IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON ARTIFICIAL INTELLIGENCE (AI)-EMPOWERED INTELLIGENT TRANSPORTATION SYSTEMS

Received December 2, 2019, accepted December 15, 2019, date of publication December 18, 2019,
date of current version December 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960633

Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things

KHALID HASEEB[1], NAVEED ISLAM[1], AHMAD ALMOGREN[2], (Senior Member, IEEE), AND IKRAM UD DIN[3], (Senior Member, IEEE)

[1]Computer Science Department, Islamia College Peshawar, 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

Corresponding author: Ahmad Almogren (ahalmogren@ksu.edu.sa)

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

ABSTRACT The infrastructure of wireless sensor networks (WSN) is structured in an ad-hoc manner and organized nodes reporting the events to the Base Station (BS). A WSN is integrated with smart technologies to develop fast Internet of Things (IoT) communications among different applications. Recently, many researchers proposed their solutions to optimize IoT data transmissions in an energy efficient manner with cost effective support. However, most of the solutions have focused on the design and development of static topologies and overlooked the dynamic structure of mobile sensor nodes. Furthermore, due to limited constraints of sensor nodes with open accessibility of wireless communications medium, data protection against malicious activities need to be redesign with the least network overheads. Therefore, the contribution of this article is to propose an intrusion prevention framework for mobile IoT devices with its integration to WSN so that to provide data security with improved network delivery ratio. The proposed framework is composed of two sub-components. Firstly, non-overlapping and autonomously organized clusters are generated and maintained the clusters' stability based on the uncertainty principle. Secondly, end-to-end secure and multi-hop routing paths are developed based on the blockchain architecture. The simulation results demonstrate a significant improvement when compared to existing solutions in terms of different network metrics.

INDEX TERMS Blockchain, intrusion prevention, mobile IoT, data privacy, security.

I. INTRODUCTION

In the last few decades, WSNs perform a vital role in development growth for different fields [1], [2]. A large number of small sized static sensor nodes also called motes are interconnected to each other for data collection and forwarding towards Base Station (BS). When BS gets the sensory data, it performs some necessary procedures on it and further transmitted to end-users. The sensor nodes are less expansive, low battery powered and placed randomly in a monitoring area [3], [4]. Due to low communication capabilities and restricted constraints of sensor nodes, most of the researchers focused on proposing a solution with efficient routing performance and network stability [5], [6]. However, the data collection in static WSN may be imprecise and leads to network disruption and unreliability. The static network pattern is not able to change their position after the nodes deployment for the purpose of data gathering. On the other hand, IoT interconnects everything embedded with hardware, software, static and mobile sensors for continues information gathering and forwarding.

Sensor nodes are portable in Mobile Wireless Sensor Networks (MWSN) and can be connected to various carriers, i.e., robotic systems [7] and smart transportation systems [8] to sense and measure the information, which can be forwarded towards the BS (or roadside units (RSUs) in terms of vehicular communications) via direct or multi-hop communication models [9]–[11]. Nowadays, the research

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

community has focused on integrating the field of MWSNs with IoT for the fast growth in network coverage and development [12], [13]. However, due to dynamic and unvarying changes in the network infrastructure, most applications degrade packet delivery ratio and energy efficiency. In addition, protected and reliable data exchanges are needed to avoid compromising data security between mobile sensors for IoT-based applications, especially for IoT-based vehicular ad hoc networks (VANETs) [14], [15].

In existing solutions, many contributions have been made towards cluster-based network infrastructure [16]–[18] for improving routing performance in terms of network lifetime and throughput. However, if nodes are mobile then the management of clusters stability with reliable data routing is the most interesting research problem [19], [20]. Furthermore, after the deployment of MWSNs, the sensor nodes are left unattended with no fixed infrastructure, therefore, the process of data routing with efficient energy consumption between mobile nodes and BS/RSU is another important challenge [11], [21]–[23]. In MWSNs, the ordinary nodes must have to track the fresh position of the newly selected mobile cluster head. Moreover, a lot of smarts devices are interconnected in IoT based systems and exchange messages in open wireless channels, such networks are prone to a variety of security threats especially when nodes are mobile [24]–[26].

The paper presents an intrusion prevention framework, which aims to longer network lifetime with lightweight secure data routing between mobile IoT devices based on WSN. Unlike other solutions, our proposed framework fragments the mobile IoT objects into various clusters and performs the cluster heads selection by using the uncertainty principle. In addition, based on network measurement and analysis, the up to date position of mobile cluster heads are determined. Moreover, in most of the existing solutions, it is not easy to guarantee a secured and reliable end to end data transmissions between mobile IoT objects due to their limited constraints. Unlike other solutions, our proposed framework presents a lightweight and reliable end-to-end secure approach based on blockchain architecuture. Accordingly, the proposed framework improves routing performance for mobile IoT devices in terms of data security and energy utilization.

The paper is structured in the following sub-sections. The background study with problem formulation is discussed in Section 2. Section 3 introduces the detail of the proposed intrusion avoidance framework for secure routing in mobile IoT. In Section 4, the simulation scenario with default parameters is described. Section 5 discussed the numerical analysis of the proposed framework against other solutions. In the end, Section 6 concludes the research article.

II. BACKGROUND STUDY

The field of WSNs is typically characterized by limited power devices in terms of computational, processing, memory and energy resources. All the nodes are interconnected through wireless transmission in an unfixed and ad-hoc based approach. The main role of sensor nodes are just capturing the information and forwarded towards end-points by using intermediate devices. To achieve routing performance in terms of network lifetime and data security, the limited constraints of the sensor nodes should not be overlooked. Furthermore, there are more chances for malicious threats in the network structure, especially when the connecting objects are mobile. The mobile IoT devices collect huge amounts of data without any user involvement and can route the data to malicious nodes thereby results in compromised data privacy. Therefore, to improve the performance of routing with respect to security, there is a need to establish secure and authentic end-to-end routing channels so that only trusted IoT devices can exchange information.

Authors in [27] proposed the Low Energy Adaptive Clustering Hierarchy (LEACH), which aims to develop different clusters. Based on the random number, a preset of a number of nodes is elected as cluster heads. All the normal nodes remain static and forwarded the information towards BS via associated cluster heads in one-hop transmission. Although, LEACH improved network lifetime, however, it was not suitable for mobility scenarios. The authors proposed a heterogeneous mobile LEACH protocol [28], which aims to improve energy efficiency with a fixed number of nodes and BS is mobile. Based on a probability function, cluster heads are selected over the network field. However, the proposed solution has routing complexity and network overheads.

The authors in [29] considered a cluster-based network and measure the mobility of cluster heads for improving network lifetime. In the solution, all the sensor nodes and sink nodes are fixed after initial deployment, while cluster heads are mobile. The main aim of the proposed solution was to decrease the network delay ratio. An energy efficient distance-aware routing protocol was proposed by [30] based on multiple sinks. By exploiting the transmission range of nodes, the sink position is identified. It uses direct transmission towards a mobile sink if nodes are in the same transmission range. During data forwarding, if nodes are far away from the sink node then communication occurs via multi-hop. Based on energy and distance factors, the next-hop is selected to achieve data routing. However, during routing decisions the link quality factor is overlooked, therefore the proposed solution causes a lot of route breakages and packet lose ratio.

LEACHDistance-M [31] was proposed by authors for improving delivery performance for MWSNs. The selection of cluster heads is based on multiple criteria, i.e., lower threshold distance, upper threshold distance, remaining energy, and least mobility factors. Although, the proposed solution increases network lifetime and throughput, however, data security against malicious threats is not taken into consideration thereby routing process may be compromised. In [32], the authors proposed an efficient clustering framework for the aggregation of data using mobile sinks.

Although, the solution presents a clustering scheme for decreases energy consumption, however, the data routing is not optimized and secured. In addition, the solution leads to high communication costs and routing overheads in identifying the latest position of mobile sink.

Similarly, in the Mobile sink-based Energy-efficient Clustering Algorithm (MECA) [33], equal sized clusters are formed, which aims to achieve uniform distribution of CHs. Furthermore, to consume less energy consumption, intra cluster communication achieved in a multi-hop manner. However, the solution imposes the replacement of intermediate nodes without network conditions, which results in bounded its applicability. In [34], [35], the authors presented a general architecture, where the sink node is placed at the center of the environment and all the remaining sensor nodes are virtually divided into different coronas. The data packets are transmitted towards innermost corona in multi-hop communication and then further forwarded to the sink node. Although, the proposed solution improved energy consumption around the sink node and prolonged network lifetime for MWSNs, however, the malicious threats are overlooked and thus transmitted sensor's information may be compromised.

Authors in [36] proposed a novel secure transport protocol for WSN, which aims to provide reliability and energy efficiency. The proposed solution offers both formal and informal security analysis and demonstrates that it improves network performance under malicious threats. Moreover, a lightweight security solution using one way hash function, bitwise exclusive operation, and physical unclonable function is proposed in [37], which improves data security as compared to other approaches with respect to different parameters. However, such solutions have not evaluated their performance under varying network sizes to determine the routing cost.

Based on the studied literature, it is noticed that most of the researchers have made an effort for improving network lifetime and energy consumption for static wireless sensor networks. Furthermore, a few efforts have been made in the integration of MWSNs with IoT devices for improving network coverage and development. However, due to mobile sensors, most of the existing solutions suffer from data delivery and network latency problems [38], [39]. Because in MWSNs, sensor nodes are not able to forward their sensed information towards mobile cluster heads until mobile cluster heads reach in the boundary of clusters. In addition, cluster heads are mobile and there are many chances for malicious nodes to be part of the existing network and compromise their data privacy [40]. Therefore, a framework must be developed for avoiding intrusion threats and improving the network lifetime of mobile IoT objects. Such a framework may increase the network performance in both industrial and academic domains.

III. PROPOSED FRAMEWORK

This section presents a short summary of the proposed framework, while its key sections are presented in the sub-sequent sections. The main phases of the proposed framework are initial network deployment with clusters management and a secure model for data routing. In the first phase, initial routing infrastructure is carried out, so the neighbor's information can be stored in the local table of every node. Moreover, the aim of this phase to also to perform an effective and energy efficient clustering scheme using mobile cluster heads. In addition, the phase has also presented a paradigm that retains the near optimal data forwarding paths towards existing positions of mobile cluster heads. In the end, the second phase presents a data security model to prevent intrusion threats and improves network reliability based on blockchain techology. In blockchain techonology, the data is divided into different blocks and all the blocks are interconnected via cryptography principles. The blocks are encrypted using a cryptographic hash function and each block has also contained the hash of its previous block [41], [42]. Such techonology helps to track data blocks and maintain network security with data integrity. Consequently, the proposed framework overtakes network performance with respect to various measurement metrics. Fig.1 illustrates the paradigm for WSNs along with mobile cluster heads and BS.

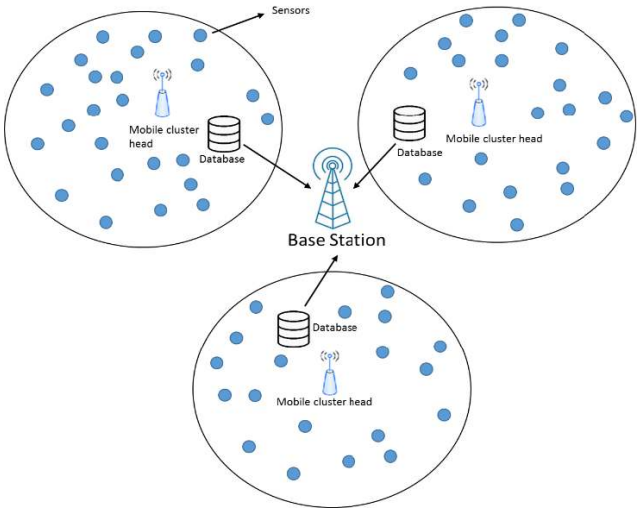

FIGURE 1. Wireless sensor network with mobile cluster heads and BS.

A. NETWORK ASSUMPTIONS

In this research study, the following network assumptions are made.

i. In a squared-sized network field, all the sensor nodes are randomly distributed.
ii. All the selected cluster heads are mobile with limited energy, computational and memory resources.
iii. The transmission distance of the nodes can be computed based on the RSSI value.
iv. The position of each node can be determined by using a GPS or positioning algorithm.
v. Structure wise all the sensor nodes are homogenous.

B. INITIAL NETWORK DEPLOYMENT WITH CLUSTERS MANAGEMENT

In the beginning, BS advertised beacon messages in the network field to discover it. In response, the one-hop neighbors of BS store the particulars of received information in their routing tables. Subsequent, source nodes increase packet counter and further transmit the information. Nevertheless, a node might obtain the discovery message of BS from several neighbors, in such a case, routing path with the minimum number of a hop count to BS is given priority and the information is stored in the routing table. In this way, all the nodes develop their routing tables for the precise path based on the least distance. After the structure of routing tables, direct transmission can be performed only those nodes whose hop count towards BS is set to 1.

Afterwards, the proposed framework makes use of voronoi architecture and divides the network field into different cells. The voronoi cells are the partition of the network field into different regions based on the distance of sensor nodes to computed mean values. Accordingly, each sensor node belongs to a particular cell with the nearest mean value. Each voronoi cell is considered as a unique cluster in the proposed framework. Moreover, to identify the mobile node, a distance threshold is set and it increases slightly until any mobile node is found in the boundary of the voronoi cell. When any mobile node is found, the role of the cluster head is assigned it it. It may be a case that within the preset distance threshold, more than one mobile node is found. In this situation, the proposed framework exploits the uncertainty principle [43] to determine the relative position of mobile nodes with the least variation as given in Equation 1.

$$\Delta x \Delta p \approx h/2 \tag{1}$$

Δx is the current position of the node, Δp is momentum or speed of node per unit time and h is Planck constant. Accordingly, to Equation.1 the proposed framework selects that mobile node as a cluster head, which gives relative position. After the selection of mobile nodes as cluster heads, they flood their information and all the ordinary nodes update their routing table and mark a particular ID of the mobile node as a cluster head. Instead of updating the routing tables on a periodic basis, the proposed framework only updates them whenever any new mobile cluster head is selected. Actually, the reason for using mobile nodes as cluster heads in the proposed framework is to improve the network connectivity with data delivery performance in a timely manner. Moreover, the ratio of energy utilization among sensor nodes is decreased and improves network stability. Algorithm 1 governs the process of voronoi cells and the selection of mobile cluster heads.

After the selection of mobile nodes as cluster heads, they initiate the process for the construction of end-to-end reliable routing chains towards BS. The downstream mobile cluster heads floods a route discovery packet in its transmission radius to determine its upstream mobile cluster head. Upon reception of the route discovery packet, the upstream cluster head verifies its residual energy. If the level of residual energy is greater than the preset threshold then the upstream mobile cluster head will become part of the routing chain. Otherwise, the upstream mobile cluster head rejects the route discovery packet and the same practice is repeatedly continue until an appropriate upstream cluster head is found. Algorithm 2 governs the process for data routing from mobile cluster heads to BS.

Algorithm 1 Voronoi Cells and Mobile Cluster Heads With Routing Chains

1. **Procedure voronoi cells**
2. Base station ADV beacon messages via
3. next-hops & node *i* maintains a local table
4. Distribute the network region into various
5. voronoi cells
6. **for each** $\text{node}_i \in [1: \text{VC}_i]$
7. **do**
8. if (mobile cluster head_i. distance $<$ preset
9. Threshold)
10. compute $\Delta x \Delta p \approx \frac{h}{2}$
11. **endif**
12. **set** the least variation mobile node as cluster head
13. **end for**
14. **for each** $\text{mobile\_node}_i \in \text{clusterhead}_i$
15. **do**
16. status message
17. **for each** node j $\in$ voronoi cell (i)
18. **do**
19. j.responsed
20. update routing table
21. **end for**
22. **end for**
23. **end procedure**

Algorithm 2 Routing Chains in Mobile Cluster Heads

1. **procedure** routing chains
2. **if** (.next-hop = BS BS)
3. send data directly
4. **while** (destination!= BS)
5. Compute energy level of mobile cluster head_i
6. **if** residual energy of mobile cluster $\text{head}_i >$
7. preset threshold
8. selected as upstream data forwarder
9. **else**
10. locate another mobile cluster head_i in
11. transmission range
12. **endif**
13. **end while**
14. **end procedure**

C. MODEL FOR DATA SECURITY

In recent years, due to promising aspects to bring remarkable changes in almost all fields of industries, blockchain

architecture has been gained a lot of interest in the research community. Blockchain [26], [44] can be used in a distributed fashion for resolving trusted and secure data routing between sensor nodes. This architecure is implemented in a decentralized fashion and provides a more secure system for data security in WSN. The architecture of blockchain is also being exploited in many areas where the nodes are participating in peer-to-peer communication. Similarly, it is thoroughly applied in many related areas including distributed consensus systems, information security, economic incentives, and data encryption.

In the proposed framework, a secure model is used to prevent malicious threats and offers secure data routing between sensor nodes, mobile cluster heads, and BS by using blockchain architecture. The mobile cluster heads are equipped with their own databases consisting of hashes. All the hashes can be redirected and each communicaiton may be audited using these hashes. The sensor nodes are in constant communication with the mobile cluster heads which is further in contact with BS.

All the mobile cluster heads are provided with private keys, which is used to establish, secure data routing with the sensors and BS. A unique hash is computed for each message, the computed hash function is like a function that needs an input value and accordingly it produces an output value as given in Equation 2.

$$f(x) = n \tag{2}$$

where x is data packet and n is the computed hash value. In the proposed framework, bitwise XOR operation is used as a hash function due to its computational efficiency and low processing requirements. Furthermore, the using of hash values in the proposed framework is due to its irreversible mechanism. Such a mechanism ensures that the original message cannot be determined by knowing the output.

In the proposed framework, the main function of the BS is to publish smart contracts, processing the data generated by sensors, and issuance of activities. The Base station is also responsible to record the activity of each data packet, which includes the location of sensors, IDs of mobile cluster heads in its immutable database. The immutable database is only permitted to a countable number of pre-authorized sensor nodes and the BS itself. Moreover, the mobile cluster heads verify the validity of the data packets with the previously acquired private keys. The proposed security scheme encrypts the routing information between mobile clusters and BS based on blockchain architecture, which makes them traceable and irreversible for malicious threats as illustrated in Fig 2. Moreover, the BS is a monitoring entity, which overlooks the working status of mobile cluster heads as well as sensor nodes. In the proposed framework, the BS is a central authority and has an overall controlled on network-wide routing, therefore it can remove any sensor node or mobile cluster head from the network field if found to be dead or suspicious. Algorithm 3 governs the data security model based on a blockchain architecture.

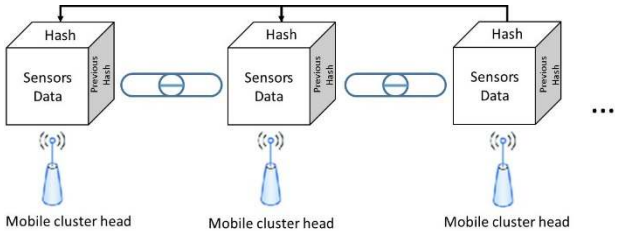

FIGURE 2. Computation of hash functions based on the blockchain.

Algorithm 3 Data Security Based on Blockchain Technology

1. **Procedure data security**
2. sensor node request to send data to BS
3. the whole block representing the transaction and
4. store in a local database
5. compute the XOR functions by using a Hash of the
6. current data packet and Hash of the previous block
7. data blocks are generated by sensor nodes
8. blocks are broadcast to all associated mobile
9. clusters mobile cluster heads validates the data
10. packets and generate a new block
11. created block is added to the chain
12. BS verified the chain and execute it.
13. **end procedure**

IV. SIMULATION SCENARIO AND PARAMETERS

This section presents the simulation scenario for WSN based on mobile IoT and default parameters as given in Table 1. To measure the impact of the proposed framework, different experiments are performed in terms of varying network nodes and data sending rates. The number of nodes is set from 100 to 500 and data sending rates are fixed from 1 sec to 5 sec. The maximum speed of mobile cluster heads varies from 1 to 10 m/sec. Moreover, sensor nodes are heterogeneous in terms of transmission range, which is set from 20m to 25m. To perform numerical analysis, a network simulator NS2 is used in this research work. We used four measurement metrics for performance evaluation of the proposed framework with existing solutions, i.e., network lifetime, energy consumption, average end-to-end delay, and packet delivery ratio.

TABLE 1. Simulation parameters for WSN based on mobile IoT.

Parameter	Value
Monitoring area	200m X 200m
Deployment	Random
Packet size, k	50 bits
Payload size	512 bytes
MAC layer	IEEE 802.15.4
Control message	20 bits
Node's transmission range	20m to 25m
Simulation time	2000sec
Network interface type	WirelessPhy

The energy model for the proposed framework is used heterogeneity mobile cluster heads with respect to their energy levels. The number of mobile cluster heads assumed as advance nodes are equipped α times the higher energy as compared to normal nodes.

V. NUMERICAL ANALYSIS

The subsequent sections demonstrate the analysis for the proposed framework against efficient distance-aware routing protocol, LEACHDistance-M, and MECA.

A. ANALYSIS OF NETWORK LIFETIME

This section explores the performance of the proposed framework against the available solutions with respect to varying network nodes. In Fig.3, it is seen that the proposed framework longer network lifetime as 23%, 26 %, and 30 %, compared to available approaches. In particular, the performance of existing solutions degrades network lifetime due to the construction of unstable network regions. Furthermore, the routing decisions of the existing solutions are non-optimal and robust. While the performance of the proposed framework in regard to network lifetime remains stable in a relative situation. This is due to the fact that energy efficient portions are developed based on distributed voronoi cells. Moreover, the construction of voronoi cells leads to achieving better load balancing among sensor nodes. In addition, the proposed framework keeps track of the near relative position of mobile cluster heads and leads to the least communication overheads. Therefore, the experimental results demonstrate that the proposed framework improved network lifetime at varying network nodes in the comparison of other solutions.

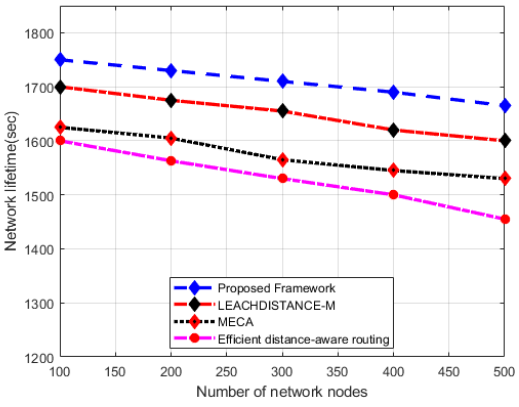

FIGURE 3. The impact of network nodes on network lifetime.

Fig.4 illustrates network lifetime with respect to varying data sending rate from 1 to 5 seconds. Based on experiment results, it is seen that the proposed framework longer the network lifetime by 28%, 33%, and 37% respectively in the comparison of existing schemes. This is due to the proposed framework provides lightweight and reliable data security mechanisms based on XOR hash function. Furthermore, unlike existing solutions that update the routing paths more frequently, the proposed framework re-adjust the routing path based on the relative position of mobile nodes with the least variation. In addition, the only limited number of mobile cluster heads across the boundary of voronoi cells are responsible for data aggregation and forwarding towards BS.

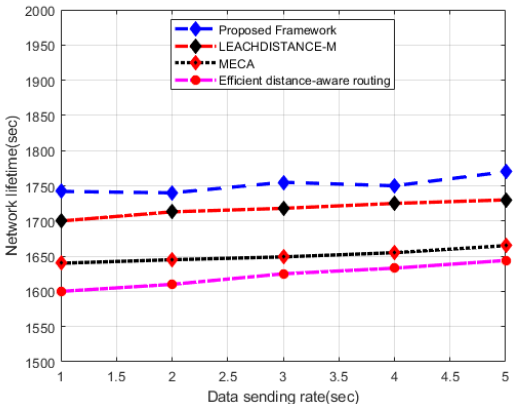

FIGURE 4. The impact of a data sending rate on network lifetime.

B. ANALYSIS OF ENERGY CONSUMPTION

Fig.5. depicts the behavior of the proposed framework in the comparison of other solutions while considering a varying number of network nodes. According to experimental analysis, it is seen that the proposed framework has improved performance than existing solutions, as it attained 28 %, 31% and 35% improvement in energy consumption. Unlike other solutions, the proposed framework keeps track of cluster heads mobility by using uncertainty principle and updates the routing paths towards BS based on network analysis. Due to network analysis, the routing paths are updated based on the node's demand. Furthermore, the proposed framework decreases the multi-hop data transmission and excessive energy consumption of sensor nodes, because it rotates the mobile cluster heads inside the voronoi cells to sense the information. In addition, mobile cluster heads re-adjust the shortest routing paths towards BS that eliminate unnecessary energy consumption in the network field. In this way,

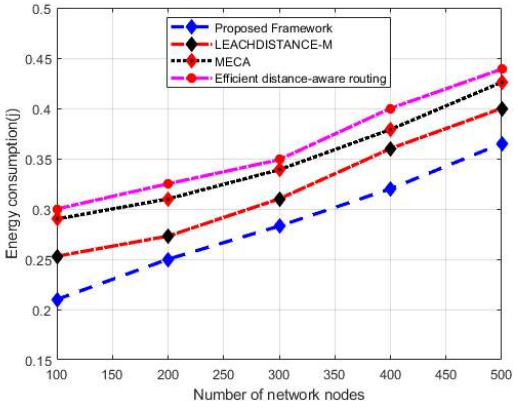

FIGURE 5. The impact of network nodes on energy consumption.

only partial mobile cluster heads are chosen to send the aggregated data towards BS.

Fig.6 illustrates the behavior of the proposed framework with existing solutions in terms of varying data sending rates from 1 to 5 seconds. Based on experimental results, it is seen the proposed framework improved energy consumption by 26%, 29 and 33% in comparison to other solutions. This is due to using of mobile cluster heads, as a lower amount of energy is consumed while sending beacon messages for routes construction. In addition, using the optimal routing decisions based on the uncertainty principle, only a set of mobile cluster heads are selected for data routing and improves overall network energy consumption.

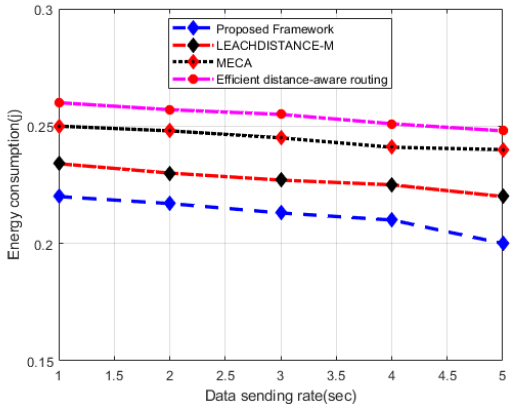

FIGURE 6. The impact of a data sending rate on energy consumption.

C. ANALYSIS OF PACKET DROP RATIO

Fig.7 depicts the behavior of the proposed framework with other solutions under a varying number of network nodes. It is observed that the proposed framework reduces the packet drop ratio as 26%, 29% and 34% in the comparison of other solutions. The existing solutions extremely lessen the attainable data delivery performance because of instability and congested data links. On the other hand, our proposed framework minimizes the packet drop ratio by selecting the energy efficient routes based on the multi-hop approach. In addition, the proposed framework avoids choosing unreachable next-hop and decreases the number of route re-adjustments. In this way, choosing distance parameters results in decreasing delivery latency and improves data delivery performance. In addition, the proposed framework provides a data security scheme based on blockchain technology, which encrypts the information using the hash function based on the XOR function. The proposed security scheme identifies the abnormal activities caused by malicious nodes and decreases the chance of packets drop ratio.

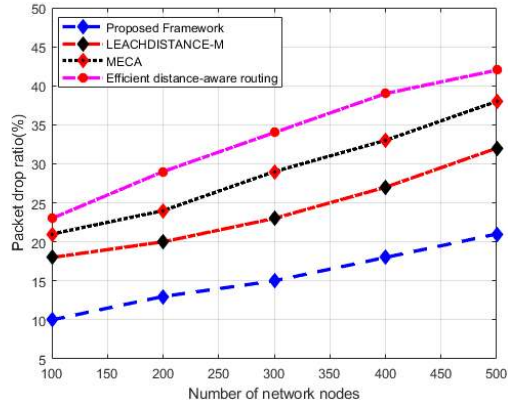

FIGURE 7. The impact of network nodes on the packet drop ratio.

Fig.8 illustrates the analysis of varying data sending rate on the packet drop ratio. It is seen that the proposed framework decreases packet drop ratio by 29%, 34%, and 39% in the comparison of existing solutions. The reason is to identify near optimum forwards from sensor nodes to mobile cluster heads and from mobile cluster heads to BS. In most of the existing solutions, data security is unnoticed, which results in dropping the data delivery ratio. The high packet drop ratio in the existing solutions is because of the rapid movement of sensor nodes as route re-adjustment process. Furthermore, in the proposed framework, a more priority is given to those mobile cluster heads for data routing that have updated optimal distance towards BS with minimum variations in their momentum.

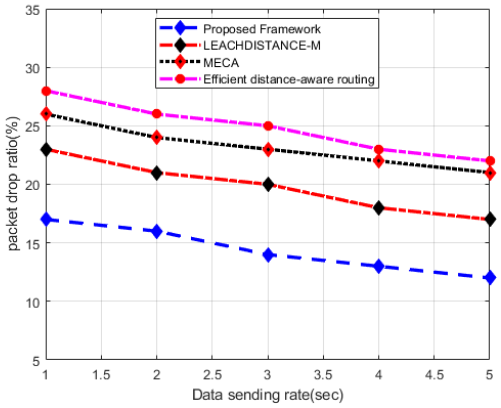

FIGURE 8. The impact of a data sending rate on the packet drop ratio.

D. ANALYSIS OF END-TO-END DELAY

Fig.9 illustrates the measurement of average end-to-end delay for the proposed framework in the comparison of existing solutions. As demonstrated in the experimental results that the proposed framework has a lower end to end delay as 26%, 29%, and 35% than compared to the existing solution, especially in high network nodes scenario. The proposed framework selects the more dynamic and robust route towards BS based on mobile cluster heads, which leads to a longer route lifetime and ultimately decreases delivery delay. The next-hop mobile cluster heads are chosen based on its near relative position and the rate of uncertainty is very low. Moreover, the proposed framework also decreases the routing hole problem towards sensor nodes and mobile cluster heads, as cluster

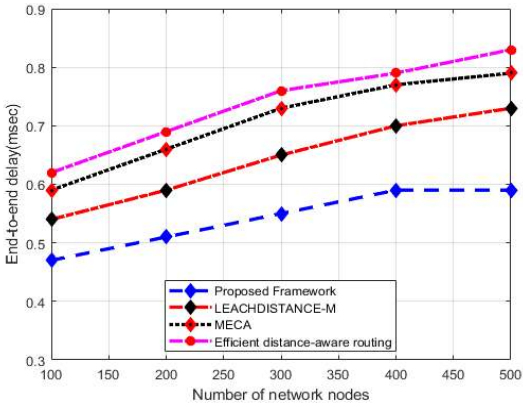

FIGURE 9. The impact of network nodes on end-to-end dela.

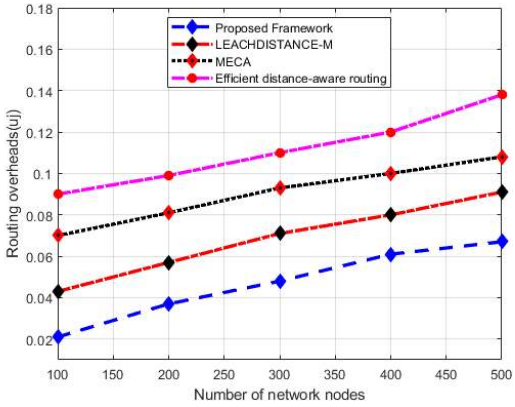

FIGURE 11. The impact of network nodes on routing overheads.

heads move around the boundary of sensor nodes, which significantly decreases the error in packet re-transmissions and ultimately the proposed framework reduces the end-to-end delay.

Fig. 10 illustrates the average end-to-end delay of the proposed framework in comparison with the existing solutions concerning varying data sending rates. Observably, higher data sending rate results in low communication overheads and decrease the ratio of end-to-end delay. It is observed as compared to existing solutions, the proposed framework decreases end-to-end delay by 24%, 28%, and 35% respectively. This is due to the identification of more reliable and secure mobile cluster heads with the least network overheads for data forwarding in comparison to the available solutions. Moreover, in support of uncertainty principle, the proposed framework minimizes the number of re-transmissions and only those mobile cluster heads are selected that have the least changes in their positions and they shorten the data transmission delay.

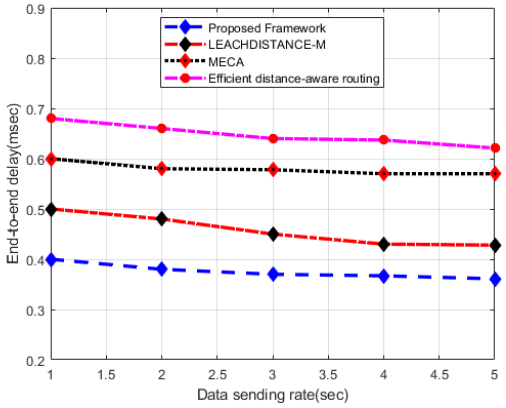

FIGURE 10. The impact of a data sending rate on network lifetime.

E. ANALYSIS OF ROUTING OVERHEADS

Fig.11 depicts the behavior of the proposed framework in the comparison of the existing solution. The proposed framework reduces the routing overhead by 28%, 30%, and 36%, respectively, as compared to the available solutions. This is because of using blockchain encryption for providing data reliability and reduces the number of attempts in data transmission. Such reduction in packets re-transmission leads to lower routing overheads and offers better network performance. Furthermore, mobile cluster heads are rotated near sensor nodes for data receiving, which results in reducing overall routing overhead. Furthermore, the proposed framework utilizes the relative position of the mobile cluster head for the best path selection, thereby improving the routing performance.

Fig.12 exhibits the routing overheads proposed framework in the comparison of existing solutions under varying data sending rate. In the experimental results, the proposed framework reduces routing overheads by 27%, 29% and 32% in the comparison of existing solutions. Unlike existing solutions that incur excessive overheads in route re-discoveries more rapidly in the presence of malicious activities. The proposed framework presents a lightweight and highly secure encryption in the form of blockchain. Moreover, the existing solutions introduced additional routing overheads that rise with high nodes mobility.

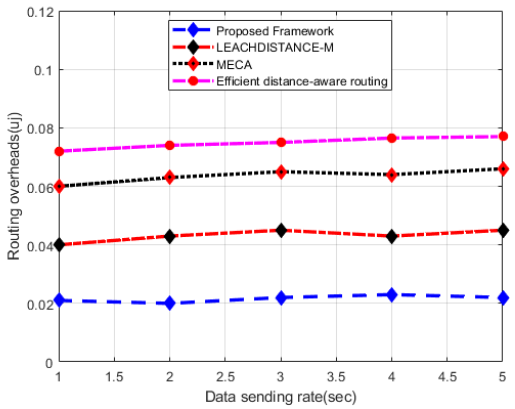

FIGURE 12. The impact of a data sending rate on routing overheads.

VI. CONCLUSION

In this paper, we present an intrusion prevention framework for secure routing in mobile Internet of Things (IoT) based on wireless sensor networks (WSN). The main aim is to improve network lifetime, data reliability with network security against malicious threats. Most of the energy efficient schemes focus on static sensor nodes and adopt the greedy algorithm for data routing. As a result, such solutions are non-feasible in dynamic scenarios. The proposed framework comprises of mobile cluster heads and chunk the network nodes in different voronoi cells. Furthermore, the proposed framework focuses on energy efficient and shortest routing chains with optimum decisions. Mobile cluster heads are chosen on the basis of uncertainty principle with the least variations in their momentum. Such an approach leads to a decrease in the routing overheads and communication costs under heavy network size. Furthermore, by using blockchain technology, secure and reliable data routing is achieved with a lightweight XOR hash function. In future work, the performance of the proposed framework will be analyzed on a realistic hardware platform.

REFERENCES

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

[2] A. B. Noel, A. Abdaoui, T. Elfouly, M. H. Ahmed, A. Badawy, and M. S. Shehata, "Structural health monitoring using wireless sensor networks: A comprehensive survey," *IEEE Commun. Surveys Tutr.*, vol. 19, no. 3, pp. 1403–1423, 3rd Quart., 2017.

[3] J. Zhang, J. Tang, T. B. Wang, and F. Chen, "Energy-efficient data-gathering rendezvous algorithms with mobile sinks for wireless sensor networks," *Int. J. Sensor Netw.*, vol. 23, no. 4, pp. 248–257, Apr. 2017.

[4] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[5] M. H. Anisi, G. Abdul-Salaam, M. Y. I. Idris, A. W. A. Wahab, and I. Ahmedy, "Energy harvesting and battery power based routing in wireless sensor networks," *Wireless Netw.*, vol. 23, no. 1, pp. 249–266, Jan. 2017.

[6] J. Wang, J. Cao, S. Ji, and J. H. Park, "Energy-efficient cluster-based dynamic routes adjustment approach for wireless sensor networks with mobile sinks," *J. Supercomput.*, vol. 73, no. 7, pp. 3277–3290, Jul. 2017.

[7] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. S. Sukhatme, "Robomote: Enabling mobility in sensor networks," in *Proc. 4th Int. Symp. Inf. Process. Sensor Netw.*, Apr. 2005, pp. 404–409.

[8] I. Din, B.-S. Kim, S. Hassan, M. Guizani, M. Atiquzzaman, and J. Rodrigues, "Information-centric network-based vehicular communications: Overview and research opportunities," *Sensors*, vol. 18, no. 11, p. 3957, 2018.

[9] Y. Yang, M. I. Fonoage, and M. Cardei, "Improving network lifetime with mobile wireless sensor networks," *Comput. Commun.*, vol. 33, no. 4, pp. 409–419, 2010.

[10] H. A. Khattak, H. Farman, B. Jan, and I. U. Din, "Toward integrating vehicular clouds with IoT for smart city services," *IEEE Netw.*, vol. 33, no. 2, pp. 65–71, Mar./Apr. 2019.

[11] I. U. Din, H. Asmat, and M. Guizani, "A review of information centric network-based Internet of things: Communication architectures, design issues, and research opportunities," *Multimedia Tools Appl.*, vol. 78, no. 21, pp. 30241–30256, 2019.

[12] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, "Convergence of MANET and WSN in IoT urban scenarios," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3558–3567, Oct. 2013.

[13] N. Tsitsiroudi, P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "EyeSim: A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs," in *Proc. 9th IFIP Wireless Mobile Netw. Conf. (WMNC)*, Jul. 2016, pp. 103–109.

[14] I. U. 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.

[15] I. U. 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.

[16] S. P. Singh and S. C. Sharma, "A survey on cluster based routing protocols in wireless sensor networks," *Procedia Comput. Sci.*, vol. 45, pp. 687–695, Jan. 2015.

[17] X. Yuan, M. Elhoseny, H. K. El-Minir, A. M. Riad, "A genetic algorithm-based, dynamic clustering method towards improved WSN longevity," *J. Netw. Syst. Manage.*, vol. 25, no. 1, pp. 21–46, 2017.

[18] P. S. Mehra, M. N. Doja, and B. Alam, "Fuzzy based enhanced cluster head selection (FBECS) for WSN," *J. King Saud Univ.-Sci.*, to be published.

[19] M. Elhoseny and A. E. Hassanien, "Expand mobile WSN coverage in harsh environments," in *Dynamic Wireless Sensor Networks*. Cham, Switzerland: Springer, 2019, pp. 29–52.

[20] A. Abuarqoub, M. Hammoudeh, B. Adebisi, S. Jabbar, A. Bounceur, and H. Al-Bashar, "Dynamic clustering and management of mobile wireless sensor networks," *Comput. Netw.*, vol. 117, pp. 62–75, Apr. 2017.

[21] A. W. Regis and E. B. Rajsingh, "Mobile entities in wireless sensor networks: Comparative study and performance analysis," *Int. J. Inf. Commun. Technol.*, vol. 11, no. 3, pp. 301–324, 2017.

[22] W. Wen, S. Zhao, C. Shang, and C.-Y. Chang, "EAPC: Energy-aware path construction for data collection using mobile sink in wireless sensor networks," *IEEE Sensors J.*, vol. 18, no. 2, pp. 890–901, Jan. 2018.

[23] M. Ahmad, T. Li, Z. Khan, F. Khurshid, and M. Ahmad, "A novel connectivity-based LEACH-MEEC routing protocol for mobile wireless sensor network," *Sensors*, vol. 18, no. 12, p. 4278, 2018.

[24] S. Pirbhulal, H. Zhang, 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. 1, p. 69, 2017.

[25] M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally, "Internet of Things (IoT): Research, simulators, and testbeds," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1637–1647, Jun. 2018.

[26] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[27] 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, HI, USA, 2000, p. 10.

[28] O. Mezghani and M. Abdellaoui, "Improving network lifetime with mobile LEACH protocol for wireless sensors network," in *Proc. 15th Int. Conf. Sci. Techn. Autom. Control Comput. Eng. (STA)*, Dec. 2014, pp. 613–619.

[29] T. Banerjee, B. Xie, J. H. Jun, and D. P. Agrawal, "Increasing lifetime of wireless sensor networks using controllable mobile cluster heads," *Wireless Commun. Mobile Comput.*, vol. 10, no. 3, pp. 313–336, 2010.

[30] J. Wang, B. Li, F. Xia, C.-S. Kim, and J.-U. Kim, "An energy efficient distance-aware routing algorithm with multiple mobile sinks for wireless sensor networks," *Sensors*, vol. 14, no. 8, pp. 15163–15181, Jun. 2014.

[31] P. Khandnor and T. Aseri, "Threshold distance-based cluster routing protocols for static and mobile wireless sensor networks," *Turkish J. Elect. Eng. Comput. Sci.*, vol. 25, no. 2, pp. 1448–1459, 2017.

[32] 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.

[33] J. Wang, Y. Yin, J.-U. Kim, S. Lee, and C.-F. Lai, "A mobile-sink based energy-efficient clustering algorithm for wireless sensor networks," in *Proc. IEEE 12th Int. Conf. Comput. Inf. Technol.*, Oct. 2012, pp. 678–683.

[34] M. Cardei, Y. Yang, and J. Wu, "Non-uniform sensor deployment in mobile wireless sensor networks," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jun. 2008, pp. 1–8.

[35] Y. Yang and M. Cardei, "Movement-assisted sensor redeployment scheme for network lifetime increase," in *Proc. 10th ACM Symp. Modeling, Anal., Simulation Wireless Mobile Syst.*, 2007.

[36] A. Dvir, V.-T. Ta, S. Erlich, and L. Buttyan, "STWSN: A novel secure distributed transport protocol for wireless sensor networks," *Int. J. Commun. Syst.*, vol. 31, no. 18, p. e3827, 2018.

[37] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 4957–4968, Sep. 2019.
[38] I. U. Din, M. Guizani, J. J. P. C. Rodrigues, S. Hassan, and V. V. Korotaev, "Machine learning in the Internet of Things: Designed techniques for smart cities," *Future Gener. Comput. Syst.*, vol. 100, pp. 826–843, Nov. 2019.
[39] K. Haseeb, N. Islam, A. Almogren, I. U. Din, H. N. Almajed, and N. Guizani, "Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs," *IEEE Access*, vol. 7, pp. 79980–79988, 2019.
[40] 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.
[41] D. Z. Morris, "Leaderless, blockchain-based venture capital fund raises 100 million, and counting," *Fortune (Mag.)*, to be published.
[42] N. Popper, "A venture fund with plenty of virtual capital, but no capitalist," New York Times, 2016
[43] P. Busch, T. Heinonen, and P. Lahti, "Heisenberg's uncertainty principle," *Phys. Rep.*, vol. 452, no. 6, pp. 155–176, 2007.
[44] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

KHALID HASEEB received the M.S.-IT degree 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 several years of experience in teaching and research and development. His research areas include wireless sensor networks, ad hoc networks, network security, the Internet of Things, software define networks, and sensor-cloud. He involves as a Referee 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 working as an Assistant Professor with the Department of Computer Science, Islamia College Peshawar, Pakistan. His research interests include computer vision, information security, machine learning, artificial intelligence, and wireless sensor networks. He is the author of numerous international journals and conference papers. He is a regular Reviewer of the IEEE, Elsevier, and Springer Journals.

AHMAD ALMOGREN received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. Previously, 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 for 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 for the development and quality with the College of Computer and Information Sciences, King Saud University. His research areas of interests include mobile and pervasive computing, cyber security, and computer networks. He has served as a guest editor for several computer journals.

IKRAM UD DIN (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 is currently a Lecturer with 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.