A Novel Secure and Energy-efficient Routing Method for the Agricultural Internet of Things Using Whale Optimization Algorithm

Yanling Wang[1,*] and Yong Yang[2]

[1]*School of faculty of Electrical Information, Changchun Guanghua University, Changchun 130031, China*
[2]*Thyssenkrupp Fuo Automotive Steering Column (Changchun) Co., LTD Changchun 130033, China*
E-mail: 18943939283@163.com
[*]*Corresponding Author*

Received 04 May 2023; Accepted 27 February 2024

Abstract

The Internet of Things (IoT) is an all-encompassing system that tracks and monitors real-world activities by gathering, handling, and interpreting data from IoT equipment. It has successfully been applied in several fields, particularly smart agriculture since there is a high demand for high-quality foodstuffs worldwide. It is essential to develop new agricultural production schemes to meet these demands. The heterogeneity of IoT devices makes security essential for IoT communication. Also, IoT devices are restricted in terms of processing, memory, and power capacities. Therefore, energy is a key factor in extending the life of an agricultural IoT network. This study

Journal of Cyber Security and Mobility, Vol. 13_4, 725–750.
doi: 10.13052/jcsm2245-1439.1347
© 2024 River Publishers

presented a novel energy-aware and secure routing scheme using the Whale Optimization Algorithm (WOA) for IoT, referred to as SRWOA. The simulation results indicate that SRWOA uniformly distributes energy consumption in IoT and maximizes the packet delivery ratio.

Keywords: Internet of Things, agriculture, energy efficiency, whale optimization algorithm.

1 Introduction

The Internet of Things (IoT) empowers physical objects in a variety of form factors to exchange data and facilitate better communication [1, 2]. In recent years, ubiquitous data access has expanded dramatically to include a variety of fields, such as embedded technology that utilizes actuators and sensors in order to gather data and respond appropriately [3]. Embedding the Internet in various things and allowing them to communicate with each other is the primary driver of IoT's development [4]. Using a combination of front-end computing devices and back-end services, IoT systems map relationships between the real and digital worlds [5]. Front-end devices can incorporate embedded computer systems that contain sensing devices, including mobile phones, cameras, wearable devices, and RFID tags. These front-end devices are typically situated in an open environment that is beyond the control of the system administrator [6]. Back-end systems are software systems that integrate, process, and analyze the data collected by the front-end devices; they may also allow users to view analyzed results [7]. IoT systems typically consist of three layers, as illustrated in Figure 1. IoT devices form the first layer. The network layer comprises the communication network, which consists of gateways to facilitate the control of IoT devices locally and link them to the Internet. In this layer, storage and upper layer application services are provided, including processing and analysis of data [8].

Machine learning and artificial intelligence are fundamental pillars of the IoT, playing a pivotal role in unlocking its full potential [9]. With the ability to analyze and interpret massive volumes of data generated by interconnected devices, machine learning algorithms can extract meaningful patterns, uncover valuable insights, and make intelligent predictions [10, 11]. Artificial intelligence techniques, such as deep learning and neural networks, enable IoT systems to adapt, learn, and make real-time decisions based on the data they receive [12]. This synergy between machine learning, artificial intelligence, and IoT empowers organizations and industries to optimize processes, improve operational efficiency, enhance predictive maintenance, enable autonomous systems, and create personalized experiences for users [13]. Moreover, by continuously learning from data streams, machine learning algorithms can identify anomalies, detect potential threats, and enhance security in IoT ecosystems [14, 15]. In essence, the integration of machine learning and artificial intelligence in IoT revolutionizes industries, drives innovation, and paves the way for a more intelligent and connected future [16]. Smart electricity networks are essential in the IoT ecosystem as they provide effective power management and promote sustainable energy usage [17, 18].

Connectivity is an integral part of IoT and has a highly distributive nature, ranging from a local to a global scale. Compared to wired connections, wireless devices offer greater cost savings and ease of installation. Furthermore, the wide range of wireless technologies contributes to the development of a unique solution to the many IoT requirements [19]. The requirements have been thoroughly reviewed, including application protocol, network suitability, range, throughput, and the available framework. As a result, IoT requires energy-constrained devices that are typically powered by batteries [20]. As battery replacement is not a feasible solution for critical applications, IoT devices are expected to be durable for years, making energy efficiency a priority [21]. A major feature of the IoT is the ability to connect heterogeneous devices together [22]. Since these devices are designed by different vendors, they are not often standardized. In this regard, interoperability, which enables different devices to communicate with one another, is also an important issue to resolve. As IoT continues to expand and exchange large amounts of data, there is also an increasing threat to security. Several types of attacks have been reported in the literature against IoT devices [23, 24].

The IoT has the potential to change the way we live by transforming ongoing systems. It has been incorporated into a variety of fields, including transport, industry, smart city, healthcare, and agriculture. In order to feed the growing population, the agriculture industry must implement IoT-based systems in its field operations [25]. IoT-driven agriculture decreases wasted water, pesticides, and increases seed productivity. By providing efficiency in water spraying or the optimization of inputs and treatments, IoT-based agriculture can have a significant impact on the environment. In agriculture, IoT platforms provide farmers with monitored data and useful solutions to address real-life issues [26]. Wireless Sensor Networks (WSNs) have become increasingly important as various IoT devices can be used to support their operations [27]. With the integration of ICT into a new era of agriculture, the agricultural sector is experiencing a fourth revolution, Farming 4.0. In recent years, a number of emerging technologies have been evaluated as part of smart agriculture, including UAV technology, artificial intelligence, big data, and data analytics [28, 29].

The IoT is transforming the agriculture industry by providing farmers with a variety of tools to handle various challenges they face in the field. IoT-enabled technologies allow farmers to access their farms almost anywhere and at any time. Farming processes are regulated by sensors and actuators, and the farm is monitored by WSN. The farm is monitored remotely with wireless cameras and sensors, and pictures and videos are collected for analysis. Agricultural land can also be monitored remotely via IoT using a smart phone from anywhere in the world [30]. The use of IoT-enabled technologies has the potential to reduce crop production costs and increase land productivity. Smart agriculture utilizes IoT in several key areas, such as crop management, Tracking and tracing, Farm Management System, Livestock monitoring, Waste management, Nutrient management, Precision farming, Weather management, Soil management, and Water management [28]. Meta-heuristic algorithms play a crucial role in IoT routing by offering adaptive and efficient solutions to address the dynamic and resource-constrained nature of IoT networks [31]. This paper proposes an IoT secure routing protocol for the agriculture sector based on clustering and tree-based strategies and employing the Whale Optimization Algorithm (WOA), called SRWOA. With this mechanism, security and energy efficiency are enhanced simultaneously. The SRWOA algorithm employs a hierarchical routing approach based on two operations: secure clustering and a WOA-based routing tree. In addition, the trust scheme proposed can be used to protect against attacks related to black holes. The main contributions of SRWOA can be summarized as follows:

- Energy-efficient routing: SRWOA employs the WOA to design an energy-efficient routing scheme for IoT networks, enhancing the longevity of agricultural IoT devices.
- Security enhancement: SRWOA integrates a secure clustering and hierarchical routing approach to mitigate potential security threats, including black hole attacks.
- Uniform energy distribution: Our proposed scheme aims to uniformly distribute energy consumption across IoT devices, ensuring a balanced energy utilization in the network.
- Packet delivery optimization: Simulation results demonstrate that SRWOA maximizes the packet delivery ratio in agricultural IoT networks, further enhancing their efficiency.

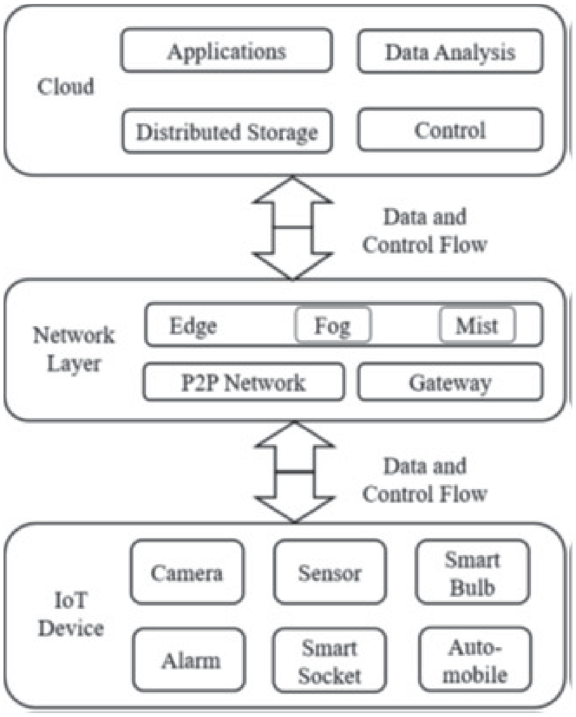

Figure 1 Typical architecture of an IoT system.

2 Related Work

Based on IoT technology, Xue and Huang [32] studied WSN routing protocols for smart agriculture and algorithms for positioning nodes. They evaluated the efficiency of different routing protocols by simulating the environment and analyzing the results. They also developed algorithms for positioning nodes in a WSN to optimize communication paths and reduce energy consumption. The simulations allowed them to analyze the performance of the protocols in a variety of situations and they used the algorithms to identify the best positions for the nodes in the WSN in order to optimize the communication paths and reduce energy consumption. They also studied the impact of factors such as node energy, distance, and mobility on the performance of the LEACH protocol. As a result, they concluded that the Low Energy Adaptive Clustering Hierarchy protocol offers increased efficiency when compared to other protocols, and its lifespan is further extended through improved algorithms.

A wide range of low-cost hardware and communication technologies have enabled the IoT to provide productive ways of cultivating soil. These technologies allow for real-time monitoring of soil conditions, such as temperature, moisture, and pH levels, which can be used to optimize crop yields and reduce water and fertilizer usage. Additionally, the use of IoT-enabled precision agriculture can reduce the need for manual labor, resulting in cost savings. By continuously monitoring soil conditions and making timely adjustments, farmers can adjust their irrigation and fertilizer schedules accordingly, which can improve crop yields and reduce water and fertilizer usage. Additionally, the use of IoT-enabled precision agriculture can help automate manual processes, leading to fewer labor costs and less time spent managing farming operations. In order to develop new functionalities based on IoT deployment paradigms, Ferrández-Pastor, et al. [33] studied industrial agricultural facilities with farmers and growers. In the process of introducing technology to agricultural applications, the user-centered design model is used as a means of acquiring knowledge and experience. This knowledge and experience are then used to create a customized design to meet the needs of the user. An IoT paradigm is used as a resource to facilitate decision making. A distributed model based on edge and fog computing paradigms is used to implement IoT architecture, operating rules, and smart processes. These technologies are used to propose a communication architecture. The objective is to assist farmers in developing smart systems in both existing and new facilities. Farmers can easily deploy different decision trees to automate the installation.

By introducing new technologies and improving existing ones, farmers can boost their yields while also reducing the use of chemicals, leading to safer and more sustainable agricultural practices. Additionally, better tracking and monitoring systems can be used to ensure the quality and safety of agricultural products, as well as stricter regulations to minimize environmental pollution caused by agricultural activities. Liu, et al. [30] proposed an integrated framework system platform incorporating IoT, cloud computing, and data mining. The new framework system provides a platform for data collection, storage, and analysis. It also enables the use of AI-based technologies for crop management, pest control, and crop yield prediction. These technologies can help increase efficiency, reduce costs, and improve the quality of agricultural products.

IoT can efficiently connect agriculture and farming bases located in rural areas with fog computing and a WiFi-based long-distance network based on cloud computing. For the specific purposes of monitoring and controlling agriculture and farms in rural areas, Ahmed, et al. [28] proposed a scalable network architecture. The proposed solution reduces network latency to some extent when compared with existing IoT-based agriculture and farming solutions. This paper proposes a cross-layer channel access and routing solution for sensing and actuating. The network structure is analyzed based on coverage range, throughput, and latency.

Precision agriculture has become a trending technology that improves agricultural productivity. This method incorporates a variety of technologies, such as IoT, remote sensing, information technology and WSN. Anand [34] proposed a novel approach to the scheduling of irrigation water in precision agriculture by utilizing wireless sensors, such as moisture and temperature sensors. Blockchain technology is used in the proposed framework to enable secure cloud data transfer. Further, the Improved LEACH algorithm is used to achieve energy efficient data transfer. PIC microcontroller modules are used to acquire data from sensors. Data acquired by the Raspberry Pi module is then transmitted to the cloud. A blockchain-based IoT technique is then used to secure and verify the collected data.

Cicioğlu and Çalhan [35] intend to enhance the productivity of corn harvesting on large-scale fields using Internet of Things hardware and software. They aim to use the hardware and software to gather data on soil fertility, moisture levels, and weather conditions in order to provide more accurate predictions about when it will be best to harvest the corn. This will enable farmers to make more informed decisions about when to harvest and maximize their yields. Using heterogeneous sensor nodes, the system can detect acoustic signals, rain, wind, light, temperature, and pH levels in cornfields. At coordinator nodes, special purpose sensors collect data on the characteristics of cornfields, and these data are then relayed to the drone through the coordinator node. Sensor nodes are only required to detect conditions at specific times of the day due to the fact that the data in cornfields does not fluctuate rapidly. In order to monitor farmers' visual devices, the drone sends data to the base stations. This eliminates the need for long-distance communication between sensors in a region of large-scale cornfields.

Sankar, et al. [36] introduced a protocol called EGDAS-RPL (Energy-aware Grid-based Data Aggregation Scheme in Routing) specifically designed for agricultural IoT applications. The protocol consists of three main processes: grid formation, grid head selection, and grid head parent selection. Initially, EGDAS-RPL establishes a grid of equal-sized cells over the square network. Subsequently, it probabilistically chooses a grid head node within each grid. Lastly, the protocol utilizes the expected transmission count metric to identify the most suitable grid head parent for efficient data transfer. To evaluate its performance, the COOJA simulator is employed for conducting simulations. Comparative analysis with RPL and E2HRC-RPL demonstrates that EGDAS-RPL effectively reduces packet loss ratio and end-to-end delay, thereby prolonging the network's lifespan.

Friha, et al. [37] present FELIDS (Federated Learning-based Intrusion Detection System), a solution designed to enhance the security of agricultural-IoT infrastructures. FELIDS adopts a federated learning approach, ensuring data privacy through local learning. In this system, devices collaborate by sharing model updates with an aggregation server, enabling the generation of an improved detection model without exposing sensitive data. To counter agricultural IoT attacks, FELIDS employs three deep learning classifiers: deep neural networks, convolutional neural networks, and recurrent neural networks. The performance evaluation of the proposed intrusion detection system is conducted using three distinct datasets: CSE-CIC-IDS2018, MQTTset, and InSDN. The findings demonstrate that FELIDS surpasses traditional centralized machine learning approaches in terms of protecting IoT device data privacy and achieves superior accuracy in detecting attacks.

With the progression of IoT technology, modern agriculture is embracing Agriculture 4.0. Agricultural IoT heavily relies on wireless communication, yet traditional site selection overlooks the impact of terrain on transmission loss, leading to power wastage and higher maintenance costs. Xie, et al. [38] propose a rapid terrain sampler using a multi-sensor fusion algorithm to collect point-cloud data of the experimental site terrain. They design an objective function considering electromagnetic wave losses, optimizing router and gateway locations using k-means and Particle Swarm Optimization (PSO) algorithm. Simulations show PSO's sensitivity to execution parameters and faster convergence compared to genetic algorithm. On-site received signal-strength indication (RSSI) measurements demonstrate improved communication quality at optimized points. The algorithm is significant for agricultural IoT node site selection. However, the objective function may require refinement in diffraction loss calculations. The proposed tool enables quicker 3D modeling of farmland compared to traditional methods, with potential applications in soil moisture analysis and plant light exposure prediction.

Research in the field of secure and energy-efficient routing for the agricultural IoT reveals critical gaps that must be addressed. Firstly, there is a need for robust security mechanisms specifically tailored to agricultural IoT routing protocols. Existing protocols may not sufficiently meet the unique security requirements and constraints of agricultural environments, necessitating the development of novel mechanisms to ensure secure data transmission and protection against various attacks. Secondly, energy efficiency is crucial in agricultural IoT systems, where devices are often deployed in remote and resource-limited areas. Research is needed to design energy-efficient routing algorithms that optimize energy consumption considering factors such as node mobility, network topology, and data transmission protocols. These algorithms should aim to extend network lifetime and minimize energy usage. Furthermore, guaranteeing quality of service (QoS) is essential for agricultural applications. Routing protocols should provide reliable and timely data delivery, low latency, high throughput, and minimal packet loss. They should be tailored to the specific requirements of agricultural applications while considering the limited resources of IoT devices.

Scalability and adaptability are additional gaps requiring attention. Agricultural IoT systems may involve numerous devices spread across large farmland areas, necessitating scalable routing protocols that can handle increasing device numbers and adapt to dynamic network topology changes. Moreover, integrating diverse technologies like wireless sensor networks, satellite communications, edge computing, and cloud platforms presents a challenge. Research is needed to seamlessly integrate these technologies into a unified routing framework, enabling efficient data exchange, seamless handoffs, dynamic resource allocation, and ensuring security and energy efficiency. Lastly, practical validation and real-world deployment of proposed routing solutions are crucial to assess their performance, scalability, and effectiveness in realistic agricultural environments. Field trials and experiments will help uncover additional challenges and opportunities not apparent in simulation-based studies. Addressing these research gaps will contribute to the development of reliable, scalable, and sustainable routing solutions for the agricultural IoT, empowering farmers with enhanced productivity, optimized resource utilization, and improved agricultural practices.

3 Proposed Method

3.1 Network Model

As shown in Figure 2, SRWOA uses a WSN-based IoT network as its model. It is composed of N heterogeneous sensor nodes that communicate with each other to monitor the environment. IoT nodes are assigned unique identifiers, and their deployment is random. In addition, all IoT nodes are equipped with the global positioning system (GPS), which allows them to determine

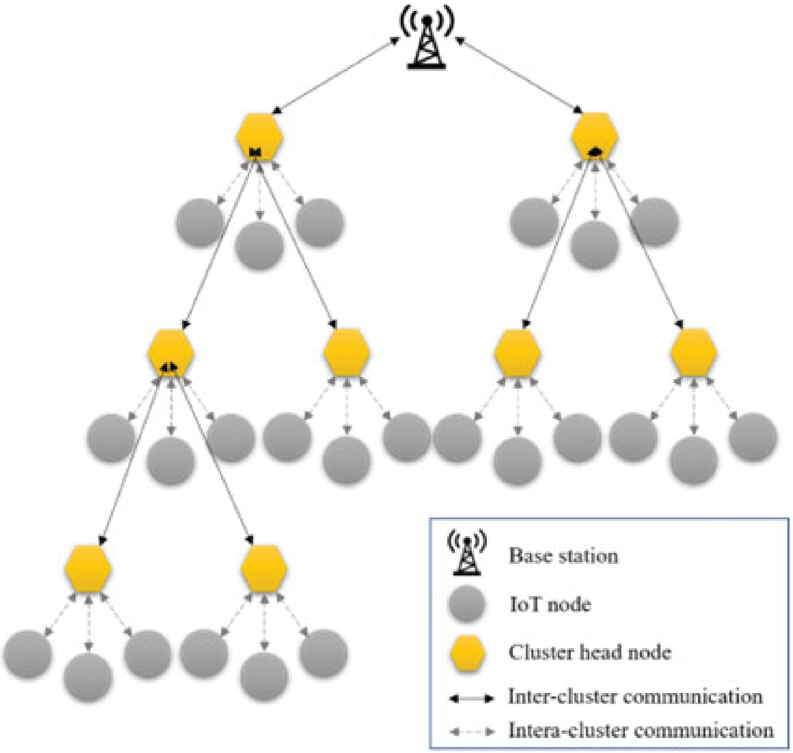

Figure 2 Network model.

their location within the network. IoT nodes' energy levels, memory capacity, and processing power vary. Cluster heads and cluster members are two roles played by the nodes in this network. An overview of the tasks assigned to each node follows:

- Cluster members: These nodes receive information from the target region and forward it to the cluster head directly.
- Cluster heads: Data collection from cluster members is the responsibility of the cluster heads, aggregating these packets, and sending them to the base station. Using a binary routing tree, data is transferred from cluster heads to base stations.
- Basic station: Data received from cluster heads is processed, analyzed, and decided by the base station. Each IoT node has a fixed and predetermined position at the base station.

3.2 Energy Model

An energy model measures the energy consumption of WSNs. The energy model accounts for the energy consumed by each node in the network, such as the radio, processor, and sensors. This model then estimates the overall energy consumption of the WSN based on the power requirements of each node. Two types of models are available: free space and multipath channel models. The free space model estimates the energy consumption of WSNs in an ideal environment without interference.

On the other hand, the multipath channel model considers the presence of obstacles and the effects of interference on the radio signal, and thus provides a more realistic view of the energy consumption of WSN. Energy models are selected based on the distance between the receiver and transmitter. Figure 3 depicts the energy model for WSNs. Equations (1) and (2) calculate the energy required to transmit and receive k bits of data:

$$E_{tran}(k,d) = \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2 \; d < d_0 \\ kE_{elec} + k\varepsilon_{amp}d^4 d \geq d_0 \end{cases} \tag{1}$$

$$E_{recie}(k) = kE_{elec} \tag{2}$$

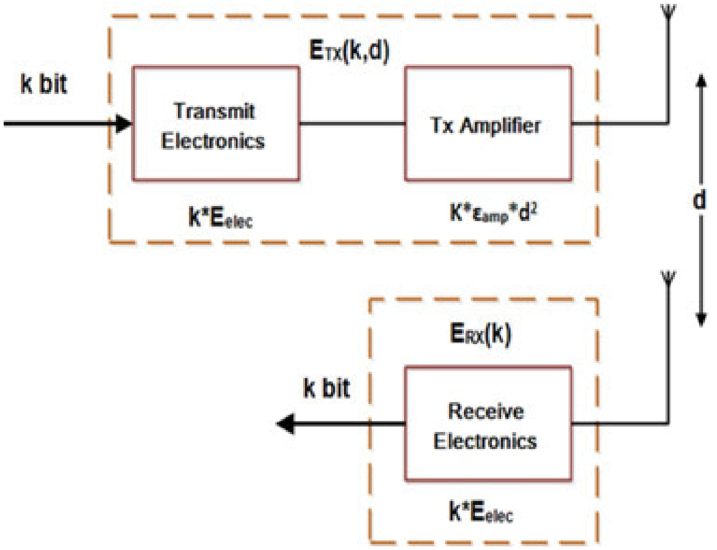

Figure 3 Energy model for WSN.

3.3 Attack Model

A wireless communication channel makes IoT vulnerable to various security attacks. An attacker may employ various security attacks to compromise secure information transfer, such as black holes, Denial of Service (DoS), flooding, and wormholes. Wormhole attacks allow an attacker to take control of the data transfer process by creating a tunnel between two endpoints. Flooding attacks can overwhelm a network with bogus traffic, making it difficult for legitimate traffic to reach its destination. DoS attacks prevent legitimate users from accessing a device or network. Black hole attacks create a void that prevents data transfer between two endpoints. Selectively forwarding attacks exploit the trust between wireless nodes to forward data packets to an attacker selectively.

In this study, we focused on black hole attacks. Black hole nodes in an IoT system quickly respond to route request messages (RREQ) by declaring they have an efficient route to the destination. This malicious behavior causes all the other routes in the system to be ignored, resulting in all the data packets being routed through it. As a result, the black hole node can intercept and modify the data packets, leading to security breaches in the system. The network forms an insecure path when the source node receives the fake route reply message. This insecure path is traversed by a black hole node that eliminates all information packets as an intermediate node. Figure 4 shows an overview of a black hole attack.

3.4 Proposed Algorithm

In this section, the secure routing protocol using the Whale Optimization Algorithm (SRWOA) is discussed in detail. SRWOA uses a bio-inspired algorithm to optimize the route selection process, considering several parameters such as the amount of energy consumed, latency, and data transmission rate. This optimization process allows the selection of the most secure and reliable route for data transmission. SRWOA includes three key stages: lightweight and distributed trust, trust-based clustering, and WOA-based routing.

3.4.1 Lightweight and distributed trust

W-trust uses a weighted trust algorithm to calculate the trustworthiness of a device by taking into account the success and failure of prior interactions and the context in which the communications occur. This allows devices to make trust decisions without needing a centralized trust authority. W-Trust monitors the behavior of each node within the IoT network and assigns them

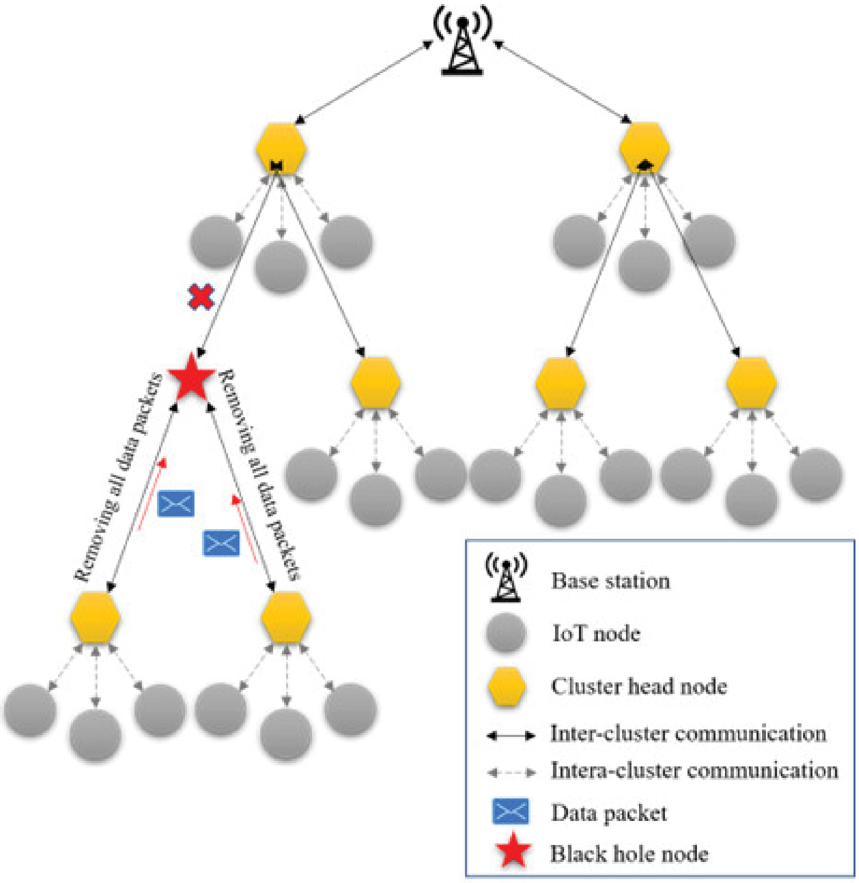
Removing all data packets
Removing all data packets
Base station
IoT node
Cluster head node
Inter-cluster communication
Intera-cluster communication
Data packet
Black hole node

Figure 4 Overview of a black hole attack.

a trust level. If a node behaves maliciously, the penalty factor is applied, and the node is isolated from the network, preventing it from carrying out its malicious activities. The reward factor is used to incentivize nodes into participating in routing protocols, as it will increase their trust level, which can then be leveraged for better routing paths and faster communication. W-Trust requires the calculation of three variables, including total trust, direct trust, and indirect trust.

$\mathrm{T}_{\mathrm{ij}}^{\mathrm{direct}}$ represents the direct trust among node i and node j. Node i produces this trust for Node j immediately. $\mathrm{T}_{\mathrm{ij}}^{\mathrm{direct}}$ can be obtained by examining the direct communication among the nodes over time, like (t-1, t). This direct trust can be derived from the interactions between the nodes and their associated states, such as the performance of tasks, the frequency of communication, and other factors. This trust can then be used to measure the reliability of the nodes and inform decisions on future interactions. The node I determine the packet sending and receiving rates to the node j over the interval (t $-$ 1, t) using Equation (3). In Equation (7), $\lambda \in [0, 1]$ represents an adjustable weight coefficient. $\mathrm{PSR_j(t)}$ and $\mathrm{PRR_j(t)}$ represent the packet sending rate and packet receiving rate of node j at time intervals of (t $-$ 1, t).

$$T_{ij}^{direct}(t) = \lambda PSR_j(t) + (1 - \lambda) PRR_j(t) \tag{3}$$

A group of recommender nodes evaluates the performance of node j to determine the indirect trust of node i to node j. The recommender nodes measure the performance of node j in terms of its interactions with node i, and use this information to calculate an indirect trust score between the two nodes. This score is then used to determine the trustworthiness of node j when it comes to making recommendations to the node i. Equation (4) is used to calculate the weighted indirect trust. $\mathrm{T_{ir}^{Weighted-direct}}$ show the direct trust assigned to node i relative to node r and $\mathrm{T_{rj}^{Weighted-direct}}$ represents the direct trust assigned to node j relative to node r. Total trust equals the sum of direct and indirect trust values, calculated by Equation (5).

$$T_{ij}^{Weighted-indirect}(t) = \frac{1}{p} \sum_{r \in Nei}^{p} (T_{ir}^{Weighted-direct} \cdot T_{rj}^{Weighted-direct}) \tag{4}$$

$$T_{ij}^{Total} = \propto T_{ij}^{Weighted-direct} + (1 - \propto) T_{ij}^{Weighted-indirect} \tag{5}$$

3.4.2 Trust-based clustering

During this stage, cluster heads are chosen only from members whose trust value exceeds a threshold value. This ensures that only honest nodes can become cluster heads, preventing malicious nodes from taking control of the network. Furthermore, by using the trust level as the criteria for selection, the trustworthiness of the clusters is increased, creating a more secure network. The clustering process generally consists of four steps: picking cluster heads, becoming a cluster member, departing from the cluster, and maintaining the cluster.

Periodically, every IoT node in the SRWOA exchanges beacons messages with its neighbors. This exchange of beacon messages allows each node to keep track of its neighbors and their relative locations. The beacon messages contain other important information, such as network topology and traffic load. This message also provides information regarding the corresponding node's location, remaining energy, and trust value. According to this message, each IoT node has a neighborhood database to store data obtained from its single-hop neighbors. Based on the information provided in this table, the nodes use Equation (6) to calculate their probability ($\mathrm{S_i}$) of being chosen as CH. Each node calculates its $\mathrm{S_i}$ value by taking into account its residual energy ($\mathrm{E_i}$), the primary energy of nodes ($\mathrm{E_{max}}$), the neighbor degree ($\mathrm{Deg_i}$), and the distance between it and the base station ($\mathrm{d(n_i, , BS)}$). This $\mathrm{S_i}$ value is then compared to the $\mathrm{S_i}$ values of all the other nodes, and the node with the highest $\mathrm{S_i}$ value is chosen to be the cluster head.

$$S_i = \frac{\left(\frac{E_i}{E_{max}}\right) \times \left(\frac{Deg_i}{N}\right)}{\left(\frac{1}{N_i}\sum_{n_j \in Nei}^{N_i} d(n_i, n_j) \times \left(\frac{d(n_i,BS)}{d_{max}}\right)\right)} \tag{6}$$

3.4.3 WOA-based routing protocol

SRWOA uses the WOA to determine the best routes between the cluster heads in the network. It then uses those results to create a binary tree structure of clusters representing the optimal paths. This binary tree is then used to route data between the cluster heads. Each cluster head transfers data packets to its parent by the proposed routing protocol, which eventually reaches the base station. This ensures that each route is the most efficient and that data packets are routed in the shortest amount of time.

Additionally, the binary tree structure allows for dynamic changes in the network, as it can adapt to changing conditions. The whales in this issue are binary routing trees between cluster heads. Four parameters are used to create a routing tree: the number of hops between a cluster head and the number of cluster members, the remaining energy, the trust level, and a base station.

The whales are initialized randomly. The number of CHs is contained in arrays of whales, and each element's value is a CH in the routing tree. With the WOA, CHs are prioritized on the network and placed at the top of the routing tree based on their priority. Each element in each whale indicates each CH's priority in the network. Four rules were adopted to create the routing tree. The base station is the root of the tree. According to WOA, the base station's left child has the CH with the highest priority, while the right child has the second-highest priority. The leftmost CH must determine its children at each level of this binary routing tree. The children on the left and right have the first and second priorities and have not yet been chosen. In the case of two

CHs with a similar priority, the CH with the higher trust level will be given a higher priority.

The generated routing trees are evaluated based on a fitness function (Equation (7)), comprising four criteria. The criteria include the trust level, number of cluster members, remaining energy, and several hops to the base station. In the proposed routing protocol, a stop condition specifies when the algorithm should be terminated. If this condition is met, the algorithm will cease, and the most effective reaction will be taken as its result. This algorithm is terminated after 300 iterations. When the algorithm has been completed, the base station sends a message informing cluster heads of their position in the routing tree.

$$F = \sum_{D=1}^{|log\ n_{CH}|} \frac{1}{D} \left(\sum_{i=1}^{C} \frac{\left(\frac{E_i}{E_{max}}\right) \times \left(\frac{T_i^{total}}{T_{max}}\right)}{\left(\frac{hop_{count}(n_i,BS)}{N-1}\right) \times \left(\frac{nc_i}{n_{max}}\right)} \right) \tag{7}$$

4 Experimental Results

The NS2 simulator has been used to compare the performance of SRWOA with that of E-BEENISH [39] and EEMSR [40]. We measured the packet delivery ratio (PDR) and energy consumption of the three routing protocols under a variety of network conditions. In order to evaluate the performance of SRWOA, the results of the tests were compared with those of the other two protocols. The simulation parameters are summarized in Table 1.

Figure 5 compares the three approaches in terms of PDR. This test clearly shows that SRWOA is performing well. Our method, however, delivers packets at a lower rate than EEMSR, about 0.4%, since EEMSR uses beta

Table 1 Simulation parameters

Parameter	Value
Population size	100
Network dimensions	(100*100)
Location of a base station	(50,100)
Number of sensor nodes	100
Connection radius	30 m
Packet size	500 bytes
$\mathrm{E_{elec}}$	50 nJ/bit
ϵ_{fs}	10 pJ/bit/m^2
ϵ_{mp}	0.0013 pJ/bit/m^4

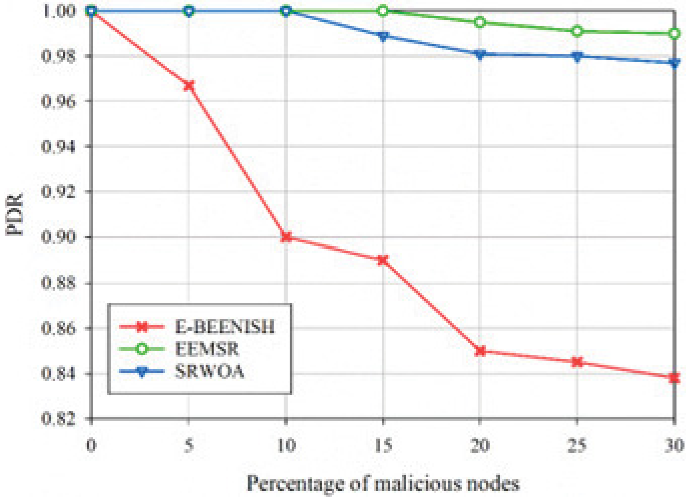

Figure 5 Packet delivery ration comparison.

distributions to build its trust system. The lack of security mechanisms causes E-BEENISH to perform poorly. A second test evaluates the security of IoT by examining received packets (Figure 6). According to several packets that the base station receives, communication is secure since the information has been properly sent and received. Communication may be less secure if a few packets indicate hostile nodes have interfered with transmission. EEMSR received the greatest number of packets, and according to the proposed method, the base station received 3.1% fewer packets than EEMSR. Furthermore, SRWOA has a higher success rate than E-BEENISH by about 14.5%.

A comparison of residual energy between various methods is presented in Figure 7, revealing their energy consumption patterns. It is evident from the figure that our proposed method, SRWOA, outperforms the other methods in terms of energy consumption. As compared to E-BEENISH and EEMSR, SRWOA stores a significant amount of energy, with gains of 16.65% and 35.35%, respectively. By optimizing energy distribution and utilization throughout the network, SRWOA achieves remarkable energy efficiency. The poor performance of E-BEENISH can be attributed to its sole reliance on energy factors for selecting CHs without considering multi-hop paths. In contrast, SRWOA takes into account various parameters such as trust, energy, intra-cluster traffic, distance, and hop count when designing a fitness function to establish an energy-efficient and secure routing tree between CHs. This holistic approach ensures a balanced energy consumption among the

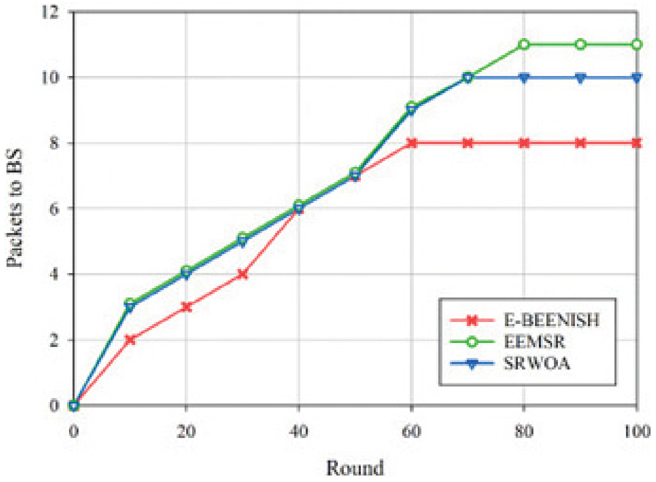

Figure 6 The number of packets received in comparison.

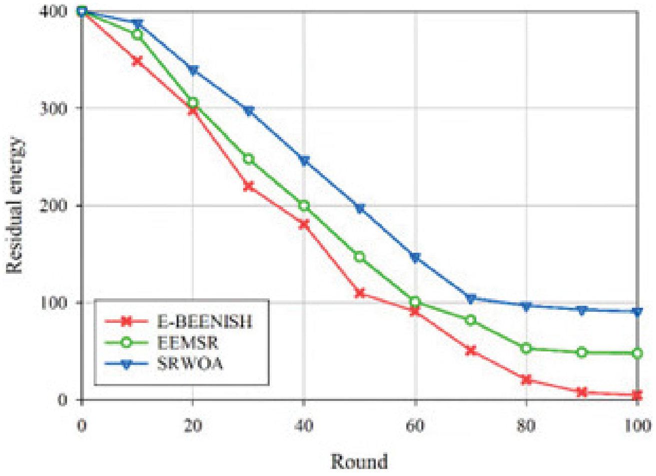

Figure 7 Energy consumption comparison.

network nodes, leading to enhanced performance and prolonged network lifetime.

Furthermore, Figure 8 introduces an additional experiment to quantify the energy consumption balance among IoT nodes by evaluating their standard deviations. A lower standard deviation indicates a more uniform distribution of energy consumption, reflecting a balanced energy utilization across

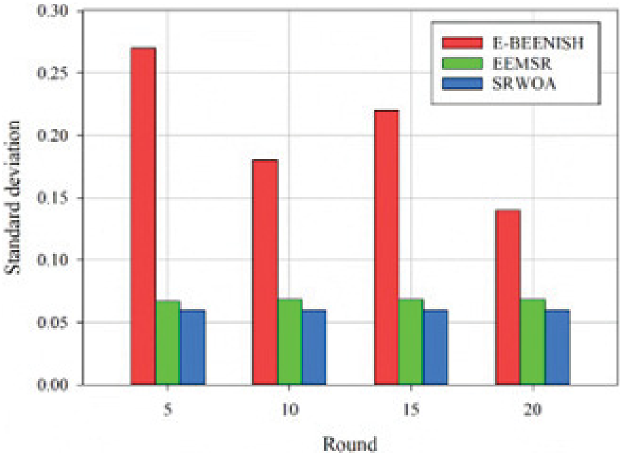

Figure 8 Standard deviation of energy consumption.

the network. The figure demonstrates that SRWOA outperforms the other methods in achieving energy consumption balance, with its standard deviation being significantly lower. The superior performance of SRWOA in terms of energy efficiency, energy storage, and energy consumption balance is a testament to its effectiveness in addressing the energy-related challenges in IoT networks. By leveraging the WOA and incorporating multi-hop routing techniques, SRWOA optimizes available energy resources, maximizes network lifetime, and ensures reliable and sustainable operation of agricultural IoT networks.

The network lifetime evaluation of different routing approaches is depicted in Figure 9. CTSRD exhibits the longest network lifetime among the compared methods, reducing the number of dead nodes by approximately 20.92% and 61.57% compared to EEMSR and E-BEENISH, respectively. SRWOA demonstrates the longest first node die time in the figure, followed by EEMSR. Conversely, E-BEENISH's performance is unsatisfactory due to its sole focus on energy efficiency, disregarding the security of IoT nodes. Malicious nodes negatively impact E-BEENISH, diminishing its lifetime. In contrast, SRWOA and EEMSR employ a multi-hop routing technique between cluster heads, effectively balancing energy consumption among network nodes. On the other hand, E-BEENISH allows each cluster head to transmit data directly to the base station, leading to imbalanced energy consumption and reduced network lifetime. Additionally, SRWOA considers multiple parameters in its fitness function, including trust, energy, intra-cluster traffic, distance, and hop count, resulting in an energy-efficient and secure routing tree. In comparison, EEMSR solely relies on the square of the distance between cluster heads in its fitness function, potentially compromising energy efficiency. The impact of these considerations is evident in the network lifetime of SRWOA and EEMSR.

5 Conclusion

The Internet is revolutionizing our world. The use of connected devices has become an essential part of daily life. The agricultural industry is evolving from precision farming to micro-farming. IoT has enriched communication by enabling human-to-human and environmental-to-environmental communication. IoT should be viewed as a core for omnipresence for developing a new architectural concept, i.e., anytime, anywhere, everywhere. Agricultural IoT networks face two critical challenges: security and energy efficiency. Both challenges must be addressed through robust security protocols and energy-saving designs to ensure these networks' success. This paper addresses these challenges by introducing a new routing protocol named SRWOA. The simulation results demonstrated that SRWOA had superior performance in terms of energy usage and PDR metrics compared to other approaches. Although our SRWOA routing protocol demonstrates encouraging outcomes in tackling the issues of security and energy efficiency in agricultural IoT networks, it is important to acknowledge the presence of specific constraints and limiting assumptions. The study focuses mainly on networks of small to medium size, and more research is needed to assess the scalability of the protocol in larger networks. Furthermore, the protocol relies on the assumption of a consistent network environment with unchanging topologies, when real-life situations may entail dynamic alterations. It is crucial to take into account the versatility and efficiency of the protocol across various IoT hardware platforms, as well as the necessity for validation in real-world scenarios. Field trials and practical deployments offer vital insights into the protocol's performance and applicability for various agricultural contexts.

Acknowledgment

This work is supported by the Youth Cultivation Fund Project of Changchun Guanghua University in 2022: “Intelligent irrigation system design based on Zigbee”. (No. QNXS2022012)

References

[1] B. Pourghebleh, N. Hekmati, Z. Davoudnia, and M. Sadeghi, "A roadmap towards energy-efficient data fusion methods in the Internet of Things," *Concurrency and Computation: Practice and Experience*, p. e6959, 2022.

[2] S. Saeidi, S. Enjedani, E. Alvandi Behineh, K. Tehranian, and S. Jazayerifar, "Factors Affecting Public Transportation Use during Pandemic: An Integrated Approach of Technology Acceptance Model and Theory of Planned Behavior," *Tehnički glasnik*, vol. 18, pp. 1–12, 09/01 2023, doi: 10.31803/tg-20230601145322.

[3] B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research," *Journal of Network and Computer Applications*, vol. 97, pp. 23–34, 2017.

[4] M. Mohseni, F. Amirghafouri, and B. Pourghebleh, "CEDAR: A cluster-based energy-aware data aggregation routing protocol in the internet of things using capuchin search algorithm and fuzzy logic," *Peer-to-Peer Networking and Applications*, pp. 1–21, 2022.

[5] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9326–9337, 2019.

[6] M. Mahbub, "IoT Ecosystem: Functioning Framework, Hierarchy of Knowledge, and Intelligence," in *Artificial Intelligence-based Internet of Things Systems*: Springer, 2022, pp. 47–76.

[7] D. P. Kumar, T. Amgoth, and C. S. R. Annavarapu, "Machine learning algorithms for wireless sensor networks: A survey," *Information Fusion*, vol. 49, pp. 1–25, 2019.

[8] S. Mishra and A. K. Tyagi, "The role of machine learning techniques in internet of things-based cloud applications," in *Artificial Intelligence-based Internet of Things Systems*: Springer, 2022, pp. 105–135.

[9] A. Larijani and F. Dehghani, "An Efficient Optimization Approach for Designing Machine Models Based on Combined Algorithm," *FinTech*, vol. 3, no. 1, pp. 40–54, 2024. [Online]. Available: https://www.mdpi.com/2674--1032/3/1/3.

[10] A. E. Jery et al., "Experimental Investigation and Proposal of Artificial Neural Network Models of Lead and Cadmium Heavy Metal Ion Removal from Water Using Porous Nanomaterials," *Sustainability*, vol. 15, no. 19, p. 14183, 2023.

[11] S. R. Abdul Samad et al., “Analysis of the Performance Impact of Fine-Tuned Machine Learning Model for Phishing URL Detection,” *Electronics*, vol. 12, no. 7, p. 1642, 2023.

[12] V. Monjezi, A. Trivedi, G. Tan, and S. Tizpaz-Niari, “Information-Theoretic Testing and Debugging of Fairness Defects in Deep Neural Networks,” *arXiv preprint arXiv:2304.04199*, pp. 1571–1582, 2023 2023, doi: 10.1109/ICSE48619.2023.00136.

[13] W. Anupong et al., “Deep learning algorithms were used to generate photovoltaic renewable energy in saline water analysis via an oxidation process,” *Water Reuse*, vol. 13, no. 1, pp. 68–81, 2023.

[14] S. P. Rajput et al., “Using machine learning architecture to optimize and model the treatment process for saline water level analysis,” *Journal of Water Reuse and Desalination*, 2022.

[15] S. Vairachilai, A. Bostani, A. Mehbodniya, J. L. Webber, O. Hemakesavulu, and P. Vijayakumar, “Body Sensor 5 G Networks Utilising Deep Learning Architectures for Emotion Detection Based On EEG Signal Processing,” *Optik*, p. 170469, 2022.

[16] A. Hazra, P. K. Donta, T. Amgoth, and S. Dustdar, “Cooperative transmission scheduling and computation offloading with collaboration of fog and cloud for industrial IoT applications,” *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 3944–3953, 2022.

[17] A. Larijani and F. Dehghani, “A Computationally Efficient Method for Increasing Confidentiality in Smart Electricity Networks,” *Electronics*, vol. 13, no. 1, p. 170, 2024. [Online]. Available: https://www.mdpi.com/2079--9292/13/1/170.

[18] S. Pazouki and M. R. Haghifam, “Optimal planning and scheduling of smart homes’ energy hubs,” *International Transactions on Electrical Energy Systems*, vol. 31, no. 9, p. e12986, 2021.

[19] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, “Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective,” *Sustainability*, vol. 15, no. 4, p. 3317, 2023.

[20] P. Behrouz, H. Vahideh, and A. A. Aghaei, “Service discovery in the Internet of Things: review of current trends and research challenges,” *Wireless Networks*, vol. 26, no. 7, pp. 5371–5391, 2020.

[21] S. Pazouki and J. Olamaei, “The effect of heterogeneous electric vehicles with different battery capacities in parking lots on peak load of electric power distribution networks,” *International Journal of Ambient Energy*, vol. 40, no. 7, pp. 734–738, 2019.

[22] P. He, N. Almasifar, A. Mehbodniya, D. Javaheri, and J. L. Webber, "Towards green smart cities using Internet of Things and optimization algorithms: A systematic and bibliometric review," *Sustainable Computing: Informatics and Systems*, vol. 36, p. 100822, 2022, doi: https://doi.org/10.1016/j.suscom.2022.100822.

[23] C. Dehury, S. N. Srirama, P. K. Donta, and S. Dustdar, "Securing clustered edge intelligence with blockchain," *IEEE Consumer Electronics Magazine*, 2022.

[24] S. Takarabt, J. Bahrami, M. Ebrahimabadi, S. Guilley, and N. Karimi, "Security Order of Gate-Level Masking Schemes," in *2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2023: IEEE, pp. 57–67.

[25] C. K. Dehury, P. K. Donta, S. Dustdar, and S. N. Srirama, "CCEI-IoT: Clustered and Cohesive Edge Intelligence in Internet of Things," in *2022 IEEE International Conference on Edge Computing and Communications (EDGE)*, 2022: IEEE, pp. 33–40.

[26] B. Pourghebleh, V. Hayyolalam, and A. A. Anvigh, "Service discovery in the Internet of Things: review of current trends and research challenges," *Wireless Networks*, vol. 26, no. 7, pp. 5371–5391, 2020.

[27] J. Zandi, A. N. Afooshteh, and M. Ghassemian, "Implementation and analysis of a novel low power and portable energy measurement tool for wireless sensor nodes," in *Electrical Engineering (ICEE), Iranian Conference on*, 2018: IEEE, pp. 1517–1522, doi: 10.1109/ICEE.2018.8472439.

[28] N. Ahmed, D. De, and I. Hussain, "Internet of Things (IoT) for smart precision agriculture and farming in rural areas," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4890–4899, 2018.

[29] M. V. Roudbari, A. Dehnavi, S. Jamshidi, and M. Yazdani, "A multi-pollutant pilot study to evaluate the grey water footprint of irrigated paddy rice," *Agricultural Water Management*, vol. 282, p. 108291, 2023, doi: 10.1016/j.agwat.2023.108291.

[30] S. Liu, L. Guo, H. Webb, X. Ya, and X. Chang, "Internet of Things monitoring system of modern eco-agriculture based on cloud computing," *IEEE Access*, vol. 7, pp. 37050–37058, 2019.

[31] S. Mahmoudinazlou, A. Alizadeh, J. Noble, and S. Eslamdoust, "An improved hybrid ICA-SA metaheuristic for order acceptance and scheduling with time windows and sequence-dependent setup times," *Neural Computing and Applications*, pp. 1–19, 2023.

[32] D. Xue and W. Huang, “Smart agriculture wireless sensor routing protocol and node location algorithm based on Internet of Things technology,” *IEEE Sensors Journal*, vol. 21, no. 22, pp. 24967–24973, 2020.

[33] F. J. Ferrández-Pastor, J. M. García-Chamizo, M. Nieto-Hidalgo, and J. Mora-Martínez, “Precision agriculture design method using a distributed computing architecture on internet of things context,” *Sensors*, vol. 18, no. 6, p. 1731, 2018.

[34] S. J. Anand, “Iot-based secure and energy efficient scheme for precision agriculture using blockchain and improved leach algorithm,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 10, pp. 2466–2475, 2021.

[35] M. Cicioğlu and A. Çalhan, “Smart agriculture with internet of things in cornfields,” *Computers & Electrical Engineering*, vol. 90, p. 106982, 2021.

[36] S. Sankar, P. Srinivasan, A. K. Luhach, R. Somula, and N. Chilamkurti, “Energy-aware grid-based data aggregation scheme in routing protocol for agricultural internet of things,” *Sustainable Computing: Informatics and Systems*, vol. 28, p. 100422, 2020.

[37] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, K.-K. R. Choo, and M. Nafaa, “FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things,” *Journal of Parallel and Distributed Computing*, vol. 165, pp. 17–31, 2022.

[38] J. Xie, G. Liang, P. Gao, W. Wang, D. Yin, and J. Li, “Research on site selection of agricultural internet of things nodes based on rapid terrain sampling,” *Computers and Electronics in Agriculture*, vol. 204, p. 107493, 2023.

[39] Y. Zhang, X. Zhang, S. Ning, J. Gao, and Y. Liu, “Energy-efficient multilevel heterogeneous routing protocol for wireless sensor networks,” *IEEE Access*, vol. 7, pp. 55873–55884, 2019.

[40] Y. Zhang, Q. Ren, K. Song, Y. Liu, T. Zhang, and Y. Qian, “An Energy-Efficient Multilevel Secure Routing Protocol in IoT Networks,” *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10539–10553, 2021.

Biographies

Yanling Wang received her master's degree in signal and Information processing from Changchun University of Technology in 2005. She worked at the Electrical Information School of Changchun Guanghua University in 2005. Her main research interests are electronic information engineering and Internet of Things engineering.

Yong Yang received his master's degree in materials engineering from Changchun University of Technology in 2005. He has been working in ThyssenKrupp Fuo Automotive Steering Column (Changchun) Co., LTD since 2022. His research direction is Smart Control.