IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 September 2024, accepted 25 November 2024, date of publication 2 December 2024,
date of current version 10 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3509692

RESEARCH ARTICLE

Mobile Secured IoT Sensors-Driven Network Using Efficient QoS Management

MOHAMMAD SIRAJ[1], (Senior Member, IEEE), MAJID ALTAMIMI[2], (Member, IEEE), AND ZEESHAN AHMAD ABBASI[2]

[1]Department of Electrical Engineering, College of Engineering, King Saud University, Riyadh 11543, Saudi Arabia
[2]University Polytechnic, Jamia Millia Islamia, New Delhi 110025, India

Corresponding author: Mohammad Siraj (siraj@ksu.edu.sa)

This work was supported by the Deputyship for Research and Innovation, 433 Ministry of Education, Saudi Arabia, under Grant IFKSUOR3-459.

ABSTRACT Autonomous services use future networks with consumer electronic devices for the growth of real-time systems. The Internet of Things (IoT) collects data from unpredictable networks using wireless systems and forwards it toward analyzing servers. Due to the uncertain behavior of devices, next-generation technologies pose significant research challenges while maintaining load balance communication and device mobility. Most solutions enhance the management of data flow using centralized computing, but distributed and heterogeneous channels still cause reliability issues. With the use of mobile agents, this research offers quality-aware services and a cooperative protocol for unbalanced IoT networks. Examining the mobility patterns of devices, it effectively achieves massive amounts of data across established connections and lowers communication faults for diverse services. Furthermore, the routes are optimized by integrating energy and resource constraints. To increase the trustworthiness of dynamic networks, mobile devices interact with intelligence with lightweight processing strategies. Secondly, different performance metrics are incorporated to assess the robustness of security for emerging IoT applications. The significance of the proposed protocol is evaluated and experimental results revealed its noteworthy performance other than state-of-the-art schemes.

INDEX TERMS Internet of Things, mobile networks, reliability, sensors management, future technologies.

I. INTRODUCTION

IoT is a cutting-edge technology that supports the observation and analysis of real-time applications to assist network users and communication devices [1], [2]. Sensors-enabled technologies and Quality of Service (QoS) are interconnected to provide a significant role in the development and implementation of next-generation services [3], [4]. The integration of IoT devices and next-generation technologies offered many real-time developments in consumer applications for healthcare, transportation, smart home, etc. They provide crucial services in unpredictable environments and facilitate communication services with timely responses [5], [6]. Moreover, edge computing provides local computing for the constraint sensors and improves the QoS performance in critical communication services [7], [8]. In this context, data forwarding and collaboration among consumer technologies describe the procedure to facilitate communication with external networks, such as cloud systems. However, achieving QoS-aware routing presents an innovative challenge in ensuring secure data management. With the incorporation of trusted and secured methods, critical operations require high-quality and timely delivery of collected data. As a result, many researchers today are concentrating on developing reliable, performance-oriented techniques for mobile networks with the support of data protection and security measurement [9], [10]. Moreover, due to unpredictable network environments, communication between real-time devices should be able to adopt the decision by exploring various realistic factors [11], [12]. In recent decades, most

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

of the existing solutions have been unable to handle the security of big data security under high-traffic distribution and provide ineffective services to consumer applications. Such inefficiency not only has an impact on data processing and transmission in real-time but also exposes sensitive data to potential security breaches [13], [14]. Therefore, the incorporation of mobile networks with IoT devices has demanded opportunities for the development of intelligent systems. These networks offer higher flexibility and coverage making them more appropriate for the growth of smart applications. The challenges, however, lie in ensuring an effective data management system with reliability and timely performance [15], [16]. Also, sensors with constrained processing, memory, and power resources require an effective and lightweight communication system to optimize the usage of resources [17], [18]. Thus, mobile networks improve the process of data collection in dynamic environments like disaster management, wildlife tracking, or smart cities by increasing coverage and flexibility. Mobility, however, also introduces difficulties in preserving network stability, efficient routing, and energy consumption. As a result, we require an autonomous, predictive communication system that can make effective decisions with a high degree of dependability [19], [20]. In the proposed protocol, sustainable communication is achieved by recording the mobility patterns and enhancing network survivability. In addition, the load balancing is examined in conjunction with QoS considerations to identify robust routes and reduce extra overheads for significant applications. Furthermore, a major security improvement is made to ensure the persistence of the network while the adaptation of high-level edge computing, results in securing data forwarding points and ultimately eliminating disruptive events. The proposed work makes the following primary contributions.

i. Distributed computing provides support for dynamic attributes and mobility patterns of communication devices. It offers congestion-free multi-path routing for prolonged network survivability.
ii. For a diverse and constrained network environment, QoS-driven decisions are combined to maintain routing trust while providing effective and intelligent resource management.
iii. It addresses various security concerns to attain privacy and authentication for real-time data.

The following subsections comprise the organization of this research work. Section II presents the related work. Section III gives the problem background of the issue. Section IV discusses the proposed protocol and system model. The simulation and a discussion of the experimental findings are covered in Section V. In Section VI, the conclusion is provided.

II. LITERATURE WORK

In smart cities, an ecosystem of interconnected devices, including mobile devices, actuators, sensors, and many intermediate devices [21], [22], [23]. Integrating consumer electronics into sensors-enabled networks provides the development of adaptive communication systems with the support of a variety of services, including smart home, industrial IoT, and healthcare monitoring [24], [25]. The next-generation network offers an integrated and more efficient communication infrastructure to support a variety of services in the digital age. Such a system improves communication services by integrating various functionalities of IoT devices [26], [27], [28]. By utilizing IoT technologies, there is a lot of potential for creating a more inventive, effective, and connected digital ecosystem. Sensor-equipped smart devices help consumer networks to collect data from different resources. However, due to the sensitive nature of the gathered information, security is also an essential factor for next-generation networks [29], [30]. In [31], authors proposed a novel protocol for WSN that utilizes sender-based responsive techniques for energy, mobility, and efficient routing. It tackles a variety of packet routing issues, particularly those related to node mobility, energy optimization, and energy balancing in communication. The proposed protocol predicts the optimal path for an effective transmission system and enhances the fundamental QoS metrics for each connection. It proposed an energy-efficient and secure routing protocol using node trust values and fuzzy rules. However, under highly dynamic environments where energy efficiency and mobility management require more advanced, context-aware mechanisms, it may face limitations in scalability and adaptability to diverse network conditions. A WSN model for forest fire detection was proposed in [32] using an effective clustering and routing technique. The proposed model is referred to as Energy Efficient Routing Protocol (EERP). It reduces cluster head idle listening, saving sensor node energy. By limiting the number of sensor nodes that can report an event to nearby nodes, EERP reduces redundant data. Data is sent from source nodes to the Base Station (BS) via multi-hop routes by EERP. The proposed model is compared with the MAC protocol to evaluate its performance under various scenarios. However, it causes uneven energy consumption between nodes, potentially due to early node failure in critical areas. Moreover, clustering may not adapt well to rapidly changing environmental conditions, affecting real-time fire detection reliability. The development of a novel energy-efficient two-stage routing protocol (EETSP) [33] aims to decrease sensor network energy consumption and extend network lifetime. It reduces network energy consumption by the cluster heads (CHs) and secondary cluster heads (SCHs) and greatly increases the amount of packets communicated to the BS. SCH serves as a backup for primary CH. There are two stages to the EETSP. In the first step, CH and SCH are chosen based on the input parameters and the second stage involves both intra-cluster and inter-cluster routing. Though, due to the two-stage process of the proposed protocol, route management incurs additional complexity and communication costs. In [34], authors proposed a secure routing model to perform optimal path selection and encryption. First, nodes or optimal paths are selected for

secure transmission in optimal link-state multipath routing. An algorithm called Crossover Mutated Marriage in Honey Bee (CM-MH) is developed and proposed for optimal path selection destination and source. To ensure secure transmission, encryption is applied. The Better Blowfish Algorithm (IBFA) is proposed as a secure authentication method. Lastly, there is monitoring of the updates. Finally, the comparison tests are performed for the proposed approach and existing work. It overlooked the factor of scalability in large networks, which results in more computational overhead as the number of devices increases. Furthermore, although the CM-MH algorithm prioritizes optimal path selection, however, the proposed model may fail to account for the dynamic nature of real-time traffic, and leads to a sub-optimal routing under different network scenarios. Relying solely on parameters like response time, distance, and queue length may not be sufficient to address security issues or dynamic traffic patterns, potentially resulting in imbalances or congestion under changing network conditions. In mobiles sensors, authors [35] examined the effects of version number attacks in RPL networks. To identify the malicious nodes carrying out version number attacks, they proposed a solution that utilizes the Q-Learning strategy. While significantly reducing the overhead on the nodes of low power and lossy networks, the proposed method accurately identifies malicious network nodes. The main drawback of the proposed solution include higher overhead in data processing that could impair scalability on wireless devices and decrease the network adaption in the context of IoT unpredictability. Authors [36] introduced a new DAG-Blockchain architecture for MANET-IoT security. The network is secured by the Multi-Factor PUF identification technique. All allowed nodes are divided into clusters according to the network topology. In addition, based on trust, Dijikstra's method was introduced to secure data transfer with multiple criteria. A Bi-Directional GRU for deep packet analysis was also presented. Intrusions are found through deep packet inspection, and later blocking mechanism stops them. Using a combination of algorithms, the proposed method increased packet delivery ratio, productivity, time analysis, detection accuracy, and security level. However, the architecture's reliance on consensus mechanism the r s may also introduce latency, which would impair eal-time performance required in dynamic MANET environments. For MANET-IoT networks, the authors proposed a gateway selection mechanism [37]. The proposed mechanism provides load balancing within the network as well as between gateways by taking into account the gateways' response time, distance, and queue length (QL). The proposed method outperforms current schemes in terms of load balancing, delay, and packet delivery ratio (PDR) according to simulation results. In the dynamic MANET-IoT scenarios, the selection of adaptive gateways may impose additional overhead and latency in the network. In addition, the unpredictable environment of MANET lead to sub-optimal selection of gateways.

III. PROPOSED METHODOLOGY

This section includes a network model and a detailed analysis of the proposed methodology.

A. NETWORK MODEL

Our proposed system incorporates geographical sensors to sense and process the environmental data. Consumer devices such as gateways are deployed to perform a vital role between sensors and edges. We consider the sensors as mobile with predefined transmission power. Sensors have limited transmission power and can communicate with neighbors either using single or multi-hop routing. Moreover, they can perform limited computing and are not allowed to communicate with edges directly. Their positions are frequently altered with time, so they are called mobile nodes. Nodes are uniformly distributed, thus each node has an approximate number of neighbors in its radius. Network operations are performed in uncertain and unreliable environments, thus leading to security issues for privacy and data authentication. The following are assumed network considerations in the development of a proposed protocol.

i. Nodes have a restricted communication range and can only communicate with nearby nodes.
ii. The deployment area has a uniform distribution of nodes.
iii. Nodes are mobile and their initial positions are known.
iv. Malicious entities may attempt to intercept the network communication.
v. Edges and sinks are enough resource devices with significant computing and processing capabilities.

B. PROPOSED PROTOCOL

In the proposed protocol, the mobile sensors initially distribute their local information and create routing tables. The routing tables are dynamically updated using the latest information and network conditions whenever any event is triggered in the field. The extracted information makes it easy to adapt reliable and more efficient paths from the sensing field toward edge devices. Each node has to maintain unique identification ID, hop count HC, and velocity VC and timestamp TS factors in its local table and share it with neighbors in the proximity, as defined in Equation 1.

$$N_i(TS) = [ID, HC, VC] \tag{1}$$

ID is a unique identifier that helps in identifying the data of sensors and involvement in any routing path. HC denotes the distance in terms of hop count from the source node towards the edge and should be the least for optimal energy consumption. Let us consider that $S_i, S_{i+1}, S_{i+2}, \ldots, S_n$ are series of neighbors from N_i to edge ED_i, then HC can be defined in Equation 2.

$$HC(N_i \rightarrow ED_i) = HC\,(S_i) + HC(S_i, S_{i+1}) + \ldots + HC(S_n, ED_i) \tag{2}$$

VC determines the mobility speed of the sensor in its proximity and the node whose velocity rate is not highest in a

particular time interval, selected for the optimal decision. We consider the distance parameter to compute the velocity of nodes as defined in Equation 3. Let us consider mobile sensor-covered distance d_j at time interval t_j from distance d_i at time interval t_i.

$$VC_i = (d_j - d_i)/(t_j - t_i) \tag{3}$$

The proposed protocol determines the distance level D of the computed node velocity within the preset distance threshold DT. If the VC_i value is higher than a threshold, then its entry is recorded separate list indicates not suitable for considering the node for the routing scheme, as defined in Equation 4.

$$\begin{cases} D(VC_i) \leq DT, \text{True} \\ D\,(VC_i) \geq DT, False \end{cases} \tag{4}$$

The proposed protocol explores the aggregation function Z with composite computing based on the weights (w_1, w_2) and criterion parameters (HC, VC) using Equation 5. Afterward, the proposed protocol chooses the mobile node for routing the data packets whose aggregated function is minimum.

$$min(Z) = w_1 \text{x} HC + w_2 \text{x} VC \tag{5}$$

where the weighted parameters w_1 and w_2 uniformly contribute to the hop count and velocity factors, so that the sum of these values equals 1. Edge nodes store the values of the aggregated functions in their table and keep track of the energy resources of the selected mobile node. In case, the energy level EL falls than a certain threshold it sends beacon messages in its proximity to recompute the Z value for the competitive nodes. The next phase of the proposed protocol is to provide the security analysis for authentication, privacy, and data availability. Edge nodes group the mobile nodes in various groups based on proximity computing. Those nodes that are closest to a certain distance limit are arranged into a particular group. We assume that G_i denotes the set of groups that are comprised of various mobile sensors as denoted by Equation 6.

$$G_i = \sum_{i=0}^{k} S_n, \tag{6}$$

where S_n is mobile nodes fall in a particular distance limit. Later, the edge node generates particular keys K_i and share among each group G_i as defined in Equation 7.

$$K_i = [K_1, K_2, \ldots\ldots, K_n] \tag{7}$$

Moreover, each key K_i is encrypted using a public key of the edge node E_{ed} and stamp time T' is incorporated as given in Equation 8.

$$ED \rightarrow G_i{:}E_{ed}\,(K_i) + T' \tag{8}$$

Whenever any mobile node needs to transfer the network data, it needs to authenticate using the grouped key and accordingly, it is allowed to be a part of the routing scheme. Furthermore, group keys are updated by the proposed protocol based on fixed time intervals. Such methods reduce the probability of data compromise and increase the trust level among the nodes. The new keys K_i' are generated by exploring the random number generator (RNG) to produce a unique random value R_i, as given in Equation 9.

$$K_i' = R_i + K_i \tag{9}$$

Figure 1 depicts the three main stages of the proposed protocol in a consumer-based networked system. In the beginning, consumer devices and sensors interact with each other based on proximity and record the routing information in the form of tables. The tables are refined by exploring the new information and network conditions. In the middle layer, edges and gateways are explored to perform the role of central hubs between consumer networks and cloud systems. The various criterion parameters are identified to compute the aggregated function and the least weighted value node is selected among sensors as a data forwarder of consumer applications. Moreover, threshold-based analysis is performed to identify another round of data forwarder selection. Later, group-based keys are generated and distributed to individual groups. Keys are updated using random numbers which reduces the chances of data leakage and increases the degree of authentication. In the end, complex data security and availability are attained between central hubs and cloud systems.

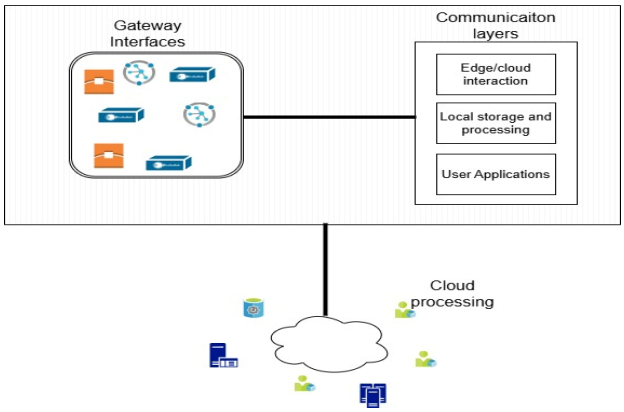

FIGURE 1. Stages of proposed mobility aware secured QoS aware routing for mobile IoT applications.

In the proposed protocol, several key strategies improve security mechanisms and address previous limitations over most of the existing work such as key compromise, replay attack, man in the middle (MitM) attack and data tampering. By using group-based key distribution and frequent key updates, the approach mitigates key compromise risk. Each group has a unique key, and periodic updates ensure that even if a group is compromised, its lifespan is short, minimizing potential damage. Moreover, by exploring secure key distribution, even if an attacker intercepts the communication, then frequent key updates with integrity checks make MitM and data eavesdropping attacks difficult. The integration of distributed edge processing mitigates Denial of Service (DoS) attacks by ensuring that other network segments can function even if one is overloaded. In addition, to the time-based methods, the proposed protocol also

provides an effective mechanism to avoid the replay attack using the unique key pattern. Figure 2 illustrates the flowchart of the developed routing protocol in the proposed protocol. The routing strategies are based on the analysis of the multi-criterion which is comprised of distance in terms of hop count and velocity of mobile sensors. Both factors are aggregated in a composite manner and offer the optimal data forwarders. Based on the preset thresholds, the evaluation criteria are re-accessed and the network is flooded with the newly selected forwarders. Accordingly, routing tables are also updated and neighbors are notified of the latest identifications of data forwarders. Figure 3 shows the flowchart for the proposed security methods. Edge devices initiate to determine the nearest mobile sensors using distance parameters. Once they are found, then groups are created and each group is assigned a particular key. The keys are securely distributed between the groups and after the time interval, the keys are updated. This provides less chances of data breaches and offers a high degree of authentication for mobile sensors. Moreover, to attain privacy and availability, the proposed protocol computes security functions on the incoming data and key patterns. The pseudocodes of the proposed protocols are depicted in Algorithm 1 and Algorithm 2. The main procedures of the developed algorithms are mobile routes detection MOB_SRoutes ( ) and device authentication DEVs_Authentication ( ). In MOB_SRoutes ( ), by exploring multiple parameters aggregated function is executed and determines the weighted value. The computed value is dynamically updated based on the energy level threshold and readjusts the mobile routes. To enable adaptive route management, the computed weighted value is dynamically modified based on the nodes' energy level threshold. The uniform weighted values contribute to each factor in a way that balances load distribution across sensor nodes and communication links, optimizing network performance. Using DEVs_Authentication ( ), the proposed protocol is made suitable for resource-constrained environments, resulting in providing an authentication mechanism for node authenticity with minimal processing overhead. Moreover, edges confirm the incoming request for the specific group, and keys are safely generated to distribute throughout the groups. To further increase the unpredictability of intrusions and reduce the likelihood of data breaches, keys are updated at random. However, as the number of nodes increases, the proposed MOB_SRoutes ( ) procedure leads to high computational complexity for constraint devices, because the recomputing of weighted values imposes additional overhead for the management of routes. Moreover, as the network grows, the generation and sharing of cryptographic keys using the DEVs_Authentication ( ) procedure also may lead to increased processing time.

C. SECURITY METHODS WITH ANALYSIS

The proposed mobile IoT protocol for edge cloud environment provides a robust mechanism to attain data security in the following ways.

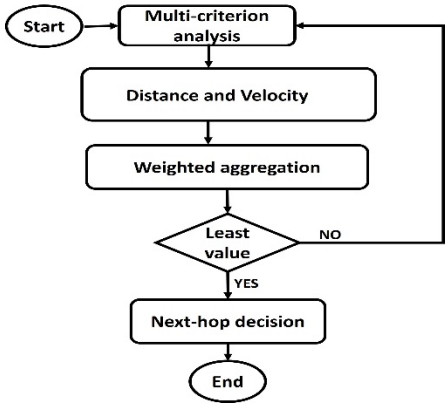

FIGURE 2. Flowchart of the proposed routing in the sensors-driven IoT network.

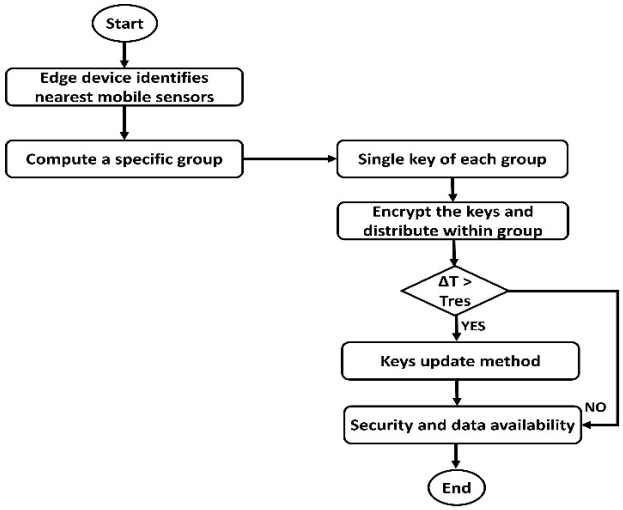

FIGURE 3. Security against authentication and privacy for the proposed protocol.

i. The use of separate keys for each group of mobile sensors ensures that data is encrypted and kept private among sensors. Unauthorized entities outside of the group cannot access the data because they do not possess the keys.
ii. In the proposed protocol, key-based authentication ensures that only authorized devices can send and receive group data. It minimizes the risk of unauthorized access caused by leaked or compromised keys by periodically updation policy.
iii. Security functions verify data integrity by exploring digital signature during transmission, ensuring it hasn't been tampered. Thus results in prevents data injection or attack by malicious entities.
iv. Distributed security functions at the edge reduce the chances of cloud service availability. Even during interruptions in cloud connectivity, it ensures that the system remains operational and responsive.

IV. RESULTS DISCUSSION

This section evaluates the proposed protocol against relevant studies. To evaluate the experimental results, we utilized

Algorithm 1 Optimized Mobility-Aware Efficient Sensors Data Routing

Procedure MOB_SRoutes ()
collect local data
update routing tables
for (i = 1; i <= N; i + +)
do
multi-criterion analysis
determine aggregated function
$min(Z) = w_1 \times HC + w_2 \times VC$
announced to neighbory
end for
compute the energy level threshold
if forwarder energy < threshold **then**
send RREQ
recall multi-criterion analysis
update the entries
end if
end procedure

Algorithm 2 Group-Based Device Authentication and Security for Sensor Data

Procedure DEVs_Authentication ()
establish a group of mobile sensors
generate keys for each group
securely distribute the set of keys K_i
if the timer is expired then
regenerate the new keys K_i' using RGN
$ED \rightarrow G_l : E_{ed}(K_i) + T'$
end if
perform data security using XoR methods for peer nodes
end procedure

network simulator NS-2.35. The scripting files are used to compute statistical analysis, and the simulations are recorded in trace files. We used mobile sensors along with edges that perform the role of gateways in the network environment. The mobile sensors are rotated in the surroundings with some mobility speed and gather the data. The size of the network field is set to 1000m X 1000m. Sensor nodes are varied from 100-400 with an initial energy of 2j. The number of sinks is set to 2. Each node is equipped with GPS and its transmission power is set to 3m. We ran 25 simulations to evaluate the average improvement of the proposed protocol with EERP and EETSP by exploring scenarios: varying iterations (1000s – 6000s) and varying numbers of nodes (100 - 400). In Table 1, the simulation parameters are provided.

The evaluation of network throughput for the proposed protocols with different numbers of iterations is depicted in Figure 4. The experimental results illustrate that the proposed protocol outperforms existing approaches by an average of 17% and 21%. The proposed protocol employs the concept of parallel route identification

TABLE 1. Network parameters.

Factor	Value
Mobile sensors	100-400
Number of packets	30-150
Malicious nodes	8
Transmission radius	10m
Initial energy	5j
Sink nodes	2
Mode of data flow	CBR
Bandwidth	2Mbps
w_1 and w_2	0.5, 0.5

and attains reliable communication channels until sensor data reaches the destination. Moreover, it optimizes the use of network resources by re-computing parameters that balance the load on transmission links, ensuring efficient traffic distribution. Also, agents are mobile and crucial components of the proposed protocol, as they serve as intermediary devices in closest proximity to the low-powered devices. They intelligently collected the IoT data and decreased the transmission distance with effective data delivery performance. To reduce risks and secure the data transmission process, the proposed protocol has a robust security stage that examines communication channels and retains the desired throughput for critical network applications.

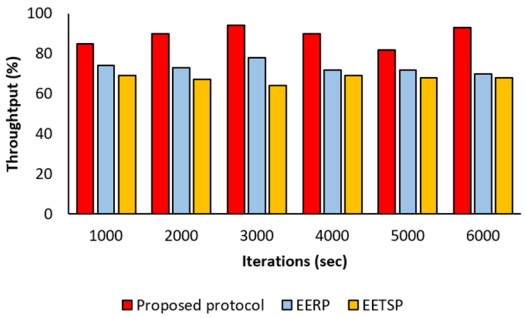

FIGURE 4. Performance of network throughput with varying iterations (1000s – 6000s).

The experimental outcomes of the proposed protocol in comparison to the existing solution are illustrated in Figure 5. The proposed protocol balances resource consumption and node congestion to optimize sensor performance through the use of distributed computing. It was noticed that the proposed protocol increases the network throughput by an average of 18% and 23.4% under different numbers of sensors, owing to the selection of several criteria-based parameters. The network edges are mobile that not only limits the transmission power of the constraint devices but also eliminates

the interrupted links for transmissions of data. The dynamic mobility of network edges, which not only reduces the transmission power requirements of resource-constrained devices but also proactively removes unstable or interrupted links, is a significant advancement in the protocol. The proposed protocol significantly improves the performance and reliability of IoT networks under a variety of network topology changes, node mobility, and traffic load conditions by utilizing adaptive routing and load-balancing techniques.

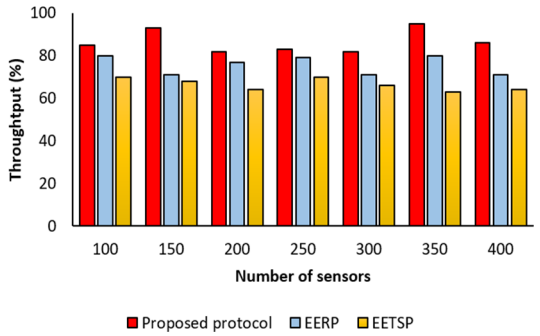

FIGURE 5. Performance of network throughput with varying sensors (100 - 400).

In comparison to the existing solutions, the proposed protocol reduces network latency for varying iterations by an average of 15.6% and 19.8%, as illustrated in Figure 6. This is because forwarding routes are utilized to assess node traffic and processing costs. Unlike most of the existing approaches, the proposed protocol temporarily marked a route as invalid when data forwarding is congested, and the source node is notified to find an alternative path. By identifying and mitigating faulty or malicious channels, mobile agents play a crucial role in enhancing network security and reliability. When a channel is compromised, mobile agents send alert messages to all nearby routes, preventing data transmission. The protocol also optimizes route selection for data transmission between constrained devices and mobile agents by evaluating multiple candidate paths and choosing the most efficient one. This optimized route selection significantly reduces communication overhead and uses the most efficient paths.

Under varying numbers of sensors, the performance of the proposed protocol in terms of data latency is shown in Figure 7 as compared to existing solutions. Based on the statistical results, it was seen that the proposed protocol improved the latency performance in terms of varying sensors by an average of 18% and 24.6% respectively. This results from the cooperative methods among sensors and mobile agents and storing the neighboring information by exploring the quality-aware assessment. Moreover, by generating route requests only in response to actual data forwarding events, extraneous routing overhead is reduced and latency is further decreased. Using distinct route IDs, the protocol can identify redundant links within already-existing routes, helping to simplify routing paths and reduce traffic. By

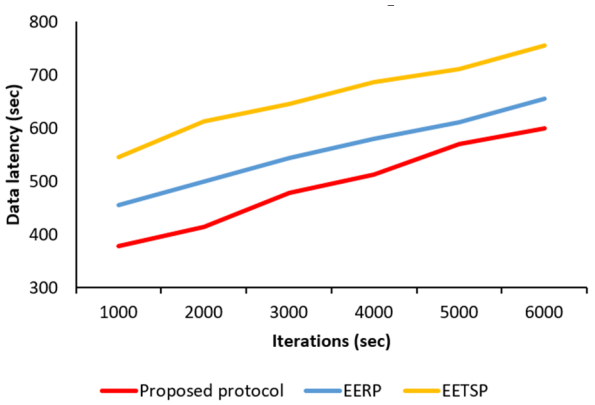

FIGURE 6. Performance of data latency with varying iterations (1000s – 6000s).

moving around their proximity, mobile agents dynamically refine their neighbor tables, marking nodes as ineffective if their cost value is below a threshold, ensuring that only the best nodes are used for routing. In addition, with effective load balancing among the devices, the rotation of edges around the network boundary reduces energy holes while simultaneously enhancing route stability and decreasing data latency.

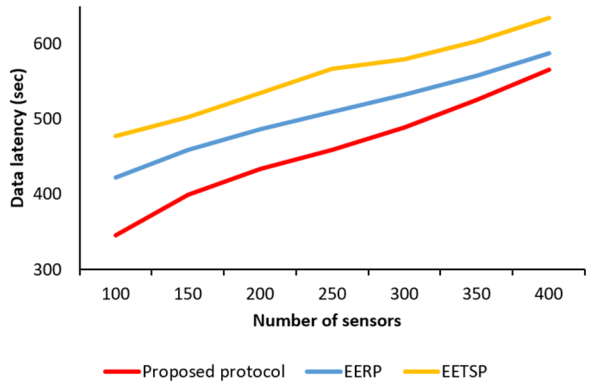

FIGURE 7. Performance of data latency with varying sensors (100 - 400).

As shown in Figure 8, the performance of the proposed protocol and the existing solution is simulated for the node residual energy. Experimental results indicate that as the number of iterations increases, the proposed protocol enhances performance by an average of 20.5% to 27.3%.

This improves the efficiency of communication bandwidth utilization by optimizing routing table information through the examination of energy, distance, and processing error parameters. The proposed protocol measures the mobile agent's distance from the source node before forwarding IoT data; if this distance is less than a predetermined threshold, data is forwarded in directly. If not, routing tables are examined to retrieve the most recent data and identify the suitable subsequent hop. If, after a certain amount of time, the designated route is still unavailable, its entry is eliminated from the routing table and the neighbors are notified.

Furthermore, the verification of nodes is established because time-oriented secret keys and encrypted timestamps are used. In this way, malicious devices are excluded from routing call, which ultimately lengthens the stability period for the network.

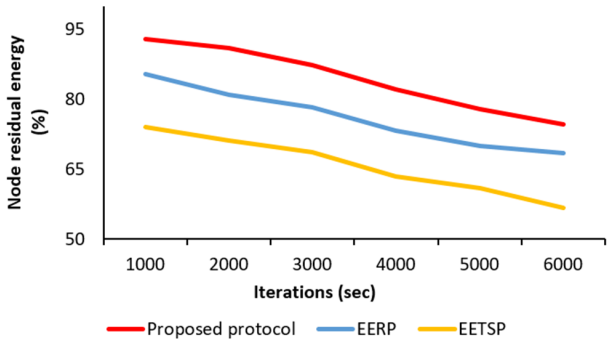

FIGURE 8. Performance of network lifetime with varying iterations (1000s - 6000s).

In Figure 9, the performance evaluation of the proposed protocol is compared with existing solutions in terms of node residual energy. It was improved for varying sensors by an average of 21.4% and 26.8% using the proposed protocol by exploring the adaptive approaches. Unlike the existing methods, the proposed protocol computes the routing criteria between the nodes using an intelligent method with balanced energy consumption across the network. Moreover, routing tables remove longer paths and only keep updated data. Unlike other systems, it sends data to wireless systems while continuously assessing device parameters and detecting the specifics of a running state. It also increases network stability by offering the most reliable neighbors for establishing node-to-node connections. Finally, mobile edges improves the nodes' consumption level of energy by collecting the sensor data with limited transmission power of the devices.

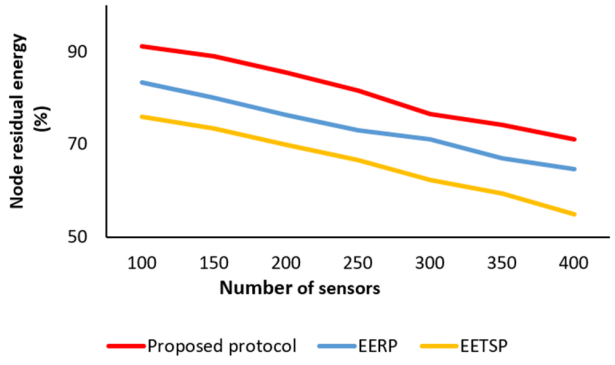

FIGURE 9. Performance of network lifetime with varying sensors (100 - 400).

Figure 10 shows the performance outcomes in terms of transmission load for the proposed protocol and existing solutions. It was observed that the transmission load increases with the deployment of malicious nodes, however, the findings indicate that the retransmission load of the proposed protocol is improved by an average of 9.4% and 12.6% as compared to earlier work for varying iterations. This is due to the involvement of mobile agents in gathering the sensed data intelligence from the low-powered sensors, and adopting the multi-hop model for data transmission. The routing decision is based on multiple parameters, and routing calls are announced in the proximity of source nodes rather than in the whole transmission area. In addition, the invalid routes are discarded from the routing tables, and up-to-date information is stored to improve the response time for end users while receiving the network data.

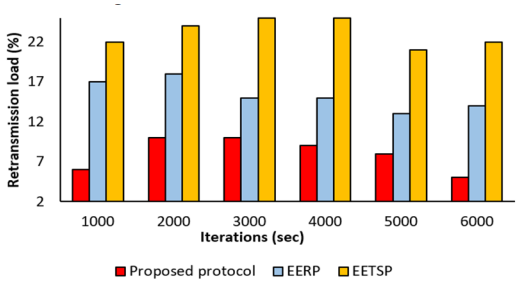

FIGURE 10. Performance of retransmission load with varying iterations (1000s - 6000s).

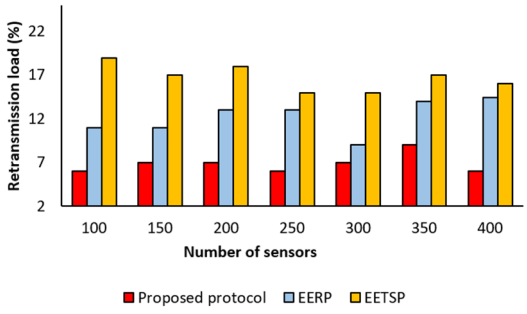

FIGURE 11. Performance of retransmission load with varying sensors (100 - 400).

The performance evaluation of the retransmission load under varying sensors is demonstrated in Figure 11. The statistical analysis shows that the proposed protocol improved the transmission load of the proposed protocol by an average of 16.7% and 26.8% respectively. The proposed protocol reduces the cost of processing and forwarding data requests by using lightweight computing techniques, ensuring a cost-effective method of resource management. To improve adaptability to changing conditions, the protocol analyzes weighted edges and takes into account multiple factors in a dynamic environment when determining the next hop. The protocol efficiently distributes the load among the sensors during the routing phase, lessening the burden on individual sensors and enhancing the network's overall reliability. Additionally, the lightweight mechanism is supported and the more trustworthy neighbors are identified for data transmission by the security process, which employs centralized

administration with the support of mobile edges. The mobile edge authenticated the incoming data from various sources and limited the overheads in case of data retransmissions.

V. CONCLUSION

Wireless networks provide seamless and secure connectivity throughout urban infrastructures, they are the driving system behind the integration of IoT devices for smart cities. To ensure protected and effective network operations, they are crucial for facilitating secure data exchange systems with the integrity of vital services. One of the main research challenges in these networks under unpredictable environments is reliable and efficient network controlling of the constraint system, despite the fact that many approaches have been developed to improve data collection and transmission operations of IoT networks. The formation of a resilient communication system critically depends on the security of data transmission over global channels. This paper presents a protocol that investigates the use of mobile sensors and intelligent computing to improve the routing between IoT-based applications, offer networked scalability, and implement security for next-generation systems. The edges implement distributed computation for communication devices and guarantee the security of the decentralized environment. It was noted, however, that the proposed protocol is unable to learn the detection strategy against threats as the number of malicious devices and false messages increases. Future work could focus on exploring machine learning algorithms to enhance QoS in mobile IoT networks by predicting patterns of network traffic and dynamic allocation of network resources. Moreover, enhanced network resilience against emerging threats can be achieved by the integration of automated vulnerability assessments with lightweight computing and regular routing updates.

REFERENCES

[1] P. K. Malik, R. Sharma, R. Singh, A. Gehlot, S. C. Satapathy, W. S. Alnumay, D. Pelusi, U. Ghosh, and J. Nayak, "Industrial Internet of Things and its applications in industry 4.0: State of the art," *Comput. Commun.*, vol. 166, pp. 125–139, Jan. 2021.

[2] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020.

[3] M. Wen, Q. Li, K. J. Kim, D. López-Pérez, O. A. Dobre, H. V. Poor, P. Popovski, and T. A. Tsiftsis, "Private 5G networks: Concepts, architectures, and research landscape," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 1, pp. 7–25, Jan. 2022.

[4] V. J. Aski, V. S. Dhaka, A. Parashar, S. Kumar, and I. Rida, "Internet of Things in healthcare: A survey on protocol standards, enabling technologies, WBAN architectures and open issues," *Phys. Commun.*, vol. 60, Oct. 2023, Art. no. 102103.

[5] A. Mishra, A. V. Jha, B. Appasani, A. K. Ray, D. K. Gupta, and A. N. Ghazali, "Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective," *Int. J. Syst. Assurance Eng. Manage.*, vol. 14, no. S3, pp. 699–721, Jul. 2023.

[6] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect," *IEEE Access*, vol. 10, pp. 4794–4831, 2022.

[7] M. Q. Aldossari and A. Sidorova, "Consumer acceptance of Internet of Things (IoT): Smart home context," *J. Comput. Inf. Syst.*, vol. 60, no. 6, pp. 507–517, Nov. 2020.

[8] S. K. Ram, B. B. Das, K. Mahapatra, S. P. Mohanty, and U. Choppali, "Energy perspectives in IoT driven smart villages and smart cities," *IEEE Consum. Electron. Mag.*, vol. 10, no. 3, pp. 19–28, May 2021.

[9] O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, "A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues," *Cluster Comput.*, vol. 24, no. 1, pp. 37–55, Mar. 2021.

[10] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, "A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things," *J. Ind. Inf. Integr.*, vol. 21, Mar. 2021, Art. no. 100190.

[11] S. Iftikhar, S. S. Gill, C. Song, M. Xu, M. S. Aslanpour, A. N. Toosi, J. Du, H. Wu, S. Ghosh, D. Chowdhury, M. Golec, M. Kumar, A. M. Abdelmoniem, F. Cuadrado, B. Varghese, O. Rana, S. Dustdar, and S. Uhlig, "AI-based fog and edge computing: A systematic review, taxonomy and future directions," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100674.

[12] G. K. Walia, M. Kumar, and S. S. Gill, "AI-empowered fog/edge resource management for IoT applications: A comprehensive review, research challenges, and future perspectives," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 1, pp. 619–669, 1st Quart., 2024.

[13] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, A. S. M. Nainar, N. M. Akim, and M. Imran, "Deep learning and big data technologies for IoT security," *Comput. Commun.*, vol. 151, pp. 495–517, Feb. 2020.

[14] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, B. Prabadevi, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, and P. N. Pathirana, "A survey on blockchain for big data: Approaches, opportunities, and future directions," *Future Gener. Comput. Syst.*, vol. 131, pp. 209–226, Jun. 2022.

[15] M. M. I. Khan and G. Nencioni, "Resource allocation in networking and computing systems: A security and dependability perspective," *IEEE Access*, vol. 11, pp. 89433–89454, 2023.

[16] N. Khan, R. B. Salleh, Z. Khan, A. Koubaa, M. Hamdan, and A. M. Abdelmoniem, "Ensuring reliable network operations and maintenance: The role of PMRF for switch maintenance and upgrades in SDN," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 10, Dec. 2023, Art. no. 101809.

[17] S. Kumar, A. Singh, A. Benslimane, P. Chithaluru, M. A. Albahar, R. S. Rathore, and R. M. Álvarez, "An optimized intelligent computational security model for interconnected blockchain-IoT system & cities," *Ad Hoc Netw.*, vol. 151, Dec. 2023, Art. no. 103299.

[18] F. H. El-Fouly and R. A. Ramadan, "Real-time energy-efficient reliable traffic aware routing for industrial wireless sensor networks," *IEEE Access*, vol. 8, pp. 58130–58145, 2020.

[19] A. Heidari, N. Jafari Navimipour, M. Unal, and G. Zhang, "Machine learning applications in Internet-of-Drones: Systematic review, recent deployments, and open issues," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–45, Dec. 2023.

[20] N. Islam, K. Haseeb, M. Ali, and G. Jeon, "Secured protocol with collaborative IoT-enabled sustainable communication using artificial intelligence technique," *Sustainability*, vol. 14, no. 14, p. 8919, Jul. 2022.

[21] L. El-Garoui, S. Pierre, and S. Chamberland, "A new SDN-based routing protocol for improving delay in smart city environments," *Smart Cities*, vol. 3, no. 3, pp. 1004–1021, Sep. 2020.

[22] M. A. Ahad, S. Paiva, G. Tripathi, and N. Feroz, "Enabling technologies and sustainable smart cities," *Sustain. Cities Soc.*, vol. 61, Oct. 2020, Art. no. 102301.

[23] A. Meslin, N. Rodriguez, and M. Endler, "Scalable mobile sensing for smart cities: The MUSANet experience," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5202–5209, Jun. 2020.

[24] Y.-C. Fan, "Emerging sensing technologies in consumer electronics," *Sensors*, vol. 21, no. 22, p. 7689, Nov. 2021.

[25] Y.-G. Ha, "Dynamic integration of zigbee home networks into home gateways using OSGI service registry," *IEEE Trans. Consum. Electron.*, vol. 55, no. 2, pp. 470–476, May 2009.

[26] S. Bansal and D. Kumar, "IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication," *Int. J. Wireless Inf. Netw.*, vol. 27, no. 3, pp. 340–364, Sep. 2020.

[27] N. Gupta, S. Sharma, P. K. Juneja, and U. Garg, "SDNFV 5G-IoT: A framework for the next generation 5G enabled IoT," in *Proc. Int. Conf. Adv. Comput., Commun. Mater. (ICACCM)*, Aug. 2020, pp. 289–294.

[28] K. Haseeb, M. Siraj, F. A. Alzahrani, Z. Ullah, and G. Jeon, "Sensor-based optimization multi-decision model for sustainable smart cities," *Sustain. Energy Technol. Assessments*, vol. 60, Dec. 2023, Art. no. 103452.

[29] J. Cook, S. U. Rehman, and M. A. Khan, "Security and privacy for low power IoT devices on 5G and beyond networks: Challenges and future directions," *IEEE Access*, vol. 11, pp. 39295–39317, 2023.
[30] L. P. Rachakonda, M. Siddula, and V. Sathya, "A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in next-generation networks (5G/6G/beyond)," *High-Confidence Comput.*, vol. 4, no. 2, Jun. 2024, Art. no. 100220.
[31] B. Dhanalakshmi, L. SaiRamesh, and K. Selvakumar, "Intelligent energy-aware and secured QoS routing protocol with dynamic mobility estimation for wireless sensor networks," *Wireless Netw.*, vol. 27, no. 2, pp. 1503–1514, Feb. 2021.
[32] R. B. Pedditi and K. Debasis, "Energy efficient routing protocol for an IoT-based WSN system to detect forest fires," *Appl. Sci.*, vol. 13, no. 5, p. 3026, Feb. 2023.
[33] A. K. Dwivedi, P. S. Mehra, O. Pal, M. N. Doja, and B. Alam, "EETSP: Energy-efficient two-stage routing protocol for wireless sensor network-assisted Internet of Things," *Int. J. Commun. Syst.*, vol. 34, no. 17, Nov. 2021, Art. no. e4965.
[34] M. Alotaibi, "Improved blowfish algorithm-based secure routing technique in IoT-based WSN," *IEEE Access*, vol. 9, pp. 159187–159197, 2021.
[35] G. Sharma, J. Grover, and A. Verma, "QSec-RPL: Detection of version number attacks in RPL based mobile IoT using Q-learning," *Ad Hoc Netw.*, vol. 142, Apr. 2023, Art. no. 103118.
[36] N. Ilakkiya and A. Rajaram, "A secured trusted routing using the structure of a novel directed acyclic graph-blockchain in mobile ad hoc network Internet of Things environment," *Multimedia Tools Appl.*, 2024, doi: 10.1007/s11042-024-18845-1.
[37] V. K. Quy, N. T. Ban, D. Van Anh, N. M. Quy, and D. C. Nguyen, "An adaptive gateway selection mechanism for MANET-IoT applications in 5G networks," *IEEE Sensors J.*, vol. 23, no. 19, pp. 23704–23712, Oct. 2023.

MOHAMMAD SIRAJ (Senior Member, IEEE) received the Bachelor of Engineering degree in electronics and communication engineering from Jamia Millia Islamia, New Delhi, the Master of Engineering degree in computer technology and applications from Delhi College of Engineering, Delhi, India, and the Ph.D. degree from Universiti Teknologi Malaysia.

Currently, he is an Assistant Professor of electrical engineering with King Saud University. He has numerous peer-reviewed publications in well-known international journals and conferences. His research interests include cognitive wireless networks, wireless mesh networks, sensor networks, the Internet of Things, cloud computing, and telecom optical networks. He is a reviewer of many well-known international journals and conferences.

MAJID ALTAMIMI (Member, IEEE) received the B.Sc.Eng. degree (Hons.) in electrical engineering from King Saud University, Saudi Arabia, in 2004, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Waterloo, Canada, in 2010 and 2014, respectively. He was a TA with the Department of Electrical Engineering, King Saud University, from 2004 to 2006. He was a TA with the Department of Electrical and Computer Engineering, University of Waterloo, in 2013. In 2015, he joined the Department of Electrical Engineering, King Saud University, as an Assistant Professor. His current research interests include analyzing the energy cost for wireless handheld devices and cloud computing architecture, integrating mobile computing with cloud computing, and studying and designing green ICT solutions.

ZEESHAN AHMAD ABBASI received the bachelor's degree in E&C engineering from the Faculty of Engineering, Jamia Millia Islamia, Delhi, the master's degree from the University of Delhi, and the Ph.D. degree from Jamia Millia Islamia. He was with the Police Wireless and Police Research and Development in the Ministry of Home Affairs, India. He taught many papers at Delhi College of Engineering, Hamdard University, IGNOU, and Mewat Engineering College at UG and PG level. Currently, he is an Assistant Professor with the University Polytechnic, JMI. His area of research interests include wireless communication, wireless mesh networks, and the Internet of Things. He has numerous peer-reviewed publications in national and international journals and conferences. He has served as a reviewer and the session chair for many reputed national and international conferences.