Received May 23, 2019, accepted June 10, 2019, date of publication June 14, 2019, date of current version July 1, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2922971

Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs

KHALID HASEEB[1], NAVEED ISLAM[1], AHMAD ALMOGREN[2], (Senior Member, IEEE), IKRAM UD DIN[3], (Senior Member, IEEE), HISHAM N. ALMAJED[2], AND NADRA GUIZANI[4]

[1]Department of Computer Science, Islamia College University, Peshawar 25000, Pakistan
[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
[4]Department of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907, USA

Corresponding authors: Ahmad Almogren (ahalmogren@ksu.edu.sa) and Ikram Ud Din (ikramuddin205@yahoo.com)

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through ViceDeanship of Scientific Research Chairs.

ABSTRACT Internet of Things (IoT) enables modern improvements in smart sensors, RFID, Internet technologies, and communication protocols. Sensor nodes are treated as smart devices and widely used to gather and forward sensed information. However, besides intrinsic constraints on sensor nodes, they are vulnerable to a variety of security threats. This paper presents an energy-aware and secure multi-hop routing (ESMR) protocol by using a secret sharing scheme to increase the performance of energy efficiency with multi-hop data security against malicious actions. The proposed protocol comprises three main aspects. First, the network field is segmented into inner and outer zones based on the node location. Furthermore, in each zone, numerous clusters are generated on the basis of node neighborhood vicinity. Second, the data transmission from cluster heads in each zone towards the sink node is secured using the proposed efficient secret sharing scheme. In the end, the proposed solution evaluates the quantitative analysis of data links to minimize the routing disturbance. The presented work provides a lightweight solution with secure data routing in multi-hop approach for the IoT-based constrained wireless sensor networks (WSNs). The experimental results demonstrate the efficacy of proposed energy-aware and secure multi-hop routing protocol in terms of network lifetime by 38%, network throughput by 34%, energy consumption by 34%, average end-to-end delay by 28%, and routing overhead by 36% in comparison with the existing work.

INDEX TERMS WSN, clusters formation, multi-hop, secret sharing, secure routing, route maintenance.

I. INTRODUCTION

Wireless Sensor Network (WSN) comprises numerous sensor nodes that are linked in temporary and ad-hoc manner to sense information and forward the collected information towards a central location called base station (BS) or sink node. Unlike other traditional wireless networks [1], [2], there are a lot of constraints imposed on sensor nodes [3]–[6] with respect to their processing power, energy resources, memory, and storage capabilities. Actually, the basic goal of WSNs is to distribute sensor nodes randomly in unattended locations and provides the connectivity wirelessly. In traditional networks, different routing algorithms are developed to increase the performance and development of network in terms of latency and delivery ratio. As structure of Internet of Things (IoT) is complex and more dynamic in an unreliable wireless environment, such traditional algorithms are not appropriate for IoT applications [7], [8]. Due to the rapid development in IoT systems, numerous information and network threats exist that obstruct its growth [9], [10]. Basically, data aggregation [11]–[14] and forwarding schemes can be classified into two main categories. Firstly, structure-free scheme, which collects the sensor information without any fixed structure and performs data aggregation based on the only partial information. Secondly, structure based scheme that divides the network field into different areas recognized as clusters. Inside each area, there is a unique local data-aggregator [15]–[18] node that collects data from all its associated members and performs accumulation functions. Afterwards, it transmit the aggregated information to sink node via an established

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Shuja.

communication link. In most of the WSN applications, sensor nodes operate individually and expose to various security threats. Although, different secure routing protocols are developed for wireless sensor networks [19]–[22], they require some standard cryptography and authentication methods, and leads to high processing capability and routing cost [23], [24]. Furthermore, such a solution does not consider secure communications on multi points against malicious nodes. As compared to single-hop communications, almost all existing solutions present multi-hop data forwarding. The reason behind this solution is because of constraint resources of sensor nodes, they have to negotiate multi-hops. However, it might happen that the forwarding node is malicious or compromised, which results in disrupting the normal operations of the network. Thus, a secure and energy-aware multi-hop routing protocol is required to exploit the hurdles for security threats in a randomized and untrustworthy environment of IoT based WSNs.

The objective of this research article is to present energy-aware and secure multi-hop routing (ESMR) protocol by using the XOR based secret sharing scheme to provide energy efficiency and reliable forwarding via secure intermediate nodes against data threats. The main contributions of the ESMR protocol in comparison with other protocols are as follows. Firstly, the ESMR protocol segments network nodes into inner and outer zones based on distance. In addition, each zone is further decomposed into different clusters using the nearest neighborhood locality. The rationale behind such nodes segmentation is to provide energy efficiency and improved network communication with minimal delay. Secondly, to cope with security and data privacy among resource constraints sensor nodes, ESMR presents a lightweight XOR based secret sharing scheme. The proposed secret sharing scheme provides data protection against malicious nodes between cluster heads and BS in a multi-hop approach through XOR mathematical operations, which results in a reliable end-to-end connection. The main aim to use the XOR operation in the proposed solution is to achieve measured calculations in cryptography with the simplest way. Moreover, the XOR encryption is easier to implement and requires less computational power in the limited resources of sensor nodes. In the end, the route maintenance scheme is accomplished to minimize the routing interruption based on quantitative analysis of the network nodes.

The said contributions of ESMR protocol provides a notable impact on the wireless medium and unreliable observing regions. Furthermore, the proposed protocol presents an improved network strength with fool-proof secure data routing in multi-hop manner under the existence of malicious threats. The rest of the paper is organized as follows. Related work is discussed in Section 2. Motivation with problem formulation is presented in Section 3. Section 4 introduces the proposed ESMR protocol with its architecture and algorithms. Section 5 presents network assumptions and model. Results and discussion of the proposed solution in comparison with the existing work is presented in Section 6. In the end, Section 7 highlights the conclusion with future directions.

II. RELATED WORK

Recently, the wireless technology provided an opportunity to design and maintain the coverage area due to low cost smart devices. Smart devices are known as sensor nodes that have various functionalities with some constraints. Sensor nodes are interconnected in ad-hoc infrastructures via wireless links to capture the information, process it, and send it back towards the BS or sink node. Nowadays, sensor nodes are broadly explored in various applications, i.e., smart homes, smart cities, agriculture, military, and healthcare.

Different solutions have been presented by researchers for WSNs to facilitate the community in various domains. However, because of the constrained battery power on the part of sensor nodes, mostly proposed solutions have compromised network lifetime. As a result, many researchers are focused to design and implement the solutions in order to prolong the energy efficiency with improved data delivery performance. Furthermore, as sensor nodes perform communications in open media, malicious nodes can capture the information or even interrupt the data transmission. Although different solutions are presented to secure wireless sensor communication, most of them have network and computational overheads. In addition, the presented solutions provide end-to-end secure communications without evaluating the security on intermediate nodes. Intermediate nodes are treated as forwarders and it might happen that they are compromised. In such condition, the forwarders may expose secret information to stripy nodes. Security threats can be divided into active or passive attacks. In a passive attack, a malicious node only captures confidential data, while on the other hand, in active attacks, a malicious node first captures the information and then changes it and further transmits to its neighbor nodes. Therefore, applying security in a distributed and multi-hop manner by imposing a lightweight solution is another challenging task.

In recent years, cluster based solutions have been presented by the research community for the improvement of network scalability, network lifetime, and communication overheads. However, the proposed solutions are overlooked in security perspective, as open media are full of network threats and malicious activities. In the cluster formation process, the selection of cluster head is the leading part as it has to perform various other activities rather than its local information gathering.

Being a central point for all activities within a cluster [25], [26], cluster heads tend to be overloaded with abundant data traffic and they are vulnerable to quick energy depletion. In addition, cluster heads in wireless communications may be compromised and are vulnerable to network attacks. Thus, discovering a secure and energy efficient routing path between end-to-end points is the demanding task [27], [28]. Moreover, the detection of malicious nodes leads to reliable routing, minimizing re-transmissions and delays.

The first dynamic routing protocol was the low energy adaptive clustering hierarchy (LEACH) [29] that comprises numerous data transmission rounds. In LEACH, clusters are formulated based on random manner. The cluster head position is rotated by using a fixed time period. The presented solution improves the network maintenance and energy efficiency in comparison with traditional algorithms. However, the network load is not uniformly distributed among clusters. Later, PEGASIS [30], which is a modified version of LEACH, was presented wherein all nodes are organized in the kind of a chain by using greedy algorithm. All nodes can send and receive data via their next-hops and all of them are considered that they have inclusive information of the entire sensor field. The construction of the routing chain is initiated from a further node from the BS, and whenever any node inside a chain drops its energy to certain threshold, the routing chain is again reconstructed. The main problem of this solution is the delay ratio as it is not applicable for vast network nodes density scenarios. The proposed LEACH-ensuring reliable data delivery (LEACH-ER) [31] aims to select the cluster head by using compound factors, i.e., energy and data reliability. The basic theme of the proposed solution is to reduce the packet reception rate with a cluster boundary between cluster heads and member nodes, which may lead to improved network lifetime and balanced energy consumption. However, the constructed routes are non-optimal and incur additional overheads and route breakages.

In the ambient trust sensor routing (ATSR) [32], the authors presented an energy and trust-aware routing protocol. To detect malicious nodes, the presented solution proposes a distributed secure routing protocol and evaluates the trust value of neighbors based on trust metrics. The ATSR protocol is feasible for large scale networks, as the decision is made by using local information of neighbors. However, this protocol incurs higher network traffic due to the flooding of route request and route response packets and lead to maximize energy consumption.

A friendship based AODV (Fr-AODV) protocol [33] is presented to counter network threats and malicious nodes over the routing path. By using node reputation and node Identity factors, a trust value is evaluated. Further, an attribute number is given to individual features, which is forwarded along with the actual data. Upon receiving, if the attribute number is matched, then the data is forwarded to the neighbor node. However, the Fr-AODV protocol uses an analogous route maintenance strategy, it suffers from route re-discoveries and re-transmissions.

Trust-aware secure routing framework (TSRF) [34] is proposed to cope with the misbehavior of malicious nodes. To evaluate the nodes' trustworthiness, both direct and indirect trusts are integrated by TSRF. In addition, an inconsistence check mechanism is incorporated in the security framework of TSRF to avoid threats from malicious nodes. TSRF solely classifies malicious nodes in a multi-hop manner, however, constraint resources of WSN in data routing are overlooked, which leads to a compromised network lifetime.

In another paper, secure and energy-efficient multi path routing (SEER) [35] protocol is presented, which aims to utilize constraint resources of WSN in an efficient manner. The proposed solution makes use of multi-path among nodes for data routing and may lead to the issue of network lifetime. Nodes forward the captured information towards the sink node by exploiting their routing tables. Furthermore, based on the number of sent/received data packets in a routing path, the BS updates the status of residual energy. SEER protocol improves network consistency with respect to network lifetime and data delivery performance, however, it incurs additional overheads due to the construction of multi path. In addition, SEER lacks the capability to adapt network measurement, which results in routes uncertainty and breakages.

III. MOTIVATIONS AND PROBLEM FORMULATION

By exploring the literature review, it is determined that most of the presented solutions do not offer tolerable security measures for consistent and secure data delivery performance. Furthermore, these schemes are proposed for traditional wireless networks, thus, the applied cryptographic techniques are not appropriate for resource constraint sensor networks. In addition, to achieve a reliable data routing, the presented schemes incur high communication cost with network overheads by interchanging numerous route request and route reply updates. Also, many of these solutions do not consider the dynamic nature of sensor nodes and may lead to network congestion and frequent route rediscoveries. Most of the proposed secure algorithms evaluate their performance with standard routing protocols [36], [37], i.e., LEACH, DSR, and AODV. We claim that such a comparison is not admissible because the findings of network threats and malicious nodes are out of the scope for the traditional data routing schemes.

Thus, the main impact of the proposed solution is to design a lightweight energy efficient and secure protocol for WSNs in multi-hop environment. The proposed solution neither impose too many computational overheads on constraint nodes nor involves a specialized set of resources. Furthermore, the proposed solution measures network conditions on demand and dynamic detection of network threats, which may lead to improved energy efficiency and network throughput.

IV. PROPOSED ENERGY-AWARE AND MULTI-HOP SECURE ROUTING PROTOCOL

A short-term introduction of the proposed energy-aware and secure multi-hop routing (ESMR) protocol based on secret sharing scheme for restricted WSNs is discussed in this section. The details of all its components are to be discussed in the following subsections. The network nodes are decomposed into inner and outer zones based on the distance factor in the first component.

Further, by using k-nearest neighbors (k-NN) algorithm, the nodes inside each zone are organized into various clusters. All the clusters are arranged in a hierarchical form to accomplish a subsequent data routing. In the second component,

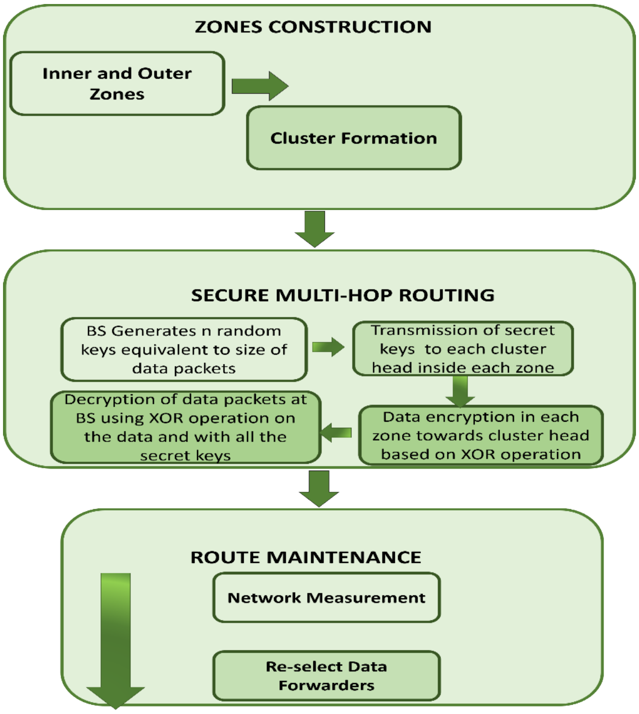
ZONES CONSTRUCTION
Inner and Outer Zones
Cluster Formation
SECURE MULTI-HOP ROUTING
BS Generates n random keys equivalent to size of data packets
Transmission of secret keys to each cluster head inside each zone
Data encryption in each zone towards cluster head based on XOR operation
Decryption of data packets at BS using XOR operation on the data and with all the secret keys
ROUTE MAINTENANCE
Network Measurement
Re-select Data Forwarders

FIGURE 1. ESMR Protocol Block Diagram.

the main aim is to balance the relationship between the energy consumption and reliable data forwarding, and to propose a secure multi-hop routing approach in an energy efficient manner against malicious threats. It gives a lightweight solution based on the XOR secret sharing scheme in constrained sensor nodes. In addition, it does not impose additional computational overheads on the network. In the third component, route maintenance is performed to identify faulty links in the constructed routing paths and decrease the chances of route breakages and re-transmissions. In such a case, the proposed protocol re-adjusts the forwarders based on the quantifiable measurement and may lead to improved network lifetime with enhanced route reliability. The presented experimental results outperform the existing approaches. Fig.1 depicts the ESMR protocol block diagram.

A. REGION BASED ZONES CONSTRUCTION

The n number of nodes is dispersed randomly to coverage the monitoring square sized area. After the deployment, all nodes are fixed with unique identities. The nodes have homogeneity in characteristics and limited constraints, while the sink node has the most powerful features with no resources restriction. In the beginning, the BS sends its identity and position information in the sensor field using a multi-hop manner. All nodes received the information of BS via their next-hop and store it in their routing tables. The routing tables of nodes are update based on their neighbor conditions. Afterwards, the boundary of each zone is constructed on the basis of dynamic distance threshold from the BS, as shown in equation 1.

$$(\beta - 1)\alpha < Z_\beta < \alpha\beta \tag{1}$$

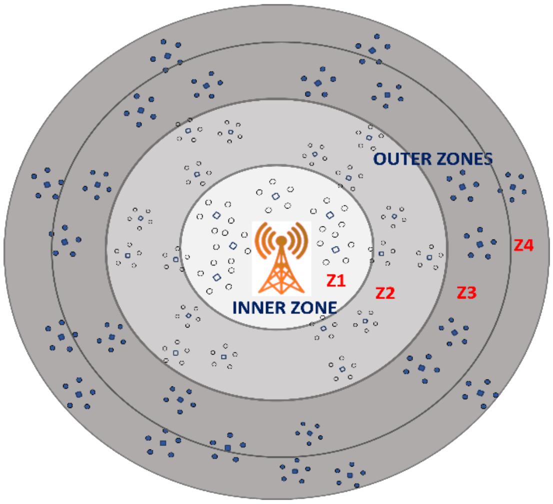

FIGURE 2. Generations of inner outer zones and clusters formulation.

where β represents the zones $\beta^{\in}(1, 2, \ldots \mathrm{n})$ and α is the preset distance. Suppose, for second zone, i.e., zone-2, $\beta = 2 \Leftrightarrow \alpha < Z_2 < 2\alpha$. Accordingly, n number of zones will be constructed around the BS in a circular form. The inner zone requires less transmission power to send data towards the BS directly. However, outer zones make use of their upper zones as intermediates for the transmission of sensory information in an energy efficient manner. Subsequently, the constructed zones are further decomposed into numerous clusters based on the lightweight and simple k-nearest neighbors (k-NN) algorithm, as revealed in Fig.2.

In the proposed solution, the K-NN technique is used to group the nearest neighbors into a particular cluster by using the distance function with low computation cost. The value of K is defined by using square root of the number of nodes in a particular zone. When each zone is decomposed into different clusters, then each cluster is given a unique identity to distinguish it from other clusters. Moreover, to decrease the network cost, a node which is closer to centroid is appointed as an initial cluster head inside each cluster. Basically, the centroid is a virtual node that localizes at the mid position of the cluster. Let $(n_1, n_2, n_3, \ldots, n_k)$, is the set of nodes within a particular cluster c_i. By exploring the nodes spatial positions, the centroid $c(x, y)$ of the cluster is calculated by

$$c(x, y) = \frac{\sum_{i=1}^{k} x_i}{m} + \frac{\sum_{i=1}^{k} y_i}{m} \tag{2}$$

where m represents the total number of nodes within a cluster.

B. (n, n) XOR BASED SECRET SHARING SCHEME (SSS) FOR MULTI-HOP SECURE DATA ROUTING

After segmenting the region around the BS into different circular zones, Z_β, the nearest region is assigned to be the zone '$Z_{\beta=1}$', followed by '$Z_{\beta=2}$' and so on till '$Z_{\beta=n}$'. If the data packet size is k bits and the total number of zones around the BS is ' n', then the proposed (n, n) XOR based secret sharing scheme for multi-hop routing is given by the following steps:

i. The BS generates n random secret keys ($S_1, \ldots, S_n$), each has an equivalent size to the data packet of 'k' bits. These keys are transmitted to the corresponding cluster heads in each zone, Z_β.

ii. The data D_n from zone 'Z_n' with a size of k bits from the cluster head is encrypte with the zone's secret key S_n by performing the XOR operation, as given in equation 3.

$$E_n = S_n \oplus D_n \tag{3}$$

iii. The encrypted data bits E_n of a particular cluster in zone n, 'Z_n' is forwarder towards the selected cluster head in the corresponding upper zone Z_{n-1}.

iv. When the data arrives at the cluster head in the zone Z_{n-1}, it is encrypted using the zone secret key S_{n-1} by performing the XOR operation, as presented in equation.1.

v. This process of encryption using XOR operation continues from cluster heads in the lowest zones Z_n to the top most zone Z_1
around the BS.

vi. At the top most zone, Z_1, the encrypted data is transmitted to the BS, which can easily be decrypted by performing XOR operations on the data with all secret keys S_i, as present in equation 4.

$$D_i = S_1 \oplus S_2 \oplus S_3, \ldots \oplus E_n \tag{4}$$

The proposed secret sharing scheme can be performed from any zone with the fear of loss of data or inconsistency in performance.

C. ROUTE MAINTENANCE

The component of route maintenance is carried out to lessening the chances of route damages and re-forwarding. If the ESMR feels that a cluster head in the upper zone is not suitable for further data forwarding, then it initiates the discovery of alternate routing path. Mainly, the route maintenance process is called in the subsequent conditions.

i. Firstly, whenever in the upper zone the energy resource of the cluster head is less than the specified threshold, the effected cluster head simply quits the data forwarding process and re-announces the election process within a particular boundary. Afterwards, a node that is nearer to the centroid is elected as a new cluster head and updates its status.

ii. Secondly, the performance of the established link between cluster heads $L_{i,j}$ are also evaluated based on the packet delay variation (PDV) parameter. The PDV gives an absolute value, which is the difference between two consecutive packets belonging to the same communication link. Let us take an example, if packet α is transmitted and it covers t_0 time to cross the network, and packet β is transmitted and that covers t_1 time to cross the network, the PDV can be computed using equation 5.

$$PDV = |t_0(\alpha) - t_1(\beta)| \tag{5}$$

Algorithm 1 Secret Sharing Based Energy-Aware and Secure Multi-Hop Routing Protocol

Inner and Outer Zones

```
Procedure zones_construction(Z)
  compute neighbors distance and produce a routing
  table
  Dynamic Distance (D) = $(\beta - 1)\ \alpha < \quad Z_\beta < \alpha\beta$
  for each node i ∈ [1:D]
  do
        decompose the nodes into particular zones $Z_i$
  end for
  if $Z_i$ [ ]! = Null
    parts the zone nodes into clusters $C_i$ using
    k-NN
  End if
  for each node i ∈ $C_i$
  do
        $c(x, y) = \frac{\sum_{i=1}^{k} x_i}{m} + \frac{\sum_{i=1}^{k} y_i}{m}$
    $Ch_i$ nearest node to $c(x, y)$
  end for
end procedure
```

Secure Multi-hop Routing

```
procedure secure multi-hop routing
  BS generates n random keys ($S_1, \ldots, S_n$),
    $S_i$ key is transmitted to cluster head $Ch_i$ in $Z_i$
  Data packets $D_n$ from zone $Z_i$ with a size of $k$ bits from
   cluster head $Ch_i$ is encrypted with the zone secret key $Z_i$
   using
        $E_n = S_n \oplus D_n$
  Upper most zone $Z_i$ encrypts data and  forwards to BS
  BS decrypts the data using XOR and a set of  secret keys
  $S_i$
end procedure
```

```
procedureroute maintenance
  while on active route
  do
  ifenergy threshold of $Ch_i$ in upper zone
     $Z_i$ < threshold then
   announce re-election for cluster head in particular
   cluster $C_i$
  End if
   Compute $|t_0(\alpha) - t_1(\beta)|$ in link $L_{i,j}$
   iftime out in packet receiving in $L_{i,j}$ then
     re-adjust data forwarders
   End if
end procedure
```

TABLE 1. Default Simulation Parameters.

Parameter	Value
Sensor arena	100 X 100m^2
Deployed nodes	100
Number of Malicious nodes	1 to 5
Transport layer protocol	UDP
E_{elect}	100nJ/ bit
E_{amp}	10nJ/bit/m^2
E_{fs}	0.0013pJ/bit/m^4
Packet size, k	25 bits
Payload size	512 bytes
Initial energy	2J
Simulation time	1000sec
Node's transmission range	25m

All the main components of the ESR protocol is explained in Algorithm 1.

V. NETWORK ASSUMPTIONS AND MODEL

This section measures the efficacy of ESMR protocol against Fr-AODV and TSRF solution using network simulator, NS2. We deployed 100 sensor nodes of homogeneous characteristics with varying malicious nodes from 1 to 5 in the network field. Malicious nodes broadcast false route response such that they are selected as forwarders for data routing. But in reality, they drop the received data packets. Initially, all nodes have 2J energy level, whereas the transmission power for each node is fixed to 25m. To measure the energy utilization over the sensor field, an energy model is utilized. We evaluate the performance results of ESMR against the existing work with respect to network lifetime, network throughput, end to end delay, and routing overhead. The default parameters that are to be used in various simulation experiments are concised in Table 1.

VI. RESULTS AND DISCUSSION

A. NETWORK LIFETIME

Fig.3 illustrates the performance of the proposed ESMR protocol in comparison with Fr-AODV and TSRF solutions in terms of network lifetime. It is seen from experimental results that ESMR protocol increases the performance of network lifetime with an average of 38% as compared to other schemes. This is done because it focusses on both energy efficiency and reliability of the network nodes. Both FR-AODV and TSRF protocols select forwarders without considering network conditions and may lead to the early energy consumption of forwarder thereby result in decreasing lifetime. Unlike other solutions, ESMR selects energy efficient and reliable forwarders in active routing paths. Moreover, the quantitative analysis also makes the energy consumption in a balanced manner among network nodes.

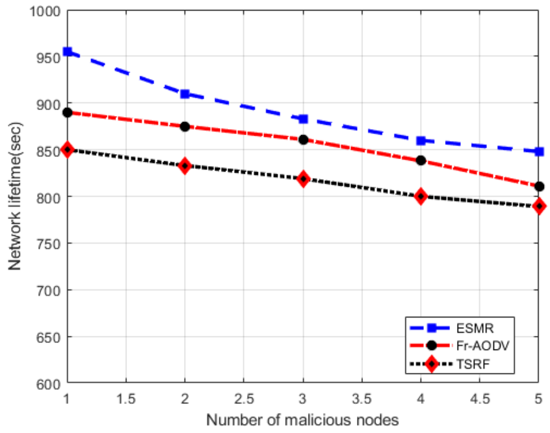

FIGURE 3. Network lifetime in varying malicious nodes.

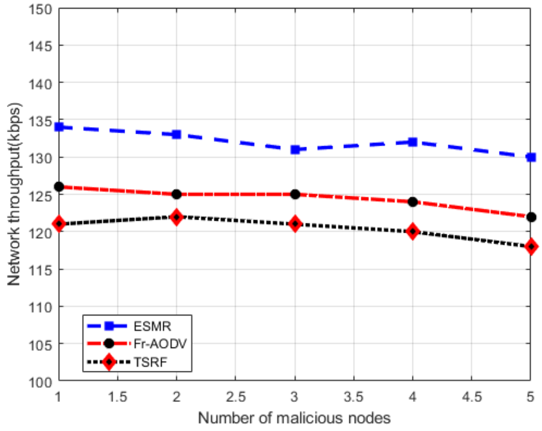

FIGURE 4. Network throughput in varying malicious nodes.

B. NETWORK THROUGHPUT

Fig.4 exhibits the network throughput of the ESMR protocol with the comparison of other solutions under a varying number of malicious nodes. By exploring experimental outcomes, it is seen that the network throughput of ESMR carries a noteworthy influence on the routing protocol performance. It may also be noticed that ESMR made an average of 34% improvement in the network throughput in the evaluation with other solutions. This is due to the fact that ESMR has an energy efficient and robust cluster management along with the incorporation of multi-hop security. The Fr-AODV and TSRF protocols lack to detect network conditions and forward data packets on energy aware and reliable routing paths in the presence of malicious threats, which lead to a decreasing network throughput.

C. ENERGY CONSUMPTION

Fig. 5 explains the assessment of energy consumption in the comparison of ESMR protocol with other schemes. It is realized that ESMR improves the energy consumption as an

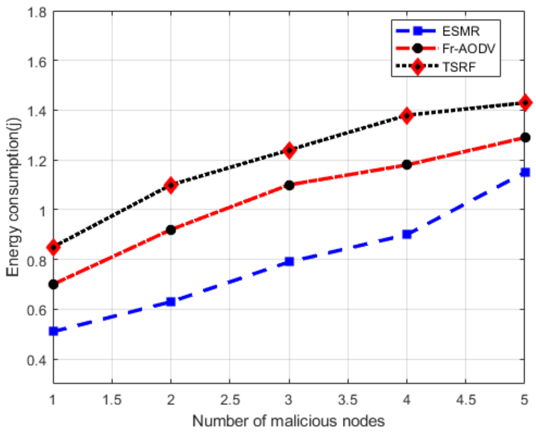

FIGURE 5. Energy consumption in varying malicious nodes.

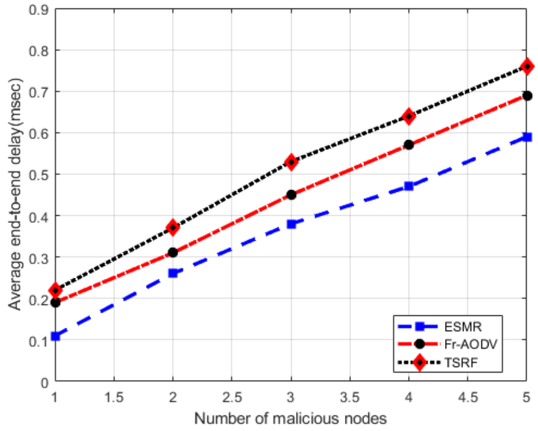

FIGURE 6. Average end-to-end delay in varying malicious nodes.

average of 34% than existing works due to the formation of clusters based on the nearest neighborhood scheme. Fr-AODV and TSRF protocols incur higher number for route breakages, which may lead to extra energy consumption. Furthermore, under the presence of malicious nodes, ESMR outperforms Fr-AODV and TSRF due to the composition of routing paths by incorporating reliable and energy sufficient nodes, which results in reducing re-transmissions and ultimately gives a positive impact of energy utilization.

D. AVERAGE END-TO-END DELAY

The ESMR protocol is evaluated in comparison with the existing solutions under a varying number of malicious nodes with respect to their end-to-end delay. Fig. 6 exhibits that the ESMR protocol achieved 28% average improvement in the end-to-end delay as compared to other solutions under the presence of malicious nodes. Moreover, ESMR outperforms Fr-AODV and TSRF solutions due to the selection of optimal forwarders with shortest routing paths. Fr-AODV and TSRF protocols consume the energy of forwarders more rapidly due to longer routing paths. The longer distance routing paths are more prone to re-transmissions and lead to more end-to-end delay. Furthermore, the existing solutions lack the measurement of quantitative analysis to identify congested and faulty links, which result in bounding the availability of wireless channels for data packets.

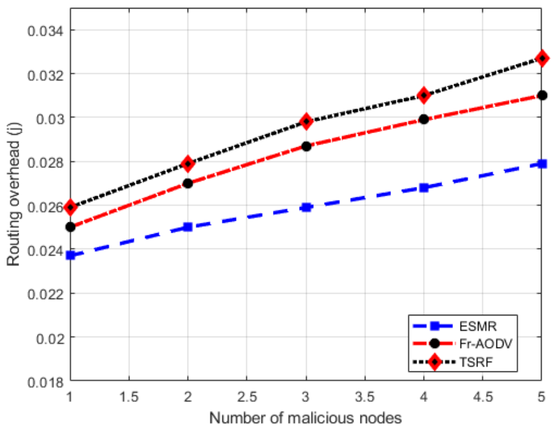

FIGURE 7. Routing overhead in varying malicious nodes.

E. ROUTING OVERHEAD

Routing overhead gives a vital influence on the evaluation of any data forwarding protocol, as the increase in the routing overhead may lead to decreasing energy efficiency and delivery outcomes. Moreover, rises in malicious threats, frequently call of alternate route construction, and re-transmissions are increased. The ESMR improves the performance of routing overhead as an average of 36%, as data forwarding paths are constructed based on reliability and energy efficiency manner (see Fig.7). In addition, ESMR proposes a lightweight XOR cryptography to secure forwarders in resource constraint networks. Fr-AODV and TSRF protocols generate too much call for route re-adjustment because of additional energy consumption among network nodes. Moreover, unpredictable and longer routes in the Fr-AODV and TSRF protocols rise to a high number of route recoveries, which result in high routing overhead that puts a negative impact on the network lifetime.

VII. CONCLUSION

This paper presents the secret sharing based energy-aware and secure multi-hop routing (ESMR) protocol for IoT based WSNs, which aims to achieve reliable and energy-aware routing against the behavior of packet forwarding of malicious nodes. The ESMR protocol generates innner and outer zones based on node locations. Futhermore, using the nearest neighborhood scheme, network nodes are divided into vaious clusters. In addition, the proposed protocol provides a lightweight XOR cryptography to secure data forwarding in a multi-hop manner in resource constraint networks. The ESMR protocol directs forwarders to send data on the shortest route, which comprises of relaible and energy efficient nodes. Futhermore, the proposed protocol evaluates the quantitative analysis for a particular link to identify the congestion over it, which results in decreasing routing disturbance and re-transmissions. The simulation experiments demonstrate the supremacy of ESMR protocol over other existing schemes. For future work, the performance of ESMR needs to be measured in mobile sensors with heterogeneous network architectures.

REFERENCES

[1] T. Meng, F. Wu, Z. Yang, G. Chen, and A. V. Vasilakos, "Spatial reusability-aware routing in multi-hop wireless networks," *IEEE Trans. Comput.*, vol. 65, no. 1, pp. 244–255, Jan. 2016.

[2] M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Athanasios, "Software-defined and virtualized future mobile and wireless networks: A survey," *Mobile Netw. Appl.*, vol. 20, no. 1, pp. 4–18, Feb. 2014.

[3] S. Rani, R. Talwar, J. Malhotra, S. H. Ahmed, M. Sarkar, and H. Song, "A novel scheme for an energy efficient Internet of Things based on wireless sensor networks," *Sensors*, vol. 15, no. 11, pp. 28603–28626, 2015.

[4] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," *J. Netw. Comput. Appl.*, vol. 60, pp. 192–219, Jan. 2016.

[5] R. A. Roseline and P. Sumathi, "Local clustering and threshold sensitive routing algorithm for wireless sensor networks," in *Proc. Int. Conf. Devices, Circuits Syst. (ICDCS)*, Coimbatore, India, Mar. 2012, pp. 365–369.

[6] F. Ruan, C. Yin, J. Chen, J. Wang, and S. Xue, "A distance clustering routing algorithm considering energy for wireless sensor networks," *Int. J. Future Gener. Commun. Netw.*, vol. 6, no. 5, pp. 73–80, 2013.

[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[8] M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 3, no. 1, pp. 45–54, Mar. 2013.

[9] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for Internet of Things," *Comput. Sci. Inf. Syst.*, vol. 8, no. 4, pp. 1207–1228, 2011.

[10] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 17–31, Sep. 2015.

[11] M. Ding, X. Cheng, and G. Xue, "Aggregation tree construction in sensor networks," in *Proc. IEEE 58th Veh. Technol. Conf. (VTC-Fall)*, Oct. 2003, pp. 2168–2172.

[12] A. M. Krishnan and P. G. Kumar, "An effective clustering approach with data aggregation using multiple mobile sinks for heterogeneous WSN," *Wireless Pers. Commun.*, vol. 90, no. 2, pp. 423–434, 2016.

[13] J. Yuea, W. Zhang, W. Xiao, D. Tang, and J. Tang, "Energy efficient and balanced cluster-based data aggregation algorithm for wireless sensor networks," *Procedia Eng.*, vol. 29, pp. 2009–2015, Feb. 2012.

[14] Z. Zhou, J. Tang, L.-J. Zhang, K. Ning, and Q. Wang, "EGF-tree: An energy-efficient index tree for facilitating multi-region query aggregation in the Internet of Things," *Pers. Ubiquitous Comput.*, vol. 18, no. 4, pp. 951–966, 2014.

[15] M. Alagirisamy and C.-O. Chow, "An energy based cluster head selection unequal clustering algorithm with dual sink (ECH-DUAL) for continuous monitoring applications in wireless sensor networks," *Cluster Comput.*, vol. 21, no. 1, pp. 91–103, 2018.

[16] P. K. Batra and K. Kant, "LEACH-MAC: A new cluster head selection algorithm for wireless sensor networks," *Wireless Netw.*, vol. 22, no. 1, pp. 49–60, 2016.

[17] U. Venkanna and R. L. Velusamy, "TEA-CBRP: Distributed cluster head election in MANET by using AHP," *Peer-Peer Netw. Appl.*, vol. 9, no. 1, pp. 159–170, 2016.

[18] K. A. Darabkh, W. S. Al-Rawashdeh, M. Hawa, and R. Saifan, "MT-CHR: A modified threshold-based cluster head replacement protocol for wireless sensor networks," *Comput. Elect. Eng.*, vol. 72, pp. 926–938, Nov. 2018.

[19] M. B. Krishna and M. N. Doja, "Multi-objective meta-heuristic approach for energy-efficient secure data aggregation in wireless sensor networks," *Wireless Pers. Commun.*, vol. 81, no. 1, pp. 1–16, 2015.

[20] K. A. Kumar, A. V. N. Krishna, and K. S. Chatrapati, "New secure routing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks," *J. Inf. Optim. Sci.*, vol. 38, no. 3, pp. 341–365, 2017.

[21] S. Ozdemir, "Secure and reliable data aggregation for wireless sensor networks," in *Proc. Int. Symp. Ubiquitious Comput. Syst.* Berlin, Germany: Springer, 2007.

[22] Z. Yu-Quan and W. Lei, "A new routing protocol for efficient and secure wireless sensor networks," *TELKOMNIKA Indonesian J. Elect. Eng.*, vol. 11, no. 11, pp. 6794–6801, 2013.

[23] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and V. Gupta, "Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography," *J. Ambient Intell. Humanized Comput.*, vol. 9, no. 3, pp. 643–653, 2018.

[24] S. Adamovic, M. Sarac, D. Stamenkovic, and D. Radovanovic, "The importance of the using software tools for learning modern cryptography," *Int. J. Eng. Educ.*, vol. 34, no. 1, pp. 256–262, 2018.

[25] S. Din, A. Paul, A. Ahmad, and J. H. Kim, "Energy efficient topology management scheme based on clustering technique for software defined wireless sensor network," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 2, pp. 348–356, 2019.

[26] K. Babber and R. Randhawa, "Energy efficient clustering with secured data transmission technique for wireless sensor networks," in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2016, pp. 3023–3025.

[27] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, "A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 28, no. 3, pp. 262–275, 2016.

[28] D. He, S. Chan, and M. Guizani, "Cyber security analysis and protection of wireless sensor networks for smart grid monitoring," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 98–103, Dec. 2017.

[29] W. R. Heinzelman and A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, Maui, HI, USA, Jan. 2000, p. 10.

[30] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in *Proc. Aerosp. Conf.*, Mar. 2002, p. 3.

[31] Y. Guo, Y. Liu, Z. Zhang, and F. Ding, "Study on the energy efficiency based on improved LEACH in wireless sensor networks," in *Proc. 2nd Int. Asia Conf. Inform. Control, Automat. Robot. (CAR)*, Mar. 2010, pp. 388–390.

[32] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 69, no. 2, pp. 805–826, 2013.

[33] T. Eissa, S. A. Razak, R. H. Khokhar, and N. Samian, "Trust-based routing mechanism in MANET: Design and implementation," *Mobile Netw. Appl.*, vol. 18, no. 5, pp. 666–677, 2013.

[34] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: A trust-aware secure routing framework in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 1, 2014, Art. no. 209436.

[35] N. Nasser and Y. Chen, "Secure multipath routing protocol for wireless sensor networks," in *Proc. 27th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Jun. 2007, p. 12.

[36] R. Bai and M. Singhal, "DOA: DSR over AODV routing for mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 5, no. 10, pp. 1403–1416, Oct. 2006.

[37] M. Barati, K. Atefi, F. Khosravi, and Y. A. Daftari, "Performance evaluation of energy consumption for AODV and DSR routing protocols in MANET," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, Jun. 2012, pp. 636–642.

KHALID HASEEB received the M.Sc. degree in information technology from the Institute of Management Sciences, Pakistan, and the Ph.D. degree in computer science from the Faculty of Computing, Universiti Teknologi Malaysia, in 2016. During his Ph.D., he was a member of the Pervasive Computing Research Group. Since 2008, he has been with the Computer Science Department, Islamia College Peshawar, Pakistan. His research interests include sensors and ad-hoc networks, network security, cloud computing, and mobile communication. He is a Reviewer for many reputed international journals and conferences.

NAVEED ISLAM received the Ph.D. degree in computer science from the University of Montpellier II, France, in 2011. He is currently an Assistant Professor with the Department of Computer Science, Islamia College University, Peshawar, Pakistan. He has authored numerous international journal and conference articles. His research interests include computer vision, machine learning, artificial intelligence, and data security. He is a Regular Reviewer of IEEE, Elsevier, and Springer Journals.

AHMAD ALMOGREN received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He was an Assistant Professor of computer science and a member of the Scientific Council, Riyadh College of Technology. He also served as the Dean of the College of Computer and Information Sciences and the Head for the Council of Academic, Al Yamamah University. He is currently a Professor and the Vice Dean of development and quality with the College of Computer and Information Sciences, King Saud University. His research interests include mobile and pervasive computing, cyber security, and computer networks. He has served as a Guest Editor at several computer journals.

IKRAM UD DIN (S'15–SM'18) received the M.Sc. degree in computer science and the M.S. degree in computer networking from the Department of Computer Science, University of Peshawar, Pakistan, and the Ph.D. degree in computer science from the School of Computing, Universiti Utara Malaysia (UUM). He also served as the IEEE UUM Student Branch Professional Chair. He has ten years of teaching and research experience in different universities/organizations. His current research interests include resource management and traffic control in wired and wireless networks, vehicular communications, mobility and cache management in information-centric networking, and the Internet of Things.

HISHAM N. ALMAJED received the bachelor's degree in information systems from the College of Computer and Information Sciences, King Saud University, in 2004, and the M.Sc. degree in computer applications and systems administration from the Computer Section, Arabeast Colleges, in 2015. He is currently pursuing the Ph.D. degree in computer science with the College of Computer and Information Sciences, King Saud University. He is also with Saline Water Conversion Corporation Head Quarter, Riyadh, Saudi Arabia, as an Information Technology Governance Team Member. His research interests include computer security and wireless sensor network security. He received several professional certifications, including PMP, CISA, ISO27001 Lead Auditor, ISO27001 Leas Implementer, TOGA9, and ITIL Expert.

NADRA GUIZANI is currently pursuing the Ph.D. degree with Purdue University, where she is also a Graduate Lecturer and completing a thesis in prediction and access control of disease spread data on dynamic network topologies. Her research interests include machine learning, mobile networking, large data analysis, and prediction techniques. She is an Active Member in the Women in Engineering Program and the Computing Research Association for Women.