IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received July 16, 2020, accepted August 29, 2020, date of publication September 7, 2020, date of current version September 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3022285

Secure and Energy-Aware Heuristic Routing Protocol for Wireless Sensor Network

KHALID HASEEB[1], KHALED MOHAMAD ALMUSTAFA[2], (Associate Member, IEEE), ZAHOOR JAN[1], TANZILA SABA[2], (Senior Member, IEEE), AND USMAN TARIQ[3]

[1]Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Pakistan
[2]Artificial Intelligence and Data Analytics Laboratory (AIDA), CCIS, Prince Sultan University, Riyadh 12435, Saudi Arabia
[3]College of Computer Engineering and Science, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia

Corresponding author: Tanzila Saba (drstanzila@gmail.com)

This work was supported by the Artificial Intelligence and Data Analytics Lab (AIDA), CCIS Prince Sultan University, Riyadh, Saudi Arabia.

ABSTRACT Wireless Sensor Networks (WSNs) achieve much attention from various domains because of its easy maintenance, self-configuration, and scalability characteristics. It is comprised of small-sized sensors that interact with the Internet of Things (IoT) for observing and recording the physical conditions. The sensor nodes are autonomous and construct inter-communication topology with each other in an ad-hoc manner. However, the main restrictions of sensor nodes are their finite resources for energy management, data storage, transmission, and processing power. Different solutions have been addressed by researchers to overcome network performance due to bounded limitations of such battery-powered nodes, however, equalize the energy consumption and maintain the network throughput are the main research problems. Furthermore, due to the compromised nodes, the data is more prone to security vulnerabilities. Therefore, their security over the unpredictable network is other research concerns. Thus, the aim of this research article to propose a secure and energy-aware heuristic-based routing (SEHR) protocol for WSN to detect and prevent compromising data with efficient performance. Firstly, the proposed protocol makes use of an artificial intelligence-based heuristic analysis to accomplish a reliable, and intellectual learning scheme. Secondly, it protects the transmissions against adversary groups to attain security with the least complexity. Moreover, the route maintenance strategy is also achieved by using traffic exploration to reduce link failures and network dis-connectivity. The simulation results demonstrated the SEHR protocol improves the efficacy for network throughput by an average of 18%, packet drop ratio by 42%, end-to-end delay by 26%, energy consumption by 36%, faulty routes by 38%, network overhead by 44%, and computational overhead by 43% in dynamic scenarios as compared to existing work.

INDEX TERMS Artificial intelligence, data privacy, energy efficiency, heuristic analysis, wireless sensor network.

I. INTRODUCTION

The field of Wireless Sensor Network (WSN) [1]–[3] is exploring by a huge number of applications such as the military, healthcare, smart buildings, agriculture to observe and gathering the physical data. The sensor nodes are distributed in a randomly or uniformly manner to gather the data on a periodic or event-driven form. The end-users access the needed sensors data from the base station (BS) through the Internet with the help of wireless broadband channels [4], [5]. Although, sensor nodes perform a vital role in different academic and industrial fields, however, many constraints limit their performance. Some of the limitations are battery power, memory, transmission, and processing power [6], [7]. Among these limitations, the most important problem for many applications is to improve the energy efficiency for WSN with timely data delivery. The infrastructure of WSN is characterized as unique from traditional networks, due to its easy installation, management, ad-hoc and self-configured attributes. Most of the solutions are based on multi-hop data transmission towards BS, especially for the large scale network region. Recently, different solutions have been proposed by researchers to cluster the sensor nodes into different boundaries. Each boundary has declared one cluster head for a particular period, which aims to collect and forward the data from members to BS [8]–[10].

As network size increases and the enormous number of sensor nodes become a part of WSN, the network scalability

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

with efficient data routing gain a lot of popularity between the research communities. The routing protocols can be categorized for data dissemination either in static or dynamic methods [11]–[13]. In the static method, the routing tables of gateway nodes and routers are manually formed and maintained. However, in dynamic topology, the routing tables are restructured automatically whenever any event occurs or changes come in the network topologies. Mostly, dynamic methods are preferred by the researchers as compared to static routing, especially in high-density scenarios. However, in small network size, the static routing is more suitable due to its lower overhead of processing power on nodes and helps to transfer the routing information from one protocol to another protocol, such phenomenon is called routing re-distribution. Unlike wired networks, the wireless network gains a lot of research attentions and challenges in routing protocols due to its channels interference and unreliable nature of the transmission medium. Many solutions have been proposed based on the extension of DSR and AODV routing protocols for the wireless network [14]–[16]. But most of them are not sufficient to deal with the dynamic nature and low powered sensor nodes and still, the network scalability, throughput with energy efficiency are some of the significant research problems for constraints oriented networks.

Moreover, IoT allows the anonymous exchange of physical information between smart devices, radio frequency identification (RFID) technologies, and WSN. The gathered information is forwarded to BS through IoT-based sensors for post analysis and decision making [17]–[19]. However, the low powered sensor nodes more prone to security threats due to their bounded constraints especially in terms of memory, battery, and processing power. Such limitation significantly increases the chances of unauthorized access and compromised network confidentiality and integrity. Most of the solutions for constraint oriented networks are proposed for improving energy efficiency and data delivery performance, but they overlooked the data security of sensors data and provide the gap for intruders to exploit the network information. Therefore, in modern years, the secure and energy-efficient routing solution must be designed for IoT-based WSN for balancing the energy load and prevent the network data from prohibited access, being tempered with and expose to malicious nodes [20], [21].

This research article aims to propose a secure and energy-aware heuristic routing protocol using artificial intelligence for WSN. Due to its limited resources, the SEHR protocol is mainly focused on energy efficiency, reliability, and secure data delivery performance. In this work, the artificial intelligence-based beam heuristics [22] is used to achieve the optimal data routing, and the SEHR protocol incorporates aggregated residual energy, hop count, and link integrity parameters to learn the routing decision. The beam-based heuristics algorithm is derived from the traditional discipline of Artificial Intelligence and it optimizes the conclusions. Furthermore, based on beam heuristics, the SEHR protocol develops a graph-based solution, which reduces the memory and processing overheads of sensor nodes. Moreover, the SEHR protocol makes use of the counter mode (CTR) [23], a cryptography algorithm, to provide data encryption and authentication for securing the inter-routing. In SEHR protocol, each data packet is dependent on the encryption of the previous data packet, which makes it more secure and authentic. The proposed work not only capable of dynamically sensing and isolating the malicious nodes during the data security phase, while on the other hand, it also provides the strategy for route maintenance. Both the energy-level alerts and traffic analysis between BS and their neighborhoods offer efficient load distribution and decrease the problem of network disjoining. The SEHR protocol significantly improves the network performance of low powered sensor nodes in terms of various network parameters as compared to other states of the art solutions.

The remainder of the paper is ordered into the subsequent sections. Section 2 discusses the literature review and problem formulation. Section 3 presents a detailed description of the SEHR protocol with its designed phases. Section 4 presents the simulation model and performance evaluation against existing work. In the end, Section 5 ends this research article with future findings. Table 1 illustrates the list of notations that are used in the SEHR protocol.

TABLE 1. **List of notations.**

Notations	Definitions
$G(N,L)$	graph with N nodes and L edges
h_{BS}	hop count to the base station
e_i	the residual energy of node i
dl_i	degree of link integrity for node i
$\|\|$	concatenation
$h(f)$	hash function
$M(c)$	message code
$energy_{thres}$	energy threshold
P_1	probe packet
n_1, n_2	connected nodes
RREQ	route request
$W(f_n)$	weighted sum
$\oplus$	XoR
N_i	nonce
E	encryption function
K	key
$D_1, D_1, \dots D_n$	data blocks
D_i	decryption function
C_i	counter bits
C_{tr}	counter block
$C_1, C_2, C_3 \dots C_n$	cipher bits

II. RELATED WORK

In modern years, many protocols based on WSN have been proposed such as healthcare, smart transportation, smart cities, and military system [24]–[27]. However, the sensor nodes have bounded resources, therefore, such limitations degrade the network performance and increase the demand for energy-efficient and secure routing. In proactive routing protocols, the nodes exchange their information among neighbors to update the node tables on a specific period. Although the proactively based routing protocols determine the data forwarding path much rapidly, however, such solutions have a large number of control packets and network congestion on the transmission links. On the other hand, reactive protocols are also called on-demand solutions, as mostly used in wireless networks. Whenever any node receives a data packet then at that time the source node searches for the next-hop by using neighbors' information. Such solutions have the least network overhead as compared to the proactive based solutions, however, they need some time to discover and forward the data packets.

The authors [28] proposed an adaptive competition-based clustering approach (ACCA) for WSN, which provides multi parameters for the selection of cluster heads. The factors are residual energy, the centrality of the nodes, and the distance between the cluster heads. The distance factor among cluster heads is exploited in the proposed solution to distribute the clusters with suitable sizes. Moreover, the data transmission is based on multi-hop from cluster head to cluster head until data packets are received at BS. However, the proposed solution does not consider the link evaluation in the selection process of cluster heads and leads to a negative impact on data delivery performance. Furthermore, the proposed solution is not appropriate for large scale regions, as sensors data can be leaked to malicious entities. In [29], the authors proposed an energy-efficient fuzzy logic-based clustering technique for WSN, which makes use of five parameters to determine the strength of the nodes. Accordingly, the proposed solution selects the nodes for the role of cluster heads. Moreover, it set a condition to cope with the even distribution of cluster heads in the network field. However, it floods too much control packets for the selection of cluster heads and consumed additional energy resources. Moreover, the conditions of wireless medium are not evaluated for data routing, therefore the proposed solution is not suitable for under the presence of malicious traffic.

In [30], the authors proposed a secure and reliable communication for next-generation networks in smart cities, which aims to decrease the quantity of unnecessary traffic flow between the edges by relying on node-to-node transmission protocol. Moreover, the integration of fog and cloud layers ensures secure communication. However, the proposed solution does not evaluate its routing performance in terms of energy efficiency and network overheads. The authors in [31], proposed Secure Routing in Multi-hop IoT-based Cognitive Radio Networks under Jamming Attack, which aims to improve the data delivery performance and secure the routing path from source to destination. However, the routing decision is not optimal by considering the significant network parameters. Moreover, the performance of the proposed solution is only analyzed based on the packet delivery ratio and overlooked other network metrics. The authors in [32] proposed a secure trust-aware RPL (*SecTrust-RPL)* routing protocol for the Internet of Things to secure the communication from rank and Sybil attacks. Although, the proposed protocol improves the routing performance against network threats, however, the routing decision is not optimal and lowers data delivery performance. The authors [33] proposed a novel security protocol for WSN using cooperative communication, which aims to improve the performance and resiliency and data reliability against cyber-attacks. The proposed solution provides a data security MAC protocol that implements a hash function to verify the message integrity along with the simple key distribution mechanism to authenticate the network entry. It improves network security, however, it is appropriate with a small number of sensor nodes, and routing performance is overlooked.

In [34], the authors proposed novel predictive efficient energy consumption reclaim PEECR-based clustering routing approach for WSN. The proposed solution presents an energy-efficient routing approach based on clustering distance between nodes, degree of nodes, and nodes residual energy. The proposed solution is based on the swarm colony optimization algorithm to achieve data routing. The experimental results demonstrated the improved performance in the comparison of other work, however, it incurs additional energy consumption in the selection of cluster heads by flooding many control messages and does not consider the misbehaving nodes to ensure data privacy with integrity, which results in compromised data security. The authors in [35], proposed a particle swarm optimization (PSO) based routing protocol. The proposed solution aims to conserve the energy consumption of the gateway nodes for improving network lifetime and routing. Moreover, a novel fitness function is designed based on the number of relay nodes, the distance among gateway from BS, and load on relay node factors. The simulated results illustrated better performance than the existing solutions, however, it lacks the security consideration and also links integrity is overlooked in routing decision.

Authors in [36] proposed an enhanced hierarchical clustering approach for mobile sensor networks using fuzzy inference systems, which aims to reduce the energy conservation and packet loss rate between mobile sensor nodes. The simulation-based experiments revealed that the proposed solution improved the performance for network lifetime and cluster deviation than other work. However, coping with the latest position of mobile nodes with nominal overheads is still a problem in the proposed solution. Also, the mobile nodes are vulnerable to security threats under the presence of malicious nodes. In [37], the authors proposed a fuzzy logic-based clustering algorithm (CAFL) for WSN, which aims to increase the network lifetime and energy efficiency. In this solution, the fuzzy logic is used for the selection of cluster heads and clusters formation based on residual energy and closeness factors. However, the optimal routing

TABLE 2. Comparative analysis for energy-efficient and secure routing protocols.

Protocol	Contributions	Limitations
ACCA	Suitable size clusters, energy efficiency, network lifetime	Not appropriate for large size network region, no link evaluation and data security
Energy-efficient fuzzy logic-based clustering	Energy efficiency and even distribution of cluster heads	Network overheads, no link evaluation, and data privacy
Secure and reliable communication for next-generation networks	Decrease unnecessary traffic flow and balance the load distribution	Routing performance is not evaluated and measurement of wireless channels is missing
Secure Routing in Multi-hop IoT-based Cognitive Radio Networks	Improve data delivery performance and secure routing	The routing decision is not optimal, no evaluation some standard network metrics
SecTrust-RPL	Provides security against rank and Sybil attacks with trust	Lower data delivery performance and routing scheme is not optimized
PEECR-based clustering routing	Energy-efficient clusters and improved data routing	Additional energy consumption and no data security is provided against malicious nodes
(PSO) based routing protocol	Reduce energy consumption with better network lifetime and routing	No data confidentiality and integrity against potential threats
A novel security protocol for WSN using cooperative communication	Network resiliency, data reliability, and integrity	Applicable to a small number of sensor nodes, routing performance is not evaluated in terms of optimal and improved network throughput
An enhanced hierarchical clustering approach for mobile sensor networks	Energy conservation and improvement in packet drop ratio for mobile sensor nodes	Managing with the latest position of mobile sensors, communication overheads, and no data security.
Fuzzy logic-based clustering algorithm (CAFL)	Improve the process for cluster heads selection and clusters formation.	No optimal routing performance and secure data transmission
enhanced clustering hierarchy (ECH) approach	Minimized data redundancy, increases the network lifetime and energy efficiency.	Overlooked the limited constraints of sensor nodes in data routing, open for network threats over the insecure transmission links.
Heuristic data dissemination for mobile sink networks	Decreases data latency, energy consumption with improves the network lifetime using the heuristic function	The valuation of wireless links is not considered in the routing performance and no security measurement against malicious threats
Novel heuristic-based energy-efficient routing strategy in WSN	The fitness function is used to decrease the load of energy consumption and packet drop ratio. Identify the energy-deficient nodes on the earlier stage of data transmission	Routing performance is not optimal based on nodes parameters, data privacy and integrity can be compromised.

performance and secure data transmissions are missing in the proposed algorithm. The authors [38], proposed an enhanced clustering hierarchy (ECH) approach for maximizing the lifetime of WSN. The proposed approach improves energy efficiency based on the sleeping-waking method for overlapping and neighboring nodes. Also, the redundant data is minimized and ultimately it improved the network lifetime. However, during data routing, the limited constraints of sensor nodes are not considered. Moreover, the proposed solution cannot cope with network threats over the insecure transmission medium.

Authors in [39] proposed Heuristic data dissemination for mobile sink networks, which aims to cope with hot spot problems and improves routing performance. To decrease the frequent location update packets of the mobile sink, it proposed a double ring that performs an intermediate role between sensor nodes and sink. Also, it uses the heuristic function based on residual energy, direction transmission distance, and perpendicular distance and increases the network outcomes. In [40], the authors proposed a novel heuristic-based energy-efficient routing strategy in WSN, which aims to decrease the load of energy consumption and packet drop ratio. The proposed solution presents a novel African Buffalo-based Two-tier Data Dissemination (AB-TTDD) strategy using fitness function for monitoring the energy de-efficient nodes at an earlier stage. Also, it developed a novel Temporary Energy Mapping Algorithm (TEMA) for maintaining the route by creating the reference node. The experimental results demonstrated the improved performance of the proposed solution than existing work in terms of packet flow ratio and power consumption. However, the proposed solutions do not incorporate any security schemes to tackle with malicious threats. Moreover, the valuation of wireless links towards the sink node is overlooked in network-wide routing, which results in frequent route re-discoveries and data retransmissions.

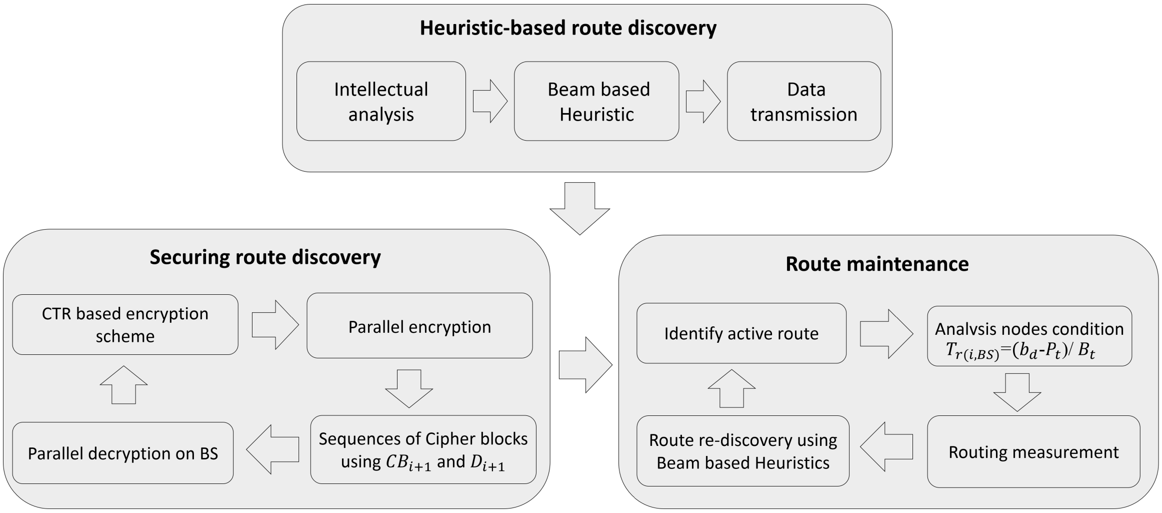

Heuristic-based route discovery
Intellectual analysis
Beam based Heuristic
Data transmission
Securing route discovery
CTR based encryption scheme
Parallel encryption
Sequences of Cipher blocks using CB_{i+1} and D_{i+1}
Parallel decryption on BS
Route maintenance
Identify active route
Analvsis nodes condition $T_{r(i,BS)}$=(b_d-P_t)/ B_t
Routing measurement
Route re-discovery using Beam based Heuristics

FIGURE 1. **The architecture design of the SEHR protocol.**

The aforementioned related work demonstrated that WSN has been explored by many academic and industrial domains due to its flexibility and light-weight infrastructure. However, the main problems in WSN are its lower constraints in terms of various resources. The main important factor that most of the researchers have been focused on improving the energy efficiency for battery-powered sensor nodes. Moreover, the stable delivery ratio within a timely manner is also considered the hot research problem for constraints oriented networks. It is observed that the majority of the routing schemes heuristic-based fitness function but they do not consider scared constraint resources on the part of the sensor nodes in the selection of next-hop, which results in rapid energy consumption of the network field and compromised network lifetime. Also, they compromised to data privacy and integrity against network threats. Furthermore, most of the existing solutions provide network reliability in the form of frequent Route REQuest (RREQ) and update packets thereby result in huge data traffic with decreasing quality of service. It is also seen that due to battery-powered sensor nodes, the network data is accessible by malicious nodes and compromised to network privacy. Although, some solutions offer data security based on traditional security approaches, however, they incur additional communication overheads that slow down the process of data routing. Therefore, the infrastructure of IoT-based WSN needs a secure and energy-efficient solution with light-weight computations to improve the process of routes discovery and maintenance with trustworthiness. Table 2 demonstrates the comparative analysis of different energy-efficient and secure routing solutions.

III. PROTOCOL DESIGN

This section discusses the detailed description of the proposed SEHR protocol and its phases. The SEHR protocol is developed for low constraint devices to improve the network outcomes for energy consumption with efficient data delivery and security. This work is comprised of two main phases. In the first phase, the proposed protocol makes use of an artificial intelligence-based graph heuristic algorithm to optimize the decision for trustworthy data routing. The beam heuristic exploits multiple parameters along with link integrity to achieve intelligent next-hop selection and reduce the memory requirement of the nodes. The second phase aims to accomplish secure and authentic data routing based on the counter encryption mode with computational simplicity and randomness. The SEHR protocol encrypts and decrypts the data packets in a parallel manner with decreasing computing resources of the nodes. Moreover, energy-alert and traffic analysis methods decrease the chances of route failures and non-uniform energy consumption in the network field. The architectural design with phases of the SEHR protocol is illustrated in Fig.1. In this work, we highlight some network assumptions that are as follows.

i. All the nodes are constraint in terms of resources, excluding BS.
ii. Nodes remain static after distribution in the square sized network area.
iii. Nodes have equipped with Global Positioning System (GPS).
iv. All the nodes are synchronized so they can awake at the same time for sensing and forwarding the data.
v. A malicious node floods a false route response for the selection of appropriate next-hop.

A. ROUTE DISCOVERY

In the first phase, let's consider that sensor nodes are set up in the undirected graph G. In the graph $G(N, L)$, N indicates the number of nodes and L is the optimized link between two directly connected nodes n_1 and n_2. Initially, the path between neighbors is computed based on the distance factor. In the first phase, the SEHR protocol makes use of the heuristic function to compute the weighted value for finding the optimum node as a next-hop. The heuristic function guides the routing decision about the direction towards the destination node. In SEHR protocol, the heuristic function offers a learned route to predict the most optimal neighbor that leads to a goal. To initiate the route discovery phase, the source node checks its route entry towards BS in a local table. If it found the route that meets the requirements of a hop count to BS h_{BS}, aggregated energy e_i and degree of link integrity dl_i, the source node selects it as a next-hop and directly sends the data packets to it. However, it might be a case that there is no valid route exists according to the routing needs in the local table of the source node. In such a case, all the neighbors are requested to participate in the selection process of next-hop.

The degree of link integrity makes use of the cryptographic hash function to ensure whether transmitted data bits are altered due to compromised links or not. Let us consider that node i generates a probe packet of k bits and need to forward it to the node j. Firstly the node i, pass the probe packet P_1 to hash function to determine its message code $M(c)$. Secondly, the obtained message code is integrated with the actual probe packet as $P_1 + M(c)$ and forwarded to the node j. Upon receiving the probe packet P_1 along with message code $M(c)$, the node j recomputes the message code of the receive probe packet P_1. If the computed message code is the same as the received message code, then j declares the integrity of the received probe message. Moreover, based on the computed hash value on a node j, the SEHR protocol gives the threshold to a particular link either low or high. The low threshold value is indicated as 0 and a high threshold value is exposed by 1. The high threshold indicates that the particular link is more reliable and may contribute to the least error rate. Also, the aggregated residual energy e_i is computed in two stages. Firstly, each node continually monitoring the residual level e_l, and secondly, it also records the rate of residual energy around its locality e_{loc} as given $\sum_{n=0}^{N} me_n - ce_n, n\epsilon$ neighbor, me_n is maximum energy and ce_n is the consumed energy of neighbor n. Accordingly, the node with higher aggregated residual energy is given a maximum priority. In the end, the node looks into its local table and checks the counter value that indicates the number of hop towards BS. The lesser the value specifies that the node is closer to BS and requires the least communication cost for data transmission. Finally, all the computed values of aggregated residual energy, hop count, and link integrity are summed up in a weighted aspect to determine the heuristic function $h(f)$ as given in equation 1.

$$h(f) = \alpha * (e_l + e_{loc}) + \beta * 1/h_{BS} + \gamma * dl_i \qquad (1)$$

In equation 1, α, β, γ are the weighting coefficients and give a significant impact on the heuristic function. After the computing of $h(f)$, each neighbor node shares its information with the source node for predicting the optimal decision to reach towards BS. The neighbor node with the highest $h(f)$ indicates a stronger rank for the selection of next-hop. Accordingly, the source node unicasts the RREQ packet to the selected neighbor as a next-hop for data sending.

Afterward, the SEHR protocol utilizes the beam heuristic algorithm, which is an informed search, and explores the connected graph by increasing the most promising next-hop in a partial set. The SEHR protocol optimizes the node tables in the sense that it restricted the memory usage for storing the non-promising nodes at any step in determining the next-hop. In this work, the beam heuristic algorithm optimizes the strategy to choose the optimal node as next-hop based on the highest weight from all possible candidates. Such a mechanism possibly decreases the computation and time complexity of battery-powered sensor nodes. The SEHR protocol stores a predetermined number w, which is called beam width, and indicates the optimal states at each level. The performance of the algorithm depends on the value of beam width, by keeping its value minimum improves the space and time complexity of sensor nodes. The beam heuristic is the improved form of best-first search by using beam value. Let's consider that d indicates depth and b indicates the branching factors. Then the time and space complexity can be computed as $O(b^d)$. Also, as sensor nodes are limited in terms of constraints, therefore, based on the beam width, only w sensor nodes are expanded in the graph by applying heuristics function $h(f)$ and ignoring the other nodes. Accordingly, this process continues until an optimal route is explored with the highest $h(f)$ value, while decreasing the energy consumption and communication cost in the sensor field. Let's consider that $h(f_0), h(f_1), h(f_2), \ldots, h(f_n)$ are the highest weighted values using beam heuristics, then their weighted sum $W(f_n)$ can be denoted as given in equation 2.

$$W(f_n) = h(f_0) + h(f_1) + \ldots. + h(f_n) \qquad (2)$$

B. SECURING ROUTE DISCOVERY

In the second phase, the SEHR protocol focused on data security for the selected beam heuristics-based routes. Also, it offers the route maintenance strategy to ensure data connectivity with the least network latency. The SEHR protocol uses a CTR mode, a cryptography algorithm that enables the nodes to encrypt the data packets in parallel with randomness [41]. The cryptography keys are pre-distributed to sensor nodes before their distribution and later they perform data transmission with neighbors. To initiate the CTR encryption scheme, three factors are needed i.e. data packet D_i, a secret key K and counter bits C_{tr}. The nonce N_i and counter bits C_{tr} are concatenated with each other and pass through an encryption function E using key K to produce a unique pattern of the counter block CB_i as given in equation 3.

$$CB_i = E(K(N_i + C_{tr})) \qquad (3)$$

Afterward, the source node n_{i} performs XoR operation between the counter block CB_i and data packet D_{i} to generate a ciphertext C_{i}, and unicast towards next-hop $n_{\mathrm{i}+1}$ as given in equation 4.

$$C_{\mathrm{i}} = CB_i \oplus D_{\mathrm{i}} \qquad (4)$$

Upon receiving, the next-hop $n_{\mathrm{i}+1}$, increments the counter bits by 1 and based on equation 3, it applies encryption function E on concatenation with nonce and the counter bits to generate the new counter block CB_{i+1} for data packet $D_{\mathrm{i}+1}$. The generated counter block CB_{i+1} is XoR with a data packet $D_{\mathrm{i}+1}$, and the outcome is concatenated with the ciphertext of the previous node C_{i} as given in equation 5.

$$C_{\mathrm{i}+1} = CB_{i+1} \oplus D_{\mathrm{i}+1} + C_{\mathrm{i}} \tag{5}$$

Accordingly, the sequences of ciphertext $C_{\mathrm{i}}, C_{\mathrm{i}+1}, C_{\mathrm{i}+2}, \ldots\ldots, C_{n-1}, C_n$ for nodes $n_{\mathrm{i}}, n_{\mathrm{i}+1}, n_{\mathrm{i}+2}, \ldots., n_{\mathrm{n}-1}, n_{\mathrm{n}}$ are received at BS, and it implies the decryption function D with the same key to obtaining the actual data packets D_i such that $i = 1, 2, 3, \ldots., n$ by using equation 6.

$$D_i = (\mathrm{D}(\mathrm{K}(N_i + CB_i) \oplus C_i \tag{6}$$

C. ROUTE MAINTENANCE

Moreover, to achieve route maintenance, the alternate routes are identified if the selected next-hop nodes fall their energy levels to the particular threshold $energy_{thres}$. Such a mechanism decreases the chances of route breakages and data re-transmissions. Whenever any energy de-efficient node is identified in the routing phase, it quit from data transmission and unicasts the error message $route_{err}$ to the source node. The source node executes the heuristic function to determine the highest weighted node, and accordingly, the new next-hop is selected to resume the data routing. The energy threshold in route maintenance significantly decreases the route breaches and network latency. Furthermore, the next-hops located in the neighborhood of BS have to relay more data packets than farther ones. Such nodes are overloaded and lead to a consumed high ratio of energy resources in data routing, which results in increasing packet loss ratio and network dis-connectivity. Therefore, the SEHR protocol evaluates the traffic ratio T_r between BS and their neighborhood next-hops. Let's consider that b_d is the bandwidth of link from next-hop i to BS, P_t shows the number of packets that are transmitting on the link from next-hop i to BS and B_t is the maximum bandwidth, then the traffic ratio T_r can be computed as given in equation 7.

$$T_{r(i,BS)} = (b_d - P_t)/B_t \tag{7}$$

Afterward, if the traffic ratio between the next-hop $\boldsymbol{i}$ and BS is exceeded then the certain threshold, it left from data forwarding and sends back an acknowledgment ACK packet to a downstream next-hop for the selection of an appropriate forwarder. Consequently, the source node floods the RREQ packet to neighbors to compute their weight, and accordingly the fresh next-hop is selected based on the heuristic function $\boldsymbol{h(f)}$. Such a mechanism of SEHR protocol considerably increases the route conservation and stability for a longer time.

IV. SIMULATION SETUP

In this section, we present the simulation setup and experimental results of the SEHR protocol against SecTrust-RPL [32], heuristic-based energy-efficient routing [40], and PSO-based routing [35] solutions. The values of weighting coefficients α, β, γ are assigned in such a manner that their summation must be equal to 1. The experiments are conducted in the simulator tool NS3, which is open source and mostly used by the research community to verify statistical results. The simulation experiments are performed based on two different scenarios i.e. varying data generation rate and the varying number of nodes. The data generation rates are considered to follow a Poisson distribution [42] and varying randomly in the range of 5 to 25 seconds. Furthermore, the network performance is evaluated between the SEHR protocol and existing work using network lifetime, energy consumption, network throughput, packet drop ratio, faulty routes, and network overhead. To evaluate the security level of the SEHR protocol against the existing solution, several malicious nodes range 10 to 15 are deployed in the network field, which aims to flood malicious traffic and drop the data packets. The deployed number of BS is set to 1 and placed at the coordinates of (100, 150). The transmission range of all the nodes is set to 20m. The initial energy level of nodes is set in the range of 2j. The simulation time is fixed to 1000sec. The data traffic between sensors is based on a constant bit rate (CBR). The data bits in an individual packet is set to 32.

We supposed the energy model adopted in [43] for the analysis of energy consumption as given in equations 8 and 9.

$$E_{Tr}(k,d) = \begin{cases} E_{elect} * k + k * E_{fs} * d^2, & if\ d \leq d_t \\ E_{elect} * k + k * E_{amp} * d^4, & if\ d > d_t \end{cases} \tag{8}$$

$$E_{Rx}(k) = E_{elect} * k \tag{9}$$

In equations 8 and 9, d denotes the transmission distance, d_t is threshold distance, k is number data bits, E_{elect} is the amount of energy consumption in single data bit, $E_{fs} * d^2$ or $E_{fs} * d^4$ denotes the energy consumption of amplifier from sender to receiver.

Table 3 lightens the default values of parameters for network and simulation setup.

TABLE 3. Simulation parameters.

Parameter	Value
Simulation area	300m X 300m
Sensor nodes	50-250
Data generation rate	5-25sec
Malicious nodes	10-15
Packet size, k	32 bits
Energy level	2J
Number of BS	1
Location of BS	(100,150)
Beamwidth (w)	2
α,β,γ	0.333,0.333,0.333
Control message	20 bits
Transmission range	20m
Traffic type	CBR

A. ANALYSIS OF NETWORK THROUGHPUT

Fig.2 and Fig. 3 illustrates the performance of network throughput in terms of a varying number of nodes and

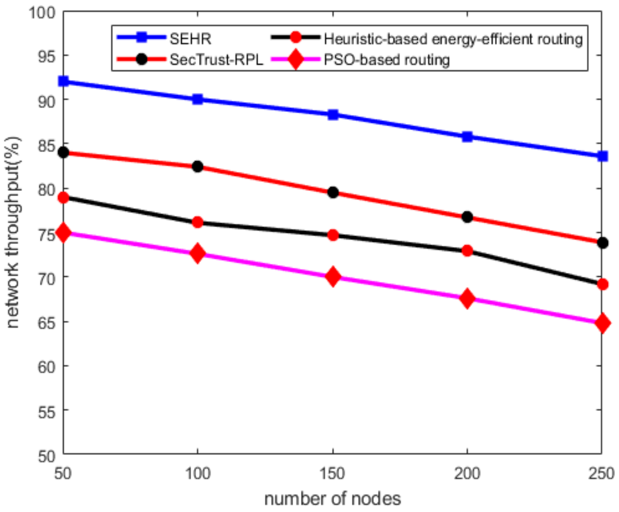


FIGURE 2. Network throughput and number of nodes.

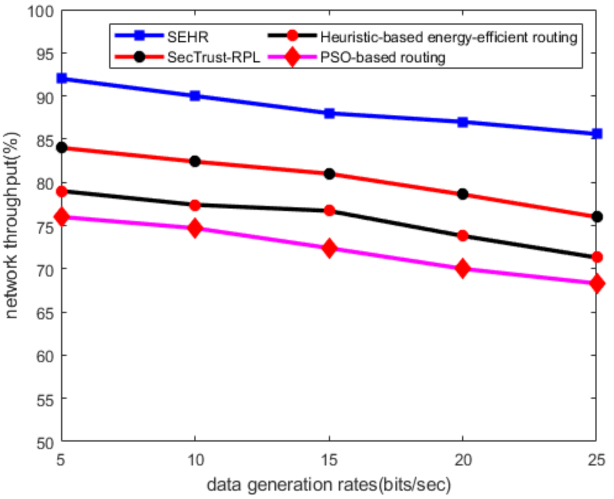


FIGURE 3. Network throughput and data generation rates.

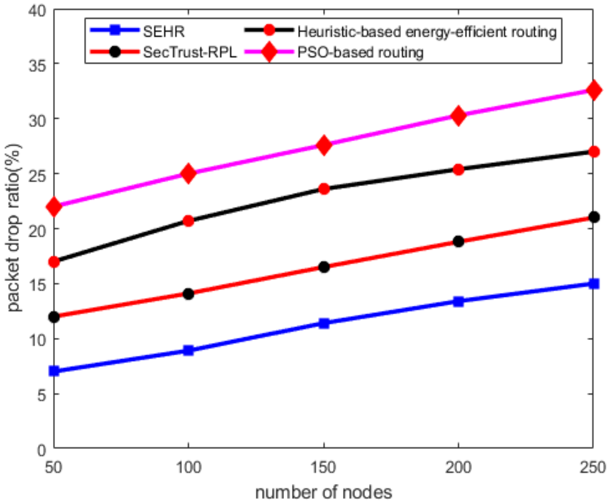


FIGURE 4. Packet drop ratio and number of nodes.

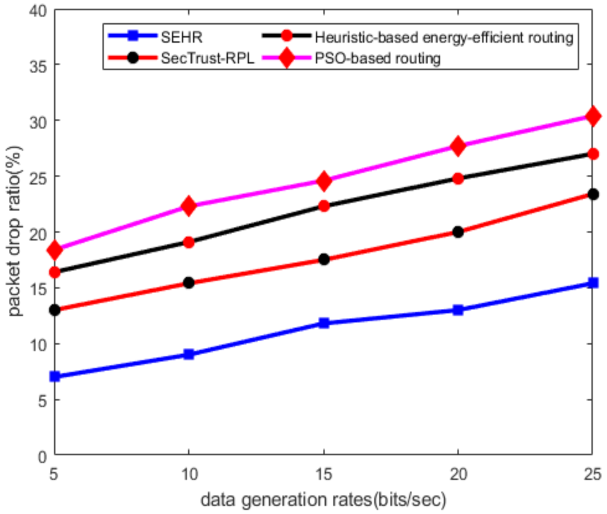


FIGURE 5. Packet drop ratio and data generation rates.

varying data generation rates. The experimental results revealed that the proposed protocol improves the network throughput by an average of 17% and 19% as compared to existing work. This is due to the construction of a robust routing decision is involved in the design of the SEHR protocol with the least communication overheads on sensor nodes. Unlike other solutions, the SEHR protocol incorporates the link integrity factor based on cryptography hash function and determines the most reliable and trusted transmission path for data forwarding, which leads to improved network throughput. Moreover, the use of CTR mode for data security, the SEHR protocol reduces the chances of malicious nodes to degrade the data delivery performance between sensors nodes and BS. Moreover, the method of traffic analysis between neighborhood nodes and BS higher increases the outcome of packets delivery and network connectivity. The SEHR protocol provides an energy-efficient, shortest, and less overloaded routes using the artificial intelligence beam heuristic technique to achieve a better way for data conversation in the network field.

B. ANALYSIS OF PACKET DROP RATIO

Fig.4 and Fig.5 depict the behavior of the SEHR protocol against the existing solution in terms of a varying number of nodes and data generate rates. The experimental results demonstrate that the SEHR protocol decreases the packet drop ratio by an average of 42% and 42% in both the network scenarios. Unlike other solutions, the SEHR protocol is designed weighted function based on residual energy, hop count to BS, and link integrity factors by using beam heuristic algorithm. Such a strategy offers the selection of most energy-efficient and trustworthiness nodes for data routing. Furthermore, the combination of CTR based data encryption with its simplicity and randomness functions also increases the level of network reliability and it is tough for malicious objects to drop the sensors data. Moreover, the avoidance of

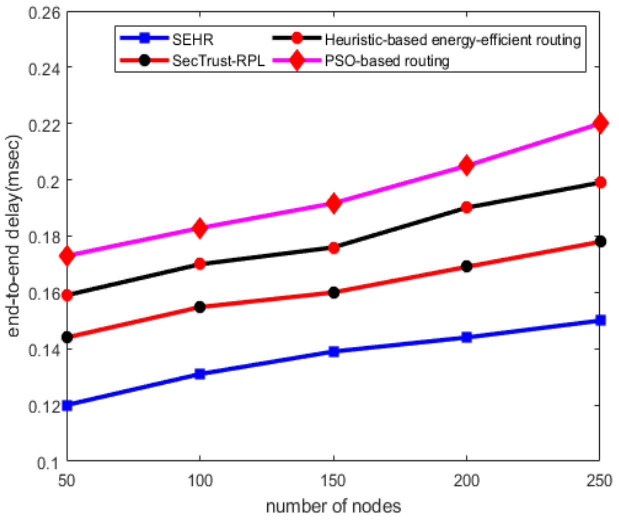


FIGURE 6. End-to-end delay and number of nodes.

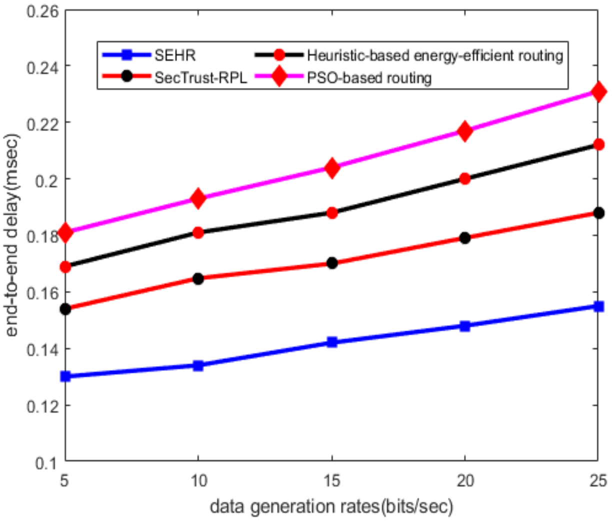


FIGURE 7. End-to-end delay and data generation rates.

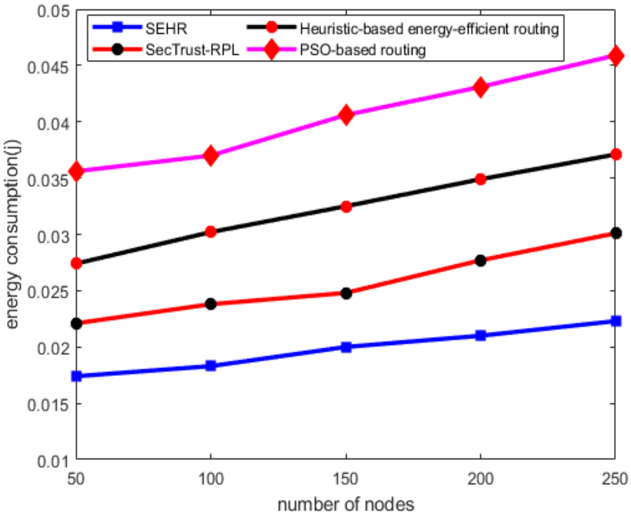


FIGURE 8. Energy consumption and the number of nodes.

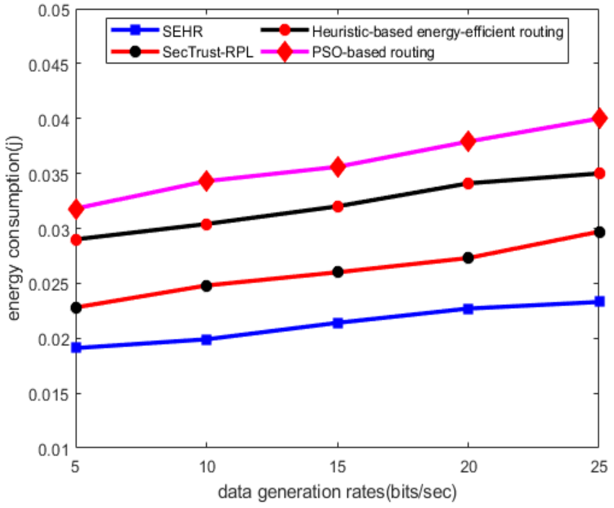


FIGURE 9. Energy consumption and data generation rates.

the link integrity factor in the existing solutions increases the probabilities for malicious nodes to produce fake and anonymous packets and decreases the available capacity of wireless channels to forward data packets and degrade network performance.

C. ANALYSIS OF END-TO-END DELAY

Fig.6 and Fig.7 illustrate the performance of the SEHR protocol with other solutions in terms of a varying number of nodes and data generation rates. It is observed from the experimental results that the SEHR protocol reduces the end-to-end delay ratio by an average of 25%, and 26% than other work in the presence of malicious nodes. This is due to the selection of optimal nodes as data carriers based on multiple criteria and give equal significance to each factor. The sensor nodes in the existing solutions deplete the energy resource rapidly due to the malicious traffic and more prone to failure, which results in increasing end-to-end delay. Moreover, without proper determination of link reliability, the constructed route is not able to forward the sensors' data for a longer time, and ultimately, most of the time spent in finding alternate routes and endure high network latency. Unlike other solutions, the SEHR protocol chooses the energy-aware and more consistent route for data routing and decreases the chances for route re-discoveries with the least re-transmission. Also, the SEHR protocol makes use of an artificial intelligence-based heuristic function, which is light-weight and makes the routing decision more intelligent. Such a routing strategy eventually reduces network congestion and appropriately exploits the bandwidth of wireless channels for routes the data packets with minimal network delay.

D. ANALYSIS OF ENERGY CONSUMPTION

In Fig.8 and Fig.9, the performance evaluation of the SEHR protocol against the existing solution demonstrates in terms of a varying number of nodes and data generation rates. The experimental results revealed that the SEHR protocol minimizes the energy consumption in the presence of malicious

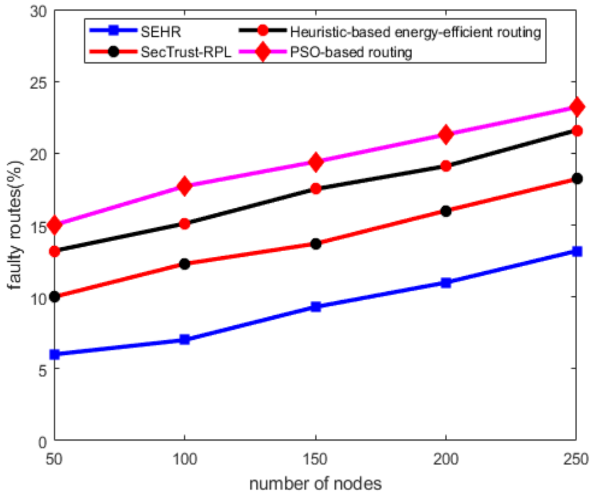


FIGURE 10. Faulty routes and the number of nodes.

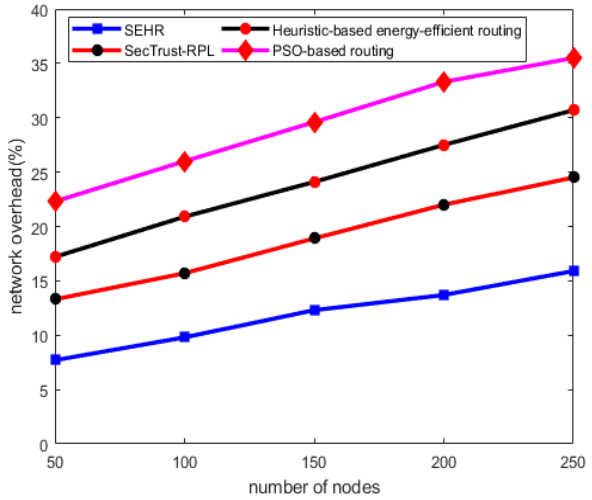


FIGURE 12. Network overhead and the number of nodes.

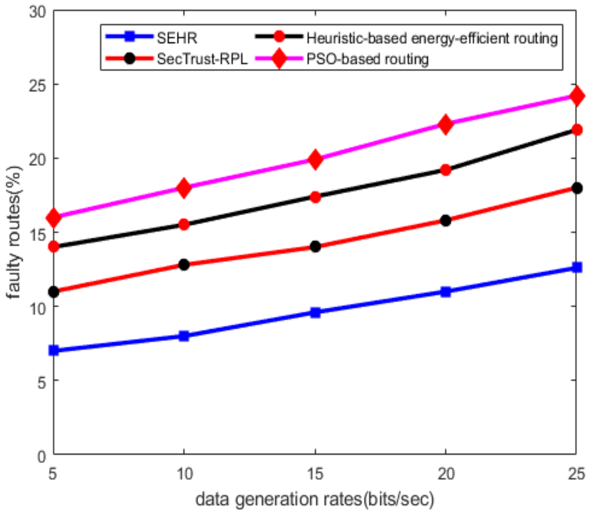


FIGURE 11. Faulty routes and data generation rates.

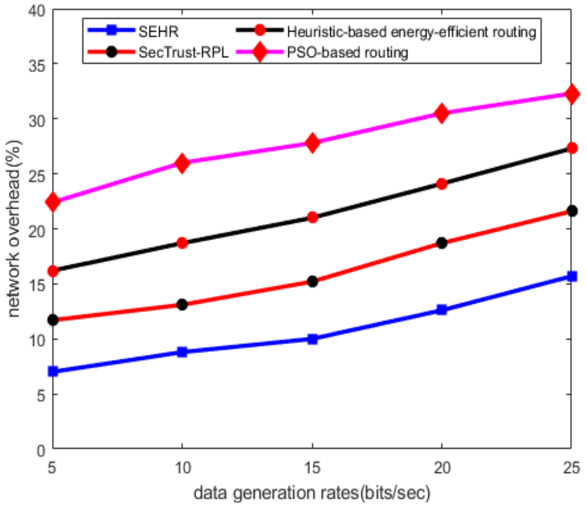


FIGURE 13. Network overhead and data generation rates.

nodes by an average of 39% and 33% respectively. This is due to the SEHR protocol stabilized the routing paths for a long time because of the intelligent and fault-tolerant routing strategy. Such a strategy minimizes the ratio of additional energy consumption in RREQ and response packets and ultimately nodes with higher energy levels are appointed as data forwarders. Unlike other solutions that overlooked the link integrity and consumed excessive energy consumption on the maintenance of the routing paths due to the undue number of route breakages. Our SEHR protocol utilizes the cryptography hash function in the valuation of link trustworthiness, which results in avoiding many data re-routing practices and make less interference on the transmission links.

E. ANALYSIS OF FAULTY ROUTES

Fig.10 and Fig.11 illustrates the performance of the SEHR protocol with the existing solution to determine faulty routes in terms of a varying number of nodes and data generation rates. It is observed from the experimental results that the SEHR protocol decreases the ratio of faulty or damaged routes by an average of 36% and 40% respectively and increases the level of data security over the routing paths. This is due that the SEHR protocol optimizes the selection of routing paths based on beam-based heuristic function. Moreover, the heuristic function provides intelligent decisions by using multiple parameters including link integrity, which leads to data consistency. Furthermore, the SEHR protocol makes use of energy level alerts and traffic analysis to identify the energy-deficient nodes in the existing routing path and decreases the chances of route breakages. Also, the SEHR protocol offers data security based on CTR mode encryption and ensures reliable and error-free routing with minimal overheads. The SEHR protocol toughens the routing paths with light-weight XoR based data encryption and decryption mathematical operations.

F. ANALYSIS OF NETWORK OVERHEAD

Fig.12 and Fig.13 depict the performance of network overhead for SEHR protocol and other solutions. The performance of such a network metric aims to analyze the cryptography-based communication burden on the sensor nodes. Although, the network overheads increases due to the computational cost of cryptography-based methods, however, it is seen from the simulation results that SEHR protocol improves the network overhead by an average of 46%, and 40% in terms of a varying number of nodes and data generation rates as compared to other solutions. This is due to the utilization of light-weight XoR based computations for data security between sensor nodes. Moreover, the SEHR protocol makes use of the concept of pre-distribution secret keys among sensor nodes, which reduces the usage of memory and no additional processing burden is required on the part of sensor nodes. The SEHR protocol performs secure routing based on CTR mode encryption using the secret key with encryption and decryption functions. Based on CTR mode the SEHR protocol performs the data encryption in a parallel manner and random access to encrypted data. Such a mechanism explicitly decrease the overheads in terms of communication between sensor nodes.

G. ANALYSIS OF COMPUTATIONAL OVERHEAD

Fig.14 and Fig.15 illustrate the performance analysis for computation overhead between SEHR protocol and other solutions. The SEHR is based on two main factors i.e. energy-efficient and secure data transmission, therefore, its communication overhead increases under a varying number of nodes and data generation rates. However, it is seen from the experimental results that SEHR protocol improves its communication overheads by an average of 43%, and 43% as compared to other solutions. This is due to the SEHR protocol makes use of an artificial intelligence-based heuristic beam search method to determine the optimal routing path with predefine search width, which reduces the space and time complexity of the solution. The proposed solution significantly decreases the additional communication overhead in routing performance due to the incorporation of the link integrity factor in heuristics function. Also, the XoR operation using lightweight CTR mode, the SEHR decreases the computational burdens of sensor nodes for providing data security in the presence of malicious nodes.

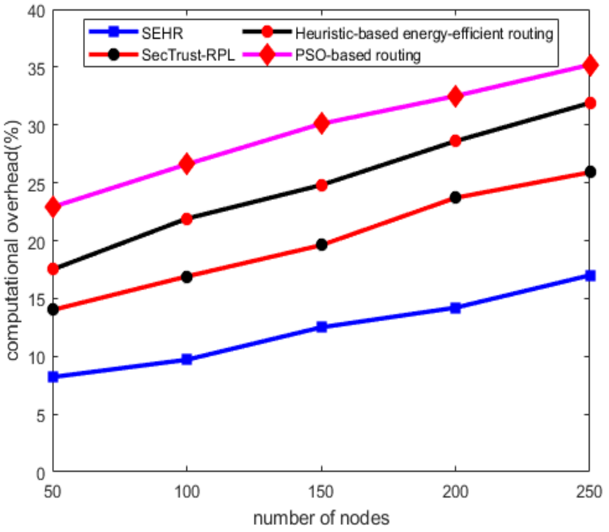


FIGURE 14. Computational overhead and the number of nodes.

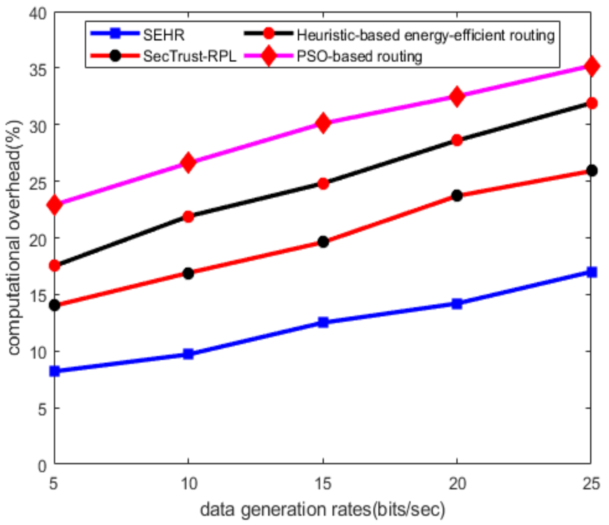


FIGURE 15. Computational overhead and data generation rates.

V. CONCLUSION

The paper presents a secure and energy-aware heuristic routing protocol for WSN, which aims to optimize the routing strategy with the intelligent decision against malicious nodes. The SEHR protocol focuses on critical factors such as energy consumption, secure data delivery, and route maintenance, which are the essential constraints to achieve reliable and trusted transmission for WSN. The SEHR protocol provides artificial intelligence-based heuristic function, which uses residual energy, hop count to BS, and link integrity factors to improve the network performance in terms of data routing and reliable transmissions. Also, the analysis of traffic exploration in the vicinity of the BS helps to prevent the network disjoining and improves route maintenance. Moreover, the SEHR protocol provides data security based on light-weight, simple, and randomness characteristics of the counter mode encryption algorithm. The simulation-based experiments are conducted based on the number of nodes and data generation rates. In the future, we aim to improve the SEHR protocol by using some light-weight machine learning-based techniques to make the network more intelligent with fault-tolerability. Also, the energy efficiency and routing performance can be further improved by considering asynchronous duty cycles between the sensor nodes.

REFERENCES

[1] O. I. Khalaf and B. M. Sabbar, "An overview on wireless sensor networks and finding optimal location of nodes," *Periodicals Eng. Natural Sci.*, vol. 7, no. 3, pp. 1096–1101, 2019.

[2] B. Bhushan and G. Sahoo, "Routing protocols in wireless sensor networks," in *Computational Intelligence in Sensor Networks*. Berlin, Germany: Springer, 2019, pp. 215–248.

[3] X. Liu, T. Qiu, and T. Wang, ''Load-balanced data dissemination for wireless sensor networks: A nature-inspired approach,'' *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9256–9265, Dec. 2019.

[4] V. Chetlapalli, K. S. S. Iyer, H. Agrawal, and S. Patil, ''A new approach to modeling time dependent problems in wireless broadband networks,'' in *Proc. ACM Workshop Distrib. Inf. Process. Wireless Netw. (DIPWN)*, 2017, pp. 1–6.

[5] B. P. Rimal, M. Maier, and M. Satyanarayanan, ''Experimental testbed for edge computing in fiber-wireless broadband access networks,'' *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 160–167, Aug. 2018.

[6] J.-A. Fernandez-Prieto, J. Cañada-Bago, and M.-A. Gadeo-Martos, ''Wireless acoustic sensor nodes for noise monitoring in the city of linares (Jaén),'' *Sensors*, vol. 20, no. 1, p. 124, Dec. 2019.

[7] S. Dutt, S. Agrawal, and R. Vig, ''Cluster-head restricted energy efficient protocol (CREEP) for routing in heterogeneous wireless sensor networks,'' *Wireless Pers. Commun.*, vol. 100, no. 4, pp. 1477–1497, 2018.

[8] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, ''Trust-based secure clustering in WSN-based intelligent transportation systems,'' *Comput. Netw.*, vol. 146, pp. 151–158, Dec. 2018.

[9] S. K. Singh, P. Kumar, and J. P. Singh, ''An energy efficient protocol to mitigate hot spot problem using unequal clustering in WSN,'' *Wireless Pers. Commun.*, vol. 101, no. 2, pp. 799–827, Jul. 2018.

[10] S. Kumar, ''Compartmental modeling of opportunistic signals for energy efficient optimal clustering in WSN,'' *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 173–176, Jan. 2018.

[11] B. K. Gupta, S. Patnaik, M. K. Mallick, and A. K. Nayak, ''Dynamic routing algorithm in wireless mesh network,'' *Int. J. Grid Utility Comput.*, vol. 8, no. 1, pp. 53–60, 2017.

[12] E. Akin and T. Korkmaz, ''Comparison of routing algorithms with static and dynamic link cost in SDN,'' in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–8.

[13] T. Nebbou, M. Lehsaini, and H. Fouchal, ''Partial backwards routing protocol for VANETs,'' *Veh. Commun.*, vol. 18, Aug. 2019, Art. no. 100162.

[14] M. Rath, B. K. Pattanayak, and B. Pati, ''Energetic routing protocol design for real-time transmission in mobile ad hoc network,'' in *Computing and Network Sustainability*. Singapore: Springer, 2017, pp. 187–199.

[15] W. B. Gong, X. L. Yang, M. Zhang, and K. Long, ''Multi-path routing protocol based on adaptation mechanism of cell in ad hoc networks,'' *J. Commun.*, vol. 35, no. 6, pp. 56–63, 2019.

[16] S. Salari-Moghaddam, H. Taheri, and A. Karimi, ''Trust based routing algorithm to improve quality of service in DSR protocol,'' *Wireless Pers. Commun.*, vol. 109, no. 1, pp. 1–16, Nov. 2019.

[17] K. Haseeb, N. Islam, T. Saba, A. Rehman, and Z. Mehmood, ''LSDAR: A light-weight structure based data aggregation routing protocol with secure Internet of Things integrated next-generation sensor networks,'' *Sustain. Cities Soc.*, vol. 54, Mar. 2020, Art. no. 101995.

[18] M. Kocakulak and I. Butun, ''An overview of wireless sensor networks towards Internet of Things,'' in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2017, pp. 1–6.

[19] I. Ud Din, M. Guizani, B.-S. Kim, S. Hassan, and M. Khurram Khan, ''Trust management techniques for the Internet of Things: A survey,'' *IEEE Access*, vol. 7, pp. 29763–29787, 2019.

[20] S. Pirbhulal, H. Zhang, M. E Alahi, H. Ghayvat, S. Mukhopadhyay, Y.-T. Zhang, and W. Wu, ''A novel secure IoT-based smart home automation system using a wireless sensor network,'' *Sensors*, vol. 17, no. 12, p. 69, Dec. 2016.

[21] J. Qian, H. Xu, and P. Li, ''A novel secure architecture for the Internet of Things,'' in *Proc. Int. Conf. Intell. Netw. Collaborative Syst. (INCoS)*, Sep. 2016, pp. 311–314.

[22] R. Bisiani, ''Beam search,'' in *Encyclopedia of Artificial Intelligence*, S. Shapiro, Ed. Hoboken, NJ, USA: Wiley, 1987, pp. 56–58.

[23] H. Lipmaa, P. Rogaway, and D. Wagner, ''Comments to NIST concerning AES modes of operations: CTR-mode encryption,'' in *Proc. Symmetric Key Block Cipher Modes Operation Workshop*, Baltimore, MD, USA, 2000.

[24] I. A. Ridhawi, M. Aloqaily, and A. Boukerche, ''Comparing fog solutions for energy efficiency in wireless networks: Challenges and opportunities,'' *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 80–86, Dec. 2019.

[25] I. Jawhar, N. Mohamed, and J. Al-Jaroodi, ''Networking architectures and protocols for smart city systems,'' *J. Internet Services Appl.*, vol. 9, no. 1, p. 26, Dec. 2018.

[26] A. Onasanya, S. Lakkis, and M. Elshakankiri, ''Implementing IoT/WSN based smart saskatchewan healthcare system,'' *Wireless Netw.*, vol. 25, no. 7, pp. 3999–4020, Oct. 2019.

[27] D. C. Huang, Y. Y. Chu, Y. K. Tzeng, and Y. Y. Chen, ''Secure routing for WSN-based tactical-level intelligent transportation systems,'' *J. Internet Technol.*, vol. 20, no. 4, pp. 1013–1026, 2019.

[28] M. Afsar, M.-H. Tayarani-N., and M. Aziz, ''An adaptive competition-based clustering approach for wireless sensor networks,'' *Telecommun. Syst.*, vol. 61, no. 1, pp. 181–204, Jan. 2016.

[29] A. Hamzah, M. Shurman, O. Al-Jarrah, and E. Taqieddin, ''Energy-efficient Fuzzy-Logic-Based clustering technique for hierarchical routing protocols in wireless sensor networks,'' *Sensors*, vol. 19, no. 3, p. 561, Jan. 2019.

[30] I. Al Ridhawi, S. Otoum, M. Aloqaily, Y. Jararweh, and T. Baker, ''Providing secure and reliable communication for next generation networks in smart cities,'' *Sustain. Cities Soc.*, vol. 56, May 2020, Art. no. 102080.

[31] H. Bany Salameh, R. Derbas, M. Aloqaily, and A. Boukerche, ''Secure routing in multi-hop IoT-based cognitive radio networks under jamming attacks,'' in *Proc. 22nd Int. ACM Conf. Model., Anal. Simul. Wireless Mobile Syst. (MSWIM)*, 2019, pp. 323–327.

[32] D. Airehrour, J. A. Gutierrez, and S. K. Ray, ''SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things,'' *Future Gener. Comput. Syst.*, vol. 93, pp. 860–876, Apr. 2019.

[33] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, ''A novel security protocol for wireless sensor networks with cooperative communication,'' *Computers*, vol. 9, no. 1, p. 4, Jan. 2020.

[34] D.-G. Zhang, H.-L. Niu, and S. Liu, ''Novel PEECR-based clustering routing approach,'' *Soft Comput.*, vol. 21, no. 24, pp. 7313–7323, Dec. 2017.

[35] D. R. Edla, M. C. Kongara, and R. Cheruku, ''A PSO based routing with novel fitness function for improving lifetime of WSNs,'' *Wireless Pers. Commun.*, vol. 104, no. 1, pp. 73–89, Jan. 2019.

[36] J.-S. Lee and C.-L. Teng, ''An enhanced hierarchical clustering approach for mobile sensor networks using fuzzy inference systems,'' *IEEE Internet Things J.*, vol. 4, no. 4, pp. 1095–1103, Aug. 2017.

[37] A. H. El and A. Najid, ''Fuzzy logic based clustering algorithm for wireless sensor networks,'' in *Sensor Technology: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2020, pp. 351–371.

[38] H. El Alami and A. Najid, ''ECH: An enhanced clustering hierarchy approach to maximize lifetime of wireless sensor networks,'' *IEEE Access*, vol. 7, pp. 107142–107153, 2019.

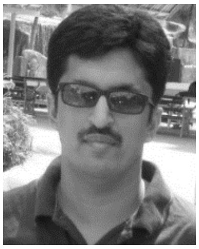
[39] H. Kuhlani, X. Wang, A. Hawbani, and O. Busaileh, ''Heuristic data dissemination for mobile sink networks,'' *Wireless Netw.*, vol. 26, no. 1, pp. 479–493, Jan. 2020.

[40] G. S. Binu and B. Shajimohan, ''A novel heuristic based energy efficient routing strategy in wireless sensor network,'' *Peer–Peer Netw. Appl.*, Jun. 2020, doi: 10.1007/s12083-020-00939-w.

[41] H. Lipmaa, P. Rogaway, and D. Wagner, ''CTR-mode encryption,'' in *Proc. 1st NIST Workshop Modes Operation*, 2000, pp. 1–4.

[42] W. Koehrsen. (2019). *The Poisson Distribution and Poisson Process Explained*. [Online]. Available: https://towardsdatascience.com/the-poissondistribution-and-poisson-process-explained-4e2cb17d459

[43] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, ''Energy-efficient communication protocol for wireless microsensor networks,'' in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2000, pp. 1–10.



KHALID HASEEB received the M.S. degree in IT from the Institute of Management Sciences, Peshawar, Pakistan, and the Ph.D. degree in computer science from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia, in 2016. He is currently working as an Assistant Professor with the Department of Computer Science, Islamia College Peshawar, Pakistan. He has experience of several years in teaching, research, and development. His research areas include wireless sensor networks, ad-hoc networks, network security, the Internet of Things, software defined networks, and sensors-cloud. He involves a referee for many reputed international journals and conferences. He won the Best Student Award in Convocation 2016, UTM.

KHALED MOHAMAD ALMUSTAFA (Associate Member, IEEE) received the B.E.Sc. degree in electrical engineering and the M.E.Sc. and Ph.D. degrees in wireless communication from the University of Western Ontario, London, ON, Canada, in 2003, 2004, and 2007, respectively. He is currently working as an Associate Professor with the Department of Information Systems (IS), College of Computer Science and Information Systems (CCIS), Prince Sultan University (PSU), Riyadh, Saudi Arabia. He has served as a General Supervisor for the Information Technology and Computer Services Center (ITCS), PSU, the Chairman for the Department of Communication and Networks Engineering (CME), and the Vice Dean for the College of Engineering, PSU. He is also the Director of the Research and Initiatives Center, PSU. His research interests include error performance evaluation of MIMO communication systems in partially known channels, adaptive modulation, and channel security, text recognition models, and control systems with renewable energy applications, as well as features selections and data prepossessing.

ZAHOOR JAN received the M.S. and Ph.D. degrees from FAST University, Islamabad, in 2007 and 2011, respectively. He is currently an Associate Professor and the Chairman of computer science with Islamia College Peshawar, Pakistan. His current research interests include image processing, machine learning, computer vision, artificial intelligence, medical image processing, and biologically inspired ideas, such as genetic algorithms, artificial neural networks, cloud computing, and the Internet of Things. He involves a referee for many reputed international journals and conferences.

TANZILA SABA (Senior Member, IEEE) received the Ph.D. degree in document information security and management from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia, in 2012. She is currently serving as an Associate Professor and the Associate Chair of the Information Systems Department, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia. Her primary research focus in recent years is medical imaging, MRI analysis, and soft-computing. She has two hundred ISI/SCEI publications that have around 4000 citations with H-index 40. Her mostly publications are in biomedical research published in ISI/SCIE indexed. She won the Best Student Award from the Faculty of Computing UTM for 2012. Due to her excellent research achievement, she is included in Marquis Who's Who (S & T) 2012. She is also an Editor and a Reviewer of reputed journals and on the panel of TPC of international conferences. She has full command of a variety of subjects and taught several courses at the graduate and postgraduate levels. On the accreditation side, she is a skilled lady with ABET & NCAAA quality assurance. She is the Leader of the Artificial Intelligence and Data Analytics Laboratory.

USMAN TARIQ received the Ph.D. degree in information and communication technology in computer science from Ajou University, South Korea. He has strong background in ad hoc networks and network communications. He has experienced in managing and developing projects from conception to completion. He have worked on a large international scale and long-term projects with multinational organizations. He is currently a Skilled Research Engineer with Ajou University. He is also attached as an Associate Professor with the College of Computer Engineering and Science, Prince Sattam bin Abdulaziz University. His research interests span networking and security fields. His current research is focused on several network security problems: botnets, denial-of-service attacks, and IP spoofing. Additionally, he is interested in methodologies for conducting security.