IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RELIABILITY IN SENSOR-CLOUD SYSTEMS AND APPLICATIONS (SCSA)

Received September 22, 2020, accepted October 7, 2020, date of publication October 12, 2020, date of current version October 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3030192

DDR-ESC: A Distributed and Data Reliability Model for Mobile Edge-Based Sensor-Cloud

KHALID HASEEB[1], IKRAM UD DIN[2], (Senior Member, IEEE), AHMAD ALMOGREN[3], (Senior Member, IEEE), ZAHOOR JAN[1], NAVEED ABBAS[1], AND MUHAMMAD ADNAN[4]

[1]Computer Science Department, Islamia College Peshawar, Peshawar 25000, Pakistan
[2]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[3]Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[4]Division of Computer and Information Sciences, Higher Colleges of Technology, Al Ain 17155, United Arab Emirates

Corresponding author: Ikram Ud Din (ikramuddin205@yahoo.com)

This work was supported by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project number RSP-2020/184.

ABSTRACT Cloud computing gained a lot of growth in the development of scientific and industrial domains due to its scalability, data analysis, portability, and storage abilities. The sensors and actuators facilitate wireless communication with real-time data gathering and local preprocessing. However, the huge amount of data collection and storage for such low powered nodes incurs the problem of reliability and efficient resource management. The technology of cloud computing provides an emerging paradigm for the sensors-based applications to improve processing, management, and storage of massive data. However, sensor nodes are organized and communicate in a distributed environment, which is harmful to network reliability and privacy. Recently, many solutions are presented for data transmissions in distributed systems through link-aware routing, but efficient utilization of network resources is still an open research issue. Also, most of the proposed solutions provide secure transmissions on the cost of computation and routing overhead. In this work, we propose a distributed and data reliability model for mobile edge-based sensor-cloud (DDR-ESC) to grow the data delivery performance and preserve the control of security. Moreover, edge-based communications with the cloud systems make the transmission intelligently and decrease the threshold of packets level overhead with high dependability. The extensive experiments validate the proposed model as compared to the state-of-the-art schemes.

INDEX TERMS Distributed routing, mobile edge nodes, cloud sensors, data reliability, nodes integrity.

I. INTRODUCTION

In recent decades, wireless technologies played an important role in the growth and development of different fields such as the Internet of Things (IoT), wireless sensor networks (WSNs), cloud computing, and smart heterogeneous systems [1]–[4]. Due to automated, self-configure, and lightweight infrastructures, different researchers exploit them in the domain of academics and industries. The wireless devices can be distributed randomly or predefined for observing data towards the central controller referred to as Base Station (BS). Due to the collection of huge observing data, many researchers have proposed cloud-based solutions to increase network scalability and storage. However, the restricted resources of sensor nodes lead to degrading the network performance in terms of energy efficiency and timely data delivery to the application users [5]–[8]. Also, the observing data from sensor nodes is transmitted towards cloud servers by the intermediate nodes. Such data routing is exposed to many network threats over the Internet. Cloud computing offers various resource-oriented services to network users for data deployment, processing, and computing [9]–[12]. However, when the network size increases, the platform of cloud computing incurs network latency and decreases the performance of network throughput on time. Different solutions based on sensors-cloud are proposed in the last decade to cope with security threats [13]–[15]. However, most of these solutions overlooked the reliable data delivery and limited constraints of sensor nodes. Such solutions raise the possibility of network disaster and erroneous transmission, especially under the harsh network field. This research presents a distributed data reliability model for mobile edge-based

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Zakirul Alam Bhuiyan.

sensor-cloud. The objectives of the model are to deliver the efficacy outcomes for network latency, error-free transmission, and data security. The proposed model deploys mobile edge nodes along with ordinary sensor nodes for collecting data from the real-world. Mobile edge nodes are more powerful as compared to ordinary sensors and are therefore placed at the edge of the network field. The need of incorporating mobile edge nodes is to decrease the latency rate while forwarding the data towards cloud servers, which ultimately increases the data delivery performance with minimal overheads on sensor nodes. This research work offers the following contributions:

- Explains the previous work of sensor-cloud for ensuring data routing and security.
- Proposes distributed routing for information collection and transmission with balancing the network load and resources using the Floyd Warshall algorithm.
- Incorporates the link asymmetry method between mobile edge nodes and forwarders to guarantee the delivery of data and transmission integrity.
- Preserves data authentication and privacy based on the security algorithm so sensors' data can be received without any disturbance on the cloud system through multiple mobile edge nodes.

The remaining paper is organized in the following sections. The literature work is argued in section 2. The description of the DDR-ESC model with its network model and system design is presented in Section 3. The experimental results are discussed in Section 4. In the end, the research work is concluded in Section 5.

II. LITERATURE WORK

The technology of cloud computing is broadly adopted in various applications to decrease the computation overhead and latency [16], [17]. Also, the WSN integrated with cloud computing has gained a rapid development for various real-world solutions due to the collection of a huge amount of data [11], [18], [19]. The cloud servers receive sensors' data via multiple intermediate nodes and provide centralized data analysis with the least computing power for constraint oriented sensor nodes. Cloud computing copes with the issue of bounded resources of IoT-based sensors for the analysis, storage, and management of big data [20], [21]. Now, most of the cloud-based solutions are adopting the services of edge computing and fog computing for efficiently utilizing network resources with the least computing power of communication nodes [22], [23]. The authors in [24] proposed a dynamic duty cycle (DDC), which aims to increase energy efficiency with nominal transmission delay. The proposed scheme delivers data packets towards the BS on time and supports delay-sensitive applications. It prolongs the active epoch of the nodes that exist in the non-hotspot areas. Due to the larger duty cycle, the data forwarders are remained awake with a larger chance. Accordingly, the sleep delay of a node decreases, while during the routing, the transmission delay is decreased. The performed experiments indicate that the proposed scheme contributes to the network lifetime and energy-efficiency with minimal transmission delay as compared to other solutions.

In [25], the authors propose Energy Efficient and Reliable Transport of Data in Cloud-Based IoT, which aims to improve the data reliability and decrease traffic power consumption. The proposed solution presents a standby routes selection scheme for replacing the nodes' failure and attains data reliability with nominal power consumption. Also, the paper proposes a reliability level scheme to minimize the traffic power consumption between IoT-based sensors in considering the needed level of reliability. The proposed scheme also prevents the overhead on the busy reliable paths in mitigating the interference. The authors in [26] proposed Edge-based differential privacy computing for sensor–cloud systems to decrease the communication cost and improve data management. Based on the technology of edge computing [27]–[29], it presents three layers for storage architecture. The collected data from the network field is managed and processed by algorithms on edge servers, which guarantees data privacy. Moreover, the edge servers transmit fewer sensors' data towards the cloud server and decrease the additional transmission cost with manageable data storage in a lightweight manner.

The authors in [30] proposed a Cloud-based scheme for Protecting Source Location Privacy (CPSLP) for WSNs using Multi-sinks, which aims to improve the network lifetime and keep smooth the privacy protection. It makes the use of multiple sink nodes to determine several routing paths. Further, the proposed solution incorporates false packets in the network field to confuse malicious nodes and presents a comprehensive privacy location. The simulation-based experimental results demonstrate that the proposed solution can prevent the oppositional capture and preserve privacy protection on a high level.

The k-means Cluster-based Location Privacy Protection (KCLP) scheme is proposed in [31], which decreases the energy consumption and network delay as compared to other solutions. It uses a fake source node to simulate the function of the real sources and protect the source location. Moreover, the proposed scheme uses fake sink nodes with a particular transmission pattern to protect the privacy of the sink location. The proposed scheme applies the k-means algorithm to formulate the cluster and the fake packets pass through the area, which results in improving the safety time. The authors in [32] proposed a mechanism, named energy-efficient intra-cluster scheme (EEICS), for secure big data communications in WSNs that is used for improving the lifetime and data security. The proposed solution parts the nodes in clusters and suggests a multi-hop routing toward cluster heads for the selection of the relay node based on residual energy. Similarly, it provides data security in the cluster to preserve the privacy of source nodes. The experimental results showed the improved performance of the EEICS as compared to other solutions.

In [33], the authors highlighted the lack of existing trust-based solutions in the scenario of sensor-cloud. The proposed solution provides a fog-based hierarchical trust mechanism to overcome such harms. This mechanism is informal to implement and can cope with heavy and fine-grained data analysis tasks of the fog layer. The experimental results prove the fog-based hierarchical structure, which improves the network energy by ensuring rapid malicious node detection. The authors in [34] proposed a fog-based model to extend the classical Hungarian algorithm. In the proposed model, the fog layer performs the role of buffer and controller between the layers of wireless sensor networks and cloud. The classical Hungarian algorithm first performs a matching function and then it schedules the free resources for attaining optimal matching. The performed experiments and theoretical analysis indicate that the proposed model improves the efficient resource utilization and reliability.

It is observed from the discussed work that cloud computing is used in different applications for data analysis, storage, and processing. The technology of WSN is integrated with the cloud paradigm to reduce the additional computational overhead of real-time applications. However, its dynamic, robust, and unpredictable factors are imposing research challenges in terms of energy efficiency and reliable routing [35], [36]. Although it is seen that authors have proposed cloud-based solutions for data management that decreases the processing overheads of the low-powered sensor nodes, such solutions lack the problem of data latency. Besides, most of the cloud-based solutions do not study reliable routing and degrade data delivery performance. Some solutions are proposed based on edge computing that guaranteed network connectivity and integrity, however, most of them overlook the constraint-oriented systems for data security and trustworthiness. Based on the discussion, it is revealed that distributed and reliable routing using a sensor-cloud paradigm is a demanding task for preserving the energy resource by minimizing the processing cost with the management of big data.

III. DISTRIBUTED AND DATA RELIABILITY MODEL FOR MOBILE EDGE-BASED SENSOR-CLOUD

The proposed DDR-ESC model includes two main algorithms. The first algorithm develops a distributed reliable routing to attain energy efficiency and a more certain data delivery performance in time. In this algorithm, normal sensor nodes are deployed with some powerful mobile edge nodes. The mobile edge nodes are placed at the boundary of the network field to reduce the probability of data loss and maintains data integrity. Unlike most of the existing solutions that exploit the greedy algorithm for the formation of routing paths and lead to energy hole systems, the proposed algorithm uses the real-time node's parameters and associates them with minimum communications cost. The DDR-ESC model makes use of the Floyd-Warshall algorithm to compute the most optimal route among all shortest paths. Also, the sensors' data is received, processed, and stored on the cloud platform through mobile edge nodes. The second algorithm offers data security between sensors and mobile edge nodes using the data authentication code. Moreover, the strength of the privacy between mobile edge nodes and the cloud servers is increased based on the multiple encryption schemes, which results in generating more complex secure blocks. Accordingly, the DDR-ESC model achieves the energy efficiency and security along with reliable data delivery with mutual authentication between sensors, mobile edge nodes, and the cloud system. The system design of the DDR-ESC model is depicted in Figure 1.

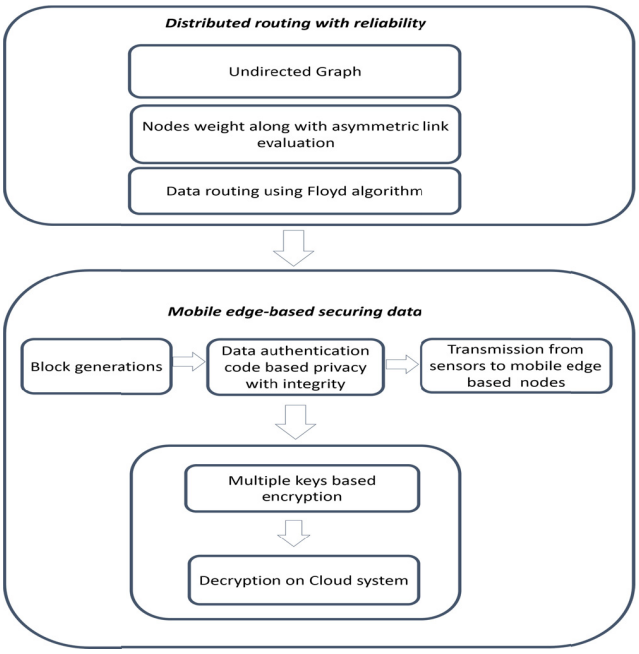

FIGURE 1. System design of DDR-ESC model.

The sub-sections present the network model and detailed algorithms of the proposed system.

A. NETWORK MODEL

In the beginning, we suppose that the sensor nodes S_i are randomly located in the square sized network field and organized in the form of undirected Graph $G\ (E, N)$. The set of edges is shown by E for the number of nodes N. There is a loop-free and unique edge between consecutive nodes that has some numeric values referred to as weight. The S_i initially compute their weighted values based on the residual energy, transmission cost T_{cs}, and link asymmetry factors. The value of T_{cs} is evaluated using hybrid distance i.e. distance of source node to a neighbor d_{sn} and distance of a neighbor node to BS d_{nb}. In this work, the radio energy consumption model [37] is used. Also, we consider some assumptions for the network model as follows.

i. S_i remain static and are densely deployed while the edge nodes are mobile.
ii. The processing and transmission capabilities of mobile edge nodes are stronger than S_i.
iii. The S_i are homogeneous in various attributes.

iv. The battery power of the S_i cannot be recharged.
v. The transmission links are asymmetric.

B. DISTRIBUTED ROUTING WITH RELIABILITY USING LINK ASYMMETRY

This section presents an algorithm for distributing routing by incorporating the link asymmetry factor to ensure the data delivery performance with the consideration of constraint resources. Also, the performance of the wireless links is analyzed in a bi-directional method for improving the quality of transmission. After the computation of weighted value, the information is shared between adjacent nodes. Let us consider that E_{net} is the total energy of the field at the time of network deployment T and consumed energy E_i of node i is obtained by the summation of transmitting and receiving k data bits to mobile edge nodes M over the distance d, then the residual energy R_{ener} can be computed as $E_{net} - (E_{tx_{i,\mathrm{M}}} + E_{rx_{i,M}})$. (k, d). The proposed distributed routing algorithm makes the use of bandwidth B_w and packet reception ratio (PRR) parameters to evaluate the link asymmetry among consecutive nodes. The highest value of link asymmetry L_s indicates the optimal choice for the transmission of gathered data. Let suppose that $P_t(n_i, n_j)$ are the transferred packets between the source node n_i and n_j, $P_d(n_i, n_j)$ is the amount of packet drop from node n_i to n_j, then $L_s(n_i, n_j)$ can be given as in Equation 1.

$$L_s(n_i, n_j) = B_w * (P_t(n_i, n_j) - P_d(n_i, n_j)) \tag{1}$$

Similarly, $L_s(n_j, n_i)$ can be computed from node n_j to n_i as given in equation 2.

$$L_s(n_j, n_i) = B_w * (P_t(n_j, n_i) - P_d(n_j, n_i)) \tag{2}$$

Finally, the weightage value $W(n_i, n_j)$ between node n_i to n_j can be computed as given in equation 3.

$$W(n_i, n_j) = R_{ener} + (1/(d_{sn} + d_{nb})) + (L_s(n_i, n_j) + L_s(n_j, n_i)) \tag{3}$$

Afterward, the computed $W(n_i, n_j)$ value is given as an input to the Floyd Warshall algorithm [38], and each node determines the shortest paths in a weighted graph, as given below:

i. Suppose $w(n_i, n_j)$ is the weighted value for node i and j. If $i = j$, then the value $w(n_i, n_j)$ is set to '0'.
ii. Similarly, if node $i \neq$ j and has some direct edge then its weighted value $w(n_i, n_j)$ is set to $W(n_i, n_j)$.
iii. If l is an intermediate node between node i and j, then its optimal routing path $R(n_i, n_j)$ is the summation $W(n_i, l)$ and $\mathrm{W}\left(l, n_j\right)$.

Accordingly, each node selects the high-quality routing path in terms of multiple features for transmitting the environmental data towards mobile edge nodes. In the proposed model, the edge nodes are mobile and rotated in clockwise around the boundary of the network field with continuous speed. The deployed mobile nodes at the network edge decrease the data latency and energy consumption in data collection. Later, the collected data from mobile edge nodes are stored on the cloud system, which is responsible to communicate with end-users through the Internet. The incorporation of the cloud paradigm not only improves the network scalability but also reduces the network and processing overhead. The routing process of the DDR-ESC model is elaborated through Algorithm 1.

Algorithm 1 Distributing Routing With Link Asymmetry

```
Procedure distributing routing
  Source node s generates request packets
  Neighbors N_i compute weights
  for each node i ∈ [1 : N_i]
    W(i, j) = R_ener + (1/ (d_sn + d_nb)) + (L_s(i, j)+
    L_s(j, i))
  end for
if i = j then
    w(n_i, n_j) = 0
end if
if node i ≠ j then
choose a direct edge using W(n_i, n_j)
    else
      if l exists then
        R(i, j) = W(n_i, l) + W(l, n_j)
      end if
    end if
end procedure
```

C. DATA SECURITY

Furthermore, the proposed model offers a data security algorithm for mobile edge-based transmission to increase privacy and integrity with the cloud system. The proposed security algorithm supports the network resources for computation and also decreases the data disruption from potential threats. It copes with data privacy and mutual authentication based on the cryptography methods from the network field to the cloud system using mobile edge nodes. The data security between data forwarders to the mobile edge nodes is accomplished using data authentication code based on the DES. The collected data that is needed to be protected from malicious machines are divided into contiguous blocks D_1, $D_2, \ldots, D_n$. The data blocks are transmitted from selected forwarders using $W(n_i, n_j)$ function to mobile edge nodes in multi-hop transmission. Each in-between node integrates the incoming data blocks with their data blocks and further transmitting. The proposed security algorithm uses the DES encryption algorithm and a random secret key K to generate a data authentication code [39]. Also, the hash codes H_i are also integrated with the encrypted blocks to ensure the data integrity as given in equation 4.

$$C_\mathrm{i} = E\left(D_\mathrm{i} \oplus K\right) + H_\mathrm{i}, \quad i \epsilon\, 0 \ldots n \tag{4}$$

The data forwarder on next-level, first confirms the data integrity by verifying the received hash code H_i, then it performs an encryption algorithm and union the incoming

cipher block with its data block and hash code as given in equation 5.

$$C_{i+1} = E\,(D_{i+1} \oplus K) + H_{i+1} \tag{5}$$

Upon receiving the encrypted data blocks D at mobile edge nodes M_n, multiple encryptions [40] are used based on different symmetric keys K_i and K_j to generate multi-facet cipher blocks C_i. The symmetric keys K_i and K_j are also securely transmitted among mobile edge nodes and cloud servers using private-public cryptographic principles. Such multi-facet blocks increase the strength of data security between mobile edge nodes and cloud servers as given in equation 6.

$$C_i = E(K_j \oplus (D \oplus K_i)) + H_i \tag{6}$$

Finally, on receiving the encrypted blocks at the cloud system, it performs the decryption function with the keys in reverse order and obtained the actual field data. Algorithm 2 shows the security process of the DDR-ESC model.

Algorithm 2 Data Security

1. Input:
2. $W(n_i, n_j)$
3. secret key K
4. encryption algorithm $D(E)$
5. contiguous blocks D_i
6. Procedure data_security
7. forwarders compute data encryption C_i and hashes H_i
8. $C_i = E\,(D_i \oplus K) + H_i$
9. upstream forwarders verify the incoming data chuck D_i,
10. performs data encryption C_{i+1} with hash H_{i+1}
11. $C_{i+1} = E\,(D_{i+1} \oplus K) + H_{i+1}$
12. multi-facet cipher blocks C_i are generated using K_i and K_j
13. between edge-based nodes and cloud system
14. $C_i = E(K_j \oplus (D \oplus K_i) + H_i$
15. cloud system recovers the contiguous blocks D_i
16. end procedure

IV. RESULTS DISCUSSION

In this section, the DDR-ESC model is evaluated with DDC [24] and CPSLP [30] under a varying number of nodes and a varying speed of mobile edge nodes. The series of experiments are carried out using open source and packet-level network simulator NS3. The simulation is executed for a period of 1000sec. The number of malicious nodes is set to 30 that is randomly placed in the field and also in between mobile edge nodes to the cloud system. The mobile edge nodes are assumed to be more powerful in terms of resources and computing power than normal sensor nodes. All nodes have a transmission range of 15m with residual energy 2j. The size of the data block is set to 64 bits. The mobile edge nodes are rotated clockwise with the speed from 4m/s to 20m/s. To evaluate the performance of DDR-ESC, five network metrics are used, i.e., network throughput, packet overhead, energy consumption, data latency, and data authenticity. Table 1 depicts the list of values that are used in the performance evaluation.

TABLE 1. Network parameters.

Factor	Value
Network field	200 x 200 m^2
Deployment	random
Structure	homogeneous
Sensor nodes	100 to 500
Malicious nodes	30
MAC layer	IEEE 802.11b
Data block	64 bits
Key size	56 bits
Payload size	512 bytes
Transmission range	20m
Simulation time	1000sec
Control message	25 bits

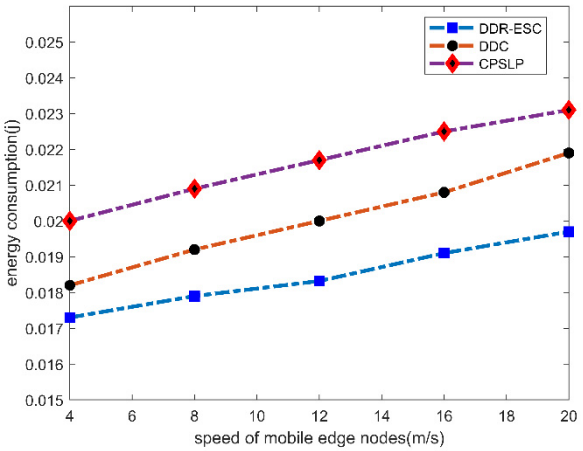

FIGURE 2. Energy consumption and mobile edge nodes.

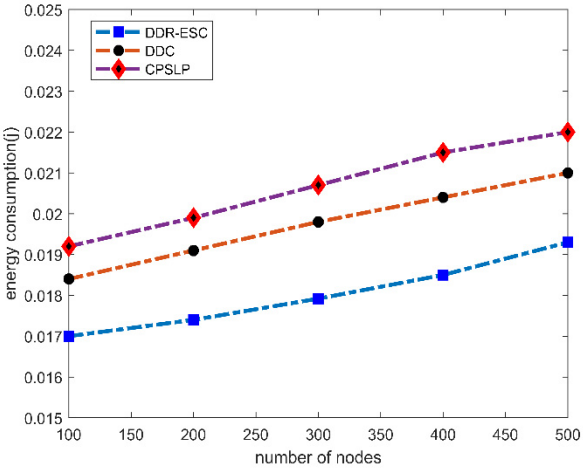

FIGURE 3. Energy consumption and the number of nodes.

Fig.2 and Fig.3 illustrate the performance evaluation of the DDR-ESC model against existing solutions for energy

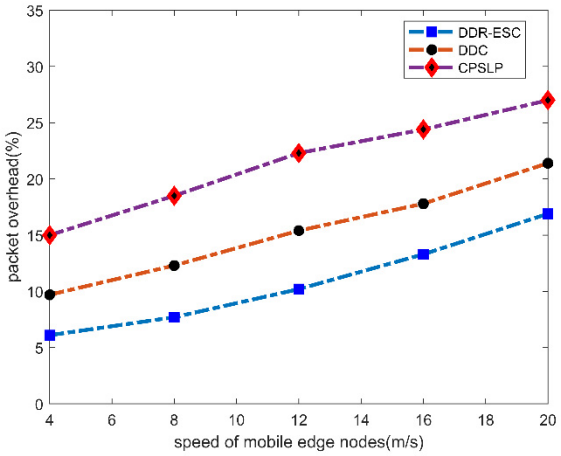

FIGURE 4. Packet overhead and mobile edge nodes.

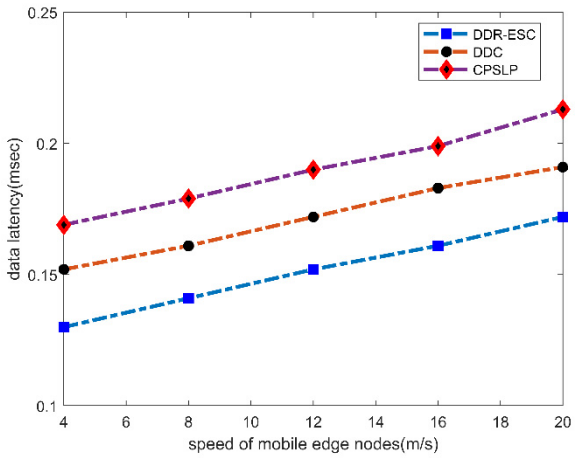

FIGURE 6. Data latency and mobile edge nodes.

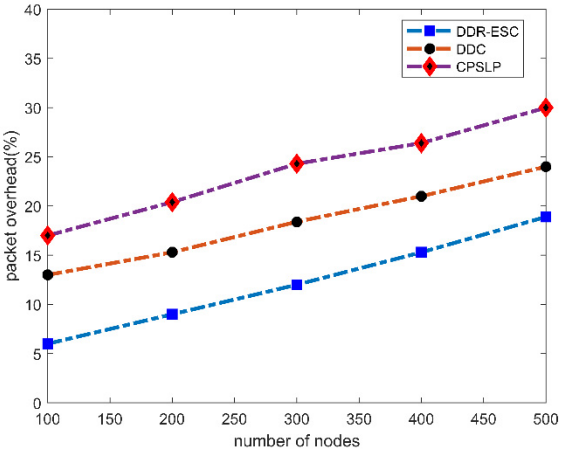

FIGURE 5. Packet overhead and the number of nodes.

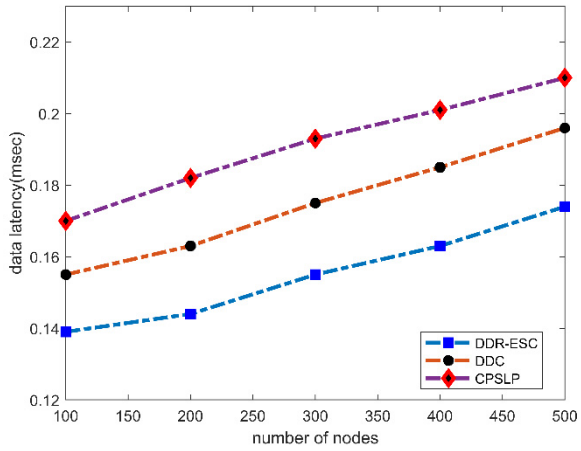

FIGURE 7. Data latency and number of nodes.

consumption under the varying speed of the mobile edge nodes and the varying number of nodes. The experimental results indicate the DDR-ESC model consumes less energy by 14% and 11% respectively. This is due to the DDR-ESC model present a distributed routing algorithm with lower routing overhead and packets' re-transmission. Also, based on the Floyd Warshall algorithm all possible optimal routes are identified and among them, the most optimal route is selected for the data transmission. The existing solutions incur additional communication overhead due to frequent data re-generation in the presence of potential threats, which results in increasing the level of energy consumption over the network field. Moreover, the DDR-ESC model balances the load among nodes in routing the observing data and based on the latest neighbor's information, the routing paths are updated. Furthermore, the deployment of mobile edge nodes significantly decreases the energy consumption of the nodes while transferring the field data towards the cloud servers.

Fig.4 and Fig.5 demonstrate the measurement of the packet overhead between the DDR-ESC model and other existing work under a varying number of mobile edge nodes and a varying number of nodes. It is noticed from the experimental results that the DDR-ESC model decreases the ratio of packet overhead than other solutions by 42% and 43%. This is due to that the DDR-ESC model evaluates the links measurement in asymmetric mode and based on the weighted value, it selects the most reliable and trustworthiness link for forwarding the field data. Also, the mobile edge nodes are rotated around the network topology with preset speed, the closest data forwarders to the mobile edge nodes handover the sensors' data over the more reliable route using the Floyd algorithm, which results in decreasing the fraction of the network overhead. Moreover, the proposed secured algorithm based on multiple encryptions and hash codes remarkably prevent the network data form malicious nodes, such a security algorithm reduces the probability of packet loss and nodes level overhead against potential threats.

Fig.6 and Fig.7 demonstrate the performance of the DDR-ESC model against other work in terms of data latency under the varying speed of mobile edge nodes and the varying number of nodes It is observed from the experimental results that the DDR-ESC model decreases the level of data latency by 13% and 18%, respectively. This is due to that the DDR-ESC model can cope with data traffic that

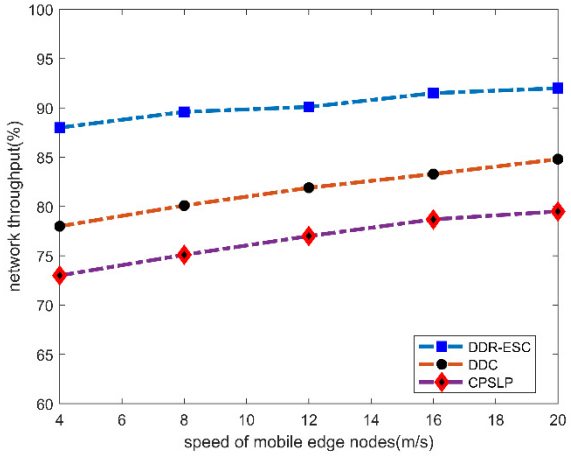

FIGURE 8. Network throughput and mobile edge nodes.

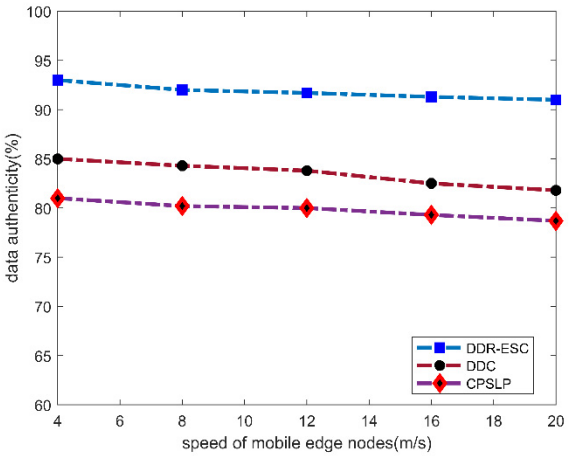

FIGURE 10. Data authenticity and mobile edge nodes.

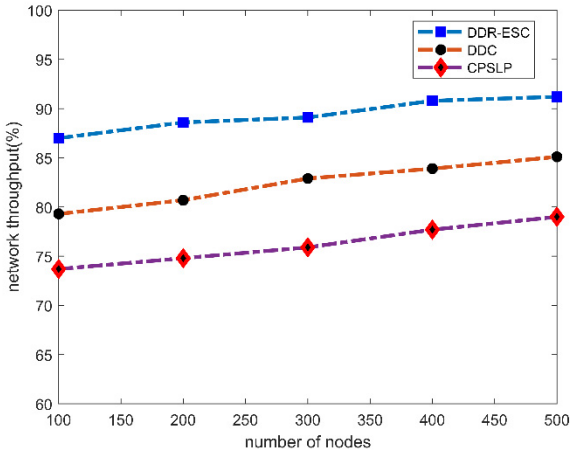

FIGURE 9. Network throughput and number of nodes.

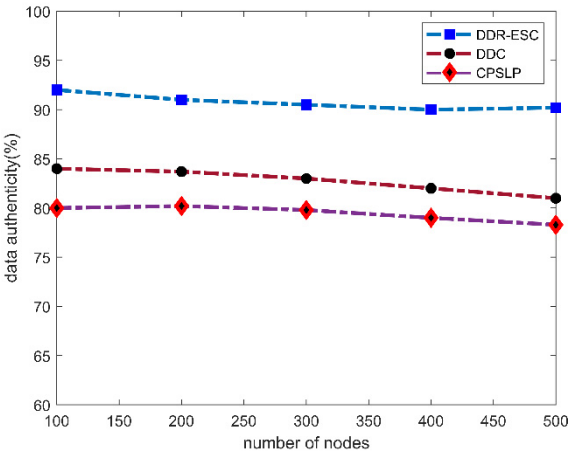

FIGURE 11. Data authenticity with the number of nodes.

is generated under varying network nodes. Unlike existing work, which mostly incurs data interruption with selected overloaded wireless links for data routing, increasing the delivery time in propagating the field data towards the cloud servers. The proposed DDR-ESC model along with residual energy it also evaluates the asymmetric link using PRR and bandwidth factors, accordingly the most optimal in terms of reliability and less congested next-hops are selected. Such an algorithm routed the data on an updated and fault-tolerant links, which results in reducing the data latency and attains better network performance. The proposed DDR-ESC model significantly decreases the frequently alternative route selection due to considering the finest route among the all shortest routes and results in delivering the data to the cloud platform by mobile edge nodes on time.

Fig.8 and Fig.9 illustrate the behavior of the DDR-ESC model against existing work for network throughput under the varying speed of mobile edge nodes and the varying number of nodes. It is observed from the analysis of the experimental results that the DDR-ESC model increases the network throughput by 13% and 11%, respectively. This improvement is due to the construction of more robust and energy-efficient routing paths based on the Floyd algorithm. Moreover, the incorporation of link measurement in the weighted function significantly increases the data delivery from sensors to the mobile edge node and from mobile edge nodes to the cloud servers. Also, due to the data authentication code based on DES increases the security level on intermediate nodes, which avoids the malicious nodes to drop the data packet, and ultimately it increases the network throughput. Moreover, the incorporation of cloud infrastructure in a mobile edge-based network offers scalable solutions for data processing and management with improved network throughput.

Fig.10 and Fig.11 exhibit the data authenticity of the DDR-ESC model with other existing work under the varying speed of mobile edge nodes and the varying number of the nodes. Based on the experimental results, it is seen that the DDR-ESC model has increased the ratio of data authenticity by 14% and 13% in the comparison of the other work. It is due to the DDR-ESC model securing the field data from malicious entities and authenticate the nodes

during transmission. The network data is protected using data authentication code based on DES, which splits the packets into fixed-sized blocks. Then, cryptography-based lightweight encryption and decryption functions are applied to each block to increase its privacy and integrity level. Also, the field data is multiple times encrypted for ensuring the authenticity in dual-mode among mobile edge-based nodes and cloud systems.

V. CONCLUSION

This article presents a distributed and data reliability model for mobile edge-based sensor-cloud (DDR-ESC) to provide network scalability, energy efficiency, and data security. The DDR-ESC model offers the distributed routing algorithm to sense the observing data and forwards towards the cloud system. The incorporation of the link asymmetric method in the distributed routing algorithm ensures data reliability and decreases the transmission cost. In the proposed model, the mobile edge nodes ensure data integrity and connectivity with the cloud system. Furthermore, the DDR-ESC model secures the transmitted data from the network field to mobile edge-based nodes and from mobile edge-based nodes to the cloud system using the data authentication code and multi encryptions scheme. Accordingly, data blocks are encrypted, authenticated, and verified on several levels until they are received on the cloud platform. The examined results illustrated that the DDR-ESC model increases data reliability and security against malicious events with energy efficiency. In the future, we aim to improve the DDR-ESC model using deep learning techniques with edge computing for mobile cloud systems. Also, the offloading algorithm for edge computing needs to be analyzed for deciding task computing.

REFERENCES

[1] M. Z. Chowdhury, M. T. Hossan, A. Islam, and Y. M. Jang, "A comparative survey of optical wireless technologies: Architectures and applications," *IEEE Access*, vol. 6, pp. 9819–9840, 2018.

[2] J. Herrera-Tapia, E. Hernandez-Orallo, A. Tomas, C. T. Calafate, J.-C. Cano, M. Zennaro, and P. Manzoni, "Evaluating the use of sub-gigahertz wireless technologies to improve message delivery in opportunistic networks," in *Proc. IEEE 14th Int. Conf. Netw., Sens. Control (ICNSC)*, May 2017, pp. 305–310.

[3] M. A. Khan, I. Ud Din, S. U. Jadoon, M. K. Khan, M. Guizani, and K. A. Awan, "G-RAT | a novel graphical randomized authentication technique for consumer smart devices," *IEEE Trans. Consum. Electron.*, vol. 65, no. 2, pp. 215–223, May 2019.

[4] K. Haseeb, N. Islam, A. Almogren, and I. Ud Din, "Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things," *IEEE Access*, vol. 7, pp. 185496–185505, 2019.

[5] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. Hanzo, "A survey of network lifetime maximization techniques in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 828–854, 2nd Quart., 2017.

[6] S. Kurt, H. U. Yildiz, M. Yigit, B. Tavli, and V. C. Gungor, "Packet size optimization in wireless sensor networks for smart grid applications," *IEEE Trans. Ind. Electron.*, vol. 64, no. 3, pp. 2392–2401, Mar. 2017.

[7] J. Wang, C. Ju, Y. Gao, A. K. Sangaiah, and G.-J. Kim, "A PSO based energy efficient coverage control algorithm for wireless sensor networks," *Comput., Mater. Continua*, vol. 56, no. 3, pp. 433–446, Jan. 2018.

[8] K. Haseeb, I. Ud Din, A. Almogren, and N. Islam, "An energy efficient and secure IoT-based WSN framework: An application to smart agriculture," *Sensors*, vol. 20, no. 7, p. 2081, Apr. 2020.

[9] C. Zhu, V. C. M. Leung, J. J. P. C. Rodrigues, L. Shu, L. Wang, and H. Zhou, "Social sensor cloud: Framework, greenness, issues, and outlook," *IEEE Netw.*, vol. 32, no. 5, pp. 100–105, Sep. 2018.

[10] C. Zhu, V. C. M. Leung, K. Wang, L. T. Yang, and Y. Zhang, "Multi-method data delivery for green sensor-cloud," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 176–182, May 2017.

[11] R. K. Dwivedi, S. Singh, and R. Kumar, "Integration of wireless sensor networks with cloud: A review," in *Proc. 9th Int. Conf. Cloud Comput., Data Sci. Eng.*, 2019, pp. 114–119.

[12] K. Haseeb, A. Almogren, I. Ud Din, N. Islam, and A. Altameem, "SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things," *Sensors*, vol. 20, no. 9, p. 2468, Apr. 2020.

[13] J. Zhou and Z. X. A. V. Cao Dong Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Feb. 2017.

[14] V. K. Verma, K. Ntalianis, C. M. Moreno, and C.-T. Yang, *Next-Generation Internet of Things and Cloud Security Solutions*. London, U.K.: SAGE, 2019.

[15] P. Massonet, L. Deru, A. Achour, S. Dupont, A. Levin, and M. Villari, "End-To-End security architecture for federated cloud and IoT networks," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2017, pp. 1–6.

[16] D. De, A. Mukherjee, A. Ray, D. G. Roy, and S. Mukherjee, "Architecture of green sensor mobile cloud computing," *IET Wireless Sensor Syst.*, vol. 6, no. 4, pp. 109–120, Aug. 2016.

[17] N.-T. Dinh and Y. Kim, "An efficient on-demand latency guaranteed interactive model for sensor-cloud," *IEEE Access*, vol. 6, pp. 68596–68611, 2018.

[18] S. Xiao, T. Li, B. Guo, and Z. Huang, "Cloud platform wireless sensor network detection system based on data sharing," *Cluster Comput.*, vol. 22, no. 6, pp. 14157–14168, Nov. 2019.

[19] R. K. Dwivedi and N. R. Kumar, "Integration of wireless sensor networks with cloud towards efficient management in IoT: A review," in *Proc. Adv. Data Inf. Sci.*, 2020, pp. 97–107.

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

[21] I. Ud Din, M. Guizani, S. Hassan, B.-S. Kim, M. K. Khan, M. Atiquzzaman, and S. H. Ahmed, "The Internet of Things: A review of enabled technologies and future challenges," *IEEE Access*, vol. 7, pp. 7606–7640, 2019.

[22] A. Manzoor, M. A. Shah, H. A. Khattak, I. U. Din, and M. K. Khan, "Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges," *Int. J. Commun. Syst.*, vol. 15, Jun. 2019, Art. no. e4033.

[23] H. A. Khattak, S. U. Islam, I. U. Din, and M. Guizani, "Integrating fog computing with VANETs: A consumer perspective," *IEEE Commun. Standards Mag.*, vol. 3, no. 1, pp. 19–25, Mar. 2019.

[24] Y. Liu, A. Liu, N. Zhang, X. Liu, M. Ma, and Y. Hu, "DDC: Dynamic duty cycle for improving delay and energy efficiency in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 131, pp. 16–27, Apr. 2019.

[25] H. M. Al-Kadhim and H. S. Al-Raweshidy, "Energy efficient and reliable transport of data in cloud-based IoT," *IEEE Access*, vol. 7, pp. 64641–64650, 2019.

[26] T. Wang, Y. Mei, W. Jia, X. Zheng, G. Wang, and M. Xie, "Edge-based differential privacy computing for sensor–cloud systems," *J. Parallel Distrib. Comput.*, vol. 136, pp. 75–85, Feb. 2020.

[27] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.

[28] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017.

[29] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1628–1656, 3rd Quart., 2017.

[30] G. Han, X. Miao, H. Wang, M. Guizani, and W. Zhang, "CPSLP: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2739–2750, Mar. 2019.

[31] G. Han, H. Wang, M. Guizani, S. Chan, and W. Zhang, "KCLP: A k-Means cluster-based location privacy protection scheme in WSNs for IoT," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 84–90, Dec. 2018.

[32] A. Wang, J. Shen, P. Vijayakumar, Y. Zhu, and L. Tian, "Secure big data communication for energy efficient intra-cluster in WSNs," *Inf. Sci.*, vol. 505, pp. 586–599, Dec. 2019.

[33] G. Zhang, T. Wang, M. Z. A. Bhuiyan, and G. Wang, "A fog-based hierarchical trust mechanism for sensor-cloud underlying structure," in *Proc. IEEE Int. Symp. Parallel Distrib. Process.*, Dec. 2017, pp. 481–485.
[34] Y. Liang, T. Wang, M. Z. Bhuiyan, and A. A. Liu, "Research on coupling reliability problem in sensor-cloud system," in *Proc. Int. Conf. Secur.*, 2017, pp. 468–478.
[35] U. Ullah, A. Khan, M. Zareei, I. Ali, H. A. Khattak, and I. U. Din, "Energy-effective cooperative and reliable delivery routing protocols for underwater wireless sensor networks," *Energies*, vol. 12, no. 13, p. 2630, Jul. 2019.
[36] H. A. Khattak and Z. U. I. M. K. Ameer Din Khan, "Cross-layer design and optimization techniques in wireless multimedia sensor networks for smart cities," *Comput. Sci. Inf. Syst.*, vol. 16, no. 1, pp. 1–17, 2019.
[37] 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.*, Maui, Kahului, 2000, pp. 1–5.
[38] R. W. Floyd, "Algorithm 97: Shortest path," *Commun. ACM*, vol. 5, no. 6, p. 345, Jun. 1962.
[39] *Computer Data Authentication National Institute of Standards and Technology*, Standards 29, 1985.
[40] R. C. Merkle and M. E. Hellman, "On the security of multiple encryption," *Commun. ACM*, vol. 24, no. 7, pp. 465–467, Jul. 1981.

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 at the Department of Computer Science, Islamia College Peshawar, Pakistan. He has experience of several years in teaching, research, and development. His research interests include wireless sensor networks, ad hoc networks, network security, the Internet of Things, software defined networks, and sensors-cloud. He involves as a Referee for many reputed international journals and conferences.

IKRAM UD DIN (Senior Member, IEEE) 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 is currently working as an Assistant Professor at the Department of Information Technology, The University of Haripur. He has 12 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. He has served as the IEEE UUM Student Branch Professional Chair.

AHMAD ALMOGREN (Senior Member, IEEE) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He is currently a Professor with the Computer Science Department, College of Computer and Information Sciences, (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia. He is the Director of Cyber Security Chair of CCIS, KSU. Previously, he worked as the Vice Dean for the Development and Quality at CCIS. He also served as the Dean of the College of Computer and Information Sciences, and the Head of the Academic Accreditation Council at Al-Yamamah University. His research interests include mobile-pervasive computing and cyber security. He served as the General Chair of the IEEE Smart World Symposium and a Technical Program Committee Member in numerous international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and IEEE HPCC.

ZAHOOR JAN received the M.S. and Ph.D. degrees from FAST University Islamabad, in 2007 and 2011, respectively. He is currently holding the rank of an Associate Professor with the Computer Science Department, Islamia College Peshawar, Pakistan, where he is also the Chairman. His research interests include image processing, machine learning, computer vision, artificial intelligence, and medical image processing, biologically inspired ideas like genetic algorithms and artificial neural networks, and their soft-computing applications, biometrics, solving image/video restoration problems using combination of classifiers using genetic programming, optimization of shaping functions in digital watermarking, and image fusion.

NAVEED ABBAS received the Ph.D. degree in computer science from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia. He is currently working as an Assistant Professor at the Department of Computer Science, Islamia College Peshawar, Pakistan. He has experience of many years in teaching and development. His research interests include image processing, machine learning, information security, the medical-based Internet of Things, and cloud computing. He serves as a Referee for many reputed journals and conferences.

MUHAMMAD ADNAN received the B.S. degree from the University of Peshawar, Peshawar, Pakistan, in 2006, the M.S. degree from the Center for Advanced Studies in Engineering, Islamabad, Pakistan, in 2008, and the Ph.D. degree from Dongguk University, Seoul, South Korea, in 2016.

He worked as a Lecturer in different public sector universities of Pakistan, from 2008 to 2012 and 2016 to 2018. He has done Postdoctoral Research at the College of Information Technology, United Arab Emirates University, United Arab Emirates. He is currently a Faculty Member with the Higher Colleges of Technology–Al Ain Men's College, United Arab Emirates. His research interests include wireless networks, security, smart grid, the IoT, and cloud computing.