

## Article

# A Lightweight Secure and Energy-Efficient Fog-Based Routing Protocol for Constraint Sensors Network

Khalid Haseeb <sup>1</sup>, Naveed Islam <sup>1</sup>, Yasir Javed <sup>2,\*</sup> and Usman Tariq <sup>3,\*</sup>

<sup>1</sup> Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Pakistan; khalid.haseeb@icp.edu.pk (K.H.); naveed.islam@icp.edu.pk (N.I.)

<sup>2</sup> College of Computer Science, Princes Sultan University, Riyadh 11586, Saudi Arabia

<sup>3</sup> Information Systems Department, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al Khraj 11942, Saudi Arabia

\* Correspondence: yjaved@psu.edu.sa (Y.J.); u.tariq@psau.edu.sa (U.T.)

**Abstract:** The Wireless Sensor Network (WSN) has seen rapid growth in the development of real-time applications due to its ease of management and cost-effective attributes. However, the balance between optimization of network lifetime and load distribution between sensor nodes is a critical matter for the development of energy-efficient routing solutions. Recently, many solutions have been proposed for constraint-based networks using the cloud paradigm. However, they achieve network scalability with the additional cost of routing overheads and network latency. Moreover, the sensors' data is transmitted towards application users over the uncertain medium, which leads to compromised data security and its integrity. Therefore, this work proposes a light-weight secure and energy-efficient fog-based routing (SEFR) protocol to minimize data latency and increase energy management. It exploits the Quality of Service (QoS) factors and facilitates time-sensitive applications with network edges. Moreover, the proposed protocol protects real-time data based on two levels of cryptographic security primitives. In the first level, a lightweight data confidentiality scheme is proposed between the cluster heads and fog nodes, and in the second level, a high-performance asymmetric encryption scheme is proposed among fog and cloud layers. The analysis of simulation-based experiments has proven the significant outcomes of the proposed protocol compared to existing solutions in terms of routing, security, and network management.

**Keywords:** energy efficiency; information security; Internet of Things; cryptanalysis; lightweight routing; wireless sensor networks



**Citation:** Haseeb, K.; Islam, N.; Javed, Y.; Tariq, U. A Lightweight Secure and Energy-Efficient Fog-Based Routing Protocol for Constraint Sensors Network. *Energies* **2021**, *14*, 89. <https://dx.doi.org/10.3390/en14010089>

Received: 10 December 2020

Accepted: 22 December 2020

Published: 26 December 2020

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

In recent years, the Internet of Things (IoT) [1–3] has undergone great evolution in the field of communication that connects different electronic devices in agriculture, smart cities, military, healthcare, etc. IoT is the system of various interconnected machines, communication devices, physical objects, and humans. The hundred to thousand IoT-based sensors are deployed in the monitoring area for data gathering and transmission with limited resources for transmission, memory, bandwidth, energy, and processing powers. Among all these, efficient utilization of energy consumption is a vital issue for a constraints sensors network, because the battery power of sensor nodes is depleted rapidly in data gathering, aggregation, and transmitting. Moreover, such tiny devices are interconnected in the form of ad-hoc topology to achieve data gathering and forwarding. Therefore, appropriate routing decisions should be determined for optimizing network connectivity and stability. The main aim of the optimal decision is to choose the best and most maintainable path among the others with efficient utilization of node resources and reliable data delivery to application users [4–8]. Also, due to the lower cost and robust features of sensor networks, most researchers have integrated it with IoT for better network performance in terms of cost-effectiveness, better network coverage, and scalability [9–12]. The technology of cloud

computing has been adopted by many solutions for data management in terms of storage, processing, and scalability. It offers the on-demand availability of various resources for storage, computing power in a shared manner. Such cloud-based facilities significantly decrease the additional overheads on sensor nodes and improve the satisfactory level of application users [13–15]. However, the cloud-based infrastructure lacks mobility and data latency for its end users. Due to high network latency between application users and cloud servers, the problem of data loss ratio has also arisen. To overcome the issues of the cloud paradigm, the Commercial & Industrial Security Corporation (Cisco) network system introduced the concept of fog computing, which is an architecture and uses various edge devices to perform an extensive amount of processing and transmission in the distributed system [16]. It works like a fog layer between the network infrastructure and cloud paradigm, and decreases the shortcoming of bandwidth utilization, network delay, and network traffic. However, the sensors' data is transmitted over the wireless network and is subject to potential threats. Therefore, network security, authentication, and integrity are major security concerns for a constraints-oriented sensors network.

The main aim of this paper is to present a lightweight secure and energy-efficient fog-based routing protocol for constraints sensors network to increase the network lifetime with an optimal routing scheme. Moreover, the sensors' data is also protected from unauthorized and malicious bodies and prevents the probabilities of compromised privacy, authenticity, and integrity in multi-levels. The key factors of the proposed work are as follows.

- i. It uses the dynamic distance threshold to decrease the transmission cost with a longer network lifetime. Also, it reduces the overheads on the frequent exchange of local information among sensor nodes and leads to minimize excessive energy consumption.
- ii. Data routing between cluster heads to fog layer and from fog layer to cloud servers is achieved by considering the QoS parameters. Additionally, incorporating a packet queuing parameter increases the route maintenance and data delivery performance.
- iii. Two levels of security are provided using cryptographic algorithms; the first level attains data privacy from cluster heads to fog nodes, and in the second level, a more authentic asymmetric encryption scheme is proposed between the fog nodes and cloud servers.

The paper is organized into the following sections. Section 2 reviewed the existing work. Section 3 explains the discussion for the proposed secure and energy-efficient fog-based routing (SEFR) protocol along with its methodology design and components. Section 4 explains the analysis of the results of the proposed SEFR protocol with other schemes. Finally, Section 5 concludes the research work.

## 2. Related Work

The IoT-based systems are comprised of physical objects with a huge number of sensor nodes that are deployed in either static or mobile scenarios with high powerful BS. All the devices are connected through wireless links to capture the monitoring area in terms of various attributes like weather, humanity, temperature, vehicle movements, etc. The observing data is collected by sensor nodes and using the selected cluster heads it is transmitted to BS. The cluster heads or gateway nodes are further connected to BS using the Internet, and different application users obtained their needed information. However, several efficient routing protocols for constraint sensors network have been proposed [17–20], and improved the network performance compared to traditional solutions. Nonetheless, the still research community is currently trying to increase the nodes' performance for such an IoT-based system in terms of stability, delivery ratio, and least delay rate due to their limited constraints. Although cloud-based paradigms have been used with the integration of IoT-based sensors and have overcome the issue of scalability and reducing computation load for sensor nodes, the problem of network latency still exists at the end of application users. Moreover, the prohibited entries of opponent nodes lead to several security threats and most of the resources like memory, processing chips, etc.,

may be inaccessible to network nodes and lead to untrustworthiness in data transmissions. Therefore, to efficiently undertake the network-wide routing, securely transfer data, and make a strong authentication, the research community is still focused on an intelligent and fault-tolerant routing solution [21–23]. In [24], the authors proposed a novel network architecture named cluster-based self-organization data aggregation that aims to organize the nodes in self-organized clusters for data aggregation and forwarding. The proposed solution improved the network lifetime and decreases the network overheads; however, the clusters of network nodes are not formulated in a uniform manner. Also, the construction of routing paths is not reliable and stable in terms of data security and robustness. Moreover, the concern for network threats is not considered in the proposed solution. In [25], the authors proposed a novel, light-weight, efficient key exchange, and authentication protocol suite called the Secure Mobile Sensor Network (SMSN) Authentication Protocol to ensure data confidentiality and validity. In the proposed solution, the mobile sensor node initiates an authentication process and obtained a re-authentication ticket from BS. Later, the mobile node exploits this obtained re-authentication ticket while exchanging multiple data to various sessions or when moving across the network. However, the proposed SMSN solution does not consider the link measurement for the performance of fault-tolerant and trustworthy routing and, as a result, the solutions lead to frequent re-routing and re-transmissions of data packets. Also, it consumed additional energy and increased network overheads to determine the up-to-date position of mobile sensors. The authors in [26] analyzed the problem data gathering from wireless sensor networks to a cloud with multiple mobile sinks, and formulated a constrained optimization problem, which proved to be NP-hard. In this solution, the authors proposed a time adaptive schedule algorithm (TASA) and used multiple mobile sinks to gather the network data. Moreover, the solution reduces the transmission cost by forming the minimum spanning tree (MST). Simulation-based experiments were performed, and it was revealed that the algorithm improves the energy consumption with the least data latency during the data transmission among WSN and cloud. However, the proposed algorithm is not able to cope with optimize routing decisions and, in addition, data security can be compromised in the existence of potential threats. In [27], the authors proposed a framework for data collection from WSN towards the cloud using elements of mobile fogs. It uses the factors of distance and residual energy for the formation of routing paths and decreases the level of energy consumption and latency ratio. The simulation-based experiments demonstrated that the proposed framework outperforms routing performance compared to traditional solutions. However, the proposed framework did not notice the network threats that may be risky for data transmission and their effects on data privacy and its integrity. Moreover, the routing paths are chosen without an in-depth analysis of uncontrolled links, which results in increased response time and communication cost. In [28,29], the authors proposed fog-based routing solutions for improving energy efficiency and trust management. The proposed solution reduces energy consumption and increases network throughput in the wireless scenario. However, they overlooked the measurements of the transmission links, and, as a result, in large size nodes distribution, the end-to-end latency increases. Also, the overburden links cause frequent data loss and unnecessary data-retransmissions, which results in network overheads. Table 1 illustrates the contributions and limitations of the existing work and proposed SEFR protocol.

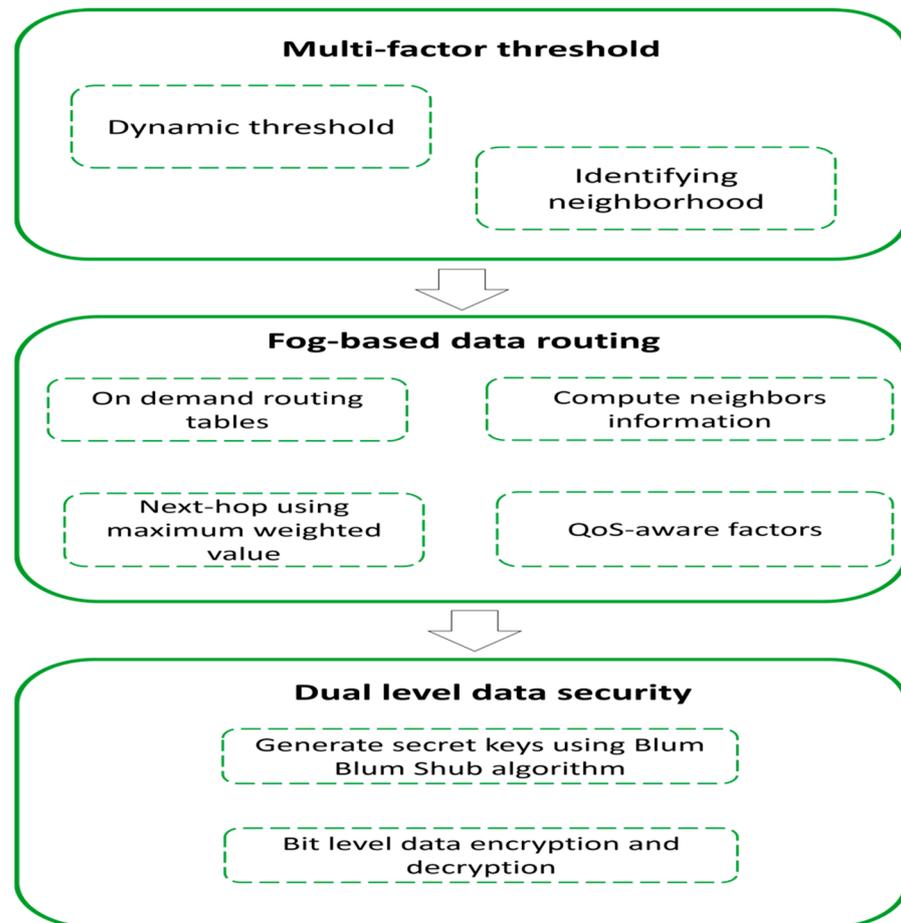
**Table 1.** Solutions comparison.

Solutions	Contributions	Limitations
Cluster-based self-organization data aggregation	improved network lifetime and overheads	link estimation is missing; insecure against malicious threats
SMSN	ensures data confidentiality and validity	energy consumption in finding up-to-date positions of mobile sensors; frequent route breakages
TASA	multiple mobile sinks; reduce the transmission cost by forming the MST	frequent update messages to locate mobile sinks; link measurement is ignored; ignored data security
Data collection from WSNs to the cloud based on mobile Fog elements	Multi factors for data routes; decreases energy consumption and latency	Unnoticed data privacy against network threats; frequent re-transmissions due to lack of congestion measurement.
A source anonymity-based lightweight secure AODV protocol	reduces energy consumption; increases network throughput	Multi factors are not considered for data routing; compromised data latency in large scale nodes region
Trust Management-Based Energy Efficient Routing Scheme	Energy efficiency; data delivery performance	Link measurement is overlooked; unnecessary route request-response messages lead to additional overheads
SEFR Protocol	Multi-facet QoS parameters for data forwarders; two-levels of data security; decrease data latency	Intelligent data management; distributed network threats model.

The background work shows the contribution of the IoT paradigm integrated with WSNs to ease different applications. Due to their dynamic and easy infrastructure, different fields obtain environmental data on time. The distributed low powered sensor nodes perform a key role for data collection and routing towards remote users for their necessary actions. However, the limited restrictions on network resources set remarkable research challenges for energy constraints and time-sensitive applications. Moreover, some solutions integrated the cloud paradigm for data management in terms of storage and processing. Such solutions increase network performance in IoT applications for cost efficiency and data management. However, such solutions encountered latency for large-scale distribution regions and additional energy consumption problems. It is also seen that some cloud-based solutions do not consider optimal forwarding, and thereby result in data disruption and insufficient time management. Although fog computing offers a distributed environment to collaborate with cloud and IoT sensors, most of the solutions result in exposure to security problems in terms of confidentiality and authentication, which is harmful to sensitive and real-time sensors' data. Also, most of the fog-based solutions ignored the valuation of data links and as a result, route breakages increase with additional route re-discoveries requests. Based on the findings from related work, it is observed that developing a lightweight secure and energy-efficient routing protocol for constraint sensor networks with the integration of fog computing is a demanding problem to ease time-sensitive and quality assurance applications [30–32].

### 3. Proposed SEFR Protocol

The capabilities of both the WSN and fog computing are combined to facilitate the on-demand and real-time network operations such as information gathering, storing, and efficient and reliable processing. The restricted resources on the part of sensor nodes impose a lot of research difficulties while designing an optimal solution. This work presents a lightweight secure and fog-based energy-efficient routing protocol to decrease network delay and energy consumption of the network field. Also, it increases the data security between cluster heads to fog nodes and fog nodes to cloud servers against potential threats. The architectural design of the proposed work is depicted in Figure 1.



**Figure 1.** Architectural design of the proposed work.

#### 3.1. Energy Model and Assumptions

The proposed protocol adopts the energy model as applied in [33]. The energy consumption depends on transmitting and receiving data. The sensor nodes consumed the energy resource  $E_{Tr}(k, D)$  while transmitting the  $k$  data bits over the communication distance  $d$ , as given in Equation (1).

$$E_{Tr}(k, D) = \begin{cases} E_e * k + k * E_{fs} * D^2, & \text{if } D \leq d_t \\ E_e * k + k * E_{amp} * D^4, & \text{if } D > d_t \end{cases} \quad (1)$$

The bit level energy consumption is shown by  $E_e$ ,  $E_{fs} * D^2$  or  $E_{fs} * D^4$  is the energy consumption of sensor nodes, and  $d_t$  is the distance threshold. The energy consumption  $E_{Rx}(k)$  during the reception of  $k$  data bits can be computed as given in Equation (2).

$$E_{Rx}(k) = E_e * k \quad (2)$$

The following network assumptions are made during the design and development of the SEFR protocol.

- i. The sensor nodes are installed randomly and stand static with limited abilities of resources.
- ii. Fog nodes are physical devices with powerful and fault-tolerant functionalities.
- iii. Source and destination nodes are exempt from malicious operations.
- iv. The malicious nodes flood bogus route reactions so they can be selected as data forwarders and drop the data packets.

### 3.2. Methodology of SEFR

The detailed discussion of the methodology for the proposed SEFR protocol is explained in this section. It is divided into three phases. Different clusters are produced for balancing a load of sensor nodes with uniform energy consumption. Each cluster has a single cluster head, which aims to collect, aggregate, and route the members' data to the adjacent cluster head. The SEFR protocol uses a dynamic threshold that is comprised of multi-factors, and accordingly, optimal nodes are identified for the role of cluster heads. The data routing is accomplished in two steps. First, sensors' data is routed from cluster heads to fog nodes, and second, fog nodes that are located at the network edges transmit the incoming data towards cloud services using QoS parameters. Such a strategy imposes the least calls of route maintenance and improves the response time for critical applications. Also, it provides two tiers of security until data is delivered to remote users.

In the beginning, sensor nodes initiate the hello message in the network field, so they may flood their positioning coordinates in the observing field. Upon receiving the information, neighbors make an entry in their routing tables and send an acknowledgment ACK message back to the source node along with their positioning coordinates. Accordingly, source nodes also make an entry of their neighbors' position in their routing tables. Once all the nodes stored the neighbors' information, then the SEFR protocol initiates the process of cluster head selection. Unlike most of the existing solutions that form the cluster boundaries only based on the distance parameter, the SEFR protocol sets a dynamic threshold to define the particular region based on distance and energy factors. The nodes that come within the computed region are considered as candidate nodes for the selection of cluster heads. Furthermore, the neighbor cluster heads are interconnected with each other to establish a virtual backbone structure and initiate the method for data routing towards fog nodes that are placed on network boundaries.

Let us consider that  $T_r$  is a transmission radius, the distance of the farthest node from the cloud server is  $D_n$  and the maximum distance is denoted by  $D_{max}$ . The  $D_{max}$  indicates the radius of the network dimensions. Similarly,  $E_n$  is the residual energy and  $E_{max}$  is the maximum energy, then the threshold value  $D$  is denoted in Equation (3).

$$D = T_r \left( \frac{D_n}{D_{max}} + \frac{E_n}{E_{max}} \right) \quad (3)$$

Based on the computed threshold  $D$ , the SEFR protocol determines the set of nodes and initiates the cluster head selection process among them. Then, the nodes that have a residual energy level more than a certain threshold are selected as cluster heads. Afterward, they announce their position, and the nodes with the least transmission distance join them, which results in formulating a unique cluster. If more than one cluster head lies in the transmission range of ordinary sensors, then the nearest cluster head is selected for the formulation of the cluster. Subsequently, the SEFR protocol slightly increases the threshold value to further gather the sensor nodes that are still not a part of any cluster, and it repeats the same procedure until the required process is completed.

When the cluster formation phase is over, the SEFR protocol initiates the process of data routing from cluster heads to fog nodes. The SEFR protocol uses QoS-aware parameters to evaluate the routing decision and achieves energy-efficient and stable data transmission. The source cluster head identifies the neighbor cluster heads from their

routing tables and inquires them to share their up-to-date information. Accordingly, the neighbor cluster heads compute their residual energy, distance to fog nodes, and packet queuing factors. In the SEFR protocol, the packet queuing factor depends on the ratio of estimated delivered and dropped packets. The source nodes flood a fixed amount of beacon messages to neighbors periodically. Suppose  $Pk_r$  is the amount of received packets and  $Pk_d$  is the number of drop packets then the estimated packet queuing  $E(PQ)$  can be computed using Equation (4).

$$\max[E(PQ)] = \frac{Pk_r}{Pk_r + Pk_d} * R_T \quad (4)$$

where  $R_T$  denotes the data transfer rate of the network. The value  $E(PQ)$  is normalized in the range of 0 to 1. The highest value of  $E(PQ)$  gives the strong probability of data reception rate over the link from the source cluster head node to a neighbor's cluster head. Accordingly, such a node has a high chance for the selection of cluster head as a forwarder rather than low  $E(PQ)$  valued node. Finally, based on the neighbor information, the SEFR protocol computes the weighted value  $W(i)$  as given in Equation (5).

$$W(i) = \max \left( \alpha * E + \beta * \left( \frac{1}{D_{i,f}} \right) + \gamma * E(PQ) \right) \quad (5)$$

$\alpha$ ,  $\beta$ , and  $\gamma$  are weighting constants and each value contributes to an equal percentage for energy, distance to fog node, and packet queuing parameters. Thus, their summation  $\alpha + \beta + \gamma$  is set to 1. In SEFR protocol, the highest weighted neighbor cluster head indicates the optimal choice for selecting it as a next-hop. When clusters' data is received by the fog node and it falls closer to the cloud server then the direct transmission is generated. Otherwise, the SEFR protocol adopts the same criteria to identify the appropriate subsequent fog node for data routing, until the clusters' data is received on the cloud server. After the accomplishment of energy-efficient and reliable routing, the next phase of the SEFR protocol is data security. It presents a lightweight security scheme for authentication, confidentiality, and integrity of data transmission from the cluster heads to fog nodes and from fog nodes to a cloud server, which is computationally efficient and low on memory. In this scheme, the fog nodes generate the secret keys for each cluster head using the Pseudo-Random Number Generator (PRNG) of the Blum Blum Shub algorithm [34]. The proposed security scheme exploits a bitwise operation exclusive-OR (XOR), which integrates both data bits and random secret keys. The random keys for each cluster head  $n_i$  are generated using the Blum Blum Shub algorithm as given by Equation (6).

$$K_{n+1} = K_n^2 \text{ mod } W \quad (6)$$

In Equation (6),  $K_n$  is the generated secret random value for cluster head  $n_i$ ,  $W = pq$  is the product of two large prime numbers  $p$  and  $q$ ,  $K_0$  is the seed integer value that is co-prime to  $W$ . Afterward when the cluster head  $n_i$  send data  $m_i$  to the cluster head  $n_j$ , it is encrypted using Equation (7).

$$E_j(m_i) = m_i \oplus K_i \quad (7)$$

Here,  $\oplus$  denotes the XOR operation of data  $m_i$  from the cluster head  $n_i$  towards cluster head  $n_j$ . The encrypted data  $E_j(m_i)$  is further transmitted towards the fog node, which can decrypt it by taking the XOR with the key  $K_i$  as given in Equation (8).

$$D_j(m_i) = E_j(m_i) \oplus K_i \quad (8)$$

The SEFR protocol makes use of a public key-based cryptographic scheme for data protection and security between the fog node and the cloud server. In this scheme, the fog node and the cloud server use pairs of public  $K_p$  and private keys  $K_u$  for the encryption and decryption of data transmissions. The keys are generated using an RSA algorithm due to its strength and simplicity [35]. It first selects two large primes  $P1$  and  $P2$ , computes their

product  $n$ , then computes the  $\lambda(n)$  (Carmichael totient of the prime product  $n$ ). Similarly, any coprime  $e$  to  $\lambda(n)$  is selected with  $1 < e < \lambda(n)$  and  $\gcd(e, \lambda(n)) = 1$ , thus making a public key of  $(e, n)$  and a private key pair  $(d, n)$ , where  $d$  is the modular inverse of  $e$  and it is determined using  $d \equiv e^{-1} \pmod{\lambda(n)}$ . The data encryption  $E_c$  towards the cloud server from the fog node is performed using Equation (9).

$$E_c \equiv D^e \pmod{s} \quad (9)$$

where  $D$  is representing the data from fog nodes.

At the receiving end, the encrypted data  $E_c$  is decrypted by the cloud server using Equation (10).

$$D \equiv E_c^d \pmod{s} \quad (10)$$

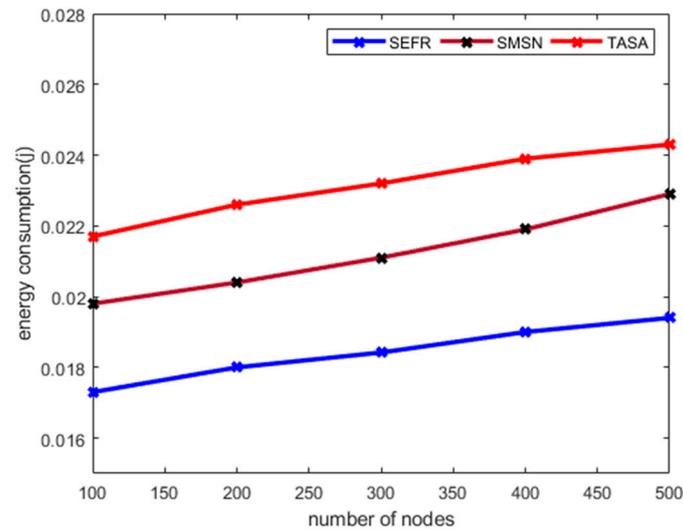
#### 4. Results

This section presents the performance results of the SEFR protocol under an unpredictable scenario. The performance evaluation is done in NS3 in terms of energy consumption, end-to-end delay, network throughput, packet drop ratio, communication overheads, and link load. The number of sensor nodes and fog nodes is set from 100 to 500 and 10 respectively. The fog nodes are placed at the network borders. The transmission range  $T_r$  of each node is fixed to 15 m. The radius of the network field is fixed to  $200 \times 200 \text{ m}^2$ . The number of malicious nodes is set to 30. Initially, the residual energy of the nodes is  $2j$  with 2000 s of simulation time. The data size of each block is 32 bits. The performance of the SEFR protocol is evaluated using various network metrics. Table 2 shows the default parameters used in simulation-based experiments.

**Table 2.** List of parameters.

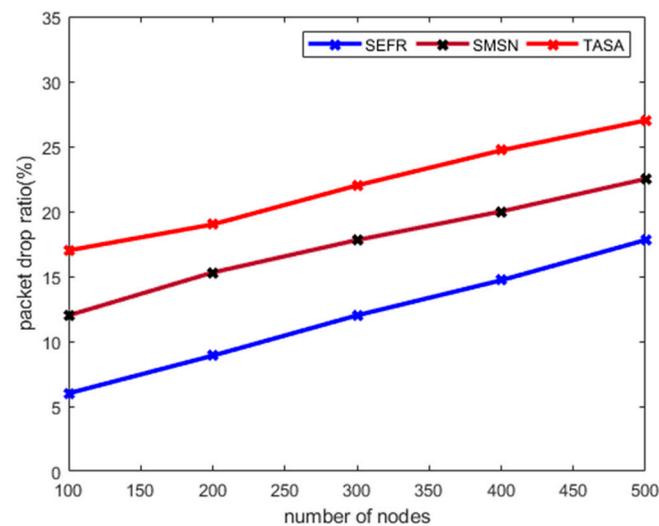
	Parameter	Value
$D_{\max}$		200 $\text{m}^2$
	Sensor nodes	100 to 500
	Malicious nodes	30
$T_r$		15 m
	$\alpha, \beta, \gamma$	0.333, 0.333, 0.333
	Residual energy	$2j$
$R_T$	Fog nodes	10
		32 bps
	Traffic flow	CBR
	Transport layer protocol	UDP
	Antenna type	Omni antenna

Figure 2 depicts the performance of the SEFR protocol against existing work for a varying number of nodes in terms of energy consumption. The experimental results denote that the SEFR protocol outperforms the energy consumption by 15.2% and 20% against SMSN and TASA. Unlike other solutions, the SEFR protocol splits the network communication into different layers, which balances the transmission load among sensors. Also, the cluster heads are selected based on the highest residual energy and the threshold of the dynamic distance increases to appoint a sufficient number of cluster heads to cover the entire environment. Furthermore, the SEFR protocol makes the intelligent process of the selection of next-hop based on QoS factors and it increases the stability of data transmission. Such methods significantly decrease the extra load from the data collectors and avoids frequent route requests and route response messages. Moreover, the energy consumption of the SEFR protocol is improved than existing work due to its least communication overheads in identifying the appropriate neighbors for data transmission. Also, the SEFR protocol has lighter and more reliable routing metrics that counting energy resource, distance, and packet queuing to make the routing performance a lightweight solution, and decreases the chances of depleting unnecessary energy consumption.



**Figure 2.** Energy consumption with a varying number of nodes.

Figure 3 illustrates the performance of the SEFR protocol against SMSN and TASA in terms of packet drop ratio. The experimental results revealed that the SEFR protocol decreases the packet drop ratio by 21%, and 34% under a varying number of nodes. This is because the proposed SEFR protocol selects the most efficient cluster heads in terms of resources and least to long-run routing paths. Also, instead of performing the route discovery in the larger region, the search zone is limited based on the dynamic distance threshold. Unlike the SMSN and TASA, that are more prone to failure in reliable and trusted data routing under a varying number of nodes, the SEFR protocol presents trustworthiness and better lifetime routes for transferring sensors' data through fog computing. Unlike other solutions that frequently drop the sensors' data due to excessive route discovery and control packets, the proposed SEFR protocol avoids forwarding the packets on an obstructed route based on the packet queuing factor.



**Figure 3.** Packet drop ratio with varying number of nodes.

Figure 4 illustrates the performance evaluation of the SEFR protocol against existing work in terms of end-to-end delay. The simulation-based experiments revealed that the SEFR protocol remarkably decreases the outcomes of end-to-end delay by 11%, and 17%. It not only minimizes the transmission distance towards cloud servers but also balances the energy consumption to control the delivery time. The routing nodes are delay tolerant and more robust in terms of network conditions including packet queuing factor. Unlike

SMSN and TASA solutions that increase the data reception time when the network size increases, the SEFR protocol efficiently collaborates the communication from the sensor field to fog nodes and from fog nodes to cloud servers, and such a paradigm minimizes the transmission distance and time intervals for data delivery. Also, the proposed SEFR protocol gives equal significance to routing factors, which results in balancing the load on the nodes, and ultimately it also strengthens the network performance in terms of end-to-end delay.

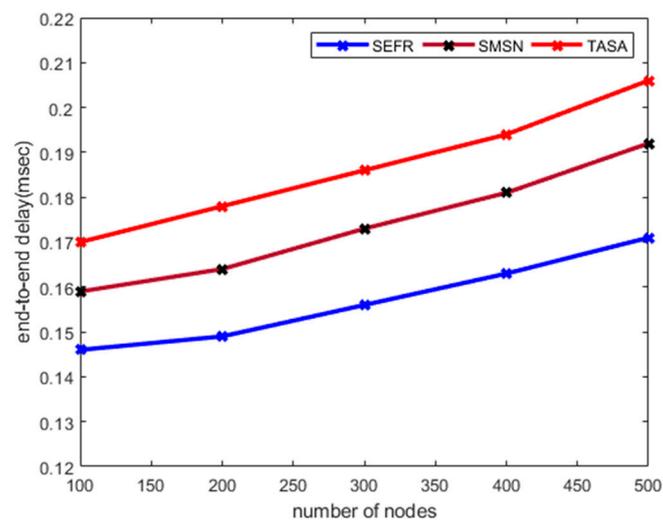


Figure 4. End-to-end delay with varying number of nodes.

Figure 5 demonstrates the performance of the SEFR protocol for network throughput in the comparison of existing work. The results showed that the SEFR protocol increases the ratio of network throughput under a varying number of nodes by 10 and 20%. The improvement is due to the fact that it utilizes multi-facet-based QoS attributes to determine the energy-efficiency and reliable data forwarders. Also, the cluster heads and fog nodes that are more powerful in terms of resources are selected for data routing towards the cloud server. Moreover, compared existing solutions that overlooked the data privacy and authentication during the routing phase, and lead to compromised network performance in terms of security, the SEFR protocol makes use of the Blum Blum Shub algorithm to ensure data confidentiality and avoid malicious nodes being part of the routing process. The basic purpose of using such an algorithm is to impose lower processing and memory overheads on smart sensors. The SEFR protocol efficiently detects the malicious nodes and avoiding network congestion by utilizing the packet queuing factor, which results in maintaining high throughput. Also, the proposed security scheme randomizes the secrets and increases the level of data encryption and decryption. Such secure methods make the data routing more consistent for network throughput and neglect the probabilities of security threats to affect the reception of sensor data.

Figure 6 illustrates the performance of the SEFR protocol against existing work in terms of communication overhead. It is seen from the analysis of the simulation-based results that the SEFR protocol improves the communication overhead by 23%, and 32.5%. This is due to it generating steady clusters based on dynamic distance threshold and only allowing appropriate nodes to participate in the selection process of cluster heads. Also, the transmission load is reduced among sensors due to multi-hop communication instead of a direct link. Unlike SMSN and TASA, which increase the call of route maintenance and data re-routing, the SEFR protocol uses the various QoS-aware factors to choose the long run and more stable routing path that decreases the communication cost in terms of route re-discoveries. Along with other parameters, the SEFR protocol also computes the end-to-end distance while selecting the routing path and decreases the network congestion of the transmission links. Furthermore, it increases the performance of network security

based on lightweight exclusive OR operation. The security keys are generated using the Blum Blum Shum algorithm and securely interchange between the sensor nodes. The proposed security algorithm protects the sensors' data from malicious threats with lower link intrusion and contributes to route maintenance.

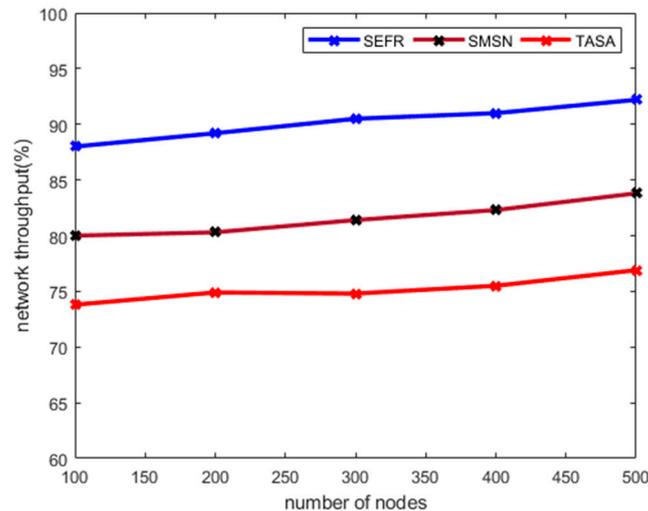


Figure 5. Network throughput with varying number of nodes.

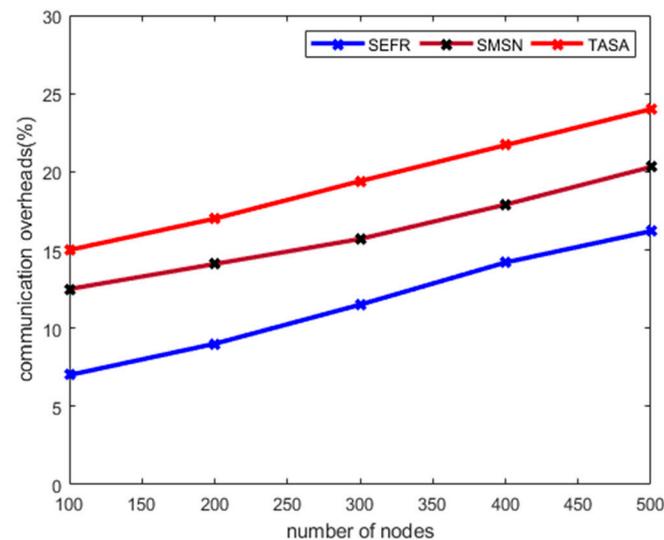


Figure 6. Communication overhead with varying number of nodes.

Figure 7 depicts the measurement of the SEFR protocol compared to other solutions in terms of link load. It is noticed that the experimental results improve the load on wireless links by 20% and 27% as compared to SMSN and TASA. This is due to the fact that SEFR increases the utilization of data links efficiently and maintains a load of transmitted packets in a balanced manner. Also, the multi-facet QoS factors including packet queuing rotate the data forwarders and decrease the number of route request-response messages, which results in efficient load balancing. Also, existing solutions frequently generate bogus route discoveries packets and make the data links more congested. The proposed SEFR protocol makes use of secret numbers using the Blum Blum Shum algorithm and avoids the chances for malicious nodes to integrate the false information in actual data packets. As a result, the proposed SEFR protocol minimizes the unnecessary data traffic on the selected links and makes the communication more flexible and trusted.

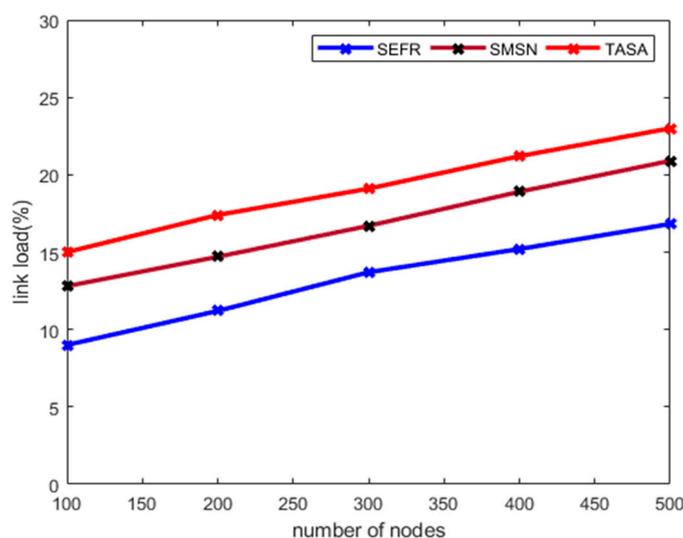


Figure 7. Link load with varying number of nodes.

## 5. Conclusions

In recent decades, IoT sensors and WSN have been merged to provide rapid routing performance for network users. The limited resources on sensor nodes impose significant optimization problems in terms of network lifetime and data security for both academic and industrial domains. This paper presents the lightweight secure and energy-efficient fog-based routing protocol for constraint sensor networks, which uses a dynamic threshold using multiple parameters for the selection of cluster heads with minimum transmission overhead. Moreover, it uses the multi-facet QoS attributes for the selection of next-hop from the observing area to fog layer with minimum energy consumption and delay rate. The SEFR protocol also ensures two levels of security using cryptographic-based secret keys using the Blum Blum Shub algorithm, that increases the trustworthiness. The results of the SEFR protocol demonstrated that it improves the performance of the constraint-oriented network in terms of energy consumption and network throughput. Also, it decreases the chances of packet drop ratio and data latency with nominal communication overheads. In the future, we aim to offer fog computing with intelligent data management based on machine learning techniques to facilitate real-time applications with the least processing cost. Also, the security level has to be investigated in terms of the distributed threats model.

**Author Contributions:** Conceptualization, K.H. and N.I.; Methodology, K.H. and N.I.; Software, K.H.; Validation, Y.J., U.T.; Formal Analysis, K.H.; Investigation, N.I.; Resources, Y.J.; Data Curation, U.T.; Writing—Original Draft Preparation, K.H.; Writing—Review & Editing, U.T.; Visualization, N.I.; Supervision, U.T.; Project Administration, Y.J.; Funding Acquisition, Y.J. All authors have read and agreed to the published version of the manuscript.

**Funding:** The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

**Acknowledgments:** The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

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

## References

1. Yaqoob, I.; Hashem, I.A.T.; Ahmed, A.; Kazmi, S.A.; Hong, C.S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Gener. Comput. Syst.* **2019**, *92*, 265–275. [\[CrossRef\]](#)
2. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Commun. Surv. Tutor.* **2020**. [\[CrossRef\]](#)
3. Haseeb, K.; Islam, N.; Almogren, A.; Din, I.U.; Almajed, H.N.; Guizani, N. Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs. *IEEE Access* **2019**, *7*, 79980–79988. [\[CrossRef\]](#)

4. Rajesh, M.; Gnanasekar, J. Path observation based physical routing protocol for wireless ad hoc networks. *Wirel. Pers. Commun.* **2017**, *97*, 1267–1289. [[CrossRef](#)]
5. Al-Ariki, H.D.E.; Swamy, M.S. A survey and analysis of multipath routing protocols in wireless multimedia sensor networks. *Wirel. Netw.* **2017**, *23*, 1823–1835. [[CrossRef](#)]
6. Sembroiz, D.; Ojaghi, B.; Careglio, D.; Ricciardi, S. A GRASP Meta-Heuristic for Evaluating the Latency and Lifetime Impact of Critical Nodes in Large Wireless Sensor Networks. *Appl. Sci.* **2019**, *9*, 4564. [[CrossRef](#)]
7. Kostrzewski, M.; Varjan, P.; Gnap, J. Solutions Dedicated to Internal Logistics 4.0. In *Sustainable Logistics and Production in Industry 4.0*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 243–262.
8. Haseeb, K.; Islam, N.; Almogren, A.; Din, I.U. Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things. *IEEE Access* **2019**, *7*, 185496–185505. [[CrossRef](#)]
9. Wu, F.; Xu, L.; Kumari, S.; Li, X. A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security. *J. Ambient Intell. Humaniz. Comput.* **2017**, *8*, 101–116. [[CrossRef](#)]
10. Sarwesh, P.; Shet, N.S.V.; Chandrasekaran, K. Energy-efficient network architecture for iot applications. In *Beyond the Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 119–144.
11. Abreu, D.P.; Velasquez, K.; Curado, M.; Monteiro, E. A resilient Internet of Things architecture for smart cities. *Ann. Telecommun.* **2017**, *72*, 19–30. [[CrossRef](#)]
12. Izal Azcárate, M.; Osés, D.M.; Lizarrondo, E.M.; García-Jiménez, S. Computation of traffic time series for large populations of IoT devices. *Sensors* **2019**, *19*, 78. [[CrossRef](#)]
13. Kumar, G.; Saha, R.; Rai, M.K.; Thomas, R.; Kim, T.-H. Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics. *IEEE Internet Things J.* **2019**, *6*, 6835–6842. [[CrossRef](#)]
14. Dizdarević, J.; Carpio, F.; Jukan, A.; Masip-Bruin, X. A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. *ACM Comput. Surv. (CSUR)* **2019**, *51*, 1–29. [[CrossRef](#)]
15. Haseeb, K.; Almogren, A.; Din, I.U.; Islam, N.; Altameem, A. SASC: Secure and Authentication-Based Sensor Cloud Architecture for Intelligent Internet of Things. *Sensors* **2020**, *20*, 2468. [[CrossRef](#)] [[PubMed](#)]
16. Antonio, S. *Cisco Delivers Vision of Fog Computing to Accelerate Value from Billions of Connected Devices*; Cisco: San Francisco, CA, USA, 2014.
17. Hamzah, A.; Shurman, M.; Al-Jarrah, O.; Taqieddin, E. Energy-Efficient Fuzzy-Logic-Based Clustering Technique for Hierarchical Routing Protocols in Wireless Sensor Networks. *Sensors* **2019**, *19*, 561. [[CrossRef](#)]
18. Kharrufa, H.; Al-Kashoash, H.A.; Kemp, A.H. RPL-based routing protocols in IoT applications: A Review. *IEEE Sens. J.* **2019**, *19*, 5952–5967. [[CrossRef](#)]
19. Khalid, M.; Ullah, Z.; Ahmad, N.; Arshad, M.; Jan, B.; Cao, Y.; Adnan, A. A survey of routing issues and associated protocols in underwater wireless sensor networks. *J. Sens.* **2017**, *2017*. [[CrossRef](#)]
20. Kang, S. Energy Optimization in Cluster-Based Routing Protocols for Large-Area Wireless Sensor Networks. *Symmetry* **2019**, *11*, 37. [[CrossRef](#)]
21. Casado-Vara, R.; Vale, Z.; Prieto, J.; Corchado, J. Fault-tolerant temperature control algorithm for IoT networks in smart buildings. *Energies* **2018**, *11*, 3430. [[CrossRef](#)]
22. Hu, S.; Li, G. Fault-tolerant clustering topology evolution mechanism of wireless sensor networks. *IEEE Access* **2018**, *6*, 28085–28096. [[CrossRef](#)]
23. Tripathi, A.; Gupta, H.P.; Dutta, T.; Mishra, R.; Shukla, K.; Jit, S. Coverage and connectivity in WSNs: A survey, research issues and challenges. *IEEE Access* **2018**, *6*, 26971–26992. [[CrossRef](#)]
24. Lehsaini, M.; Guyennet, H.; Feham, M. A novel cluster-based self-organization algorithm for wireless sensor networks. In Proceedings of the 2008 IEEE International Symposium on Collaborative Technologies and Systems, Irvine, CA, USA, 19–23 May 2008.
25. Bilal, M.; Kang, S.-G. An authentication protocol for future sensor networks. *Sensors* **2017**, *17*, 979. [[CrossRef](#)] [[PubMed](#)]
26. Wang, T.; Li, Y.; Wang, G.; Cao, J.; Bhuiyan, M.Z.A.; Jia, W. Sustainable and efficient data collection from WSNs to cloud. *IEEE Trans. Sustain. Comput.* **2017**. [[CrossRef](#)]
27. Wang, T.; Zeng, J.; Lai, Y.; Cai, Y.; Tian, H.; Chen, Y.; Wang, B. Data collection from WSNs to the cloud based on mobile Fog elements. *Future Gener. Comput. Syst.* **2020**, *105*, 864–872. [[CrossRef](#)]
28. Fang, W.; Zhang, W.; Xiao, J.; Yang, Y.; Chen, W. A source anonymity-based lightweight secure AODV protocol for fog-based MANET. *Sensors* **2017**, *17*, 1421. [[CrossRef](#)]
29. Fang, W.; Zhang, W.; Chen, W.; Liu, Y.; Tang, C. TME 2 R: Trust Management-Based Energy Efficient Routing Scheme in Fog-Assisted Industrial Wireless Sensor Network. In *International Conference on 5G for Future Wireless Networks*; Springer: Berlin/Heidelberg, Germany, 2019.
30. Sun, G.; Sun, S.; Sun, J.; Yu, H.; Du, X.; Guizani, M. Security and privacy preservation in fog-based crowd sensing on the internet of vehicles. *J. Netw. Comput. Appl.* **2019**, *134*, 89–99. [[CrossRef](#)]
31. Sun, Z.; Wei, L.; Xu, C.; Wang, T.; Nie, Y.; Xing, X.; Lu, J. An energy-efficient cross-layer-sensing clustering method based on intelligent fog computing in WSNs. *IEEE Access* **2019**, *7*, 144165–144177. [[CrossRef](#)]
32. 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.* **2019**, *26*, 3169–3182. [[CrossRef](#)]

- 
33. Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd IEEE Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2000.
  34. Blum, L.; Blum, M.; Shub, M. A simple unpredictable pseudo-random number generator. *SIAM J. Comput.* **1986**, *15*, 364–383. [[CrossRef](#)]
  35. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [[CrossRef](#)]