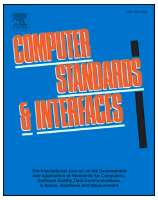
Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi



Intelligent and trusted metaheuristic optimization model for reliable agricultural network

Amjad Rehman [a], Ibrahim Abunadi [a], Khalid Haseeb [a], Tanzila Saba [a], Jaime Lloret [b,*]

[a] Artificial Intelligence and Data Analytics (AIDA) Lab, CCIS Prince Sultan University, Riyadh, 11586, Saudi Arabia
[b] Instituto de Investigacion para la Gestion Integrada de Zonas Costeras, Universitat Politecnica de Valencia, C/Paranimf, 1, 46730 Grao de Gandia, Valencia, Spain

ARTICLE INFO

Keywords:
Agriculture
Metaheuristic
Ubiquitous sensors
Economic growth
Natural resource

ABSTRACT

Artificial intelligence (AI) is gaining demanding growth in the field of smart cities, agriculture, food management, and weather forecasting due to the lack of computing power on sensing devices. The applications of artificial intelligence are integrated with various Internet of Things (IoT) and ubiquitous sensors for the improvement of the agriculture sector and to decrease its management cost. Due to the bounded resources of wireless technologies, most of the solutions are designed for efficient delivery of agriculture data to cloud systems, however, still optimizing the resources management and data load for forwarding nodes, especially those closest to edge boundaries is a challenging issue. Moreover, due to the collection of incorrect environmental data, the decision-making process leads to a decrease in the productivity of the optimization process. To overcome such issues, this work proposes a trustworthy and intelligent agricultural model that uses metaheuristic optimization to enhance resource management to address these problems. The proposed model approach employs the decision-making function to overcome information loss and inconsistency. Moreover, it builds trust in agricultural data collection by using secure IoT devices and facilitating reliable communication. In terms of performance metrics, the proposed model is simulated to assess its importance in comparison to state-of-the-art solutions. It not only collects updated data from agricultural land but also uses artificial intelligence's lightweight optimization technique to reduce the overheads on IoT devices. The experiment findings demonstrate the importance of the proposed model for resource monitoring and overheads on the IoT system.

1. Introduction

In recent years, intelligent sensor systems have gained a lot of interest in agriculture, water monitoring, etc. They are utilized in smart cities to plan several operations and missions effectively in data collection for distributed networks [1–3]. The need for food is rising rapidly with the world's population growth rate, which will double in the coming decades. Farmers' traditional methods are ineffective in meeting the rising demands. When nutrients, water, pesticides, and fertilizers are used improperly, agricultural growth is disrupted and the land remains unproductive [4,5]. Farmers are increasingly turning to sophisticated agricultural technology to cultivate plants. Temperature, humidity, light intensity, water nutrient level, etc. must all be carefully regulated during plant management and growth. Several scientific fields have evolved in recent years that employ data-intensive methods to increase agricultural productivity while minimizing environmental issues [6–8]. It combines machine data with agricultural, soil, and atmospheric information to enable more precise and earlier decision-making. Based on the learning signal, machine learning tasks are separated into supervised and unsupervised learning [9,10]. The goal of supervised learning [11,12] is to develop a general rule that connects inputs and outputs. The trained model predicts missing results (labels) for the test data in supervised learning. Unsupervised learning, on the other hand, does not differentiate between training and test sets. Instead, the learner investigates the data to find hidden patterns [13,14]. Recently, numerous IoT systems and smart physical devices have worked together to produce smart agricultural land and make it easier for farmers to monitor and manage their plants, crops, and other agricultural products [15,16]. However, a limited number of methods have been offered to improve the learning process in the automated system due to the resource limitation of the wireless system [17–19]. To enable an automated system employing lightweight computation for the wireless network, this study proposes an intelligent and reliable optimization model for agricultural land. It achieves trust-oriented transmission from

[*] Corresponding author.
E-mail address: jlloret@dcom.upv.es (J. Lloret).

https://doi.org/10.1016/j.csi.2023.103768
Received 24 March 2022; Received in revised form 6 May 2023; Accepted 11 June 2023
Available online 12 June 2023

agricultural equipment to cloud systems by using security techniques. The proposed model makes extensive use of environmental parameters and offers a highly reliable delivery performance with network optimization. In addition, the edge nodes around the sink node efficiently manage the delay time when transferring agricultural data to cloud systems. Moreover, the proposed model incorporates the security paradigm to deliver reliable communication with nominal breaches in the IoT system.

Our proposed model provides the following contributions.

i By employing a metaheuristic algorithm, the proposed model provides the most reliable and effective selection criteria for forwarding nodes.

ii The ubiquitous network and IoT system combined to achieve a high level of direct security. It decreases the chances of unauthorised access and leakage of data privacy.

iii Moreover, unlike most of the traditional approaches, the proposed model uses intelligent edges as intermediary devices between agricultural and sink nodes. It smartly manages the resources while forwarding the data.

iv The smart agricultural model is tested and verified its efficacy using simulations with varying experiments against other work.

The remainder of this work is divided into the following sections. The related study and the finding of the research problem are presented in Section 2. The details of the proposed model are covered in Section 3. The simulation environment and experimental findings are given in Section 4. Finally, Section 5 provides the conclusion of this work.

2. Related work

In ubiquitous sensor networks [20,21], the technologies of wireless networks and IoT paradigms are gaining rapid development for sensing the unpredictable environment and supporting remote clients [22–24]. The collected information is processed and transformed towards a cloud system by utilizing the processing and storage capabilities of the constraint device [25–27]. Most real-time applications such as agriculture, transportation, military, etc. demand an optimized wireless system for the efficient management of their resources and productivity cost [28,29]. Wireless sensor networks (WSNs) have emerged as a viable precision farming technique and increase the performance of agricultural land. Static clustering solutions [30] offer the easiest way to handle the coverage-hole problem and balance the constraint resources effectively. During information collection, the sensed data regarding the agricultural environment is broadcast to the base station (BS) and remote users obtain the needed information by utilizing the IoT system. In [31], the authors offer a scalable WSN for monitoring and regulating agriculture and farming in remote places. Precision agriculture and farming (PAF) need two important management components: water resource irrigation and effective water resource consumption. It uses an IoT system to optimize the connectivity of a large number of wireless sensors to boost farmer productivity. The performance of the deployed structure is tested and verified in terms of throughput, latency, SNR, lowest mean square error, and expanded coverage area. Agriculture is one of the many domains where AI has made gains in terms of monitoring and management. Low-power sensing devices with fully functional AI, on the other hand, are still in the early phases of development. To increase the lifetime of the network, authors in [32] presented an Energy-aware Grid-based Data Aggregation Scheme in Routing (EGDAS-RPL) protocol for the IoT system. It is comprised of grid formation, grid head (GH) selection, and grid head parent selection. EGDAS-RPL initially creates a grid of the same size on the square network. Second, it chooses the GH node inside the grid using probabilistic methods. Finally, it takes into account the expected transmission count (ETX) while choosing the optimal GH parent for data transfer. A ground-breaking lightweight trust decision-making framework for QoS clustering was developed by the authors [33], which guarantees secure intercluster and intracluster communication. A variable that the Cluster Head (CH) creates for each Cluster Member (CM) inside the cluster is the measured anomalous trust value. Between master nodes, member nodes, and the BS, the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol makes groups and transfers trust values. The proposed work decreases the communication costs and the risk of attacks like an eavesdropper, sink hole and black hole. The authors [34] proposed the Secure Energy-Aware Meta-Heuristic Routing (SEAMHR) protocol for WSNs to improve network performance and security. It explores Meta-Heuristic analysis based on Mutation Elephant Herding Optimization (MEHO). The protocol learns the routing decisions using hop counts, connection integrity characteristics, and aggregated residual energy. Moreover, the Counter Mode Cryptography method is explored by the protocol with the support of Auto encoders (AEs) called CTR-AEDL, which aims to offer secured data with authentication-oriented inter-routing. Furthermore, as part of route maintenance methods, traffic explorations prevent link failures. An energy-aware Grouping Memetic Algorithm (GMA) is proposed in [35] as a solution to the SET K-COVER problem. The proposed GMA differs from existing SET K-COVER problem-solving algorithms in four crucial ways. The proposed method was thoroughly tested in this work using a variety of targets and sensors under a WSN environment. A novel bumble bees mating optimization (CBBMO) algorithm was proposed in [36] to provide secure transmissions using a trust sensing model, also called as CBBMOR-TSM model. The mating behavior of a swarm of bumble bees stimulates the BBMO. To increase the convergence of the conventional BBMO technique, the chaotic idea is incorporated into the BBMO technique CBBMO model is formed. The summary of the discussed work is shown in Table 1.

Table 1
Summary of existing related studies.

Overview with shortcomings	
Existing approaches	The related research has shown that integrating wireless networks with IoT systems allows for the rapid development of smart systems. Smart devices are equipped with standardized communication methods in addition to the ability to data sensing. Moreover, many researchers have explored machine learning approaches to reduce the computational burden on smart systems, although the majority of these solutions are still insufficient to support the optimization process. Due to security and trust concerns caused by the integration of numerous smart devices for collecting agricultural data, most of the communication systems are comprised due to the existence of malicious attacks. As a result, we require a smart agricultural system based on the IoT paradigm to support a remote sensing system with a high level of optimization and data reliability.
Proposed work	This work presents an intelligent model with the combination of a robust forwarding scheme to maintain the balance load among agricultural devices and optimizes the performance. Using a multi-level heuristic approach reduces the additional cost of the communication devices and reduces the delay factor. Moreover, it also offers security for protecting agricultural data against network and communication threats.

3. Proposed authentic and optimizing smart IoT agriculture system

The proposed model is thoroughly described in this section. It consists of the following sub-sections.

3.1. Methodology

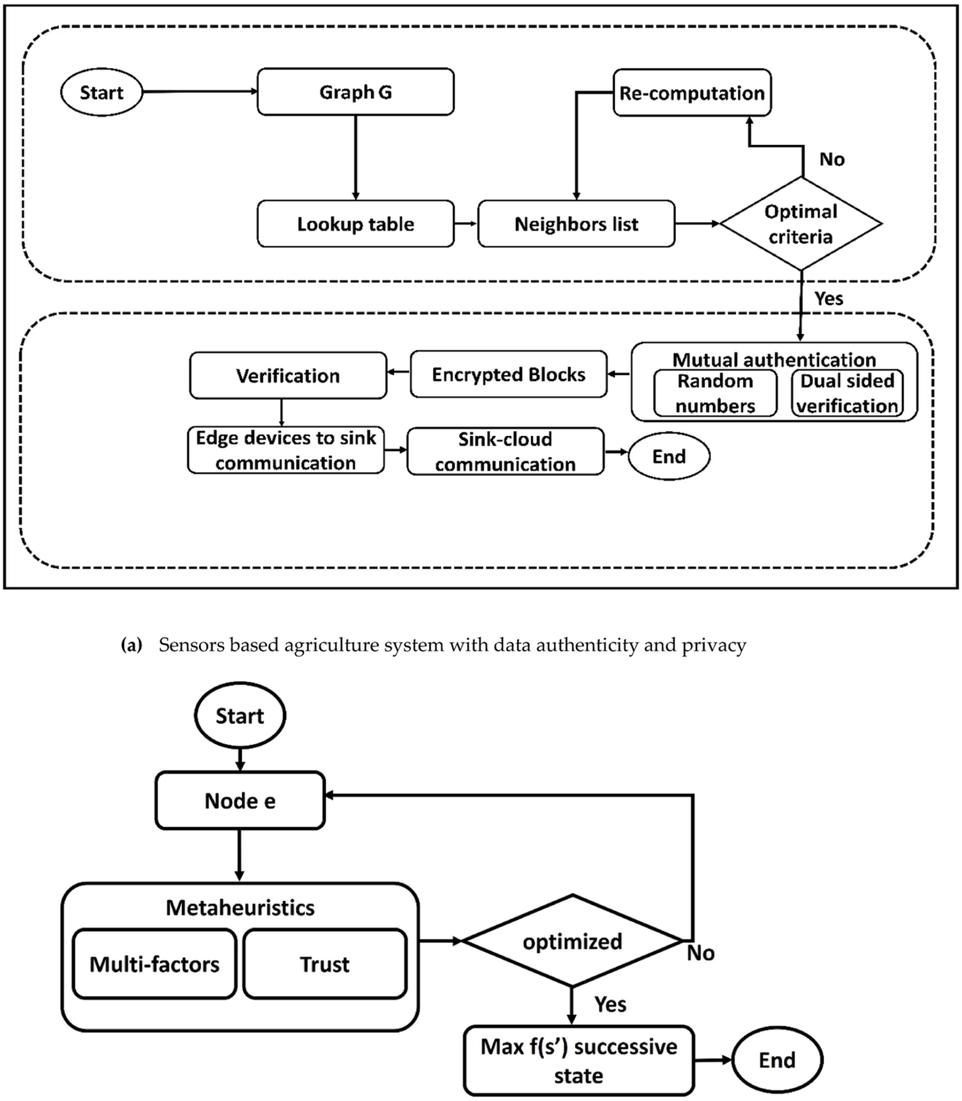
An intelligent and trusted smart agricultural model is proposed using optimization techniques. Unlike traditional approaches, the proposed model decreases the management load of the sensors and optimally delivers the agricultural data toward cloud processing. It decreases the computing power of constraint nodes and supports the reliable decision-making process. Our proposed model is comprised of agricultural sensors to collect and forward the land information with balancing the energy consumption and efficiently splitting the data traffic over the alternate routes. In addition, the data is sent to the sink node using a multi-hop and with the help of smart edges. The data from the sink node is further transmitted to a cloud system and after processing it offers precise statistics to farmers on their smart devices. To cope with consistent and authentic communication, the proposed model utilizes the threshold of direct trust among agricultural devices and maintains the secured environments with various cryptography functions. The value of trust is determined using two factors i.e. nodes' statistics and link behavior. The higher the trust indicates a more optimal choice for transmitting agricultural data thus imposing secured methods for malicious threats. Also, nonauthentic smart devices are treated as foreign nodes that cannot be allowed to access the information directly.

3.2. Discussion

In the proposed model, the ubiquitous network is comprised of sensors and organized in the form of graph G with the composition of nodes N and edges E. To accomplish the delivery of agricultural data, the

Table 2
Format of routing parameters.

ID (1-byte)	Neighbor status (1-byte)	Sink distance SD (1-byte)	Energy e (1-byte)	Delay time d_y (1-byte)	Successive state $f(s')$ (2-byte)



(a) Sensors based agriculture system with data authenticity and privacy

(b) Optimization criteria for sensing devices

Fig. 1. Flowchart of the reliable IoT agricultural model.

neighboring nodes are extracted for the G and formulate a set $N = \mathrm{n}_1, \mathrm{n}_2, \ldots, \mathrm{n}_\mathrm{k}$. The data is transmitted using a multi-hop model until it is received by the sink node. During information forwarding, the optimization process is initiated by exploring a random route from the search space. Firstly, each node lookups at its routing table to identify the location of the sink node, if it is found in its routing table, then the route is marked as optimal and sensors data is forwarded directly. In case, if entry is not found in the routing table then the source node executes the metaheuristic optimizing scheme for finding the reliable set of nodes using multi-hopping. Table 2 shows the format of routing parameters. It comprised of identity ID, neighbor status, distance to sink SD, energy e, delay time d_y and successive rate $f(s')$. The routing parameters are updated when a condition or circumstance changes closer to the source node.

The proposed model executes artificial intelligence techniques in an incremental approach to find the next optimal state from the search space [37,38]. Due to memory and processing time limits in gathering and processing real-time data, the hill-climbing algorithm has been explored. It uses the multi inputs from the environment and computes the value for successive state $f(s')$ such that $f(s)$ ε N. Eq. (1) states the parameters value of energy e, sink distance SD, and delay d_y to compute $f(s')$.

$$\max f(s') = e + \frac{1}{SD} + 1/d_y \tag{1}$$

The value of the current state $f(s)$ is compared with $f(s')$ and based on Eq. (2), the optimization process is initiated.

$$if\ f(s) < f(s')\ \text{then next} - \text{hop} = s'[i] \tag{2}$$

otherwise stopped at s. where $s'[i]$ is the list of extracted neighboring nodes. The proposed model also incorporates the value of direct trust value t_r in optimization function and increases its trustworthiness for newly selected state S_{new} as defined in Eq. (3).

$$S_{new} = P(f(s'),\ t_r) \tag{3}$$

To compute the t_r, the proposed model utilizes the transmitted packets and the number of loss packets as given in Eq. (4).

$$t_r = p_{snd}/p_{loss} \tag{4}$$

where p_{snd} is the number of sent packets and p_{loss} is the number of lost packets. It indicates that highest the value of lost packets decreases communication trust.

Afterward, edges and sensor nodes perform dual authentication by utilizing random numbers. This process is comprised of two phases. Initially, the node generates a random number α_i and shared it with the edge device e_i by integrating its identity id_{si} as given in Eq. (5).

$$s_i \rightarrow e_i:\ \alpha_i + id_{si} \tag{5}$$

Subsequently, upon receiving the information, the edge node verifies the id_i in its routing table and recovers the random number α_i. Later, it generates a random number β_i and resend the computed information to the node s_i along with its identity id_{ei}. The entire communication is encrypted E using a secret key k as given in Eq. (6).

$$e_i \rightarrow s_i:\ E_k(\alpha_i,\ \beta_i,\ id_{ei}) \tag{6}$$

The same process is applied by the node s_i for matching the identity of the edge node in its routing table and recovers the random number α_i that is the previous one sent.

Accordingly, now both the sensors and edges are mutually authenticated and can proceed to data transmission. To attain data privacy, the proposed model uses the xor function to encrypt the data blocks m_k based on security keys k_i where $i = 1, 2, \ldots, n$, as given in Eq. (7).

$$C = (E_{k1}(m_1),\ E_{k2}(m_2),\ \ldots,\ E_{kn}(m_k)) \tag{7}$$

Algorithm 1
Reliable route discovery with trusted metaheuristics.

```
Input:
N: Sensors
NE: Network edges
Ki: Security key
α_i, β_i: Random numbers
f(s'): successive state
f(s): current state
Output: route discovery with authenticity and confidentiality
Procedure metaheurisitics_Opt
Determine neighbors
Create a list of neighbors with IDs
Initiate Route request
Compute successive state $f(s')$
Compare $f(s')$ with current $f(s)$
if $f(s) < f(s')$ then next hop = $s'[i]$
otherwise stopped at $s$.
end if
Determine the trust $tr$ and incorporate it in the selected state
end procedure
Procedure Dual_authen()
Perform dual authentication for sensors and edges
    $s_i \longrightarrow e_i$: $\alpha_i + id_{si}$
    $e_i \longrightarrow s_i$: $E_k(\alpha_i, \beta_i, id_{ei})$
end procedure
Procedure Secured_data()
data blocks $m_k$ security with keys $k_i$
$C = (E_{k1}(m_1), E_{k2}(m_2), \ldots, E_{kn}(m_k))$
end procedure
```

Figs. 1(a) and (b) describe the flowchart of the proposed model for the smart agricultural system using a ubiquitous sensors network. Firstly, the nodes are extracted from the graph and construct the neighbor tables. Afterward, the optimization algorithm is applied to determine the appropriate successor state and selected as a data forwarder with the support of an artificial intelligence algorithm. The optimization function not only evaluates the node's parameters but also incorporates trust values using computed packet information. Secondly, the secure methodology is proposed to construct mutual authentication using random numbers, and after successful verification, both the sensor nodes and edge devices employ encryption methods to protect data from malicious threats. With the use of the sink and edge nodes, agricultural data may be processed more rapidly on both ends, resulting in reduced data delay. Also, smart devices can obtain agricultural data with the high processing capabilities of cloud servers. Algorithm 1 illustrates the pseudocode for the various phases.

4. Simulation

We discuss the simulation parameters and experimental results of the proposed model with existing approaches in this section. The simulations are carried out using an NS-3 simulator [39] with a varying number of nodes. The dimensional area for the evaluation of the performance is set as 350 m x 350 m. The simulation is executed for 4000 s and evaluates the performance results of the proposed model with

Table 3
Simulation parameters.

Parameter	Value
Simulation area	350 m X 350m
Malicious nodes	5, 10, 15
Initial energy	5j
Edge devices	1–5
Sensor nodes	200
Transmission range	5m
MAC layer	IEEE 802.11b
Sink	1
Simulation time	4000 s
Simulations	20
Data traffic	CBR
Performance metrics	packet drop ratio, waiting time, energy consumption

SEAMHR and EGDAS-RPL. The number of edge devices is varying from 1 to 5. The initial energy of the nodes is fixed to 5j. The number of malicious nodes is fixed to 5, 10, and 15, and the transmission range is set to 5 m. 20 simulations were run and each simulation was executed for 4000 s. Table 3 illustrates the list of network parameters used for the conduction of the extensive simulations. The experiments are conducted for two scenarios. i.e. varying number of edges and varying data generation rate.

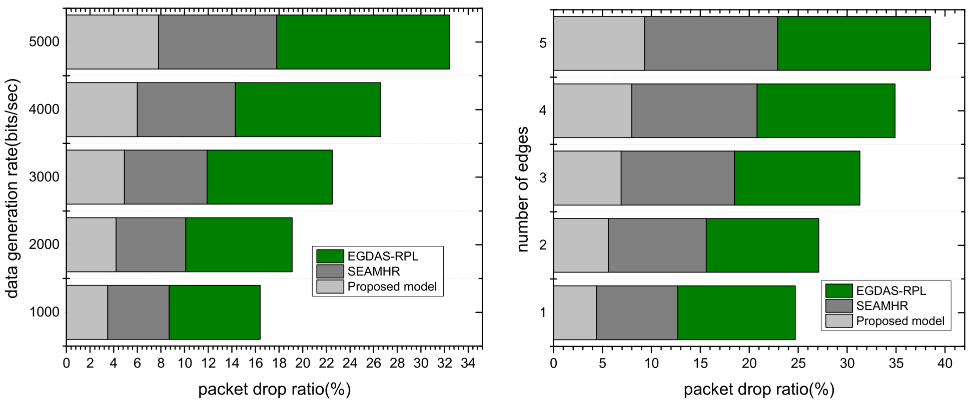
4.1. Results analysis

The proposed model is compared with EGDAS-RPL and SEAMHE approaches under various simulation tests. The tests are performed in terms of packet drop ratio, waiting time, and energy consumption under varying numbers of edged devices and data generation rates, as depicted in Table 4. All the results are recorded in a simulated trace file and later, using needed information is extracted to show the performance results.

Table 4
Performance comparison under varying edges and data generation rate.

Proposed Model with existing approaches	Packet drop ratio(%)	Waiting time (*sec*)	Energy consumption (j)
Varying number of edges			
Proposed model	9.3	1.44	1.23
EGDAS-RPL	13.6	1.51	1.38
SEAMHE	15.6	1.57	1.51
Varying Data generation rates			
Proposed model	7.8	2.02	1.2
EGDAS-RPL	10	2.1	1.38
SEAMHE	14.6	2.12	1.49

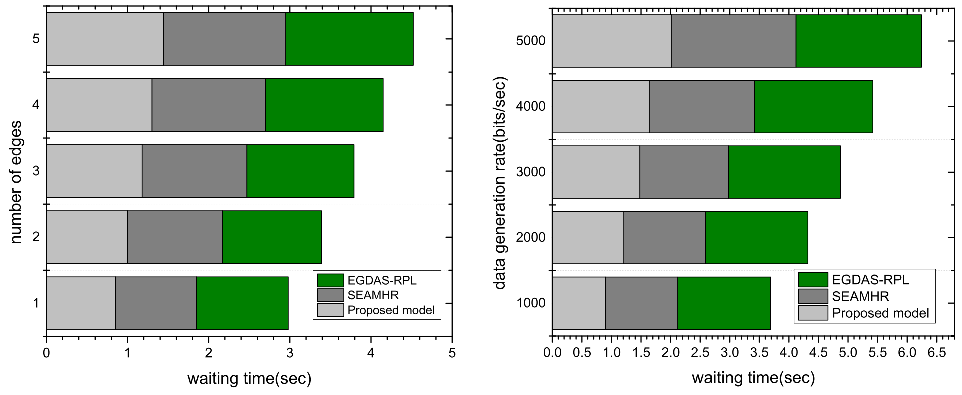
In terms of packet drop ratio, Fig. 2(a) and (b) depict the performance results of the proposed model and existing work. It is seen that with increasing network load in terms of dynamic attributes, the number of packets lost also increases. However, according to experimental findings, the proposed model significantly decreases the ratio of packets lost. This improvement is the result of computing direct trust using packet receiving and packet loss rate. As a result, in the process of optimizing, the paths with a higher degree of re-transmission are avoided. Furthermore, multi-hop paradigms improve delivery performance by reducing the load on the communication links. Lookup tables for smart agricultural sensors help them estimate the more trusted peer nodes that keep the most up-to-date data across neighbors. The performance analysis of the proposed model in comparison to prior work for waiting time is shown in Fig. 3(a) and (b). With an increase in the data generation rate and the number of malicious nodes, it is demonstrated that the waiting time for receiving sensor data toward the sink node increases. It results from overloading the transmission channels and delivering excessive amounts of route requests to adjacent nodes. However, the waiting time for forwarding agricultural data from smart devices was remarkably improved by the proposed model as compared to existing work. It enables less congestion on forwarders that are close to the sink border and shortens the time it takes for data forwarding from



a) number of edges and packet drop ratio

(b) data generation rate and packet drop ratio

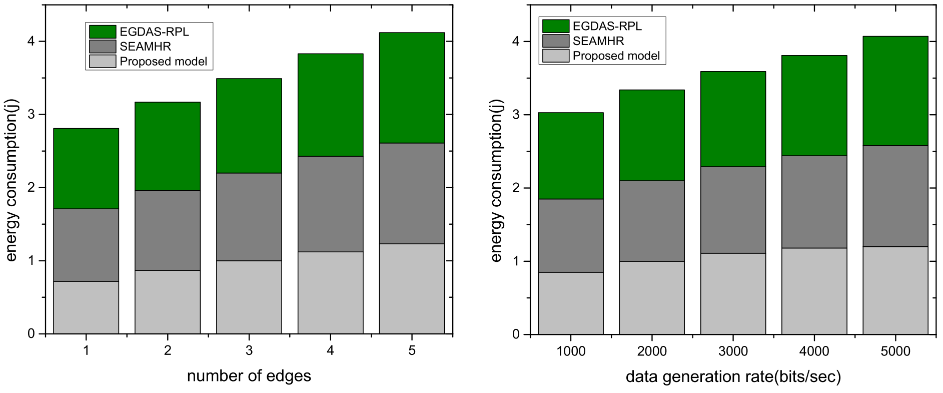
Fig. 2. Packet drop ratio for the varying number of edges and data generation rate.



a) number of edges and waiting time

b) data generation rate and waiting time

Fig. 3. Waiting time for the varying number of edges and data generation rate.



a) number of edges and energy consumption

b) data generation rate and energy consump tion

Fig. 4. Energy consumption for the varying number of edges and data generation rate.

the data originating node to the destination. Fig. 4(a) and (b) compare the performance of the proposed model with alternative approaches in terms of energy consumption. According to the experimental findings, the proposed model has increased energy consumption efficiency under varying numbers of edges and data generation rates. Unlike other work, this is due to consideration of the metaheuristics-based optimal route discovery process. Moreover, all of the neighbors are assessed based on specific criteria, and the selection of the next hop is made appropriately. The acknowledgement of packet data is additionally used by optimization functions to get effective consequences for energy consumption. The proposed model utilizes the extracted list from the graph, which reduces the number of hops in the transmission network rather than flooding route requests on unnecessary paths. To limit energy depletion with fewer control messages, only highly secure nodes are chosen for data transfer.

4.2. Performance results

Figs. 2, 3 and 4.

5. Conclusions

Recently, the ubiquitous network has been extensively used to support automated systems and the development of smart systems. To effectively monitor the plants, crops, etc., physical objects and sensors work together, and the gathered information is sent to the sink node. Although there have been many solutions to use artificial intelligence for reducing the communication cost of managing agricultural data, the research community still needs a trustworthy optimization process. Also, a lot of solutions fail to protect the data gathered by deployed sensors, which makes it easier for malicious attackers. Such systems increase the overhead on the tiny devices in data forwarding and overlooked the constrained resources of the network infrastructure. To increase the level of optimal criteria and productivity control, this study proposes a smart and reliable metaheuristics optimization model based on a ubiquitous IoT system. The incorporation of trust value with the optimal function provides a significant role in the reliability of data forwarding. Moreover, the dual authentication among smart sensors and edge devices negotiates the security level in a controlled manner and makes it harder for malicious attacks.

Author statement

All authors certify that they have participated sufficiently in the work to take public responsibility for the content, including participation in the concept, design, analysis, writing, or revision of the manuscript. Furthermore, each author certifies that this material or similar material has not been and will not be submitted to or published in any other Publication.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgement

This work was technically supported by Artificial Intelligence & Data Analytics (AIDA) Lab CCIS Prince Sultan University, Riyadh, Saudi Arabia. The authors are thankful for the support.

References

[1] I.A. Lakhiar, G. Jianmin, T.N. Syed, F.A. Chandio, N.A. Buttar, W.A. Qureshi, Monitoring and control systems in agriculture using intelligent sensor techniques: a review of the aeroponic system, J. Sensors 2018 (2018).

[2] J. Lloret, J. Tomas, A. Canovas, L. Parra, An integrated IoT architecture for smart metering, IEEE Commun. Mag. 54 (12) (2016) 50–57.

[3] M.A. da Cruz, J.J.P. Rodrigues, J. Al-Muhtadi, V.V. Korotaev, V.H.C. de Albuquerque, A reference model for internet of things middleware, IEEE Internet Things J. 5 (2) (2018) 871–883.

[4] S.I. Hassan, M.M. Alam, U. Illahi, M.A. Al Ghamdi, S.H. Almotiri, M.M. Su'ud, A systematic review on monitoring and advanced control strategies in smart agriculture, IEEE Access 9 (2021) 32517–32548.

[5] L. Nóbrega, P. Gonçalves, P. Pedreiras, J. Pereira, An IoT-based solution for intelligent farming, Sensors 19 (3) (2019) 603.

[6] K.G. Liakos, P. Busato, D. Moshou, S. Pearson, D. Bochtis, Machine learning in agriculture: a review, Sensors 18 (8) (2018) 2674.

[7] L.K. Singh, M.K. Jha, M. Pandey, Framework for standardizing less data-intensive methods of reference evapotranspiration estimation, Water Resour. Manage. 32 (13) (2018) 4159–4175.

[8] D.S. Bullock, M. Boerngen, H. Tao, B. Maxwell, J.D. Luck, L. Shiratsuchi, L. Puntel, N.F. Martin, The data-intensive farm management project: changing agronomic research through on-farm precision experimentation, Agron. J. 111 (6) (2019) 2736–2746.

[9] M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain, A.J. Aljaaf, A systematic review on supervised and unsupervised machine learning algorithms for data science, Supervised and unsupervised learning for data sci. (2020) 3–21.

[10] A.S. Kwekha-Rashid, H.N. Abduljabbar, B. Alhayani, Coronavirus disease (COVID-19) cases analysis using machine-learning applications, Appl. Nanosci. (2021) 1–13.

[11] L. Muhammad, E.A. Algehyne, S.S. Usman, A. Ahmad, C. Chakraborty, I. A. Mohammed, Supervised machine learning models for prediction of COVID-19 infection using epidemiology dataset, SN comput. sci. 2 (1) (2021) 1–13.

[12] D.R. Schrider, A.D. Kern, Supervised machine learning for population genetics: a new paradigm, Trends Genet. 34 (4) (2018) 301–312.

[13] B. Prenkaj, P. Velardi, G. Stilo, D. Distante, S. Faralli, A survey of machine learning approaches for student dropout prediction in online courses, ACM Comput. Surveys (CSUR) 53 (3) (2020) 1–34.

[14] M.W. Berry, A. Mohamed, B.W. Yap, Supervised and Unsupervised Learning For Data Science, Springer, 2019.

[15] B.B. Sinha, R. Dhanalakshmi, Recent advancements and challenges of Internet of Things in smart agriculture: a survey, Future Generation Comput. Sys. 126 (2022) 169–184.

[16] I. Charania, X. Li, Smart farming: agriculture's shift from a labor intensive to technology native industry, Internet Things 9 (2020), 100142.

[17] B. Cao, L. Zhang, Y. Li, D. Feng, W. Cao, Intelligent offloading in multi-access edge computing: a state-of-the-art review and framework, IEEE Commun. Mag. 57 (3) (2019) 56–62.

[18] A.H. Wheeb, N.A.S. Al-Jamali, Performance analysis of OLSR protocol in mobile ad hoc networks, Acta Med. Indones 16 (01) (2022) 107.

[19] K. Haseeb, A. Rehman, T. Saba, S.A. Bahaj, J. Lloret, Device-to-device (d2d) multi-criteria learning algorithm using secured sensors, Sensors 22 (6) (2022) 2115.

[20] F. Al-Turjman, Optimized hexagon-based deployment for large-scale ubiquitous sensor networks, J. Network Syst. Manage. 26 (2) (2018) 255–283.

[21] M. Losavio, A. Elmaghraby, A. Losavio, Ubiquitous networks, ubiquitous sensors: issues of security, reliability and privacy in the internet of things, in: International Symposium on Ubiquitous Networking, Springer, 2018.

[22] K. Lakshmanna, N. Subramani, Y. Alotaibi, S. Alghamdi, O.I. Khalafand, A. K. Nanda, Improved metaheuristic-driven energy-aware cluster-based routing scheme for IoT-assisted wireless sensor networks, Sustainability 14 (13) (2022) 7712.

[23] A.H. Wheeb, M.T. Naser, Simulation based comparison of routing protocols in wireless multihop adhoc networks, Int. J. Electr. Comput. Eng. 11 (4) (2021) 3186.

[24] M.A. da Cruz, J.J. Rodrigues, P. Lorenz, V.V. Korotaev, V.H.C. de Albuquerque, In. IoT—A new middleware for Internet of Things, IEEE Internet Things J 8 (10) (2020) 7902–7911.

[25] O. Diallo, J.J. Rodrigues, M. Sene, J. Lloret, Distributed database management techniques for wireless sensor networks, IEEE Trans. Parallel Distrib. Syst. 26 (2) (2013) 604–620.

[26] K. Haseeb, A. Almogren, I. Ud Din, N. Islam, A. Altameem, SASC: secure and authentication-based sensor cloud architecture for intelligent internet of things, Sensors 20 (9) (2020) 2468.

[27] A. Caggiano, Cloud-based manufacturing process monitoring for smart diagnosis services, Int. J. Computer Integr. Manuf. 31 (7) (2018) 612–623.

[28] F. Al-Turjman, H. Zahmatkesh, A Comprehensive Review on the Use of AI in UAV Communications: enabling Technologies, Applications, and Challenges, Unmanned Aerial Vehicles in Smart Cities (2020) 1.

[29] V.K. Quy, V.H. Nam, D.M. Linh, N.T. Ban, N.D. Han, Communication solutions for vehicle ad-hoc network in smart cities environment: a comprehensive survey, Wireless Personal Commun. (2021) 1–25.

[30] S. Maurya, V.K. Jain, Energy-efficient network protocol for precision agriculture: using threshold sensitive sensors for optimal performance, IEEE Consumer Electronics Magazine 6 (3) (2017) 42–51.

[31] P. Sanjeevi, S. Prasanna, B. Siva Kumar, G. Gunasekaran, I. Alagiri, R. Vijay Anand, Precision agriculture and farming using Internet of Things based on wireless sensor network, Trans. Emerging Telecommun. Technol. 31 (12) (2020) e3978.

[32] S. Sankar, P. Srinivasan, A.K. Luhach, R. Somula, N. Chilamkurti, Energy-aware grid-based data aggregation scheme in routing protocol for agricultural internet of things, Sustain. Comput. 28 (2020), 100422.

[33] S. Ramesh, C. Yaashuwanth, Enhanced approach using trust based decision making for secured wireless streaming video sensor networks, Multimed. Tools Appl. 79 (15) (2020) 10157–10176.

[34] G.V. Gurram, N.C. Shariff, R.L. Biradar, A secure energy aware meta-heuristic routing protocol (SEAMHR) for sustainable IoT-wireless sensor network (WSN), Theor. Comput. Sci. 930 (2022) 63–76.

[35] M.B. Dowlatshahi, M.K. Rafsanjani, B.B. Gupta, An energy aware grouping memetic algorithm to schedule the sensing activity in WSNs-based IoT for smart cities, Soft comput. 108 (2021), 107473.

[36] S. Gali, V. Nidumolu, An intelligent trust sensing scheme with metaheuristic based secure routing protocol for Internet of Things, Cluster Comput. 25 (3) (2022) 1779–1789.

[37] B. Selman, C.P. Gomes, Hill-climbing search, Encycl. cognitive sci. 81 (2006) 82.

[38] Norvig, P.R. and S.A. Intelligence, *A modern approach.* Prentice Hall Upper Saddle River, NJ, USA: rani, M., Nayak, R., & Vyas, OP (2015). An ontology-based adaptive personalized e-learning system, assisted by software agents on cloud storage. Knowl. Based Syst., 2002. 90: p. 33–48.

[39] G.F. Riley, T.R. Henderson, *The ns-3 Network simulator*, in *Modeling and Tools For Network Simulation*, Springer, 2010, pp. 15–34.