameters.

Parameters	Values
IoT Devices	30–150
Initial energy	5 J
Simulator	NS-3
Network diameter	500 m × 500 m
Topology	Wireless
Packet size	8 bytes to 40 bytes
Transmission range	5 m
Sink deployment	Random
Simulation interval	5000 s
Edges	10
Malicious devices	20
Number of simulations	30

5.1. Network Throughput

Figure 3a,b displays the results of the two scenarios for analyzing network throughput experiments. It is defined as the amount of data transmitted successfully from the source to the destination end. It has been shown that the RDSE method improves network throughput by an average of 10% and 13% for different nodes and packet sizes in comparison to other research. This is the outcome of the multi-hop data transmission in the network region by balancing the energy efficiency on each route. In addition, even in the presence of malicious nodes, the multi-regression analysis provides an optimal service for data routing. Moreover, the RDSE algorithm stores the forwarders' information in the routing tables and updates it whenever a trigger occurs. Furthermore, the security of the RDSE algorithm decreases the chances of data loss and increases the network's reliability with the integration of OTP. The proposed security scheme in the proposed work does not impose extra overhead on the nodes.

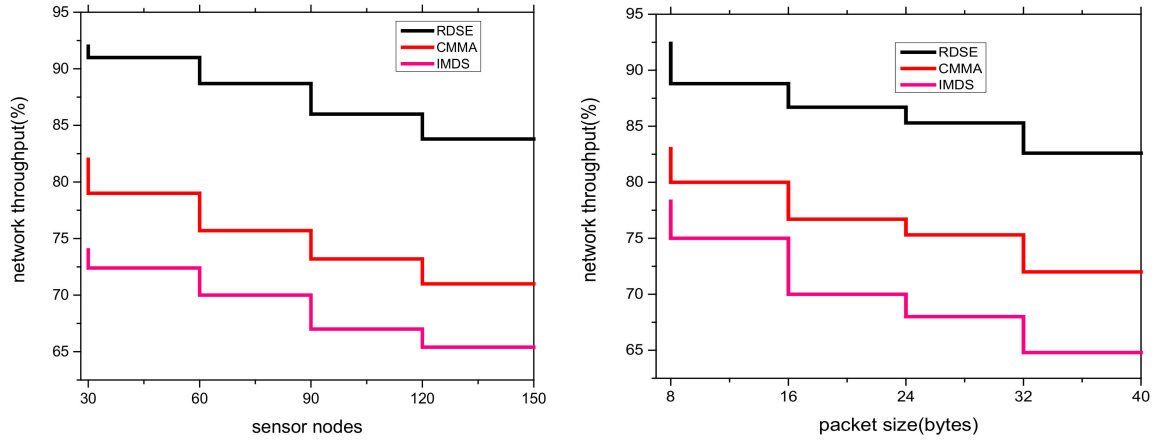

Figure 3. Network throughput with (**a**) varying sensors "30–150" and (**b**) varying packet sizes "8–40 bytes".

5.2. Nodes Overhead

Figure 4a,b illustrates the comparison of the RDSE algorithm with existing work when the number of sensors and data size are varied. It is defined as the amount of processing and transmission time used by the network nodes. Based on the findings, it was found that the RDSE algorithm significantly reduces the node overhead by an average of 17% and 19% compared to other solutions This is because when a node needs to transmit data, the RDSE algorithm uses machine learning techniques to identify the optimal forwarders and lowers the communication overhead on the channels. The routing paths are cycled each time when nodes attempt to locate the next hop in the search space. This provides efficient load distribution in the routes and reduces the overhead on the constraint devices. Compared to most of the work, the independent variables provide the optimal value for the dependent variable, and accordingly, the RDSE algorithm chooses the least interference vertices for data transmission. With a manageable cost for connected nodes, such a mechanism enables the timely delivery of the data to the sink node.

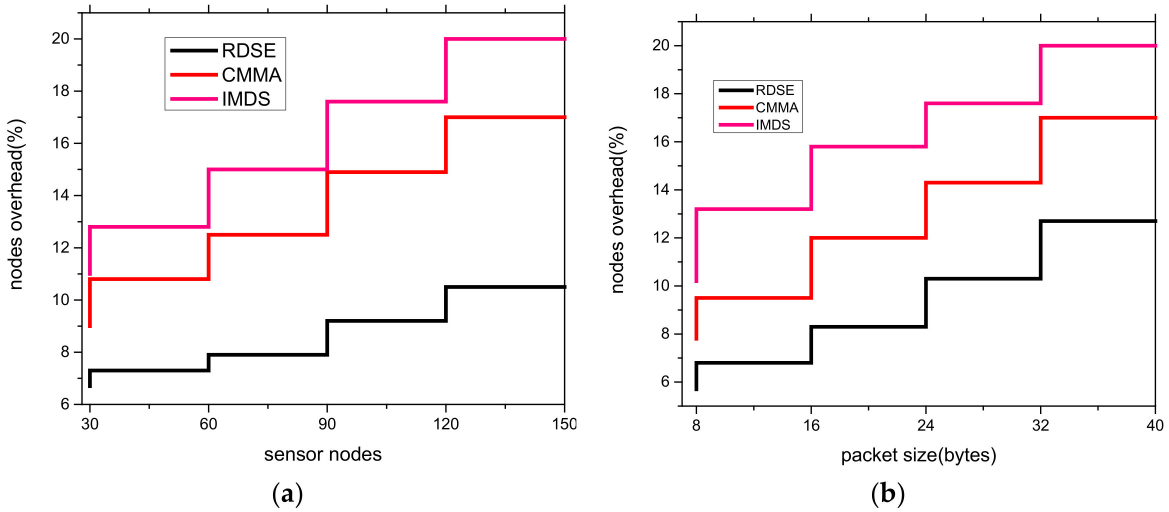

Figure 4. Nodes overhead with (**a**) varying sensors "30–150" and (**b**) varying packet sizes "8–40 bytes".

5.3. Data Latency

Figure 5a,b displays the experimental results for the RDSE algorithm with existing work using various sensors and packet sizes. Data latency indicates the communication delay over the network medium. According to the findings, the RDSE algorithm significantly reduced the data latency by an average of 11% and 12% as compared to other relevant studies. Unlike most of the existing work, it is the result of utilizing intelligent decisions for the formulation of routing paths and based on the multi-regression model, it also offers reliable forwarders with efficient usages of network resources. Furthermore, the random walk provides a simple method for choosing forwarders and provides a rapid design of the initial network structure with random routes. Later, using the weighted function, it provides optimal routes by extracting the information of random paths, and, with the help of edge computing, the proposed protocol increases the stability of the green network. Moreover, the RDSE technique uses symmetric keys and OTP to secure sessions and achieve data privacy in some encryption sequences. Finally, the removal of network threats increases the performance of the RDSE algorithm in terms of data damages and provides the routes with a long-run lifetime with a nominal delay rate.

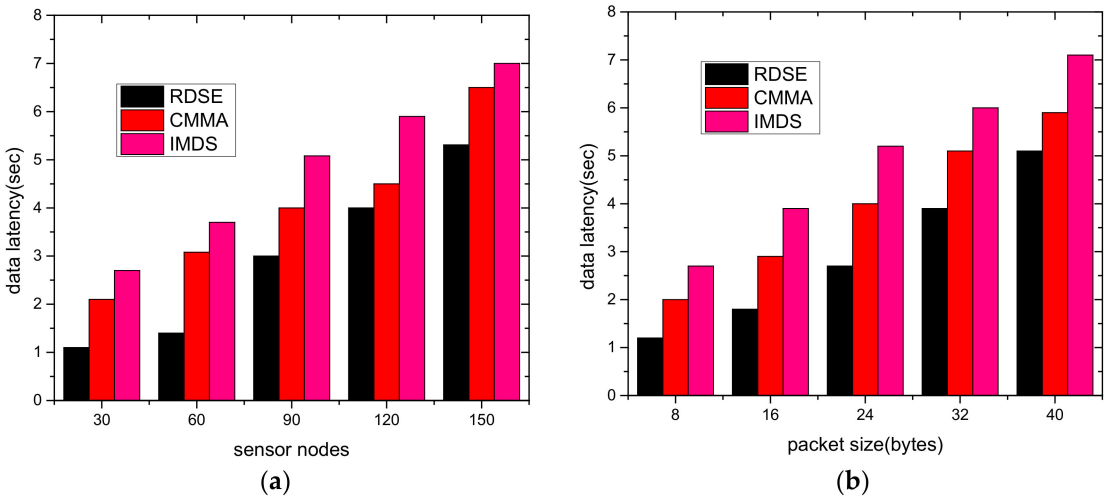

Figure 5. Data delay with (**a**) varying sensors " 30–150" and (**b**) varying packet sizes "8–40 bytes".

5.4. Number of Rounds

Using varied sensors and packet sizes, the efficiency of the RDSE algorithm is evaluated in Figure 6a,b in terms of rounds. The experimental results demonstrate that the RDSE algorithm increases the network lifetime by running the maximum no. of rounds. The improvement is made by an average of 13% and 15% with varying sensors and varying packet sizes, respectively, compared to related work. It results from the introduction of a machine learning-based model and multiple independent variables offering more reliable choices for the chosen routing paths. Moreover, it balances the load between devices and intelligently manages the edges to cope with data delivery performance. The RDSE algorithm makes use of multi-regression analysis to monitor the nodes' behavior in terms of network metrics and then modifies the routing scheme based on demand. Due to the Xor operations among devices, the RDSE algorithm also lowers the complexity factors and ultimately increases the runtime of the proposed algorithm with an improved network lifetime.

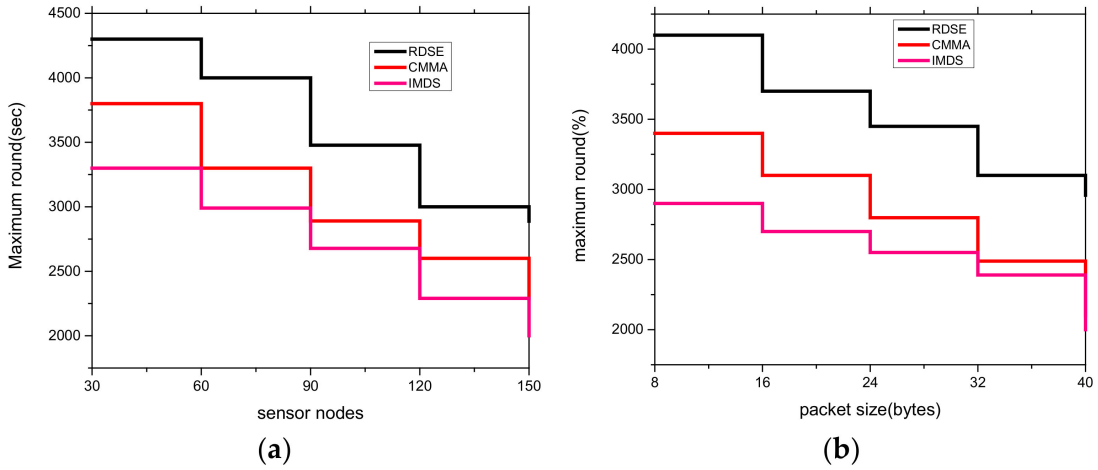

Figure 6. The number of rounds with (**a**) varying sensors "30–150", and (**b**) varying packet sizes "8–40 bytes".

6. Conclusions

Wireless systems with the support of IoT technologies are demonstrating enormously sophisticated uses for environmental monitoring. In addition to providing remote data sensing, they also make edge computing more effective and demanding. Smart systems with edge devices are performing a significant role in the development of green networks, however, in contrast to the high amount of network traffic, most solutions impose additional overhead on the devices. Furthermore, it was shown that many solutions cannot cope with lightweight communication paradigms in the presence of network threats. Such solutions incur several route damages and compromise smart devices. This study presents a smart random walk-based secured edge algorithm with the insurance of optimal load distribution among forwarders. The RDSE algorithm lowered the data latency with the help of edge devices, and the multi-regression model enhanced the network's stability and efficacy for constraint devices. The RDSE algorithm also offers secured communication with the integration of OTP and the randomness of communication patterns among devices. By evaluating the packet loss rate, the RDSE algorithm also recognizes lossy connections, and, as a result, these links are prohibited from the list of data transfers. However, in future work, we aim to introduce some fading models to compute the stability of the mobile sensor network and increase the nodes' trust under a large-scale region.

Author Contributions: Conceptualization, T.S.; Methodology, T.S.; Validation, A.R., R.D. and S.A.B.; Formal analysis, K.H. and S.A.B.; Investigation, K.H. and A.R.; Writing—original draft, T.S. and K.H.; Writing—review & editing, A.R., R.D. and S.A.B.; Supervision, T.S. and K.H.; Funding acquisition, R.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Prince Sultan University, Riyadh, Saudi Arabia (SEED-CCIS-2022{110}).

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 the Artificial Intelligence and Data Analytics Research Lab, CCIS. The authors are thankful for the support.

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

Abbreviations

IoT	Internet of Things
RDSE	Random walk Distributed Secured Edge algorithm
WSNs	Wireless Sensor Networks
M2M	Machine to Machine
NLP	Natural Language Processing
FBIS	Fuzzy-Based Inference System
CMMA	Clustering Model for Medical Applications
CMs	Cluster Members
IMDS	Intelligent Multimedia Data Segregation
Decision Tree	DT
CH	Cluster Head
DoS	Denial-of-Service
DT	Data Trustworthiness
CWSNs	clustered-WSNs
N2N	Node-to-Node
OTP	One-Time Pad
RREQ	Route REQuest

References

1. Al-Ansi, A.; Al-Ansi, A.M.; Muthanna, A.; Elgendy, I.A.; Koucheryavy, A. Survey on intelligence edge computing in 6G: Characteristics, challenges, potential use cases, and market drivers. *Future Internet* **2021**, *13*, 118. [CrossRef]
2. Dai, W.; Nishi, H.; Vyatkin, V.; Huang, V.; Shi, Y.; Guan, X. Industrial edge computing: Enabling embedded intelligence. *IEEE Ind. Electron. Mag.* **2019**, *13*, 48–56. [CrossRef]
3. Attaran, M. The impact of 5G on the evolution of intelligent automation and industry digitization. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–17. [CrossRef] [PubMed]
4. Tang, Y.; Dananjayan, S.; Hou, C.; Guo, Q.; Luo, S.; He, Y. A survey on the 5G network and its impact on agriculture: Challenges and opportunities. *Comput. Electron. Agric.* **2021**, *180*, 105895. [CrossRef]
5. Chettri, L.; Bera, R. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet Things J.* **2019**, *7*, 16–32. [CrossRef]
6. Yunana, K.; Alfa, A.A.; Misra, S.; Damasevicius, R.; Maskeliunas, R.; Oluranti, J. Internet of Things: Applications, Adoptions and Components—A Conceptual Overview. In *Hybrid Intelligent Systems*; Springer International Publishing: Cham, Switzerland, 2021; pp. 494–504. [CrossRef]
7. Yasin, Q.; Iqbal, Z.; Khan, M.A.; Kadry, S.; Nam, Y. Reliable multipath flow for link failure recovery in 5G networks using SDN paradigm. *Inf. Technol. Control.* **2022**, *51*, 5–17. [CrossRef]
8. Verma, P.K.; Verma, R.; Prakash, A.; AshishAgrawal, A.; Naik, K.; Tripathi, R.; Alsabaan, M.; Khalifa, T.; Abdelkader, T.; Abogharaf, A. Machine-to-Machine (M2M) communications: A survey. *J. Netw. Comput. Appl.* **2016**, *66*, 83–105. [CrossRef]
9. Zhang, S.; Xu, X.; Wu, Y.; Lu, L. 5G: Towards energy-efficient, low-latency and high-reliable communications networks. In Proceedings of the 2014 IEEE International Conference on Communication Systems, Macau, China, 19–21 November 2014.
10. Agiwal, M.; Roy, A.; Saxena, N. Next generation 5G wireless networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1617–1655. [CrossRef]
11. Qian, X.; Chen, H.; Cai, Y.; Chu, K.-C.; Xu, W.; Huang, M.-C. Transfer Learning Model Knowledge Across Multi-sensors Locations over Body Sensor Network. *IEEE Sens. J.* **2022**, *22*, 10663–10670. [CrossRef]
12. Jabbar, M.; Shandilya, S.K.; Kumar, A.; Shandilya, S. Applications of cognitive internet of medical things in modern healthcare. *Comput. Electr. Eng.* **2022**, *102*, 108276. [CrossRef]
13. Sangulagi, P.; Sutagundar, A.V. Sensor Cloud-Based Theoretical Machine Learning Models for Predicting Pandemic Diseases. In *Intelligent Interactive Multimedia Systems for E-Healthcare Applications*; Apple Academic Press: Palm Bay, FL, USA, 2022; pp. 167–196.
14. Okewu, E.; Misra, S.; Maskeliūnas, R.; Damaševičius, R.; Fernandez-Sanz, L. Optimizing green computing awareness for environmental sustainability and economic security as a stochastic optimization problem. *Sustainability* **2017**, *9*, 1857. [CrossRef]
15. Saba, T.; Rehman, A.; Haseeb, K.; Bahaj, S.A.; Damaševičius, R. Sustainable data-driven secured optimization using dynamic programming for green internet of things. *Sensors* **2022**, *22*, 7876. [CrossRef]
16. Fedele, R.; Merenda, M. An IoT system for social distancing and emergency management in smart cities using multi-sensor data. *Algorithms* **2020**, *13*, 254. [CrossRef]
17. Pekar, A.; Mocnej, J.; Seah, W.K.G.; Zolotova, I. Application domain-based overview of IoT network traffic characteristics. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–33. [CrossRef]
18. Ye, F.; Zhou, X.; Ren, Z.; Yang, S. Energy allocation for stochastic event detection in rechargeable sensor networks. *Inf. Technol. Control.* **2022**, *51*, 283–293. [CrossRef]

19. Abdulkareem, K.H.; Mohammed, M.A.; Gunasekaran, S.S.; Al-Mhiqani, M.N.; Mutlag, A.A.; Mostafa, S.A.; Ali, N.S.; Ibrahim, D.A. A review of fog computing and machine learning: Concepts, applications, challenges, and open issues. *IEEE Access* **2019**, *7*, 153123–153140. [CrossRef]
20. Aceto, G.; Persico, V.; Pescapé, A. A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3467–3501. [CrossRef]
21. Wang, Y.; Wang, K.; Huang, H.; Miyazaki, T.; Guo, S. Traffic and computation co-offloading with reinforcement learning in fog computing for industrial applications. *IEEE Trans. Ind. Inform.* **2018**, *15*, 976–986. [CrossRef]
22. Saba, T.; Haseeb, K.; Shah, A.A.; Rehman, A.; Tariq, U.; Mehmood, Z. A Machine-Learning-Based Approach for Autonomous IoT Security. *IT Prof.* **2021**, *23*, 69–75. [CrossRef]
23. Shanmuganathan, V.; Kalaivani, L.; Kadry, S.; Suresh, A.; Harold Robinson, Y.; Lim, S. Eeccrn: Energy enhancement with css approach using q-learning and coalition game modelling in crn. *Inf. Technol. Control.* **2021**, *50*, 171–187. [CrossRef]
24. Ogundokun, R.O.; Arowolo, M.O.; Misra, S.; Damasevicius, R. An Efficient Blockchain-Based IoT System Using Improved KNN Machine Learning Classifier. In *Blockchain based Internet of Things*; Springer: Singapore, 2022; pp. 171–180. [CrossRef]
25. Wang, Y.; Su, Z.; Ni, J.; Zhang, N.; Shen, X. Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions. *IEEE Commun. Surv. Tutor.* **2021**, *24*, 160–209. [CrossRef]
26. Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Tariq, U. Secured Big Data Analytics for Decision-Oriented Medical System Using Internet of Things. *Electronics* **2021**, *10*, 1273. [CrossRef]
27. Moin, S.; Karim, A.; Safdar, Z.; Safdar, K.; Ahmed, E.; Imran, M. Securing IoTs in distributed blockchain: Analysis, requirements and open issues. *Future Gener. Comput. Syst.* **2019**, *100*, 325–343. [CrossRef]
28. Tariq, N.; Asim, M.; Al-Obeidat, F.; Zubair Farooqi, M.; Baker, T.; Hammoudeh, M.; Ghafir, I. The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors* **2019**, *19*, 1788. [CrossRef] [PubMed]
29. Wu, Y.; Dai, H.-N.; Wang, H. Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet Things J.* **2020**, *8*, 2300–2317. [CrossRef]
30. Alrowaily, M.; Lu, Z. Secure edge computing in IoT systems: Review and case studies. In Proceedings of the 2018 IEEE/ACM Symposium on Edge Computing (SEC), Seattle, WA, USA, 25–27 October 2018.
31. El Zouka, H.A.; Hosni, M.M. Secure IoT communications for smart healthcare monitoring system. *Internet Things* **2021**, *13*, 100036. [CrossRef]
32. Casado-Vara, R.; Prieta, F.D.L.; Prieto, J.; Corchado, J. Blockchain Framework for IoT Data Quality via Edge Computing. In Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems 2018, Shenzhen, China, 4 November 2018.
33. Wang, T.; Qiu, L.; Sangaiah, A.K.; Liu, A.; Alam Bhuiyan, Z.; Ma, Y. Edge-computing-based trustworthy data collection model in the internet of things. *IEEE Internet Things J.* **2020**, *7*, 4218–4227. [CrossRef]
34. Han, T.; Zhang, L.; Pirbhulal, S.; Wu, W.; de Albuquerque, V.H.C. A novel cluster head selection technique for edge-computing based IoMT systems. *Comput. Netw.* **2019**, *158*, 114–122. [CrossRef]
35. Wang, T.; Zhang, G.; Liu, A.; Alam Bhuiyan, Z.; Jin, Q. A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing. *IEEE Internet Things J.* **2018**, *6*, 4831–4843. [CrossRef]
36. Kishor, A.; Chakraborty, C.; Jeberson, W. A novel fog computing approach for minimization of latency in healthcare using machine learning. *Int. J. Interact. Multimedia Artif. Intell.* **2021**, *6*, 7–17. [CrossRef]
37. Abdalzaher, M.S.; Muta, O. A game-theoretic approach for enhancing security and data trustworthiness in IoT applications. *IEEE Internet Things J.* **2020**, *7*, 11250–11261. [CrossRef]
38. Abdalzaher, M.S.; Fouda, M.M.; Ibrahem, M.I. Data Privacy Preservation and Security in Smart Metering Systems. *Energies* **2022**, *15*, 7419. [CrossRef]
39. Moustafa, S.S.R.; Abdalzaher, M.S.; Yassien, M.H.; Wang, T.; Elwekeil, M.; Hafiez, H.E.A. Development of an optimized regression model to predict blast-driven ground vibrations. *IEEE Access* **2021**, *9*, 31826–31841. [CrossRef]
40. Abdalzaher, M.S.; Samy, L.; Muta, O. Non-zero-sum game-based trust model to enhance wireless sensor networks security for IoT applications. *IET Wirel. Sens. Syst.* **2019**, *9*, 218–226. [CrossRef]
41. Corchado, J.M.; Ossowski, S.; Rodríguez-González, S.; De la Prieta, F. Advances in explainable artificial intelligence and edge computing applications. *Electronics* **2022**, *11*, 3111. [CrossRef]
42. Venckauskas, A.; Stuikys, V.; Damasevicius, R.; Jusas, N. Modelling of internet of things units for estimating security-energy-performance relationships for quality of service and environment awareness. *Secur. Commun. Netw.* **2016**, *9*, 3324–3339. [CrossRef]
43. Yigitcanlar, T.; Mehmood, R.; Corchado, J.M. Green artificial intelligence: Towards an efficient, sustainable and equitable technology for smart cities and futures. *Sustainability* **2021**, *13*, 8952. [CrossRef]