Cluster Computing (2023) 26:2921–2931
https://doi.org/10.1007/s10586-022-03916-5

Cloud-edge load balancing distributed protocol for IoE services using swarm intelligence

Tanzila Saba[1] · Amjad Rehman[1] · Khalid Haseeb[1,2] · Teg Alam[3] · Gwanggil Jeon[1,4]

Received: 11 June 2022 / Revised: 21 September 2022 / Accepted: 9 December 2022 / Published online: 4 January 2023

Abstract

Rapid development of the Internet of Everything (IoE) and cloud services offer a vital role in the growth of smart applications. It provides scalability with the collaboration of cloud servers and copes with a big amount of collected data for network systems. Although, edge computing supports efficient utilization of communication bandwidth, and latency requirements to facilitate smart embedded systems. However, it faces significant research issues regarding data aggregation among heterogeneous network services and objects. Moreover, distributed systems are more precise for data access and storage, thus machine-to-machine is needed to be secured from unpredictable events. As a result, this research proposed secured data management with distributed load balancing protocol using particle swarm optimization, which aims to decrease the response time for cloud users and effectively maintain the integrity of network communication. It combines distributed computing and shift high cost computations closer to the requesting node to reduce latency and transmission overhead. Moreover, the proposed work also protects the communicating machines from malicious devices by evaluating the trust in a controlled manner. Simulation results revealed a significant performance of the proposed protocol in comparison to other solutions in terms of energy consumption by 20%, success rate by 17%, end-to-end delay by 14%, and network cost by 19% as average in the light of various performance metrics.

Keywords Particle swarm optimization · Cloud-edge · Internet of everything · Security analysis · Technological development

1 Introduction

To support Internet communities, the IoE connects a huge number of smart communication objects and integrates them with heterogeneous networks [1, 2]. They develop many critical applications such as smart buildings, security, target tracking, industrial automation, etc. A wireless sensor network (WSN) typically comprises thousands of small, low-cost sensor nodes with limited computing, communication, memory, and power capabilities [3, 4]]. Such technologies are one of the many viable data sources for network systems and produce a massive amount of data.

✉ Gwanggil Jeon
gjeon@inu.ac.kr

Tanzila Saba
tsaba@psu.edu.sa

Amjad Rehman
arkhan@psu.edu.sa

Khalid Haseeb
khalid.haseeb@icp.edu.pk

Teg Alam
t.alam@psau.edu.sa

[1] Artificial Intelligence and Data Analytics (AIDA) Lab, CCIS Prince Sultan University, Riyadh 11586, Kingdom of Saudi Arabia

[2] Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan

[3] Department of Industrial Engineering, College of Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Kingdom of Saudi Arabia

[4] Department of Embedded Systems Engineering, Incheon National University, Incheon 22012, South Korea

Emerging 5G and beyond networks have been proposed to offer connectivity for enormous devices and the Internet of Things (IoT), which can be widely referred to as an IoE. With these next-generation networks, massive amounts of data will be produced, processed, stored, and shared everywhere, at any time [5, 6]. Recently, cloud computing has become crucial because of the constantly growing IoT network [7, 8]. It remains the best approach for performing complex and high-cost computations. Moreover, provides scalable solutions for huge data processing. However, data latency and privacy are some major research objectives in the cloud-based paradigm. Many machine learning-based methods have been proposed to solve the process of data aggregation and routing issues for IoT-based constraint networks and drastically reduce the disturbance of wireless channels [9–11]. However, the collaboration of heterogeneous IoE demands for edge computing to bring the data processing closer towards the source network. Furthermore, as all the devices are operated on the open medium and they are accessble through entire channel, thus, providing security is also an essential functionality for such communication technologies. Although edge networks are offering maintainable and timely data delivery performance for wireless technologies, it is prone to network threats and compromised sensitive information with unauthorized devices association [12–14]. Thus, with the rising complexity of IoE deployment, we require a lightweight solution that can detect communication irregularities and provide an alternate paradigm for their successful accomplishment. The goal of this research is to demonstrate considerable performance for IoE-based applications in the effective management of heterogeneous resources, energy efficiency, bandwidth requirements, and privacy. This research reveals smart big data management using a secured cloud-edge system. Through load balancing, it controls the network's resources and evenly distributes the communication tasks across connected devices. This paper outline the contributions as follows.

i. It develops an effective routing technique that facilitates intelligent communication for IoE services using particle swarm optimization. The fitness function effectively generates quality-aware routes.
ii. The proposed system maintains a high computing solution that keeps data flowing effectively and conserves energy through the use of mobile edge devices and artificial intelligence techniques. It not only lessens the chances of data loss but simultaneously manages the timely delivery.
iii. In addition, the mobile edges offer a harmless method for data aggregation, storage, and processing to increase trust in cloud systems.
iv. Extensive experiments show the efficacy of the proposed protocol for managing network resources and data accessibility.

The rest of the research paper is organized as follows. Section 2 underlines the related work. Section 3 formulates the problem statement. Section 4 discusses the detail of the proposed protocol and its working stages. Section 5 exhibits the experimental results along with their comparison against the existing solution. In the end, Sect. 6 provides the conclusion and future work.

2 Related work

Edge computing provides valuable services for advanced development in IoE-enabled technologies. It controls the topology and data management near the cloud system and efficiently manages the resource distribution [15, 16]. However, smart devices [17, 18] offer real-time data aggregation and improve performance in a distributed manner. However, many solutions often fail to meet remote users' rising demands, especially for big data management with the least computing power and security for constraint nodes [19, 20]. Thus, many recent solutions explore network edges for manipulating operations and attaining a high response time [21–23]. Authors in [24], proposed fog-based healthcare for decreasing energy consumption with improved delivery delay. Its performance is evaluated in terms of network delay and energy usage with the cloud-based solution and experimental results demonstrate the better performance of the proposed solution. Moreover, it also suggested significant methods for improving the management of fog devices, especially in healthcare solutions.

The authors [25], the authors proposed an efficient WSN model for Adaptive Coverage and Connectivity (ACC) to provide optimum coverage for all target items, whereas the mathematical model assures coverage rate. Furthermore, its second strategy addresses network connection and energy usage. Unlike current systems, the proposed ACC plan can maintain the network for a long period with improved delivery performance. Numerous fields, including object recognition, WSNs, image processing, environment mapping, and localization, have made extensive use of data mining. WSN is being used by the IoT as a crucial platform for data sensing and communication. On the collected sampled by sensor nodes, mining of spatial and temporal data is carried out for efficiency. This research [26], therefore, proposes a redundancy removal approach that minings the acquired data to choose the appropriate data before forwarding it to a base station or a cluster head (CH) in the WSN. Numerous simulations were run, and the

resulting data demonstrated that the proposed solution performed better than competing schemes.

In [27], a unique IC-MADS, a lightweight cross-layer trust computing approach, was proposed for man-in-a-middle attack (MIMA). Two key contributions to the IC-MADS are cross-layer attack detection and energy-efficient clustering. The CH selection algorithm was proposed by utilizing a probabilistic computation and evaluation method. The probability of each sensor node is calculated using variables such as residual energy, base station distance, and node degree factors. The CH is determined by the node with the highest probability value. This fixes the load balancing and energy imbalance issues. To identify MIMA attackers in the network, node evaluation was introduced using the cross-layer trust evaluation approach. The threshold value is compared against the aggregated values of the trust for each sensor node to determine whether the node is an attacker or not. The energy-efficient hierarchical routing protocol for wireless sensor networks based on fog computing (EEHFC) is proposed by the authors [28] and aims to improve data transmission with effective energy consumption. Because fog computing can maximize the limited power supply of WSNs and scale to meet the demands of IoT applications, it is included in the proposed protocol. Additionally, it enhanced the ant colony optimization algorithm that may be utilized to produce the optimal path for sensor nodes with efficient network transmissions.

Authors in [29] suggested a Cloud-IoMT-based big data analytics framework. The data from wearable sensors such as body temperature, glucose, heartbeat, and chest were sent to an integrated cloud with a data analytics layer. Data acquired during COVID-19 monitoring and surveillance may be processed in parallel using Hadoop MapReduce cloud database technologies. With IoMT devices connected to the cloud and powerful data analytics layer, clinicians can quickly track, evaluate, and approve data from various wearable sensors. It may assist monitor patient health issues internationally, reducing workloads and stress on healthcare providers, and improving medical diagnostic and treatment outcomes. In [30], Ambient Intelligence assisted Health Monitoring System (AmIHMS) with the Internet of things is proposed to monitor the students' health. With the Ami environment, the constraint sensor nodes are explored for collecting medical data. Furthermore, the cloud handles the big data and transferring to network users with a manageable network structure. Based on simulation results, it was observed that the proposed AmIHMS improves the data reliability and accessibility of other popular methods. Table 1 summarizes the limiations and contributions of the recent work.

3 Problem statement

IoT systems have been extensively used to produce several reliable applications with some level of intelligence. Additionally, edge computing manages the reduction of data routing latency toward cloud services. It has been observed that numerous solutions have been presented to enhance the functionality of IoT networks but at the expense of significant data loss and frequent route failures. The majority of solutions reduce the response time for emergency operations, are unable to handle high-density traffic across restricted devices, and inefficiently use the system's capacity. Furthermore, many hardware-oriented communication systems make extensive use of sensor-based systems with IoT-cloud computing. However, providing security is a significant research challenge for heterogeneous applications, especially in mobile networks.

4 Proposed protocol

This section divides the working processes of the proposed protocol into the following sub-sections. Also, it comprised diagrammatical notations and algorithms for the developed components.

4.1 Overview

In this section, we first present a brief introduction of the SDM-DLB protocol, and later its developed components are discussed. It is made up of numerous sensors that are randomly deployed. The edge devices provide

Table 1 Summarization of related discussion

Discussed work	Contributions with limitations
Existing solutions	IoE is a heterogeneous service to collaborate with various sensors and hardware for the formulation of smart cities
	Most of the solution efficiently manages the transmissions for the IoT nodes with affordable delaying techniques
	Nevertheless, most of the existing work is not able to fully provide timely performance with scalable network services
	Moreover, as IoT nodes are limited in terms of resources, thus, it was seen that many developed schemes are imposing additional energy consumption on the network infrastructure
	It was also observed that providing privacy is another significant research challenge for heterogeneous networks, especially when there is no restriction on the communication medium

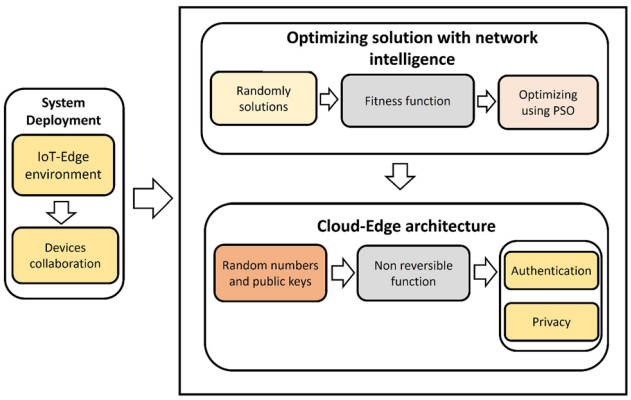


Fig. 1 Working components of the proposed SDM-DLB protocol

intermediate-level services between sensors and cloud platforms. Edge devices are mobile and require all the information regarding the network region. In the proposed SDM-DLB protocol, sensors flood their initial information to edge devices, and accordingly, they maintain the local schema in memory. Each edge device only stores the information of those sensors that are in their radius range. The edge devices provide two main functionalities. Firstly, all the smart data collected from sensors are collected and aggregated on network edges. Secondly, not only data is aggregated on network edges, but on the other side, the authenticity of incoming data is also verified. Using artificial intelligence techniques, the proposed SDM-DLB protocol determines the optimized solution in iterations. Figure 1 illustrates the developed components of the proposed system. It has three main components; system setup, artificial intelligence optimization, and edge computing-enabled security. The system setup, sensors, edges, and other devices are deployed in the communication field and initially, all the feasible solutions are identified. The second component extracted random solutions and explored fitness functions using an iterative process to compute the global with an optimal solution. In the end, sensors and edge devices are secured against privacy and security attacks, which ensures a reliable communication network and increases the authenticity of trusted data.

4.2 Secured and intelligent sensing distributed protocol with cloud-edge

In this section, we present the detail and description of the processes that are developed for the proposed protocol. It offers an energy-efficient optimal solution for heterogeneous devices using an artificial intelligence approach. The proposed protocol aims to decrease the communication cost with a minimum length taken by the source node regarding forwarding the IoE data towards network edges. Also, it provides an efficient data sensing solution and intelligently identified the data threats. In the beginning, the sensor nodes identify their neighboring list using its transmission power. If no neighbors are identified, the sensor increases its transmission power by amount α and recomputes the neighboring list. Once neighbors are determined, then they need to share their information such as identity *ID*, energy e, location l, and memory space m towards the source node. Accordingly, the source node stores the obtained information inside its local memory. Additionally, the same information is forwarded towards mobile edges to maintain the structure for global data. In the proposed SDM-DLB protocol, nodes execute particle swarm optimization algorithms collaboratively to extract the optimized forwarders for sending collected data toward network edges. PSO is an iterative learning procedure that measures the changes of network parameter by computing the cost function for a feasible solution [31]. It is a stochastic-based optimization technique that utilizes the intelligence and movement of swarms. In PSO, the concept of interface between agents is explored for solving a problem and offering the optimal solution by reducing the search space. For example, let us consider N is the number of sensors if we are at node $x \varepsilon N$, then goal state g can be defined as Eq. 1.

$$x \rightarrow g : f(x),\ m(x,y) \tag{1}$$

where $f(x)$ is the set of initial feasible solutions $(t_1, t_2, \ldots, t_k)$, and $m(x,y)$ is the cost value. To determine the set of intermediate forwarders y' from source node x to goal state g, the process is defined in Eq. 2.

$$m(x,y) = g\left(m\left(x,y'\right)\middle| y' \varepsilon f(x)\right) \tag{2}$$

For each solution, a fitness value $f(t)$ is determined by using collected information and advertising the computed value. $f(t)$ is determined using weighted computing based on energy e and channel reliability c_r, as defined in Eq. 3.

$$maxf(t) = \alpha.e + \beta.c_r \tag{3}$$

where

$$c_r = 1/Round_{time} + 1/path_{length} \tag{4}$$

$f(t)$ value is utilized to compute the local best *LB* and global best *GB* for the initial solutions. In case, if the computed *LB* is better than the previous *LB* in history then the current LB value is set as a new *LB*. However, *GB* is the best value of the optimal global solution.

To attain security and mutual authentication between mobile edges and sensors, random numbers, and public keys are utilized, as given below.

$$s \rightarrow n_i : E_{n_i}(r_i, e_{id}) \tag{5}$$

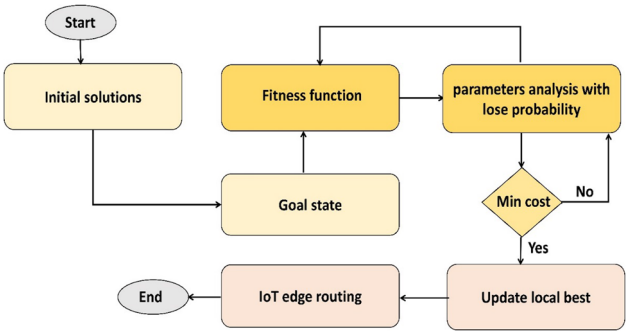


Fig. 2 Workflow of the IoE edge routing

$$n_i \rightarrow s : E_{si}(r_i, r_j) \tag{6}$$

$$s \rightarrow n_i : E_{n_i}(r_j) \tag{7}$$

Initially, the edge device sends an encrypted message using the node's public key n_i. The encrypted message comprised of a random number r_i and identity of the edge device e_{id}. The node n_i recovers the random number r_i from message derived from Eq. 5 and returns a random number r_j by using public key of edge device s_i, as defined in Eq. 6. Afterward, the edge device resends the encrypted random number r_j to the node n_i as defined in Eq. 7. Accordingly, edge device e_{id} and node n_i jointly authenticate each other using encrypted random numbers. To generate the session key s_k between n_i and e_{id}, the non-reversible function f is used as given in Eq. 8.

$$S_k : f(r_i, r_j) \tag{8}$$

Now, using Eq. 9, data encryption E is obtained for the message d_i and session key S_k.

$$E(d_i) = d_i \oplus S_k \tag{9}$$

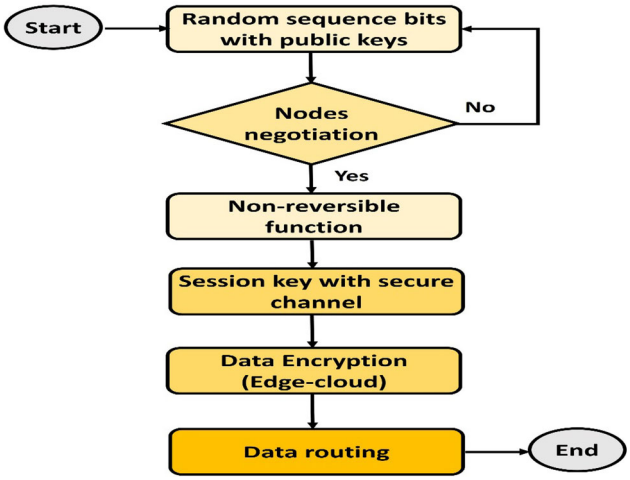


Fig. 3 Workflow of the node negotiation with security

4.3 Edge-cloud communication with authentication and data security

This section presents the working of SDM-DLB protocol to secure and authentic communication of edges and cloud servers. It explores the Blum-Blum-Shub pseudorandom bit generator [32] based on Eq. 10.

$$X_{n+1} = X_n^2 mod m \tag{10}$$

where X_n is the generated secret key for the edge device a e_{id} and cloud server c. m is the product of two large prime p and q. X_0 is the seed integer value and co-prime to m. After generating the secret key, the cloud server c further encrypts it using master key K and concatenates a timestamp as defined in Eq. 11.

$$c \rightarrow e_{id} : E_K(X_n, \mathrm{t}) \tag{11}$$

Algorithm 1: SDM-DLB protocol

1. Procedure distributing routing
2. sensors use transmission power to identify neighbors
3. collaborate and maintain a tables
4. each sensor determines the feasible solutions and cost value
5. $x \rightarrow g$: $f(x)$, $m(x, y)$
6. intermediate forwarders y'
7. compute the fitness function using edges
8. $max\ f(t) = \alpha.e + \beta.c_r$
9. c_r= 1/Round$_{time}$ + 1/ path$_{length}$
10. Sensor-edges mutual authentication
11. non reversible function S_k: $f(r_i, r_j)$
12. data encryption using $E_j(d_i) = d_i \oplus S_k$
13. secret key generation for edges and cloud using $X_{n+1} = X_n^2 mod\ m$
14. cloud encrypts the secret key with its master key $c \rightarrow e_{id} : E_K(X_n, t)$
15. data encryption in dual modes using $c \leftrightarrow s$: $xor\ (d_i, (X_n)$
16. end procedure

The edge device e_{id} obtained the encrypted secret key X_n and recovered it using the master key of cloud server c, after decrypting process the edge device e_{id} verifies the authenticity of cloud server c. Afterward, the data encryption is obtained for the message d_i by computing the xor operation using the secret key X_n as given in Eq. 12.

$$E : xor(X_n, d_i) \tag{12}$$

Figures 2 and 3 show the functionalities of the SDM-DLB protocol. The PSO method is used during the iteration process to achieve effective routing and detection of link failure. It provides low latency, energy-efficient edge environment and enables network architecture for accessing required information closer to the source nodes. Additionally, the optimal local and global evaluations provide reliable outcomes by examining fitness functions with trustworthy energy and channel characteristics. Both the RTT and loss probability cope with identifying more trustable channels from the identified solutions and increase resource efficient utilization with edge computing. In addition to providing timely large data collection from the IoE environment, the mobile edges also play a crucial intermediary function in overcoming data security. In the proposed system, mobile edges cooperate with the IoE network and cloud-based technologies to produce shared random numbers using encrypted secret keys. It provides a secure way for nodes' negotiations and avoids the possibility of hostile machines recovering the network data. As a result, it explored an intelligent communication model with high bandwidth and secure access to assure reliable smart facilities. Algorithm 1 governs the procedural steps for the development of the SDM-DLB protocol.

Table 2 Simulation parameters

Parameter	Value
Sensors	200–1000
Sensors position	Mobile
Sink node	2
Field dimension	1000 m x 1000 m
Transmission range	10 m
Initial energy	5 J
Packet size	32 bytes
Simulation time	5000 s
Edge devices	20
Simulations run	20
Malicious devices	2–10

5 Experimental discussion

This section presents the experimental environment and discussion on results. The proposed SDM-DLB protocol is analyzed and verified using simulation tests. Sensors are randomly distributed over the dimension size 1000 m × 1000 m. The transmission range of distributed sensors is set to 10 m. All the sensors are mobile and send their latest position periodically. Initially, the nodes are set for initial energy with 5 J. We supposed 2 static sink nodes. Edge devices are 20 in number and periodically flood the positioning messages to advertise their latest location. We deployed malicious nodes with 2 to 10 in number. The malicious nodes are abnormal that are compromised by network threats and attackers. Such nodes send frequent irrelevant data on the communication channels and make them congested. Also, they can drop the data packets over the transmission medium. The packet size is set as 32 bytes. The number of sensors are varying from 200 to 1000. The speed of the deployed sensors is varying from 10 to 50 m/s. Table 2 illustrates the parameters of the simulation configuration. The proposed SDM-DLB protocol is tested based on energy consumption, end-to-end delay, network cost, and success rate performance metrics.

In terms of energy consumption, we compared the performance of the proposed SDM-DLB protocol to the existing solution. Figure 4a and b depict the assessment of the proposed SDM-DLB protocol and related work, and it is noticed that the proposed solution increases the efficiency of energy use by 19% and 22% on average in terms of varying sensors and their mobility speed. On the other hand, it has been observed that the energy consumption rate increases as the number of devices increases. Nevertheless, the SDM-DLB protocol provides an intelligent energy solution using a fitness function by integrating the channels' reliability and selection of updated routes based on local optimality. Due to the low number of control messages and retransmissions, the proposed SDM-DLB protocol also offers uniform energy consumption for the IoT network and improves network stability. Additionally, routing strategies are only altered when network edges become aware of the unstable condition of the network.

The evaluation of the proposed SDM-DLB protocol and existing solutions is shown in Fig. 5a and b, and it was found that the proposed SDM-DLB protocol impressively reduces the end-to-end delay by 17% and 18% as an average for varying sensors and their mobility speed. It is because edge devices have been integrated over the targeting area's perimeter and can handle the quick transport of sensor data to cloud systems using the intelligent decision of the PSO algorithm. Additionally, eliminating the overburdened nodes from routing decisions highly

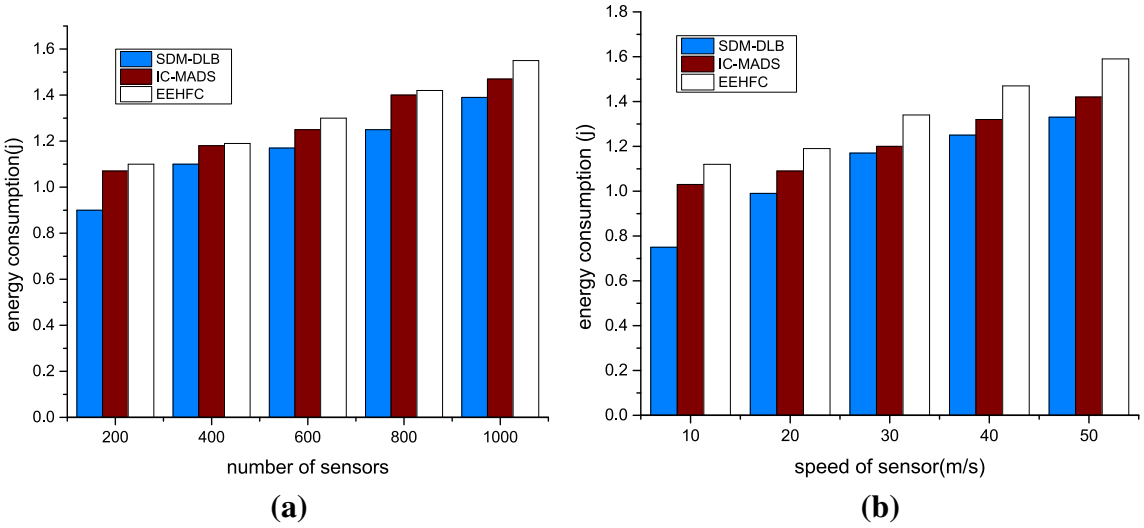


Fig. 4 **a** Energy consumption with varying sensors, **b** Energy consumption with varying speed of sensors

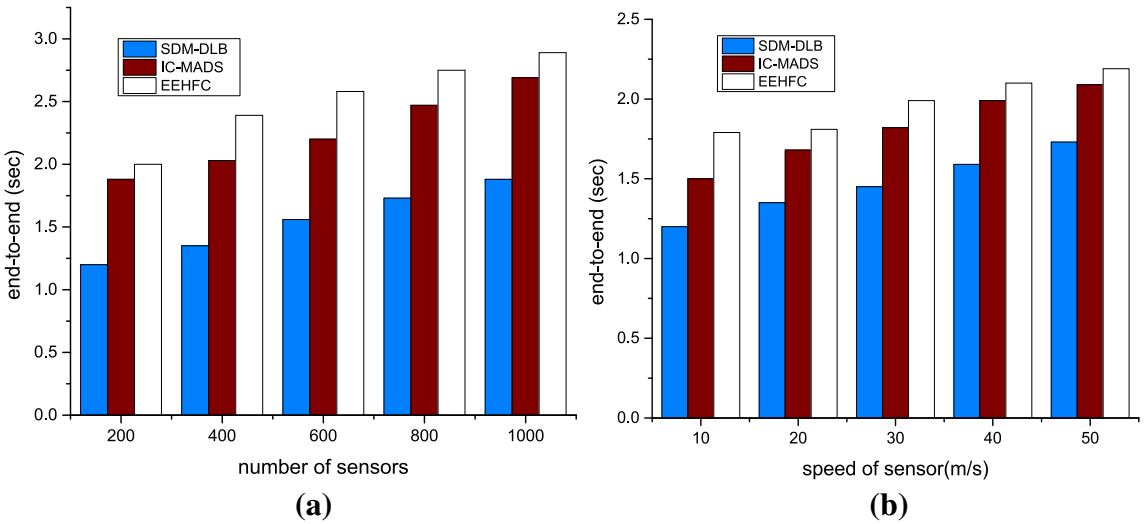


Fig. 5 **a** End-to-end delay with varying sensors, **b** End-to-end delay with varying speed of sensors

increases the route's lifetime and accordingly, it improves the delivery of messages. The edges between IoT sensors and cloud systems deliver the collected timely and made the decision system closer to the source nodes. Also, congested links are coped using channel reliability parameters, and only such nodes are incorporated in routing processes whose success rate is high. Moreover, the security solution decreases unwanted traffic across the open transmission system and stops malicious devices from sending false routing messages and requests.

In terms of network complexity, Fig. 6a and b demonstrate the performance assessment of the proposed SDM-DLB protocol for varying sensors with their mobility speed. Observations indicate that the proposed SDM-DLB protocol lowers the ratio of network cost in terms of flooding of malicious packets and drop rate as compared to other work. It was revealed that performance was improved by an average of 14% to 17% respectively in the presence of malicious nodes. It is a result of the devices' mutual authentication by utilizing the generation of random numbers and the production of private/public keys. Also, security measurement helps the routing process to reduce the harmful attacks for the proposed SDM-DLB protocol, and ultimately decreases the additional data retransmission.

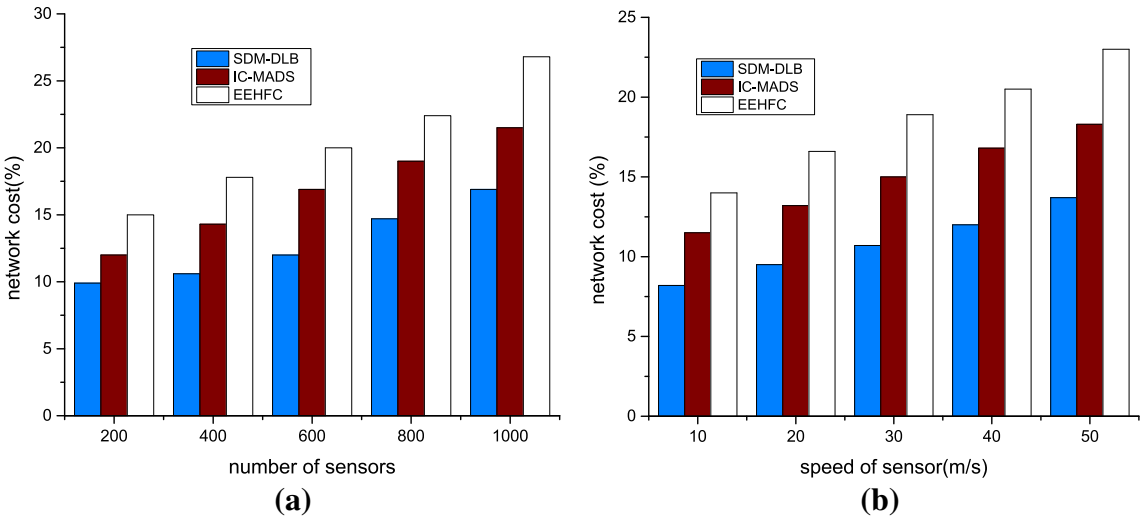


Fig. 6 **a** Network cost with varying sensors, **b** Network cost with varying speed of sensors

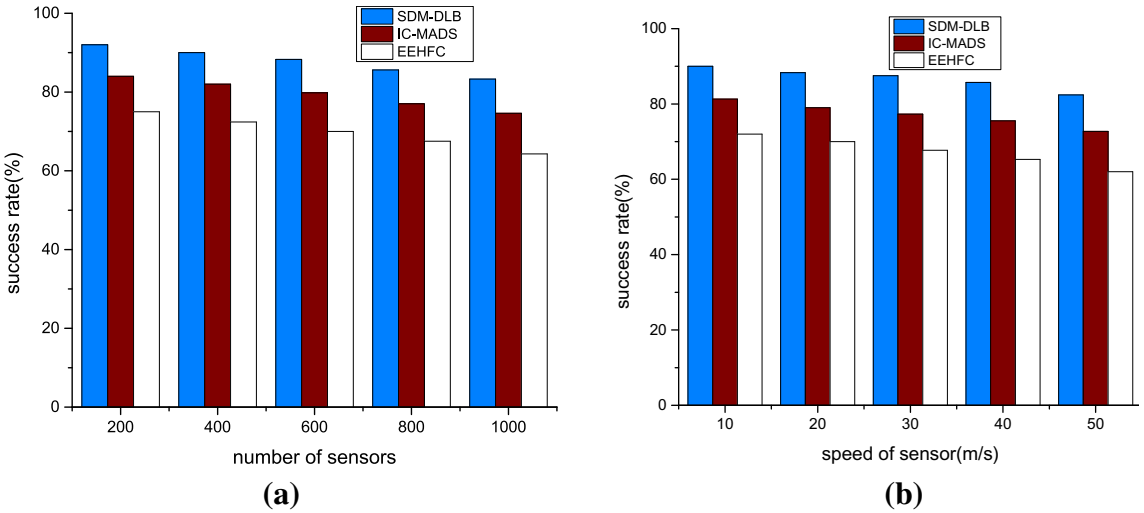


Fig. 7 **a** Success rate with varying sensors, **b** Success rate with varying speed of sensors

The random numbers and secret keys facilitate the rapid verification of unsafe devices and the accomplishment of the IoE system's data availability. In addition, the edge devices are more resilient and operate as a supervisor for sensor data arriving from constrained devices; after appropriate authentication, the obtained data is sent to the application user with the computing intelligence.

The success rate of the proposed SDM-DLB protocol and the existing solutions is shown in Fig. 7a and b. The proposed SDM-DLB protocol increases the delivery ratio as compared to other work by an average of 15% and 16% under various sensors and their speed. This is because the proposed SDM-DLB protocol employs a PSO for effectively learning the communication process using the fitness function, and regulating the power distribution among sensors. The iterative process of PSO learning supports the IoE networks with the capacity to formulate more robust and efficient routing paths. Moreover, the intelligent decision-making composite function reduces the probability of data loss and interruption. The proposed SDM-DLB protocol reevaluates routing paths wherever malicious entry is found by processing the route request packets and accordingly it discarding the risk indicators.

6 Conclusion

This study describes a secured and intelligent solution for dynamic application environments based on the IoE. Utilizing cloud-edge computing, it promises to deliver

high-performance computing approach with efficient resource management and load balancing. In addition, the proposed protocol found efficient solutions with the optimal local and global fitness functions using the PSO approach. The fitness function employs the energy and channel's reliability parameters to provide a stable network connection with minimal latency. In addition, network edges preserve data collection and storage against network threats while imposing minute costs on distributed and restricted hardware devices. A system with efficient nodes' decision-making and the provision of trusted services in a realistic situation is offered to control real-time activities. Extensive testing was conducted, and the findings demonstrated that the proposed protocol significantly improved than existing work. In future studies, we will incorporate deep learning to train the proposed protocol and overcome distributed security attacks.

Acknowledgements This work was supported by the research SEED project "Low-power consumption optimizing algorithm using artificial intelligence for embedded IoT sensing system." Prince Sultan University, Riyadh Saudi Arabia, (SEED-CCIS-2022{110}) under Artificial Intelligence & Data Analytics Research Lab. CCIS". The authors are thankful for the support.

Author contribution TS: Software, Validation, Writing, Visualization. AR: Conceptualization, Software, Validation. KH: Methodology, Visualization, Investigation. TA: Software, Writing, Visualization, Investigation. GJ: Validation, Data curation, Reviewing and Editing, Reviewing and Editing.

Funding There is no funding supported for this work.

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest Not declared.

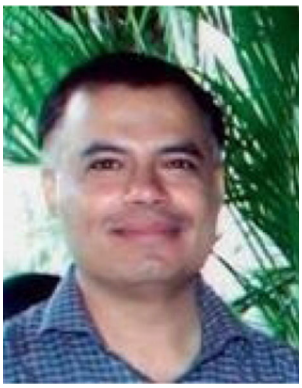
Informed consent N/A.

References

1. Miraz, M.H., et al.: A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT). In: Proceedings of the 2015 Internet Technologies and Applications (ITA). IEEE (2015)
2. Swarna Priya, R.M., et al.: Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything. J. Parallel Distrib. Comput. **142**, 16–26 (2020)
3. Ullah, A., et al.: Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. Peer-to-Peer Netw. Appl. **13**(1), 163–174 (2020)
4. Haseeb, K., et al.: Device-to-Device (D2D) multi-criteria learning algorithm using secured sensors. Sensors **22**(6), 2115 (2022)
5. Sirma, M., Kavak, A., Inner, B.: Cloud based IoE connectivity engines for the next generation networks: challenges and architectural overview. In: Proceedings of the 2019 1st international informatics and software engineering conference (UBMYK). IEEE (2019)
6. Chen, X., et al.: Massive access for 5G and beyond. IEEE J. Sel. Areas Commun. **39**(3), 615–637 (2020)
7. Angel, N.A., et al.: Recent advances in evolving computing paradigms: cloud, edge, and fog technologies. Sensors **22**(1), 196 (2021)
8. Stergiou, C.L., et al.: Secure machine learning scenario from big data in cloud computing via internet of things network. In: Handbook of Computer Networks and Cyber Security, pp. 525–554. Springer, New York (2020)
9. Alfarraj, O.: A machine learning-assisted data aggregation and offloading system for cloud–IoT communication. Peer-to-Peer Netw. Appl. **14**(4), 2554–2564 (2021)
10. Krishnan, M., Lim, Y.: Reinforcement learning-based dynamic routing using mobile sink for data collection in WSNs and IoT applications. J. Netw. Comput. Appl. **194**, 103223 (2021)
11. Khan, Z.A., et al.: A neighborhood and machine learning-enabled information fusion approach for the WSNs and internet of medical things. Comput. Intell. Neurosci. **2022**, 1–14 (2022)
12. Pal, S., Jadidi, Z.: Analysis of security issues and countermeasures for the industrial internet of things. Appl. Sci. **11**(20), 9393 (2021)
13. Senevirathna, T., et al.: A survey on XAI for beyond 5G security: technical aspects, use cases, challenges and research directions. https://arxiv.org/abs/2204.12822 (2022)
14. Hegland, A.M., Hauge, M., Holtzer, A.: Federating tactical edge networks: ways to improve connectivity, security, and network efficiency in tactical heterogeneous networks. IEEE Commun. Mag. **58**(2), 72–78 (2020)
15. Chen, B., et al.: Edge computing in IoT-based manufacturing. IEEE Commun. Mag. **56**(9), 103–109 (2018)
16. Yang, X., et al.: Multi-semi-couple super-resolution method for edge computing. IEEE Access **6**, 5511–5520 (2018)
17. Jeon, G., et al.: Image enhancement in embedded devices for internet of things. Concurr. Comput. Pract. Exp. **33**(3), e5398 (2021)
18. Saqlain, M., et al.: Framework of an IoT-based industrial data management for smart manufacturing. J. Sens. Actuator Netw. **8**(2), 25 (2019)
19. de Araujo-Zanella, A.R., da Silva, E., Albini, L.C.P.: Security challenges to smart agriculture: current state, key issues, and future directions. Array **8**, 100048 (2020)
20. Elhoseny, M., et al.: IoT solution for AI-enabled PRIVACY-PREServing with big data transferring: an application for healthcare using blockchain. Energies **14**(17), 5364 (2021)
21. Cao, K., et al.: Exploring placement of heterogeneous edge servers for response time minimization in mobile edge-cloud computing. IEEE Trans. Ind. Inf. **17**(1), 494–503 (2020)
22. Mastorakis, S., et al.: Icedge: when edge computing meets information-centric networking. IEEE Internet Things J. **7**(5), 4203–4217 (2020)
23. Zhao, L., Liu, J.: Optimal placement of virtual machines for supporting multiple applications in mobile edge networks. IEEE Trans. Veh. Technol. **67**(7), 6533–6545 (2018)
24. Feng, C., et al.: Towards energy-efficient framework for IoT big data healthcare solutions. Sci. Prog. **2020**, 1–9 (2020)
25. Prasanth, A., Jayachitra, S.: A novel multi-objective optimization strategy for enhancing quality of service in IoT-enabled WSN applications. Peer-to-Peer Netw. Appl. **13**(6), 1905–1920 (2020)
26. Kumar, S., Chaurasiya, V.K.: A strategy for elimination of data redundancy in internet of things (IoT) based wireless sensor network (WSN). IEEE Syst. J. **13**(2), 1650–1657 (2018)
27. Kore, A., Patil, S.: IC-MADS: IoT enabled cross layer man-in-middle attack detection system for smart healthcare application. Wirel. Pers. Commun. **113**(2), 727–746 (2020)

28. Abidoye, A.P., Kabaso, B.: Energy-efficient hierarchical routing in wireless sensor networks based on fog computing. EURASIP J. Wirel. Commun. Netw. **2021**(1), 1–26 (2021)
29. Awotunde, J.B., Ogundokun, R.O., Misra, S.: Cloud and IoMT-based big data analytics system during COVID-19 pandemic. In: Efficient Data Handling for Massive Internet of Medical Things, pp. 181–201. Springer, New York (2021)
30. Hong-Tan, L., et al.: Big data and ambient intelligence in IoT-based wireless student health monitoring system. Aggress. Viol. Behav. **2021**, 101601 (2021)
31. Anand, V., Pandey, S.: New approach of GA–PSO-based clustering and routing in wireless sensor networks. Int. J. Commun. Syst. **33**(16), e4571 (2020)
32. Blum, L., Blum, M., Shub, M.: A simple unpredictable pseudo-random number generator. SIAM J. Comput. **15**(2), 364–383 (1986)

Tanzila Saba earned a Ph.D. in document information security and management from Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia in 2012. She won the best student award in the Faculty of Computing UTM for 2012. Currently, she is serving as Associate Prof. and Associate Chair of Information Systems Department in the College of Computer and Information Sciences Prince Sultan University Riyadh KSA. Her primary research focus in recent years is medical imaging, MRI analysis, and Soft-computing. She has two hundred ISI/SCEI publications that have around 4000 citations with h-index 40. Her mostly publications are in biomedical research published in ISI/SCIE indexed. Due to her excellent research achievement, she is included in Marquis Who's Who (S & T) 2012." Currently, she is an editor and reviewer of reputed journals and on the panel of TPC of international conferences. She has full command of a variety of subjects and taught several courses at the graduate and postgraduate levels. On the accreditation side, she is a skilled lady with ABET & NCAAA quality assurance. She is the senior member of IEEE. Dr. Saba is the leader of the Artificial Intelligence & Data Analytics Lab.



Amjad Rehman is a Senior Researcher in the Artificial Intelligence & Data Analytics Lab CCIS Prince Sultan University Riyadh Saudi Arabia. He received his PhD & Postdoc from Faculty of Computing Universiti Teknologi Malaysia with a specialization in Forensic Documents Analysis and Security with honor in 2010 and 2011 respectively. He received rector award for 2010 best student in the university. Currently, he is PI in several funded projects and also completed projects funded from MOHE Malaysia, Saud Arabia. His keen interests are in Data Mining, Health Informatics, Pattern Recognition. He is author of more than 200 ISI journal papers, conferences and is a senior member of IEEE.

Khalid Haseeb received the MS-IT degree from Institute of Management Sciences, Peshawar, Pakistan. He completed his Ph.D. in Computer Science from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia in 2016. He is working as an Assistant Professor in the Department of Computer Science, Islamia College Peshawar, Pakistan. He has an experience of several years in teaching, research and development. His research areas include wireless sensor networks, ad-hoc networks, network security, Machine learning, Internet of Things, Software Define Networks and cloud computing. He involves as a referee for many reputed international journals and conferences.

Teg Alam is presently working as a faculty member at the Industrial Engineering Department, College of Engineering, Prince Sattam Bin Abdulaziz University, Al Kharj; Kingdom of Saudi Arabia. Before joining Prince Sattam Bin Abdulaziz University, he worked at Azad Institute of Engineering and Technology, U.P. Technical University Lucknow, India, as an Associate Professor. His areas of teaching and research interests are Operations Research, Quantitative Analysis, and Applied Statistical Methods. He has published numerous researches in different reputed peer-reviewed scientific journals.

Gwanggil Jeon received the B.S., M.S., and Ph.D. (summa cum laude) degrees from the Department of Electronics and Computer Engineering, Hanyang University, Seoul, Korea, in 2003, 2005, and 2008, respectively. From 2009.09 to 2011.08, he was with the School of Information Technology and Engineering, University of Ottawa, Ottawa, ON, Canada, as a Post-Doctoral Fellow. From 2011.09 to 2012.02, he was with the Graduate School of Science and Technology, Niigata University, Niigata, Japan, as an Assistant Professor. From 2014.12 to 2015.02 and 2015.06 to 2015.07, he was a Visiting Scholar at Centre de Mathématiques et Leurs Applications (CMLA), École Normale Supérieure Paris-Saclay (ENS-Cachan), France. From 2019 to 2020, he was a Prestigious Visiting Professor at Dipartimento di Informatica, Università degli Studi di Milano Statale, Italy. He is currently a Full Professor at Xidian University, Xi'an, China and at Incheon National University, Incheon, Korea. He was a Visiting Professor at Sichuan University, China, Universitat Pompeu Fabra, Barcelona, Spain, Xinjiang University, China, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand, and University of Burgundy, Dijon, France. Dr. Jeon is an IEEE Senior Member, an Associate Editor of Sustainable Cities and Society, IEEE Access, Real-Time Image Processing, Journal of System Architecture, and MDPI Remote Sensing. Dr. Jeon was a recipient of the IEEE Chester Sall Award in 2007, ACM's Distinguished Speaker in 2022, the ETRI Journal Paper Award in 2008, and Industry-Academic Merit Award by Ministry of SMEs and Startups of Korea Minister in 2020.