electronics

MDPI

Article

Energy-Aware Next-Generation Mobile Routing Chains with Fog Computing for Emerging Applications

Khalid Haseeb [1], Fahad A. Alzahrani [2], Mohammad Siraj [3], Zahid Ullah [4] and Jaime Lloret [5,*]

[1] Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan
[2] Computer Engineering Department, College of Computer and Information Systems, Umm Al-Qura University, Makkah 21955, Saudi Arabia
[3] Electrical Engineering Department, College of Engineering, King Saud University, Riyadh 11421, Saudi Arabia
[4] Institute of Management Sciences, Peshawar 25000, Pakistan
[5] Integrated Management Coastal Research Institute, Universitat Politecnica de Valencia, Camino Vera s/n, 46022 Valencia, Spain
* Correspondence: jlloret@dcom.upv.es

Abstract: The Internet of Things (IoT) provides robust services to connected sensors in a distributed manner, and maintains real-time communication using wireless standards. The smart network has offered many autonomous smart systems to collect information from remote nodes, and share it by exploring the network layer. Researchers have recently offered a variety of ways to increase the effectiveness of emerging applications using trustworthy relaying systems. However, there are still many issues with route reformulation due to frequent disconnections of mobile devices and resource limitations. Furthermore, most of the existing methods for IoT systems are unable to utilize network resources, which lowers the performance of green networks. Thus, providing a foolproof solution for the autonomous system with energy efficiency is a challenging task. Therefore, this paper presents an algorithm for the mobile network using fog computing to reduce network disconnectivity. Furthermore, using security services, the proposed algorithm efficiently explores the characteristics of the device, and avoids malicious traffic to drain the additional energy consumption of the network. The main aspects of the proposed algorithm are as follows: (i) using the adjustable transmission power, the proposed algorithm offers a fault-tolerant solution to transmit the aggregated data over the unpredictable wireless system; (ii) with the support of fog nodes, the data load is reduced among devices with the offering of a secured authentication scheme. Using simulations, the proposed algorithm is tested, and its significance is demonstrated against other related studies.

Keywords: energy systems; fog computing; distributed services; Mobile-IoT; next generation

check for updates

Citation: Haseeb, K.; Alzahrani, F.A.; Siraj, M.; Ullah, Z.; Lloret, J. Energy-Aware Next-Generation Mobile Routing Chains with Fog Computing for Emerging Applications. *Electronics* **2023**, *12*, 574. https://doi.org/10.3390/electronics12030574

Academic Editor: Antonio Brogi

Received: 17 December 2022
Revised: 18 January 2023
Accepted: 19 January 2023
Published: 23 January 2023

1. Introduction

A new paradigm called the IoT intends to connect all intelligent physical objects so that they can work together to offer intelligent services to users. Smart cities, smart grids, smart hospitals, and other IoT applications are some emerging applications of IoT systems [1–3]. IoT systems are built with a variety of hardware and networking technologies, extracting massive volumes of data [4–6]. IoT uses wireless sensor networks (WSNs) to sense the environment, gather data, and transfer it to the base station and other places for analysis. Intelligent routing is a key phenomenon that is required in WSNs for IoT to improve the quality of various smart applications [7–9]. WSNs must be mobile rather than static for many real-time applications, including smart transportation systems, habitat monitoring, and underwater monitoring. The development of mobile networks has gained rapid popularity in recent decades due to the unpredictable nature of communication devices [10–12].

Furthermore, mobile systems are capable of increasing the coverage range for data sensing and information transmission; however, because of the frequent changes in the locations of the devices, most of the solutions are not able to tackle route discontinuity and data losses [13–15]. Thus, researchers are trying to propose energy-efficient and consistent route maintenance methods for increasing delivery performance with the support of heterogeneous and distributed services [16–18]. On the other hand, in IoT networks, especially for mobile communication, security is another demanding research challenge. It not only affects the system performance but also decreases the trustworthiness among remote devices [19–21]. IoT systems have been extensively researched in recent years to handle remote sensing with the aid of sensors, but most of the solutions are unreliable in the case of mobile devices, and frequently lead to data breaches. Moreover, routing holes are increasing, which eventually raises the packet drop ratio. Thus, our study proposes an energy-efficient next-generation mobile routing with the combination of fog nodes. The proposed work not only reduces the latency for receiving data but also places the least overhead on the devices with low restrictions. We also offer trusted communication with secured authentication schemes, and ultimately increase the nodes' reliability in a distributed environment. The major objectives of the proposed model are as follows. The following are the primary contributions made in this work.

i. Developed a reliable and load-balanced routing protocol for mobile devices using analysis of QoS parameters by exploring lightweight methods.
ii. The overburden routes are excluded from routing chains and only optimal end-to-end communication is attained with the integration of fog computing.
iii. Using a lightweight authentication scheme, the proposed algorithm achieves security in terms of device verification, link confidentiality, and replay attacks. Such communication ensures trust in an unpredictable environment with efficient computing strategies.
iv. Using simulations, the proposed algorithm is evaluated in terms of numerous performance parameters in the comparison of existing work.

The following sections comprise the remainder of this research article. Section 2 presents a discussion of existing studies. The proposed algorithm is described in Section 3. The findings of the experiment are covered in Section 4. Section 5 provides the conclusion and outlines future research.

2. Related Literature

Future 6G networks provide storage and computing services by exploring fog computing and IoT devices [22,23]. However, because IoT devices and fog nodes have some resource constraints, energy-efficient solutions are needed for storage and computation services. Fog computing is an emerging technology for facilitating cloud networks [24–26]. Several issues with cloud architectures have recently emerged as a result of the rapid increase in IoT devices [27–29]. Fog computing can be used to increase the processing and storage capacity of the cloud by acting as a middle layer between consumer devices and the cloud. Offloading is a technique that can be used to move computations, data, and energy use from resource-constrained devices to resource-rich fog/cloud layers to enhance application quality, and improve system performance [30,31]. However, security is still a demanding challenge from constraint networks even in the existence of fog nodes. Many solutions have been presented to cope with network anomalies, but at the expense of nodes' overhead and network complexity [32,33]. The authors of [34] offer an efficient routing method called an energy-efficient hierarchical routing protocol. It is based on fog computing to transfer the sensors' data, and provides a scalable solution to meet the demands of IoT applications while maximizing the limited power supply of constraint networks. It also offers an improved ant colony optimization algorithm that may be used to choose the optimal path for achieving data routing.

In [35], using a novel paradigm, the authors expanded the network computing infrastructure for the 5G communication system. To improve the Quality of Service (QoS) and Quality of Experience (QoE), a new design of the fog computing framework is explored in this work. Moreover, the proposed solution offers a method for managing mobility in fog networks that takes into account both static and dynamic mobile nodes. The authors in [36] proposed a solution to improve the secure flow of information for the multimedia network. The Message Queue Telemetry Transport (MQTT) protocol over SSL/TLS is used in the proposed system. To mitigate man-in-the-middle attacks, the Elliptic curve-ElGamal cryptography method is introduced because MQTT is disposed to eavesdropping. According to the data topic, the proposed solution uses dynamic key change and proportionate offloading methods to send data selectively to the cloud and the fog, thereby conserving nodes' energy. Authors in [37] proposed a comprehensive trust management system, based on a Gaussian distribution (GDTMS). Furthermore, to achieve the trade-off between security, transmission efficiency, and energy consumption, grey decision-making is included in the trust decision. The proposed trade-off can successfully choose a trust management-based secure routing strategy as the reliable and secure relay node. The proposed strategies can also be used to defend against bad mouthing attacks. Simulation findings demonstrate that GDTMS performs more efficiently than other related algorithms. The authors of [38] offer a node-to-node communication architecture for 5G networks that is based on fog computing. It permits communication that is purely network infrastructure-dependent. The associated next-generation evolved node base station (gNB) imports the necessary data from neighboring fog servers to establish the connection. In data analytical units (DAUs), the information is processed after it has been retrieved. The DAUs are built-in processing units that work closely with gNBs and fog servers. Furthermore, a robust mobility management strategy is proposed for dynamic mobile users to facilitate node-to-node communication. The following elements have been found in relevant studies to give attention to dynamic and unpredictable networks. In [39], the Trust based Next Forwarding Node Selection algorithm and the Fuzzy Based Stable and Secure Routing algorithm are two novel algorithms that are combined for achieving secure routing. Effective routing performance is provided by the Trust based Next Forwarding Node Selection method, which employs the trust based node selection process. It also utilizes the fuzzy inference system to explore the qualitative analysis of trust values and links performance with discovering trustworthy routes and handling uncertainty. Table 1 shows the summary of the discussed work and contributions of the proposed algorithm.

Table 1. Summary of existing related studies.

	Overview and Limitations
Existing solutions	Sensors and fog computing are frequently utilized for real-time emerging networks to automate the devices' connection and communication systems. Moreover, fog nodes are increasing the scalability of constraint networks and reducing the energy consumption of interconnected devices for data transmission. However, due to the limited computing powers of the nodes, many solutions are not able to cope with robust stability for the communication systems. Furthermore, it was observed that many solutions do not offer security systems for wireless systems, and impose additional overhead for protecting network data. It was also noted that most proposed solutions have a longer delay for crucial network operations due to issues with frequent network disconnectivity.
Proposed algorithm	In this research study, we proposed for a mobile network to offer an energy-aware solution with the combination of data trustworthiness using fog computing. Moreover, a lightweight authentication system is developed to support real-time communication in a reliable discipline.

3. Proposed Load-Balanced and Energy-Efficient Mobile Routing Protocol

This section describes the proposed algorithm with interaction among developed phases.

3.1. System Model

Let us assume that sensors are denoted by $S_i = (S_1, \ S_2, \ldots, \ S_n)$ and are deployed randomly. The nodes that are not in the same radius can only be communicated using multi-hop mode. Nodes are mobile and rotated, and periodically announce their positions. Fog nodes are placed between sensors and the sink node. Initially, nodes cooperatively share their attributes to initiate the formulation of routing tables. Later, routing tables are refined using cooperative decisions of the devices. The sink node is static and has sufficient resources to control the network environment. It keeps track of the entire monitoring field and announces alert messages if any faulty action is identified. Each cluster has only one cluster head at a time, and with the analysis of QoS parameters, the role is updated. Before discussing the proposed algorithm, we highlight the following network assumptions.

i. Nodes have heterogeneous resources for energy, transmission power, and memory constraints.
ii. Each path is assigned a unique identity.
iii. After deployment, no batteries can be replaced for sensor nodes.
iv. Aggregated data are transmitted to the sink node with the support of fog nodes over the unpredictable communication links
v. The transmission power of the nodes can be adjusted using Received Signal Strength Indicator (RSSI).

3.2. Overview

In this section, the detail of the proposed algorithm is presented. It comprises two phases. The first phase deals with traffic distribution over the mobile nodes with an efficient scheme. In addition, the second is for establishing reliable and trusting communication links with the support of fog nodes. In the beginning, nodes advertise their initial parameters in their communication range. All the nodes receive such information and record it in their local tables. The local table is updated with the analysis of QoS factors. Whenever any node shifts to another range, its record is removed from the table and the new node associates its information. Moreover, the dynamic routing metrics explicitly reduces the time of route formulation and offers more effective connections from node to node (N2N). Each route has a unique identity, and such information copes with a replay attack between the devices. The security keys provide improved authentication methods for mobile devices against data anomalies. Such actions decrease the chances of network compromising and intelligently manage the overall communication under the supervision of the sink node.

Figure 1 depicts the three stages of the proposed algorithm. It includes communications equipment, network services, and secured services. In the deployed environment, communication entities include IoT devices, fog nodes, and cloud systems. IoT devices act as sensors that sense the data and send it to the fog nodes, which then send it to the sink node. Later, the sink node collaborates with the cloud system for data processing and storage. The first phase of the proposed algorithm provides clustering and services for link performance. Based on the adjustable transmission range, the nodes are separated into distinct regions. Furthermore, cluster heads are identified and their locations are made known to all members. The final stage concerns secured sessions for both low-level and high-level communication. N2N communications take place at the low level, whereas fog-to-sink node communication is carried out at the high level.

3.3. Proposed Algorithm

In this section, we explained the working of the proposed algorithm. The detail is comprised of two main phases. In the first phase, transmission power is explored to achieve clustering with optimal data forwarding methods. The links are identified in a more reliable way to attain long-run communication paths. The second phase offers the trustworthiness routes with the supervision of the sink node and reduces the level of threats from malicious devices.

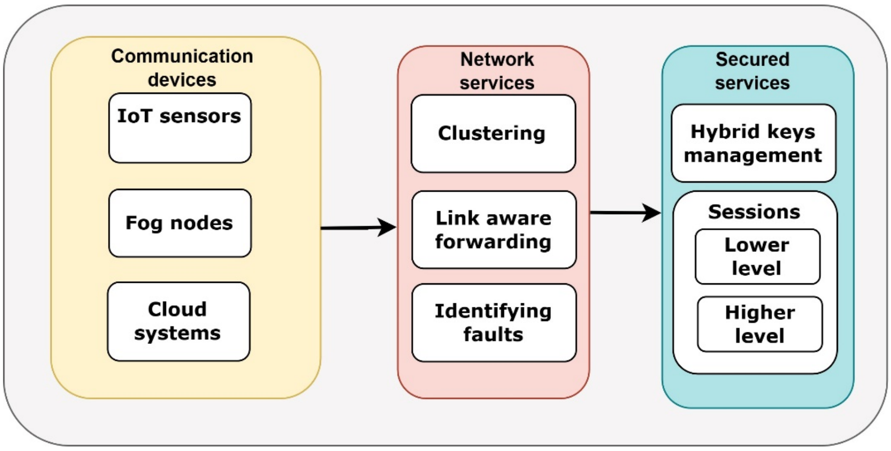


Figure 1. Various stages of the proposed protocol.

3.3.1. Routing Chains and Resources Allocation (RCRA)

This section presents a detailed explanation of the routing process with the usage of network resources in an efficient manner. The source node $s(i)$ records the entries of the neighbors that fall in their transmission radius R, as defined in Equation (1).

$$s(i)= D(n,\ i)\ \leq R \tag{1}$$

where n is the neighbor. However, if none of any node is identified in the transmission range of the source node, then the source node increases its transmission power tr_p gradually £. However, transmission power cannot be increased more than a certain threshold T, as defined in Equation (2).

$$tr_p(i)= tr_p(i) + £ \tag{2}$$

where $tr_p(i) \leq T$

Once the neighbor nodes are identified, they are grouped in a similar cluster. Afterward, each cluster has a specific identity $CLUS\_ID$ assigned. Each node also records its $CLUS\_ID$ into the local table. Within clusters, the node i whose distance d is closest to the centroid c, highest residual energy e, and minimum rotation speed RS is declared as a cluster head CH_i. All such computations are performed in a weighted manner and probability must be highest, as defined in Equation (3).

$$CH_i= 1/(d,\ c) + e\ +1/RS \tag{3}$$

Nodes notify their status when they are elected to serve as cluster heads, and all receiving nodes record the information in their local tables. In the proposed algorithm, since nodes are mobile, re-selection is performed in either one of the conditions i.e., if the energy of the CH_i is dropped down to a certain threshold or CH_i is moved far away from the centroid of the cluster. In this situation, nodes again announce the re-election process and the new node is selected for the role of cluster head. In addition, for data forwarding to the sink node, each cluster head forms a chain with its nearest and most reliable cluster head. The chain is refined each time when data need to be transferred from the origin cluster. Each routing chain RC_i is established based on the distances among cluster heads and link analysis LA parameters, as defined in Equation (4).

$$RC_i= D\left(CH_i,\ CH_j\right),\ LA(i,\ j) \tag{4}$$

To compute the LA, the proposed algorithm utilizes the delay time DT for transmitting packets TP as defined in Equation (5).

$$LA(i,\ j)= DT\ \ltimes\ TP \tag{5}$$

DT is directly proportional to the number of packets transmitted over the link $(i,\ j)$. When the number of packets increases on the link $(i,\ j)$, it indicates a high degree of traffic, such a link is marked as congested and avoids include in the routing chains. The flowchart of the proposed algorithm, in terms of fog-based routing, is shown in Figure 2. First, the nodes are organized into regions based on the adjustable transmission radius with individual identification. Each region is responsible for exploring its cluster head and sending the information to the fog nodes. The proposed algorithm offers a multi-hop model for data forwarding thus it lowers energy consumption when data are transmitted over a longer distance. In data forwarding, link analysis is also employed, in addition to the least distance between cluster heads. For link analysis, the number of sent packets on the specific link is used to compute the delay time. The proposed algorithm initiates the process of data transmission after finding a trustworthy link.

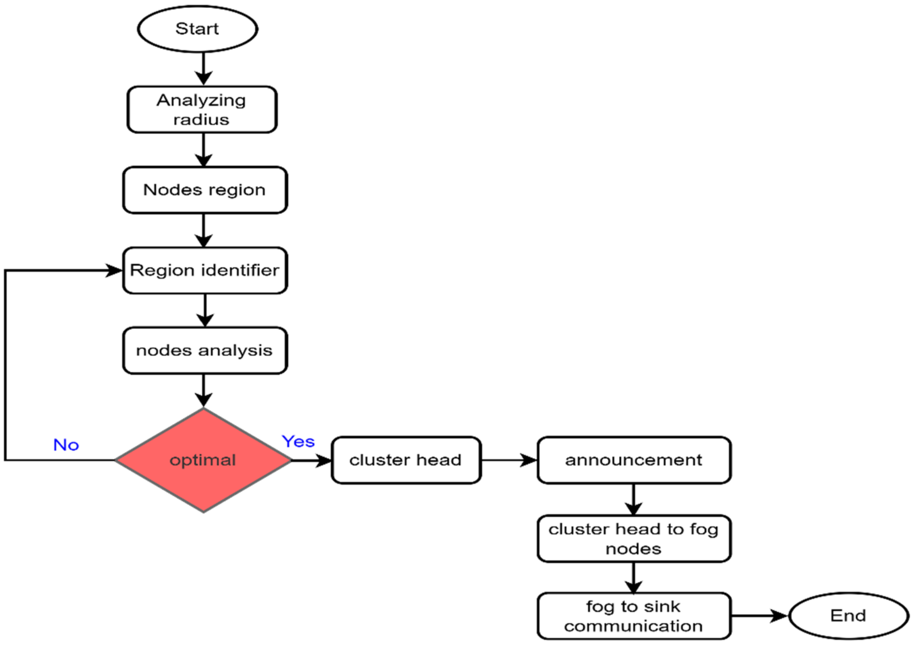


Figure 2. Flowchart of the proposed algorithm.

Algorithm 1 elaborates the pseudocode of the proposed algorithm in terms of data routing using efficient chaining and resource utilization.

Algorithm 1 Network routing with efficient resource allocation

```
Procedure RCRA
  compute the transmission range of nodes
  nodes are divided into regions
  assign a unique id to each region
  for (i = 1; i <= N; i++)
      do
         analyze the members' parameters
         if node (i) is optimized then
            set as cluster head
         end if
    end for
    cluster head to fog communication
    establish routing chain using $RC_i = D\left(CH_i,\ CH_j\right),\ LA(i,\ j)$
    fog to sink communication
end procedure
```

3.3.2. Reliability-Based Lightweight Authentication (RLA)

In this section, the detail of network reliability with lightweight authentication methods is discussed. The proposed algorithm provides a simple and lightweight security mechanism for achieving reliable communications. It explores the concepts of hybrid cryptography and utilizes the methods of symmetric and asymmetric key management. In the proposed algorithm, the peer devices d_i and d_j nodes shared the session key SK for the link $(i,\ j)$, as defined in Equation (6).

$$d_i - > \ d_j\colon\ SK(i,\ j) \tag{6}$$

Moreover, before sharing the SK, the proposed algorithm encrypts the key with the support of private/public keys. d_i encrypts the SK denoted by $SK\prime$, using the public key of d_j and upon receiving, the $SK\prime$ is decrypted by using the private key of d_j. In this way, both the devices have the secured session key and can use it for data forwarding of message M along with time stamp TS as defined in Equation (7).

$$d_i - > \ d_j\colon\ E(SK(M){+}TS \tag{7}$$

In Figure 3, key management and reliable forwarding are the two main stages. In keys management, various keys are generated based on hybrid cryptography. Moreover, keys are verified and securely distributed among the devices. Afterward, the received keys are utilized for N2N low-level security. Furthermore, later, fog nodes are communicated with sink nodes with the same practice for achieving secure key distribution and data encryption. Algorithm 2 shows the pseudocode of the proposed algorithm for securing the network connections with lightweight authentication.

Algorithm 2 Secured network connections with a lightweight authentication scheme

```
Procedure RLA
if devices $d_i$ and $d_j$ has any data to transmit then
  call con_dev( )
end if
devices $d_i$ and $d_j$ nodes shared the session key $SK$ for the link $(i,\ j)$
   $d_i - > \ d_j\colon\ SK(i,\ j)$
      $d_i$ encrypts the $SK$ denoted by $SK\prime$, using the public key of $d_j$
  $SK\prime$ is decrypted by using the private key of $d_j$
  if $SK'$ is verified then
    send the data packets $M$
      $d_i - > \ d_j\colon\ E(SK(M) + TS$
  end if
  if the session time is expired then
    call con_dev( )
  end if
end procedure
```

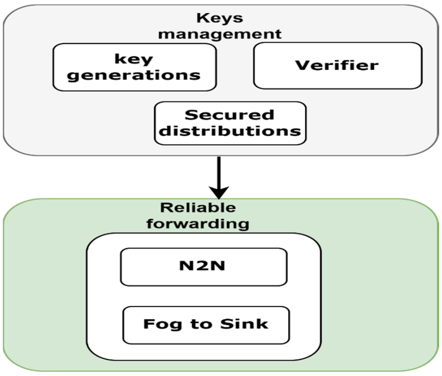


Figure 3. Developed components of the proposed model.

4. Simulation Environment

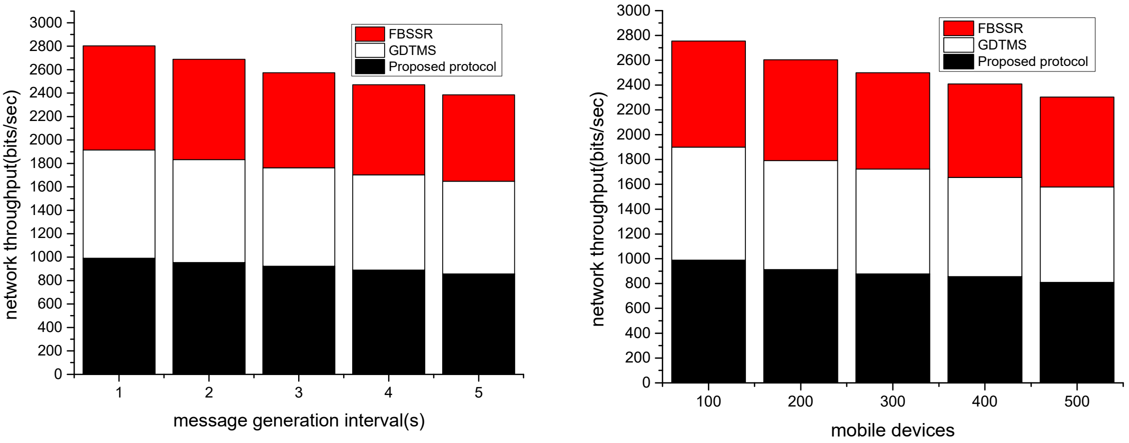
In this section, we provide the parameters used in simulation configurations along with the evaluation of results. The results are conducted through various simulations using Matlab (R2021b). We adopted the free space model in conducting the simulations. All the simulation generated data are recorded in log files, and later, using scripting modules, the required information is extracted to evaluate the performance metrics. The comparisons are performed with the existing techniques, FBSSR and GDTMS. Mobile devices, fog nodes, and sink nodes make up the simulation environment. For mobile devices, the fog nodes are placed closer to the sink node to reduce communication latency and overhead. Mobile devices are in the range of 100 to 500, and they are rotated with the predefined speed in their radius. The transmission range is set to 3m for each device. Each device is assigned a unique address, and no data is allowed for direct transmission in case the distance is higher than the threshold. The initial energy of devices is set to 2j with limited memory and processing resources. We deployed 10 fog nodes in the simulation environment. The packets are sensing with the rate of 1s to 5s. The packet size is up to 100 bytes. We ran 35 simulations to analyze the performance and recorded the average result of each metric. The results were analyzed in terms of varying message generation intervals and the varying number of mobile devices. The parameters used in simulation experiments are described in Table 2. Network throughput, packet drop rate, overhead, reliability, delay, and node level energy consumption are evaluated for performance evaluation. We also perform experimental testing for delay and packet reception in terms of varying times.

Table 2. Simulation parameters.

Parameters	Values
Mobile devices	100–500
Network diameter	500 m × 500 m
Deployment	Random
Path loss model	Free space
Transmission range	3 m
Number of sinks	3
Number of simulations	35
Packet size	100 bytes
Message generation interval	1s to 5s
Initial energy	2j
Fog nodes	10
Malicious nodes	20

In this section, we also describe the security analysis of our proposed algorithm against threats. Our proposed algorithm is based on cryptography principles and offers a secure method to support data reliability and authentication. Each time, peer devices need to initiate the connection CON for forwarding the IoT data. This connection is valid for a particular period, and afterward, it needs to be re-initiated by the peer devices if they further require data transmission. Each device is assigned a unique identification Dev_ID and in case any node is identified as having a duplicate identity, then both nodes are declared as malicious. The record of the malicious nodes is sent to neighboring nodes and the affected routes are reformulated. The connection is secured using the session key which is further encrypted using public and private keys. Before forwarding the data on the link, the sessional needs to be verified. The proposed algorithm is based on hybrid cryptography techniques and makes use of encryption methods by exploring the message units and session keys.

In terms of network throughput, we compared the effectiveness of the proposed algorithm with existing solutions. The proposed protocol has observed that it increases the number of packets transmitted by an average of 11% and 14%, in comparison with FBSSR and GDTMS, as shown in Figure 4a,b. During experiments, it was noticed that as the mobility of devices increases, the congestion also increases and ultimately slows the delivery performance over the communication links. However, the improvement of the proposed algorithm compared to other work is due to the splitting of the network load among the optimal cluster heads. The proposed algorithm also provides an intelligent energy-efficient approach to cope with balancing communication costs on mobile devices. It offers a systematic approach to handling route management in case of route damages by evaluating the link performance. If any link has an increased data loss rate, then such paths are removed from the existing routing tables and updated with alternate and optimal routes. We contrasted the performance of the proposed algorithm with related work in terms of packet drop rate.

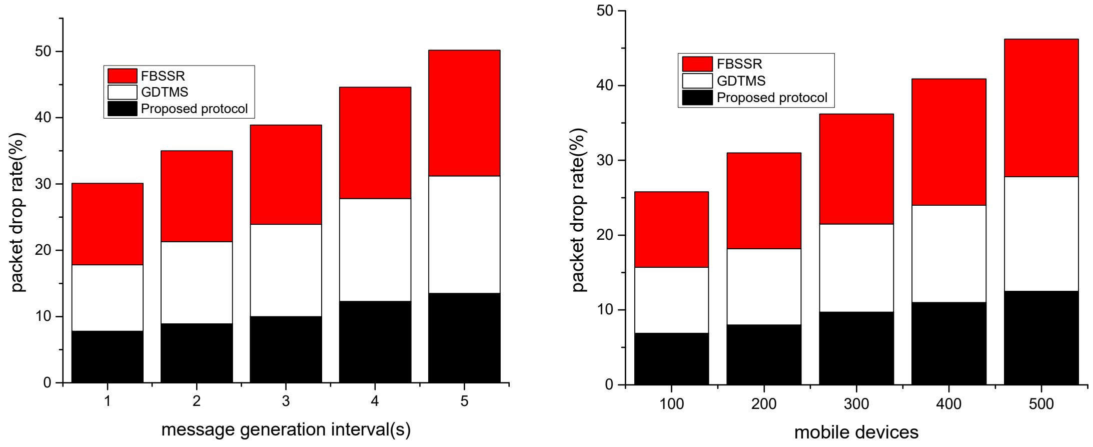


(**a**) (**b**)

Figure 4. (**a**) Network throughput with message generation interval. (**b**) Network throughput with mobile devices.

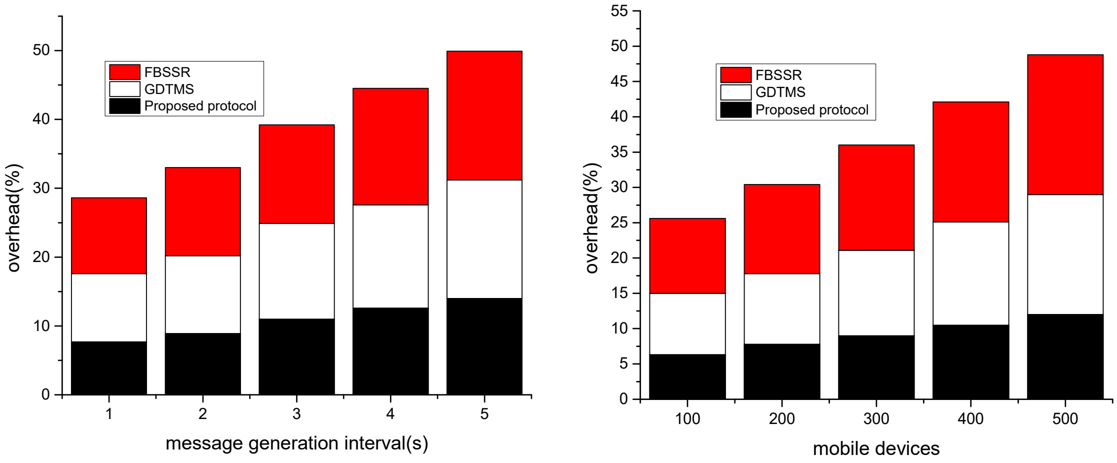
According to Figure 5a,b, it was found that the proposed algorithm reduces the ratio for packet dropping by an average of 10% and 13%, respectively. This is due to the integration of fog nodes with mobile devices, which enhances the route maintenance phase and increases the stability of the chosen route. Moreover, by exploring the delay time over the particular link, the proposed algorithm efficiently determines the faulty links and marks them infeasible in the neighboring table. The forwarder nodes are continuously re-evaluated in their status based on the network metrics, and if they identified themselves as not sufficient to be a part of the routing phase, then they declare their status with the neighbors. The lightweight authentication process also increases the security against malicious devices and decreases the level of packets capturing and dropping.

The performance comparison of the proposed algorithm and existing in terms of overhead is shown in Figure 6a,b. Under varying mobile devices and message generation intervals, it can be demonstrated that the proposed algorithm significantly improves the overhead by an average of 9% and 12% as compared to other work. This is because the proposed algorithm effectively manages the energy resources among mobile devices, and utilizes the support of fog nodes. The fog node reduces the transmission distance of the forwarders to transmit the environment data toward the sink node. The proposed algorithm also re-evaluates the routing states when the delay time over the communication link is greater than a certain threshold. Accordingly, it identified the congested routes from the available list and selected the alternative option for the transmission of the data. The security solution also decreases the non-authentic data flowing on the links and avoids malicious devices from flooding the false packets.



(**a**) (**b**)

Figure 5. (**a**) Packet drop rate with message generation interval. (**b**) Packet drop ratio with mobile devices.



(**a**) (**b**)

Figure 6. (**a**) Overhead with message generation interval. (**b**) Overhead with mobile devices.

The performance comparison of the proposed protocol with related studies in terms of reliability is illustrated in Figure 7a,b. With varying devices and data generation rates, it was observed that the proposed algorithm offers a high degree of reliability in network communication. We tested the reliability of the proposed algorithm and other solutions by deploying the malicious nodes, and it was noticed that the proposed algorithm increases the reliability by an average of 10% and 11%, respectively. This is due to the incorporation of a lightweight security scheme to verify the devices for involvement in the process of data forwarding. Moreover, keys are randomly generated, and by exploring the hybrid cryptographic principles, the proposed algorithm established the secured session by utilizing private and public keys. Once the node is declared authentic, the data routing phase is initiated for the particular node, with the combination of trusted and optimal forwarders.

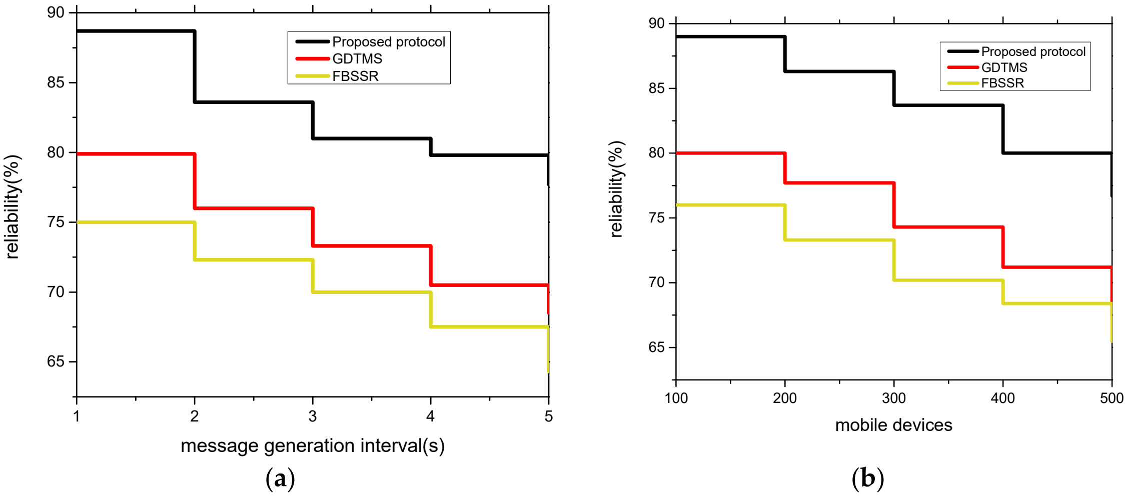


Figure 7. (**a**) Reliability with message generation interval. (**b**) Reliability with mobile devices.

Figure 8a,b illustrates the performance of the proposed protocol with other work in terms of varying times. We conducted two experiments under varying times for delay and the number of received packets. In both experiments, the proposed solution provides significant improvement by an average of 14% and 16%. It is due to the consideration of resource consumption while taking forwarding decisions. Furthermore, the link performance is evaluated periodically and upon identification of any fault in the existing communication channel, the proposed solution readjusts the routing paths. However, the security strategy of the proposed protocol offers the reduction of congestion flooding by malicious nodes. Accordingly, the routes are available for sending the data toward the sink node in a timely and precise manner.

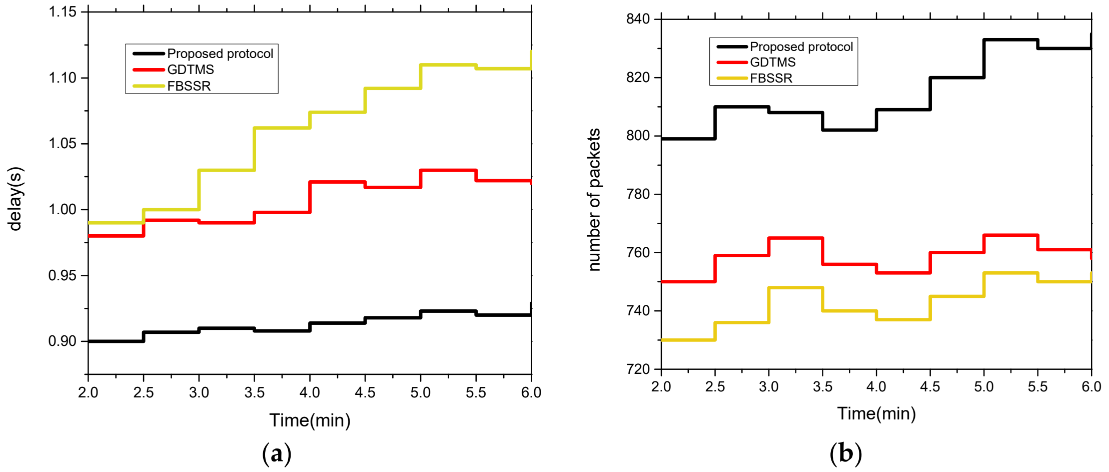


Figure 8. (**a**) Delay with varying time. (**b**) Number of packets with varying time.

In Figure 9a,b, we demonstrate the performance analysis of the proposed algorithm and existing solution in terms of energy consumption. The experiments are conducted under varying message generation intervals, and varying mobile devices. Based on the results, it was observed that with time, the energy resource dropped down. However, the proposed algorithm still gives a lower rate of energy consumption of an average of 15% and 16% compared to other existing work. This is because of the lower transmission distance, in terms of hops, while forwarding the data toward the sink node. Moreover, the nodes are balancing their load over the routing path and efficiently exploring the QoS parameters. The delay time is intelligently managed for carrying the real-time data, and decreases the ratio of routing requests repeatedly. It reduces the energy load on the devices and accordingly offers an energy-aware solution.

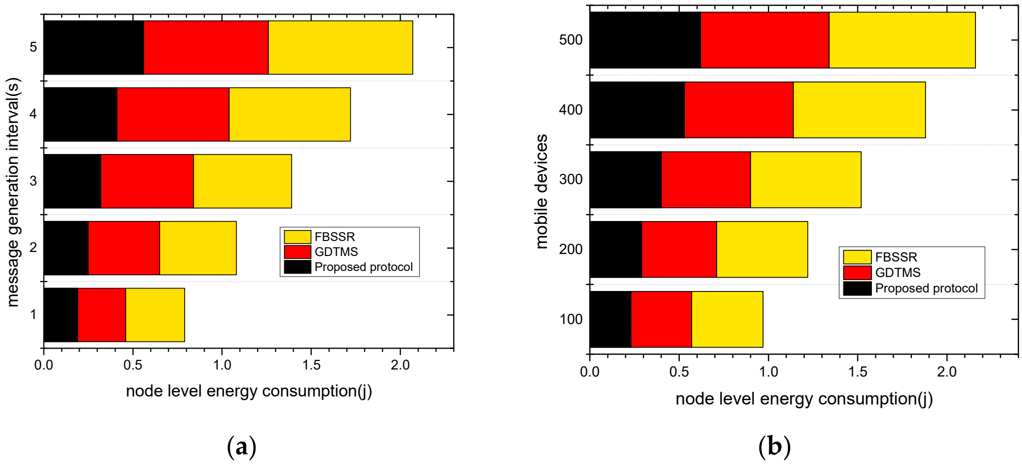


Figure 9. (**a**) Energy consumption with message generation interval. (**b**) Node level energy consumption with mobile devices.

5. Conclusions

This work explores fog computing to propose a technique for energy-efficient mobile routing. The proposed algorithm provides data forwarding by exploring reliable search techniques and shortening the data transmission time. Moreover, the proposed algorithm provides the balancing of energy consumption among the devices, with the support of optimal criteria. The mobile device not only decreases the latency with the combination of fog nodes, but it also offers a lightweight authentication scheme for the node verifier. Another contribution of the proposed algorithm is protecting the data in the presence of attacks. The performance results demonstrate the significant outcomes of the proposed algorithm against existing work; however, it was observed that still, the proposed algorithm produces additional overhead and communication costs when the number of mobile devices increases. Furthermore, methods need to be designed for more efficient routing with the combination of deep learning models. In our future work, we aim to combine the intelligence and processing power of software-defined networks to cope with the efficient management of nodes and network resources. In addition, improved and lightweight intrusion detection systems require by exploring machine learning.

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

Funding: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through project number: IFP22UQU4170008DSR265.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Omoniwa, B.; Hussain, R.; Javed, M.A.; Bouk, S.H.; Malik, S.A. Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues. *IEEE Internet Things J.* **2018**, *6*, 4118–4149. [CrossRef]
2. Alavi, A.H.; Jiao, P.; Buttlar, W.G.; Lajnef, N. Internet of Things-enabled smart cities: State-of-the-art and future trends. *Measurement* **2018**, *129*, 589–606. [CrossRef]
3. Haseeb, K.; Islam, N.; Javed, Y.; Tariq, U. A lightweight secure and energy-efficient fog-based routing protocol for constraint sensors network. *Energies* **2020**, *14*, 89. [CrossRef]
4. Sobin, C. A survey on architecture, protocols and challenges in IoT. *Wirel. Pers. Commun.* **2020**, *112*, 1383–1429. [CrossRef]
5. Cui, S.; Farha, F.; Ning, H.; Zhou, Z.; Shi, F.; Daneshmand, M. A survey on the bottleneck between applications exploding and user requirements in IoT. *IEEE Internet Things J.* **2021**, *9*, 261–273. [CrossRef]
6. Islam, N.; Altamimi, M.; Haseeb, K.; Siraj, M. Secure and Sustainable Predictive Framework for IoT-Based Multimedia Services Using Machine Learning. *Sustainability* **2021**, *13*, 13128. [CrossRef]
7. Thangaramya, K.; Kulothungan, K.; Logambigai, R.; Selvi, M.; Ganapathy, S.; Kannan, A. Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. *Comput. Netw.* **2019**, *151*, 211–223. [CrossRef]
8. Sharma, S.; Verma, V.K. An integrated exploration on internet of things and wireless sensor networks. *Wirel. Pers. Commun.* **2022**, *124*, 2735–2770. [CrossRef]
9. Mehmood, A.; Lv, Z.; Lloret, J.; Umar, M.M. ELDC: An artificial neural network based energy-efficient and robust routing scheme for pollution monitoring in WSNs. *IEEE Trans. Emerg. Top. Comput.* **2017**, *8*, 106–114. [CrossRef]
10. Haseeb, K.; Ahmad, I.; Awan, I.I.; Lloret, J.; Bosch, I. A machine learning SDN-enabled big data model for IoMT systems. *Electronics* **2021**, *10*, 2228. [CrossRef]
11. Miglani, A.; Kumar, N.; Chamola, V.; Zeadally, S. Blockchain for Internet of Energy management: Review, solutions, and challenges. *Comput. Commun.* **2020**, *151*, 395–418. [CrossRef]
12. Chen, R.; Long, W.-X.; Mao, G.; Li, C. Development trends of mobile communication systems for railways. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3131–3141. [CrossRef]
13. Bai, T.; Pan, C.; Deng, Y.; Elkashlan, M.; Nallanathan, A.; Hanzo, L. Latency minimization for intelligent reflecting surface aided mobile edge computing. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 2666–2682. [CrossRef]
14. Chen, S.; Liang, Y.-C.; Sun, S.; Kang, S.; Cheng, W.; Peng, M. Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed. *IEEE Wirel. Commun.* **2020**, *27*, 218–228. [CrossRef]
15. Budhiraja, I.; Tyagi, S.; Tanwar, S.; Kumar, N.; Rodrigues, J.J.P.C. Tactile Internet for smart communities in 5G: An insight for NOMA-based solutions. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3104–3112. [CrossRef]
16. Wang, D.; Liu, J.; Yao, D. An energy-efficient distributed adaptive cooperative routing based on reinforcement learning in wireless multimedia sensor networks. *Comput. Netw.* **2020**, *178*, 107313. [CrossRef]
17. Memon, I.; Hasan, M.; Shaikh, R.; Nebhen, J.; Bakar, K.; Hossain, E.; Tunio, M. Energy-efficient fuzzy management system for internet of things connected vehicular ad hoc networks. *Electronics* **2021**, *10*, 1068. [CrossRef]
18. Li, S.; Kim, J.G.; Han, D.H.; Lee, K.S. A survey of energy-efficient communication protocols with QoS guarantees in wireless multimedia sensor networks. *Sensors* **2019**, *19*, 199. [CrossRef]
19. 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]
20. Chen, S.; Sun, S.; Kang, S. System integration of terrestrial mobile communication and satellite communication—The trends, challenges and key technologies in B5G and 6G. *China Commun.* **2020**, *17*, 156–171. [CrossRef]
21. Ahmed, A.; Abu Bakar, K.; Channa, M.I.; Haseeb, K. Countering node misbehavior attacks using trust based secure routing protocol. *Telkomnika Telecommun. Comput. Electron. Control.* **2015**, *13*, 260–268. [CrossRef]
22. Malik, U.M.; Javed, M.A.; Zeadally, S.; Islam, S.U. Energy efficient fog computing for 6G enabled massive IoT: Recent trends and future opportunities. *IEEE Internet Things J.* **2021**, *9*, 14572–14594. [CrossRef]
23. Bhat, J.R.; Alqahtani, S.A. 6G ecosystem: Current status and future perspective. *IEEE Access* **2021**, *9*, 43134–43167. [CrossRef]
24. Qi, Q.; Tao, F. A smart manufacturing service system based on edge computing, fog computing, and cloud computing. *IEEE Access* **2019**, *7*, 86769–86777. [CrossRef]
25. Mutlag, A.A.; Ghani, M.K.A.; Arunkumar, N.; Mohammed, M.A.; Mohd, O. Enabling technologies for fog computing in healthcare IoT systems. *Future Gener. Comput. Syst.* **2019**, *90*, 62–78. [CrossRef]
26. Ghobaei-Arani, M.; Souri, A.; Rahmanian, A.A. Resource management approaches in fog computing: A comprehensive review. *J. Grid Comput.* **2020**, *18*, 1–42. [CrossRef]
27. Sofla, M.S.; Kashani, M.H.; Mahdipour, E.; Mirzaee, R.F. Towards effective offloading mechanisms in fog computing. *Multimed. Tools Appl.* **2022**, *81*, 1997–2042. [CrossRef]
28. Alnoman, A.; Sharma, S.K.; Ejaz, W.; Anpalagan, A. Emerging edge computing technologies for distributed IoT systems. *IEEE Netw.* **2019**, *33*, 140–147. [CrossRef]
29. Avasalcai, C.; Murturi, I.; Dustdar, S. Edge and fog: A survey, use cases, and future challenges. *Fog Comput. Theory Pract.* **2020**, 43–65. [CrossRef]
30. Hong, C.-H.; Varghese, B. Resource management in fog/edge computing: A survey on architectures, infrastructure, and algorithms. *ACM Comput. Surv. CSUR* **2019**, *52*, 1–37. [CrossRef]

31. Habibi, P.; Farhoudi, M.; Kazemian, S.; Khorsandi, S.; Leon-Garcia, A. Fog computing: A comprehensive architectural survey. *IEEE Access* **2020**, *8*, 69105–69133. [CrossRef]
32. Sicari, S.; Rizzardi, A.; Coen-Porisini, A. 5G in the internet of things era: An overview on security and privacy challenges. *Comput. Netw.* **2020**, *179*, 107345. [CrossRef]
33. Erhan, L.; Ndubuaku, M.; Di Mauro, M.; Song, W.; Chen, M.; Fortino, G.; Bagdasar, O.; Liotta, A. Smart anomaly detection in sensor systems: A multi-perspective review. *Inf. Fusion* **2021**, *67*, 64–79. [CrossRef]
34. Abidoye, A.; Kabaso, B. Energy-efficient hierarchical routing in wireless sensor networks based on fog computing. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 1–26. [CrossRef]
35. Biswash, S.K.; Jayakody, D.N.K. A fog computing-based device-driven mobility management scheme for 5G networks. *Sensors* **2020**, *20*, 6017. [CrossRef] [PubMed]
36. Gupta, S.; Garg, R.; Gupta, N.; Alnumay, W.S.; Ghosh, U.; Sharma, P.K. Energy-efficient dynamic homomorphic security scheme for fog computing in IoT networks. *J. Inf. Secur. Appl.* **2021**, *58*, 102768. [CrossRef]
37. Fang, W.; Zhang, W.; Chen, W.; Liu, Y.; Tang, C. TMSRS: Trust management-based secure routing scheme in industrial wireless sensor network with fog computing. *Wirel. Netw.* **2020**, *26*, 3169–3182. [CrossRef]
38. Babu, S.; Biswash, S.K. Fog computing–based node-to-node communication and mobility management technique for 5G networks. *Trans. Emerg. Telecommun. Technol.* **2019**, *30*, e3738. [CrossRef]
39. Rajeswari, A.R.; Kulothungan, K.; Ganapathy, S.; Kannan, A. A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks. *Peer-to-Peer Netw. Appl.* **2019**, *12*, 1076–1096. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.