energies

MDPI

Article

An Energy-Efficient and Secure Routing Protocol for Intrusion Avoidance in IoT-Based WSN

Khalid Haseeb [1], Ahmad Almogren [2,*], Naveed Islam [1], Ikram Ud Din [3] and Zahoor Jan [1]

[1] Islamia College Peshawar, Peshawar 25000, Pakistan; khalid.haseeb@icp.edu.pk (K.H.); naveed.islam@icp.edu.pk (N.I.); zahoor.jan@icp.edu.pk (Z.J.)
[2] Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[3] Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan; ikramuddin205@yahoo.com
* Correspondence: ahalmogren@ksu.edu.sa; Tel.: +966-1146-96073

Received: 25 September 2019; Accepted: 28 October 2019; Published: 1 November 2019

Abstract: Due to the advancement of information and communication technologies, the use of Internet of Things (IoT) devices has increased exponentially. In the development of IoT, wireless sensor networks (WSNs) perform a vital part and comprises of low-cost smart devices for information gathering. However, such smart devices have constraints in terms of computation, processing, memory and energy resources. Along with such constraints, one of the fundamental challenges for WSN is to achieve reliability with the security of transmitted data in a vulnerable environment against malicious nodes. This paper aims to develop an energy-efficient and secure routing protocol (ESR) for intrusion avoidance in IoT based on WSN to increase the network period and data trustworthiness. Firstly, the proposed protocol creates different energy-efficient clusters based on the intrinsic qualities of nodes. Secondly, based on the (*k*,*n*) threshold-based Shamir secret sharing scheme, the reliability and security of the sensory information among the base station (BS) and cluster head are achieved. The proposed security scheme presents a light-weight solution to cope with intrusions generated by malicious nodes. The experimental results using the network simulator (NS-2) demonstrate that the proposed routing protocol achieved improvement in terms of network lifetime as 37%, average end-to-end delay as 24%, packet delivery ratio as 30%, average communication cost as 29%, network overhead as 28% and the frequency of route re-discoveries as 38% when compared with the existing work under dynamic network topologies.

Keywords: Internet of Things; network lifetime; smart devices; intrusion defence; secure routing

1. Introduction

Internet of Things (IoT) is a worldwide communication infrastructure that consists of different connectivity objects that impart networking, sensory and information processing tools [1–4]. The basic theme of IoT is to provide connectivity anywhere, of anything and anywhere between homogeneous objects. Radio-frequency identification (RFID) [5–7] is an initial technology for IoT that allows electromagnetic fields to transfer the identification data automatically towards the reader via wireless connectivity devices. Radio signal transponder (tag) and tag readers are the two main parts of RFID system. Usually, RFID tags encompass electronically stored information and people can classify, track and monitor the objects. The RFID tags are attached to any object for information gathering and monitoring the target location.

Wireless sensor networks (WSNs) [8–11] is a further foundational technology for IoT, which comprises of smart objects called sensor nodes. These nodes are deployed in an unstructured

manner for information capturing with limited constraints in terms of different resources i.e., energy, computational, memory and processing power. However, due to the complex structure of WSN and restricted constraints on sensor nodes, implementing security for IoT systems is hard to process and communication may compromise with the variety of network attacks [12,13].

Moreover, WSNs based on IoT are used in both attended and unattended environments such as air pollution, water quality monitoring, smart cities, etc., another critical matter is to improve energy efficiency [14,15] besides reliable data forwarding. In the past, different researchers have been presented with a cluster-based solution for WSN to achieve energy efficiency [16–20]. In clustering schemes, the nodes are separated into different regions with one cluster head referred to as the leader node. The aim of the cluster head is to collect the data from member nodes, aggregate them and further forwarded towards the base station (BS). The data transmission from cluster heads to BS may be accomplished either using single hop or multi-hop strategy. Probabilistic and non-probabilistic methods are mainly two kinds of clustering solutions. In probabilistic [21–25], clusters are generated in randomly order, which results in unbalanced load distribution and energy consumption. On the other hand, the non-probabilistic method [26–29] uses multiple factors for the selection of cluster heads. Although, the non-probabilistic methods give an improved performance as compared to traditional probabilistic methods, however, because of dynamic nature of sensor nodes [30–34], improving energy conservation and routing robustness are still open challenges for IoT based on WSN.

This research paper focuses on developing an energy-efficient and secure routing protocol to achieve reliable network communication against malicious threats. As compared to existing energy efficient IoT based WSN systems, our proposed energy-efficient and secure routing protocol (ESR) protocol differs in two major aspects. Firstly, the ESR protocol makes use of the inherent abilities of nodes and generates various energy efficient clusters by considering the quality of service (QoS) requirements. Further, ESR protocol exploits a practice of bounded clustering to update the status of cluster heads with minimum communication cost, as least number of re-election packets are flooded inside each cluster. Secondly, to achieve trustworthiness and secure network-wide data routing, ESR protocol adopts a light-weight secret sharing scheme between cluster heads and BS. In this scheme, the BS generates a secret key, which is partitioned and shared among the set of cluster heads. During the transmission between cluster heads and BS, based on the proposed secret sharing scheme the incoming packets are encrypted. Similarly, on the arrival of the packets from cluster heads towards the BS, decryption is performed before further transmission to the end user based on the proposed data security scheme.

The proposed scheme is computationally secure, extensible with respect to the increase in the network field and dynamic in terms of changing the keys. Based on the aforementioned contributions, the ESR protocol is appropriate for a large scale IoT based WSN systems that need energy-awareness, trustworthiness and fault-tolerability.

The remainder of the research paper is as given. The related work and detailed for the research formulation are discussed in Section 2. The introduction of ESR protocol along its design, functionality and algorithms are discussed in Section 3. The sensitivity analysis of weighted factors for optimizing the ESR protocol is addressed in Section 4. The simulation model and numerical results of ESP protocol against related work are illustrated in Section 5 followed by Section 6, which concludes this article.

2. Related Work and Research Formulation

In most of the large scale networks such as IoT and restricted constraint of sensor nodes, the energy conservation goal is a demanding parameter. Normally, in cluster-based networks [17,19,35,36], cluster heads are considered as a controlling entity, which performs a symbolic role during data gathering and transmission. Being a focal point for all activities within a cluster, due to abundant network traffic they are exposed to quick energy consumption. Therefore, the selection of optimal cluster heads has a symbolic effect on the network performance especially with respect to network stability and homogeneity. Moreover, in large scale IoT based WSNs, secure data routing is another crucial part due

to constraint resources. Most of the existing schemes [37–40] have unreliable and insecure network communication due to the absence of protection mechanisms against malicious threats.

The first proposed cluster based routing protocol, low energy adaptive clustering hierarchy (LEACH) [21] comprises different stages and the individual stage partition into two sub phases. In the setup phase, clusters are generated whereas data transmission occurs in a steady phase. In addition, cluster head selection is done periodically, every node in the network field produces a number based on random strategy and if the generated number is smaller than the preset threshold, the role of the cluster head is assigned to the node. Although, LEACH is distributed protocol, however, it might happen that nodes with lower energy levels to be selected as cluster heads. In addition, over the sensor field, cluster heads are not evenly distributed, which causes additional energy dissipation.

In [41], the authors improved the performance of the LEACH protocol by incorporating multi-hop criteria for data transmission. However, initially, the clusters are generated randomly, which leads to unbalanced energy consumption. Further, constructed multi-hop paths are non-optimized thereby results in routing holes and route breakages. In addition, chain–chain based routing protocol (CCBRP) [42] aims to improve energy conservation of sensor nodes in data forwarding. CCBRP integrates the functions of LEACH and Power Efficient Gathering in Sensor Information Systems (PEGASIS) by arranging the entire nodes into different chains. CCBRP offers a hybrid scheme and executes the constructed chains in two different stages. The main problem of this protocol is high energy consumption and latency rate with the increase in network size. Consequently, due to restricted scalability, CCBRP is inappropriately suitable for huge scale networks.

Authors [43] proposed load balancing and the data collection algorithm aims for saving energy consumption and improved the performance of network with respect to data aggregation and forwarding. The proposed algorithm generates a set of layers based on hop counts among nodes and sinks node. However, the selection procedure of next-hop works in the hop by hop manner, which results in increasing communication costs. Moreover, an increase in network size leads to a higher number of route discoveries and additional transmission delays. Furthermore, robust and energy efficient authentication protocol for industrial IoT [44] presented three-factor authentication and provides data security for WSN. The proposed solution offers proper mutual authentication between nodes, however, unnecessary energy is consumed during the authentication process and compromised network lifetime. Similarly, the Shamir secret sharing scheme [45] has been exploited in [46,47], and aims to provide data security over the network field. The schemes are composed of two main phases i.e., share generation and share re-construction. A generated secret key is partitioned between set of nodes by using (t, n) threshold-based, where a subset of any nodes is sufficient for reconstructing the secret key. However, the proposed solutions exchange a lot of messages in the network field that dissipate additional energy and lead to routing overhead.

In the energy efficient balanced cluster-based data aggregation (EEBCDA) algorithm [48], the network field is structured into unequal sized rectangular grids with one cluster head. The cluster head's position is shifted among member nodes within each grid. By exploiting the information of residual energy, the set of few nodes are selected as cluster heads within each grid. However, the operation of generating a grid is more complex and required more overheads. Furthermore, the remaining structure of EEBCDA is comparable to LEACH. Moreover, reliable and energy-efficient data collection for large scale WSNs [49] aims to improve the energy resource of nodes with consistent routing. In the hotspot region, a fewer number of nodes are selected for capturing information while more monitor nodes are selected in a non-hotspot region. Moreover, based on converging the multi-path route for event monitoring nodes, the aggregated data packets are sent towards the sink node. However, data security is overlooked in the proposed solution and networks may compromise information disclosure in a harsh and complex environment.

In LEACH-ensuring reliable data delivery (LEACH-ER) [50], by exploiting energy and data reliability factor the selection process for the cluster head, is initiated. The main idea behind LEACH-ER was to reduce the rate of packets reception inside a cluster among cluster heads and

member nodes, which results in improving network lifetime and energy efficiency. However, routes are non-optimized, which causes retransmission and route breakages. Energy efficient in [51], a multi-hop communication routing (MCR) protocol is proposed and aims to improve network lifetime and load balancing. In MCR, based on weighted metrics, the cluster head election is made. Furthermore, multi-hop criteria adopted for data forwarding forwards BS. However, the constructed routings are not optimum and within the cluster, the data transmissions occur based on single-hop.

3. Proposed Intrusion Avoidance Protocol

This section summarizes the proposed energy-efficient and secure routing (ESR) protocol for IoT based WSN. The basic structure of a cluster based network is illustrated in Figure 1. The proposed ESR protocol divides the overall its functionality into two main components that are discussed in the next sections. In the first component, ESR protocol organizes optimum hierarchical topology construction and the thresholding based secret sharing scheme (SSS) [45] for secure data routing. Based on multiple criteria along with QoS constraints, the optimized cluster heads are determined in association to the distributed clusters in energy efficient and balanced manner. Furthermore, the proposed clustering scheme improves network lifetime with low overhead and power consumption ratio between the sensor nodes. In the second component, the secure and trustworthy routing path is constructed between cluster heads and BS to avoid any intrusions caused by malicious nodes. To achieve reliable data forwarding, the BS generates a secret key, which is shared among selected cluster heads. In data forwarding from cluster heads, the data packets are encrypted using the SSS mechanism. On the other hand, BS reconstructs the inbound data packets from cluster heads using the proposed secret sharing scheme. Furthermore, the relative impact of each factor in an optimized selection process of the cluster head is evaluated based on a sensitivity analysis, which is a mathematical model that provides an understanding of the affiliation among input and output values in development. Simulation results of ESR outperform other relevant schemes with respect to packet delivery ratio, network lifetime, end-to-end delay, communication cost, number of route discoveries and network overhead. Figure 2 illustrates the block diagram of the ESR protocol.

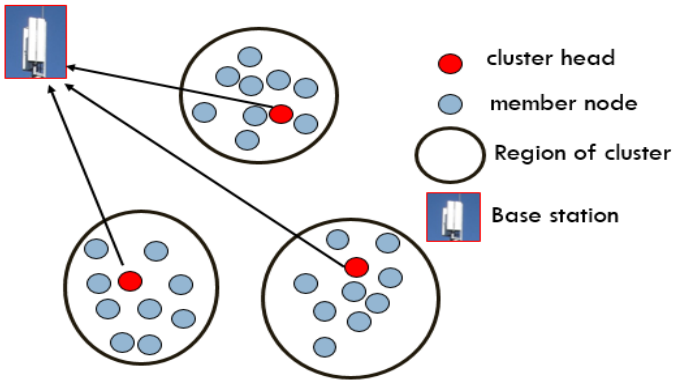

Figure 1. Structure of the cluster based network.

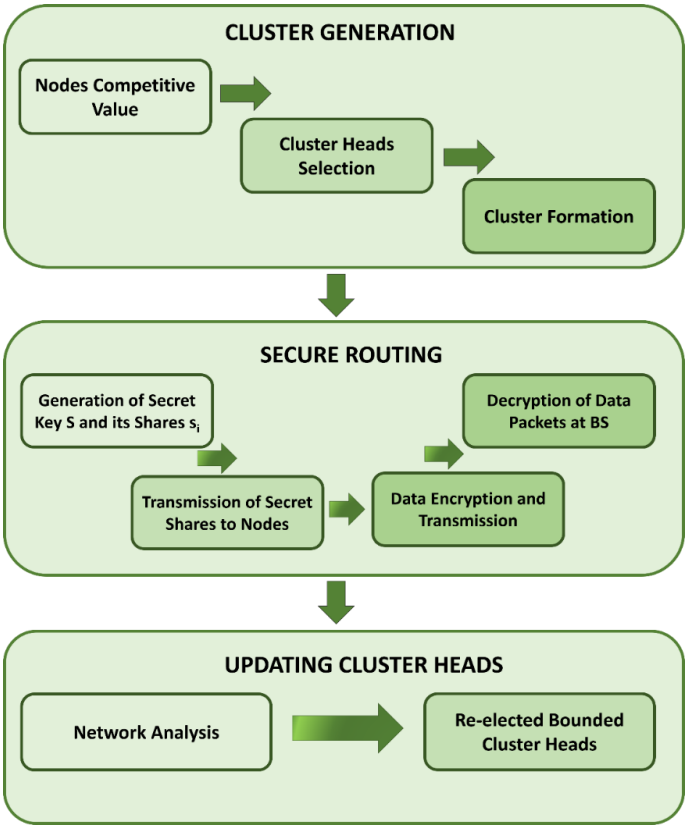

Figure 2. Block diagram of the energy-efficient and secure routing protocol (ESR) protocol.

3.1. Optimize Clusters

The number of nodes is dispersed randomly in a square sized network field at the beginning of initialization phase. Each node remains static and has a unique ID with limited constraints. The BS has no restriction in terms of innumerable resources. In the beginning, BS broadcasts its locality in hop-by-hop manner over the monitoring field and all the nodes received it. Furthermore, the routing table of each node is updated by incorporating the neighbor's information. Afterwards, ESR protocol announces the cluster head selection mechanism in the network field in a scattered manner. By using residual energy e_i, the Received Signal Strength Indicator ($RSSI_i$), proximity from BS $d_{i\ to\ BS}$ and queue length QLi_i factors, the competitive value C_v is computed for all the nodes. Each node receives its neighbor's information through the exchange of control messages. Firstly, node energy is the most contributing factor in the survival of the network thus maximum residual energy of a node is given more significance. Secondly, the uses of RSSI measure the performance of the wireless link that offers a good packet reception rate if the RSSI value is more than a certain threshold. ESR protocol computes the RSSI threshold, which is the average reception rate of beacon packets from N neighbors at a certain time period (Δt) as given in Equation (1). The node's RSSI value must be greater than the computed threshold. If the RSSI value is less than the threshold, it indicates low link quality, which results in a rise in the probability of packets lose ratio. Let X denote the reception rate of beacon packets, then the following equation is used to compute the value of the RSSI threshold.

$$RSSI_{threshold} = \frac{X}{N} \tag{1}$$

Thirdly, the shortest path of node towards BS minimizes energy consumption and longer the network lifetime. In the end, the factor of queue length QLi_i improves data delivery performance and measures the congestion level at the node level. RR_i is the reception of packets in bytes at node i,

and TB is the total buffer size in bytes, then the queue length QL_i of a node i can be computed using Equation (2).

$$QL_i = \frac{RR_i}{TB} \tag{2}$$

Finally, all the factors are summarized based on weighted means as shown in Equation (3), and the nodes are appointed as initial cluster heads based on the highest competitive value C_v Accordingly, proposed ESR protocol selects an optimize cluster heads based intrinsic qualities and generated clusters are more adaptable. The computed value of C_v is normalized in the series of [0,1].

$$C_{\mathrm{v}} = \mathrm{w1} \times e_i + \mathrm{w2} \times RSSI_i + \mathrm{w3} \times \left(\frac{1}{d_{i\ to\ BS}}\right) + \mathrm{w4} \times QL_i \tag{3}$$

In Equation (3), weighting factors are denoted by w1, w2, w3 and w4 for different selection aspects, namely the node's residual energy, RSSI, proximity from BS and queue length. During the selection process, all the weighting factors signify the particular impact in computing the competitive value of nodes, whereas w1 + w2 + w3 + w4 = 1. The sensitivity analysis of the weighting factors is discussed in Section 4. The evaluated competitive value is in the series of [0,1] as all the residual energy, RSSI, proximity from BS and queue length have values in the same range. Firstly, the residual energy metric makes the cluster selection mechanism more adaptive. Furthermore, the RSSI facet is unified in the selection mechanism of the cluster head, which shows the performance of the wireless link. Moreover, based on the smallest distance from BS, an appropriate node is considered for the selection of the cluster head. Each node transmits beacon packets to its neighbors at an interval of the fixed period. On receiving beacons packets, the neighbor node evaluates its RSSI value and sends back towards the source node. In the end, the queue length factor is incorporated in the selection mechanism of cluster head, thus a node is given higher priority to be elected as a cluster head if its transit queue length is higher than a certain threshold. After the selection of primary cluster heads, they advertised their status in a precise manner. All the normal nodes join their adjacent cluster head for the formation of clusters, upon receiving the status messages. Normal nodes might receive status messages from more than one adjacent cluster heads and associate themselves with those cluster heads, having the strongest RSSI value. At the end of the clusters formation process, ESR protocol assigns a unique ID for all generated clusters in order to specify their boundaries. The set of nodes selected as cluster heads announce channel access schedules based on time-division multiple access (TDMA).

3.2. (t, n) Thresholding Based Secret Sharing Scheme (SSS) for Secure Data Routing Against Intrusions of Malicious Nodes

In the proposed approach, the BS generates a secret key S, which is to be partitioned among a set of n cluster head using (t, n) threshold-based Shamir's secret sharing scheme where any t subset of cluster heads are enough to reconstruct the secret key S. It must be noted that for Shamir's secrete sharing scheme, the following two conditions must be satisfied:

i. Any combination of t or higher number of subkeys $(S_0,\ S_1, \ldots, S_{t-1})$ can reconstruct the secret key S.
ii. Less than t or fewer number of subkeys can not reconstruct the secret key S.

In SSS, for construction of t subkeys, a $t-1$ degree polynomial is constructed. For creating a (t, n) threshold scheme, $t-1$ random numbers $(b_1,\ b_2, \ldots, b_{t-1})$ greater than zero are selected. If $b_0 = S$, the numbers $(b_1,\ b_2, \ldots, b_{t-1})$ are coefficients of the polynomial as given in Equation (4).

$$f(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 +, \ldots,\ b_t x^{t-1} \tag{4}$$

The reconstruction of the secret keys S requires computing the Lagrange basis polynomial given in Equation (5).

$$l_j(x) = \prod_{\substack{0 \le m \le t \\ m \ne j}} \frac{x - x_m}{x_j - x_m} \tag{5}$$

After computing $t - 1$ Lagrange values, these are put in Equation (6) for the computation of secret key S.

$$f(x) = \sum_{j=0}^{t-1} y_j l_j(x) \tag{6}$$

Each share of the key S_i is diffused towards the cluster heads, which is flooded towards an individual node in the particular cluster. When the node forwards the sensory data D_i towards the cluster head, it is encrypted by applying the Exclusive OR (XOR) operation with the key S_i as given in Equation (7).

$$E_i = S_i \oplus D_i \tag{7}$$

After receiving the encrypted data E_i from the member nodes, the cluster head transmits it to the BS for further processing. Similarly, on the arrival of encrypted data, the BS decrypts the data using the decryption key S and transmits it to the end user.

3.3. Updating of Cluster Heads

As WSNs have restricted resources, thus ESR protocol re-formulate the role of cluster heads in a dynamic manner. The main aim behind updating of cluster heads component is to achieve uniform load balancing and energy consumption. ESR protocol observes the subsequent to evaluate the network measure.

i. When any cluster head j receives the data packet then firstly it verifies whether it already received the same data packet or not. If yes, then cluster heads simply drop the duplicate data packet to reduce network congestion and energy consumption.

ii. It might be a case that the cluster head receives a new data packet, but it has no enough energy resource, i.e., $e_j < threshold$, then it quits from data forwarding and initiates re-election mechanism inside a particular cluster boundary. Furthermore, the ESR protocol also computes the congestion rate C_r of each cluster based on the function, which signifies the normalized congestion value in the range of [0,1] as shown in Equation (8).

$$C_r = \frac{ADR}{ARR} \tag{8}$$

where ADR represents the average delay ratio among data packets and ARR represents the average reception rate of data packets.

ESR protocol continuously checks the C_r value, and if it does not fall in the range of [0,1], ESR protocol assumes that a particular cluster head has extended to congestion limit and needs to initiates the re-election process as described in Section 3.1.

In Algorithm 1, all the main modules of the proposed ESR protocol are lightened.

Algorithm 1: Energy-efficient and secure routing protocol

Optimized clusters

Procedure clusters generation (K)
  Evalutes next-hop and generate local table
  for each nodes $i \in [1 : n]$
    do
      $C_{\mathrm{v}} = \mathrm{w1} * e_i + \mathrm{w2} * RSSI_i + \mathrm{w3} * \left(\frac{1}{d_{i\ to\ BS}}\right) + \mathrm{w4} * QL_i$
  end for
  if C_v [ ]! = Null
    set the highest C_{v} node as a primary cluster head
  for each node $i \in$ *clusterhead* (i)
    do
      normal_node responsed to $clusterhead_i$
  end for
    $clusterhead_i$ generates clusters and announces channel access schedules based on TDMA
  end procedure

Secure Data Routing

procedure secure-routing
BS generates secret key S
The secret key S is partitioned into a set of t cluster heads
Share of key S_i transmits to the set of t cluster heads
Node n_i transmits the data D_i to the cluster head
Data is encrypted using XOR operation with the key S_i: $E_i = S_i \oplus D_i$
BS decrypt the received data packets from a set of t cluster heads using the decryption key S
end procedure

Updating cluster heads

procedure updating of cluster head
  for each *node* ∈ *clusterheadi*
    do
      if $n_i.energy <$ threshold OR
        $C_r = \frac{ADR}{ARR}$
        then
          compute C_{v} *value* re-elect new cluster head$_{\mathrm{j}}$
          update TDMA channel access scheme
        end if
  end for
  end procedure

4. The Sensitivity Analysis

This section performs the sensitivity analysis of weighting factors for the selection process of cluster heads in dynamic network topology. By using weighting factors w1, w2, w3 and w4, Equation (1) optimizes the process of cluster heads selection that incorporates the values of residual energy, RSSI, proximity from BS and the queue length factor. All the factors are integrated in a weighted manner and used to conclude the measurement of the impact for each factor in the respective evaluation. The summation of the fractions of effects for all the weighted factors represents must be equal to 100%

i.e., w1 + w2 + w3 + w4 = 1. Actually, there are no optimum values for weighting factors; therefore, sensitivity analysis is accomplished to conclude the most suitable values for making any decision. To perform sensitivity analysis, 100 sensor nodes are deployed randomly in a square sized network field. Furthermore, during experiments all the nodes maintain their positions, i.e., non-mobile. The nodes are homogeneous with a initial energy level is set to 5 J. Furthermore, the transmission power for all the nodes is fixed to 20 m. To evaluate sensitivity analysis under dynamic topology, varied number of nodes are selected as cluster heads. The range for selected cluster heads is varying from 2 to 10.

To evaluate the optimized performance for cluster head selection, four different values of weighted factors are used, where configuration-1 corresponds to w1 = 0.5, w2 = 0.3, w3 = 0.1 and w4 = 0.1, configuration-2 denotes w1 = 0.1, w2 = 0.5, w3 = 0.3 and w4 = 0.1, configuration-3 represents w1 = 0.3, w2 = 0.1, w3 = 0.5 and w4 = 0.1, configuration-4 shows w1 = 0.2, w2 = 0.1, w3 = 0.1 and w4 = 0.6. All configurations are measured with respect to energy consumption, route breakages, transmission distance, and packet delivery performance as a benchmark to accomplish the optimum values for w1, w2, w3 and w4. In addition, the graphical representation using error bars is also used to indicate the error or uncertainty in the experimental results.

In Figure 3, configuration-1 gives better results as an average of 31% in the comparison of configuration-2, configuration-3 and configuration-4 in terms of energy consumption. The computation of energy consumption depends on the average ratio of power consumption between sensor nodes in send/receive cluster head election packets. Figure 4 illustrates the effects of route breakages for all considered configurations, and configuration-2 outperforms the results as an average of 38% than configuration-1, configuration-3 and configuration-4. Figure 5 shows the transmission distance for each of the evaluated configurations. Accordingly, configuration-3 results in better performance as an average of 36% than configuration-1, configuration-2 and configuration-4. In the end, Figure 6 illustrates that configuration-4 in terms of packet delivery ratio gives better outcomes as an average of 37% than other configurations.

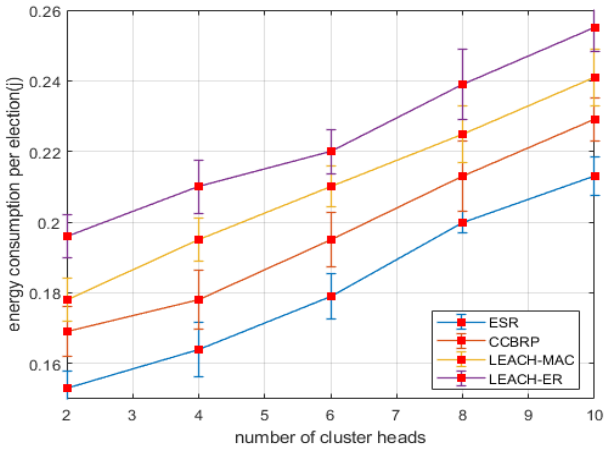

Figure 3. Energy consumption per selection with various numbers of cluster heads under different weighting factors.

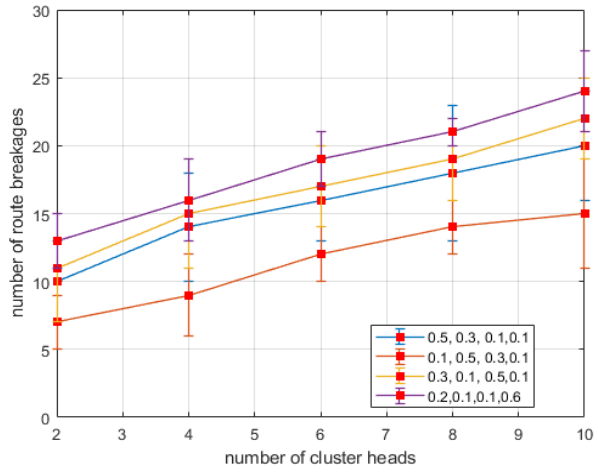

Figure 4. Route breakages with various numbers of cluster heads under different weighting factors.

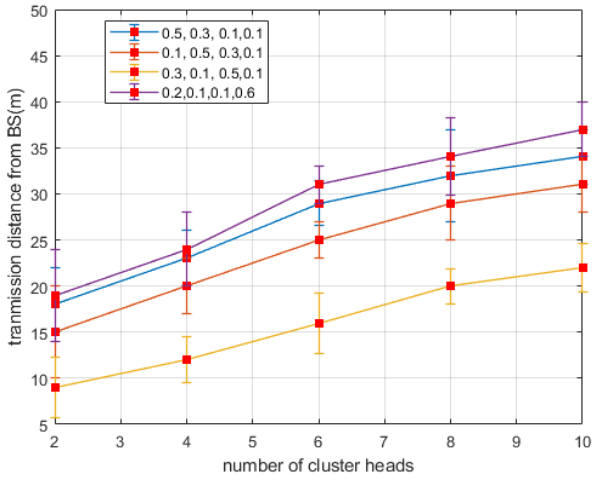

Figure 5. Transmission distance various numbers of cluster heads under different weighting factors.

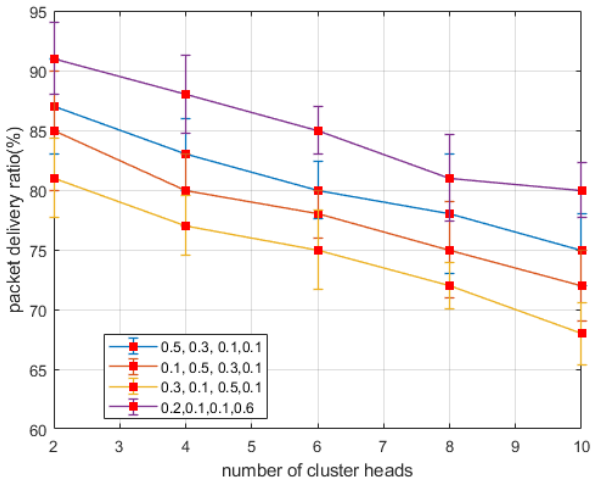

Figure 6. Packet delivery ratio various numbers of cluster heads under different weighting factors.

Based on the performed sensitivity analysis in Figure 3 to Figure 6, the experimental results illustrated that each weighted factor has a significant impact on the selection of cluster head under various IoT based WSN topologies. Thus, to expose the balanced contribution and optimizes the cluster head election process, the weighted factors are set to uniform values.

5. Network Model and Discussion

In this research work, the implementation and evaluation phases were carried out in NS2 as a network simulator [52] along with the mannasim framework [53]. A varying number of nodes are distributed in random order with 10 malicious nodes. The malicious nodes broadcast false route reaction packets in order to be selected as next-hop for data forwarding. We considered a squared size sensor field by keeping a fixed number of nodes. Initially, nodes have 5 J of energy level and homogeneous in terms of various resources. Further, the transmission range was set to 20 m for each node. A constant bit rate (CBR) connection was established between sending and receiving nodes. To evaluate the energy consumption over the sensor field, the energy model [21] was used in this research work. The energy model evaluated the energy consumption (E_t and E_r) related to data transmission and receiving by using Equations (9) and (10). In this research study, Table 1 gives the default simulation parameters, where the units of m is meter, s is second, J is joule and nJ is nana joule.

$$E_t = \begin{cases} \left(E_{elect} + d^2 \times E_{amp1}\right) \times k, & d \leq d_t \\ \left(E_{elect} + d^4 \times E_{amp2}\right) \times k, & d > d_t \end{cases}, \tag{9}$$

$$E_r = E_{elect} \times k, \tag{10}$$

where:

k shows the number of data bits;
d is the transmission distance;
E_{elect} is the amount of consumed energy in data transmission;
d_t is the distance threshold value.

Table 1. Parameters.

Parameter	Value
Network field	100×100 m^2
E_{elect}	100 nJ/ bit
E_{amp}	10 nJ/bit/m^2
E_{fs}	0.0013 pJ/bit/m^4
Packet size, k	50 bits
Payload size	512 bytes
Initial energy	5 J
Simulation time	2000 s
Node's transmission range	20 m
Beacons interval	1 s

5.1. Numerical Results of ESR Protocol

In this section, we evaluated the numerical results of ESR protocol in the comparison of LEACH-ER, LEACH-MAC and CCBRP. The numerical results of ESR protocol were measured with other solutions under different network topologies. The network topologies were varied based on a different number of nodes from 100 to 500. To establish the dynamic network topologies, all the nodes were distributed randomly over the sensor field. The comparison among protocols was performed with respect to network lifetime, average end-to-end delay, packet delivery ratio, average communication cost, network overhead and the frequency of route re-discoveries parameters. Moreover, error bars based on varying standard deviations were used to indicate error or uncertainty in the measurement of experimental results.

5.2. Network Lifetime

For varying node density topologies, Figure 7 proves the performance of the ESR protocol with respect to the network lifetime as compared to existing work. It is observed in Figure 6 that ESR had a

prolonged network lifetime, especially in high network load, as an average of 37% enhancement was accomplished in the comparison of other solutions. This is due to optimizing the clusters formation process and initiating the re-election mechanism on the network analysis. In addition, ESR protocol used local clustering functionality that decreased overheads and unnecessary energy consumption in the re-clustering phase. Further, the ESR gave a light-weight secure routing mechanism to route the encrypted sensory information towards BS.

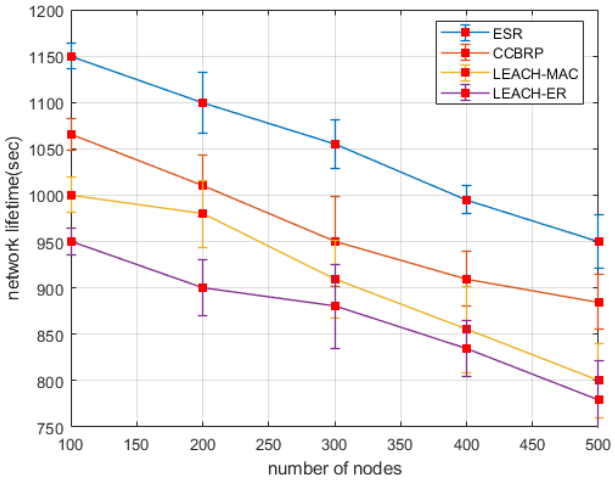

Figure 7. Network lifetime in varying node density topologies.

5.3. Packet Delivery Ratio

Figure 8 demonstrates the performance measurement in terms of packet delivery ratio for ESR protocol against the existing work under varying nodes density topologies. In Figure 8, ESR has shown the highest data delivery ratio as an average of 30% improvement than existing solutions, especially in high nodes density topologies. This is due to the fact that ESR protocol considering multiple and optimal criteria for the selection of cluster head, and more priority was given to the more suitable nodes for generating stable and energy efficient clusters. In addition, after the formation of clusters, they remained fixed and ESR re-initiated inbound process for the selection of cluster heads. Moreover, the reliability of the data packets that were communicated between the base station (BS) and cluster head was achieved using the (k, n) threshold-based Shamir secret sharing scheme, which results in reducing route breakages and ultimately increased data delivery performance.

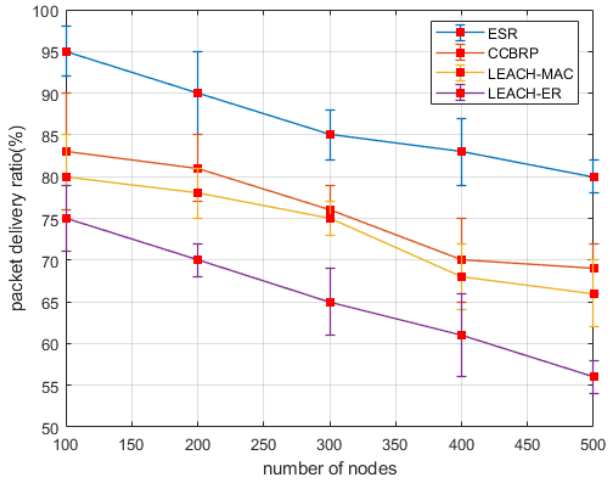

Figure 8. Packet delivery ratio in varying nodes density topologies.

5.4. Average End-to-End Delay

Under varying nodes density topologies in Figure 9, the performance of ESR protocol was evaluated against other solutions with respect to average end-to-end delay. In fact, due to high data traffic, congestion and an increasing number of malicious nodes, the value of end-to-end delay also increased. However, it was seen that the proposed ESR protocol had a lower end-to-end delay in the comparison of other solutions, particularly in large sized and high network load. The numerical results illustrated that ESR protocol achieved a 24% average decrease of end-to-end delay in the comparison of other solutions. Actually, the proposed ESR protocol formed the clusters in an adaptive manner and updates the status of cluster heads within a particular boundary of a cluster. In addition, ESR protocol gave more consistent and robust data forwarding nodes based on a link quality RSSI values that led to routing performance. Unlike other existing solutions, ESR protocol performed the measurement of network analysis to revolve the position of cluster heads in the sensor field, which reduced the chances of routing hole and minimized the data latency ratio.

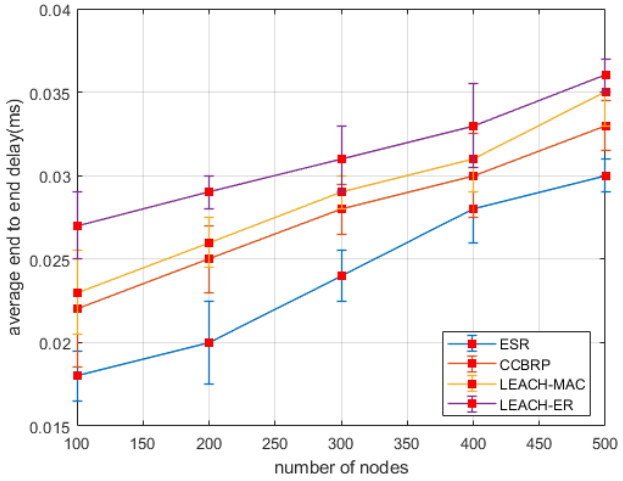

Figure 9. End-to-end delay in varying nodes density topologies.

5.5. Average Communication Cost

Figure 10 illustrates the comparison of ESR protocol with other protocols in terms of average communication cost under varying nodes density topologies and in the presence of malicious nodes. Remarkably, with a varied number of nodes and malicious nodes, a network led to traffic jamming and network disconnections, which resulted in increases in communication cost and transmission interruption. However, based on Figure 9, it is seen that ESR protocol reduced the communication cost in the comparison of other schemes especially when network load increased. ESR protocol had achieved an average of 29% reduction in communication cost under varying nodes topologies. This was due to making use of neighbor's information, and in the selection process of cluster heads only a limited number of nodes contributed. Moreover, the re-election for cluster heads was re-called based on the demand and network analysis. Furthermore, support of data security and reliability, ESR protocol decreased the number of route re-transmissions, which resulted in shortening the communication cost.

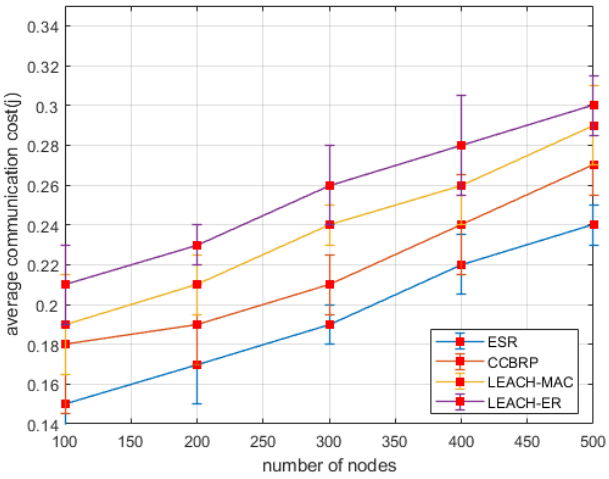

Figure 10. Communication cost in varying nodes density topologies.

5.6. Network Overhead

In Figure 11, the comparison of ESR protocol is illustrated against the existing solution under varying nodes density topologies. The numerical results demonstrated that ESR protocol had attained an average of 28% reduction in network overhead than the existing solutions because ESR protocol provided a light-weight secret sharing scheme between cluster heads and BS, which was not only computationally secure to handle the intrusions against malicious nodes but also extensible in terms of varying network topologies. In addition, trustworthy routing paths led to a fewer number of route re-construction messages in the sensor field and thus reduced network overhead. Furthermore, the wireless channels were less congested, as ESR protocol minimized re-election packets because of bounded clustering.

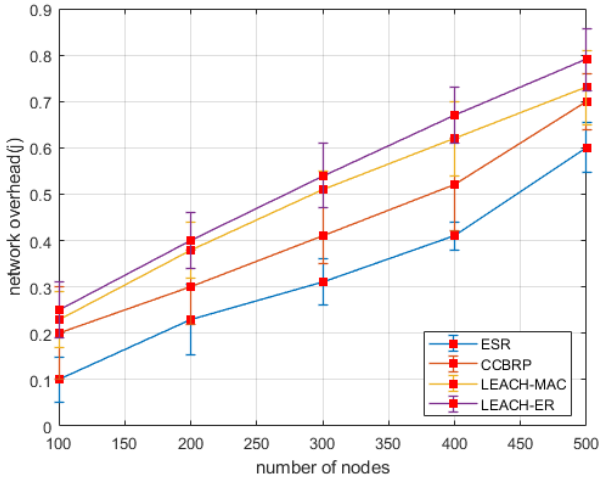

Figure 11. Network overhead under varying nodes density topologies.

5.7. Ratio of Route Re-Discoveries Packets

Figure 12 illustrates the comparison of ESR protocol with other protocols in terms of a ratio of route re-discoveries under different nodes density topologies. It is observed that in the presence of malicious nodes, a network incurred a high number of packets for route discoveries and re-transmissionnns. Nevertheless, based on Figure 12, it is seen that ESR protocol decreased the packets of route re-discoveries in the evaluation of other solutions specifically when the network size increased. ESR protocol had attained an average of 38% reduction in the number of packets for route re-discoveries under the scenario of different nodes density topologies. The reason behind this was that ESR measured the

network congestion over the elected cluster heads and based on network conditions ESR updated the routing flags of cluster heads. Accordingly, ESR protocol re-adjusted the routing paths from normal nodes to their associated cluster head by flooding the route discoveries packets within a precise region rather than the entire network field.

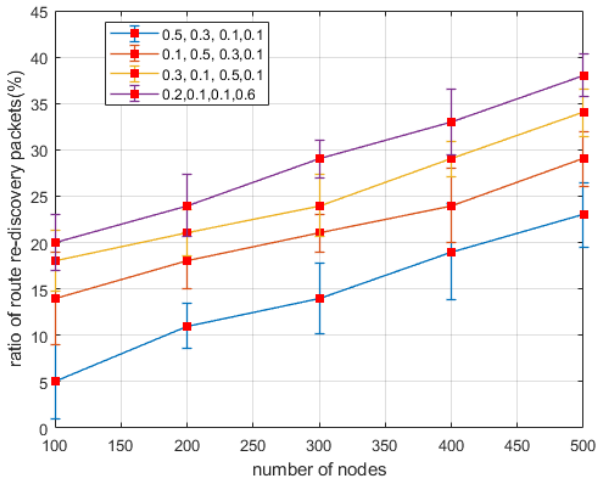

Figure 12. Ratio of route re-discovery packets under varying nodes density topologies.

6. Conclusions

The aim of this paper was to present the energy-efficient and secure routing (ESR) protocol for intrusion defense in IoT based on wireless sensor networks. In the existing solution, most of them used a greedy algorithm for the construction of the routing path, overlooked intrusions in an infrastructure-less and unattended environment. This results in a high number of route discoveries and re-transmissions, particularly under the number of malicious nodes and high network load scenario. Basically, ESR optimized the selection process of cluster heads and used a distributed stretegy to generate clusters for uniform distribution of energy consumption. Furthermore, by considering higher values of RSSI and least network congestion improved the routing performance with respect to QoS constraints and data reliability. Moreover, to achieve a secure network-wide data routing against malicious nodes, ESR protocol adopted a light-weight secret sharing scheme between cluster heads and BS. This provided data security from nodes towards the cluster heads and further to the BS against malicious threats. For future work, the proposed protocol will be extended by considering multi-hop network communication along with the mobility standards.

Author Contributions: Conceptualization, K.H. and N.I.; methodology, I.U.D.; validation, A.A. and Z.J.; writing—original draft preparation, K.H.; writing—review and editing, I.U.D.; visualization, N.I. and Z.J.; supervision, A.A.; funding acquisition, A.A.

Funding: The authors are grateful to the Deanship of Scientific Research, king Saud University for funding through Vice Deanship of Scientific Research Chairs.

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

References

1. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
2. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. Security of the internet of things: Perspectives and challenges. *Wirel. Netw.* **2014**, *20*, 2481–2501. [CrossRef]
3. Uckelmann, D.; Harrison, M.; Michahelles, F. An architectural approach towards the future internet of things. In *Architecting the Internet of Things*; Springer: Heidelberg, Germany, 2011; pp. 1–24.
4. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [CrossRef]

5. Downie, J.D.; Nederlof, L.; Sutherland, J.S.; Wagner, R.E.; Webb, D.A.; Whiting, M.S. Radio Frequency Identification (RFID) Connected Tag Communications Protocol and Related Systems and Methods. U.S. Patent No. 9,652,707, 16 May 2017.
6. Koch, M.J.; Swope, C.B.; Bekritsky, B.J. System for, and Method of, Accurately and Rapidly Determining, in Real-Time, True Bearings of Radio Frequency Identification (RFID) Tags Associated with Items in a Controlled area. U.S. Patent 9,773,136, 26 September 2017.
7. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516. [CrossRef]
8. Hezaveh, M.; Shirmohammdi, Z.; Rohbani, N.; Miremadi, S.G. A fault-tolerant and energy-aware mechanism for cluster-based routing algorithm of WSNs. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, Canada, 11–15 May 2015; pp. 659–664.
9. Mahajan, S.; Malhotra, J.; Sharma, S. An energy balanced QoS based cluster head selection strategy for WSN. *Egypt. Inf. J.* **2014**, *15*, 189–199. [CrossRef]
10. Mehrani, M.; Shanbehzadeh, J.; Sarrafzadeh, A.; Mirabedini, S.J.; Manford, C. FEED: Fault tolerant, energy efficient, distributed clustering for WSN. In Proceedings of the 2010 The 12th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea, 7–10 February 2010; pp. 580–585.
11. Tarigh, H.D.; Sabaei, M. A new clustering method to prolong the lifetime of WSN. In Proceedings of the 2011 3rd International Conference on Computer Research and Development (ICCRD), Shanghai, China, 11–13 March 2011; pp. 143–148.
12. Ning, H.; Liu, H.; Yang, L.T. Cyberentity security in the internet of things. *Computer* **2013**, *46*, 46–53. [CrossRef]
13. Pirbhulal, S.; Zhang, H.; Alahi, M.E.E.; Ghayvat, H.; Mukhopadhyay, S.C.; Zhang, Y.-T.; Wu, W. A novel secure IoT-based smart home automation system using a wireless sensor network. *Sensors* **2017**, *17*, 69. [CrossRef]
14. Sharma, N.; Sharma, A.K. Cost analysis of hybrid adaptive routing protocol for heterogeneous wireless sensor network. *Sādhanā* **2016**, *41*, 283–288. [CrossRef]
15. Wang, K.; Wang, Y.; Sun, Y.; Guo, S.; Wu, J. Green industrial Internet of things architecture: An energy-efficient perspective. *IEEE Commun. Mag.* **2016**, *54*, 48–54. [CrossRef]
16. Abo-Zahhad, M.; Ahmed, S.M.; Sabor, N.; Sasaki, S. Mobile sink-based adaptive immune energy-efficient clustering protocol for improving the lifetime and stability period of wireless sensor networks. *IEEE Sens. J.* **2015**, *15*, 4576–4586. [CrossRef]
17. Batra, P.K.; Kant, K. LEACH-MAC: A new cluster head selection algorithm for wireless sensor networks. *Wirel. Netw.* **2016**, *22*, 49–60. [CrossRef]
18. Chen, G.; Li, C.; Ye, M.; Wu, J. An unequal cluster-based routing protocol in wireless sensor networks. *Wirel. Netw.* **2009**, *15*, 193–207. [CrossRef]
19. Hassanabadi, B.; Shea, C.; Zhang, L.; Valaee, S. Clustering in vehicular ad hoc networks using affinity propagation. *Ad Hoc Netw.* **2014**, *13*, 535–548. [CrossRef]
20. Xiong, Z.; Guo, T.; Xue, Z.; Cai, W.; Cai, L.; Luo, N. Online energy-efficient deployment based on equivalent continuous DFS for large-scale web cluster. *Clust. Comput.* **2018**, *22*, 583–596. [CrossRef]
21. Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 7 January 2000; pp. 1–10.
22. Irkhede, T.; Jaini, P. Cluster and traffic distribution protocol for energy consumption in wireless sensor network. In Proceedings of the 2013 Students Conference on Engineering and Systems (SCES), Allahabad, India, 12–14 April 2013; pp. 1–5.
23. Khalil, E.A.; Ozdemir, S. Reliable and energy efficient topology control in probabilistic wireless sensor networks via multi-objective optimization. *J. Supercomput.* **2017**, *73*, 2632–2656. [CrossRef]
24. Tarachand, A.; Kumar, V.; Raj, A.; Kumar, A.; Jana, P.K. An Energy efficient Load Balancing Algorithm for cluster-based wireless sensor networks. In Proceedings of the 2012 Annual IEEE India Conference (INDICON), Kochi, India, 7–9 December 2012; pp. 1250–1254.
25. Younis, O.; Fahmy, S. HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *Mob. Comput. IEEE Trans.* **2004**, *3*, 366–379. [CrossRef]

26. Abdulsalam, H.M.; Kamel, L.K. W-LEACH: Weighted Low Energy Adaptive Clustering Hierarchy aggregation algorithm for data streams in wireless sensor networks. In Proceedings of the 2010 IEEE International Conference on Data Mining Workshops (ICDMW), Sydney, Australia, 13 December 2010; pp. 1–8.
27. Bednarczyk, W.; Gajewski, P. An enhanced algorithm for MANET clustering based on weighted parameters. *Univers. J. Commun. Netw.* **2013**, *1*, 88–94.
28. Chauhan, N.; Awasthi, L.K.; Chand, N.; Chugh, A. A Distributed Weighted Cluster Based Routing Protocol for MANETs. In *Computer Networks and Information Technologies*; Springer: Heidelberg, Germany, 2011; pp. 147–151.
29. Muthuramalingam, S.; RajaRam, R.; Pethaperumal, K.; Devi, V.K. A dynamic clustering algorithm for MANETs by modifying weighted clustering algorithm with mobility prediction. *Int. J. Comput. Electr. Eng.* **2010**, *2*, 709–714. [CrossRef]
30. Mittal, N.; Singh, U.; Sohi, B.S. A stable energy efficient clustering protocol for wireless sensor networks. *Wirel. Netw.* **2017**, *23*, 1809–1821. [CrossRef]
31. Xu, Z.; Chen, L.; Liu, T.; Cao, L.; Chen, C. Balancing energy consumption with Hybrid clustering and routing strategy in wireless sensor networks. *Sensors* **2015**, *15*, 26583–26605. [CrossRef]
32. Zhang, B.; Tong, E.; Hao, J.; Niu, W.; Li, G. Energy efficient sleep schedule with service coverage guarantee in wireless sensor networks. *J. Netw. Syst. Manag.* **2016**, *24*, 834–858. [CrossRef]
33. Zhu, N.; Vasilakos, A.V. A generic framework for energy evaluation on wireless sensor networks. *Wirel. Netw.* **2016**, *22*, 1199–1220. [CrossRef]
34. Das, S.; Barani, S.; Wagh, S.; Sonavane, S. Extending lifetime of wireless sensor networks using multi-sensor data fusion. *Sādhanā* **2017**, *42*, 1083–1090.
35. Bian, X.; Liu, X.; Cho, H. Study on a cluster-chain routing protocol in wireless sensor networks. In Proceedings of the 2008 Third International Conference on Communications and Networking in China, Hangzhou, China, 25–27 August 2008; pp. 964–968.
36. Enam, R.N.; Qureshi, R.; Misbahuddin, S. A uniform clustering mechanism for wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2014**, *2014*, 1–14. [CrossRef]
37. Das, S.K.; Tripathi, S.; Burnwal, A. Intelligent energy competency multipath routing in wanet. In *Information Systems Design and Intelligent Applications*; Springer: Heidelberg, Germany, 2015; pp. 535–543.
38. Latif, K.; Ahmad, A.; Javaid, N.; Khan, Z.; Alrajeh, N. Divide-and-rule scheme for energy efficient routing in wireless sensor networks. *Procedia Comput. Sci.* **2013**, *19*, 340–347. [CrossRef]
39. Lou, C.; Zhuang, W. Energy-efficient routing over coordinated sleep scheduling in wireless ad hoc networks. *Peer-to-Peer Netw. Appl.* **2016**, *9*, 384–396. [CrossRef]
40. Rani, S.; Talwar, R.; Malhotra, J.; Ahmed, S.H.; Sarkar, M.; Song, H. A novel scheme for an energy efficient Internet of Things based on wireless sensor networks. *Sensors* **2015**, *15*, 28603–28626. [CrossRef]
41. Yang, H.; Xu, J.; Wang, R.; Qian, L. Energy-Efficient Multi-hop Routing Algorithm Based on LEACH. In *Advances in Wireless Sensor Networks, Proceedings of 6th China Conference on Wireless Sensor Networks, (CWSN 2012), Huangshan, China, October 25–27, 2012*; Revised Selected Papers; Springer: Berlin/Heidelberg, Germany, 2013; pp. 578–587.
42. Ali, S.A.; Refaay, S.K. Chain-chain based routing protocol. *IJCSI Int. J. Comput. Sci. Issues* **2011**, *8*, 105–112.
43. Guan, X.; Guan, L.; Wang, X.G.; Ohtsuki, T. A new load balancing and data collection algorithm for energy saving in wireless sensor networks. *Telecommun. Syst.* **2010**, *45*, 313–322. [CrossRef]
44. Li, X.; Peng, J.; Niu, J.; Wu, F.; Liao, J.; Choo, K.-K.R. A robust and energy efficient authentication protocol for industrial internet of things. *IEEE Internet Things J.* **2017**, *5*, 1606–1615. [CrossRef]
45. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
46. Sun, Y.; Zhang, J.; Ji, H.; Yang, T. KMSGC: A Key Management Scheme for Clustered Wireless Sensor Networks Based on Group-oriented Cryptography. In Proceedings of the 2008 IEEE International Conference on Networking, Sensing and Control, Sanya, China, 6–8 April 2008; pp. 1259–1262.
47. Harn, L. Group authentication. *IEEE Trans. Comput.* **2012**, *62*, 1893–1898. [CrossRef]
48. Yuea, J.; Zhang, W.; Xiao, W.; Tang, D.; Tang, J. Energy efficient and balanced cluster-based data aggregation algorithm for wireless sensor networks. *Procedia Eng.* **2012**, *29*, 2009–2015. [CrossRef]
49. Dong, M.; Ota, K.; Liu, A. RMER: Reliable and energy-efficient data collection for large-scale wireless sensor networks. *IEEE Internet Things J.* **2016**, *3*, 511–519. [CrossRef]

50. Guo, Y.; Liu, Y.; Zhang, Z.; Ding, F. Study on the energy efficiency based on improved LEACH in wireless sensor networks. In Proceedings of the 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR), Wuhan, China, 6–7 March 2010; pp. 388–390.
51. Kumar, D.; Aseri, T.C.; Patel, R. Multi-hop communication routing (MCR) protocol for heterogeneous wireless sensor networks. *Int. J. Inf. Technol. Commun. Converg.* **2011**, *1*, 130–145. [CrossRef]
52. Issariyakul, T.; Hossain, E. *An Introduction to Network Simulator NS2*, 2nd ed.; Springer: Heidelberg, Germany, 2012.
53. Pereira, R.M.; Ruiz, L.B.; Ghizoni, M.L.A. MannaSim: A NS-2 extension to simulate wireless sensor network. In Proceedings of the Fourteenth International Conference on Networks (ICN 2015), Barcelona, Spain, 19–24 April 2015; p. 107.